# Deep Security 11.1

AWS Marketplace

# Legal Notices

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the release notes and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

https://help.deepsecurity.trendmicro.com/software.html

Trend Micro, and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

© 2018 Trend Micro Incorporated. All rights reserved

Protected by U.S. Patent No. 7,630,982 B2.

Privacy Policy

Trend Micro, Inc. is committed to protecting your privacy. Please read the Trend Micro Privacy Policy available at www.trendmicro.com.

**Document Number:** APEM118327/180614

**Publication Date:** 8/24/2020 2:49 PM

# Contents

**Contents** ..... 3

**Get Started** ..... 56

Privacy and personal data collection disclosure ..... 56

Deep Security Software ..... 56

Buy Deep Security AMI from AWS Marketplace ..... 57

Check Deep Security pricing and billing on AWS Marketplace ..... 57

Deep Security pricing ..... 57

What Deep Security considers as a protection hour ..... 58

When Deep Security considers a computer protected ..... 59

Computers in a cloud ..... 59

Computers not in a cloud ..... 59

Change your Deep Security AMI from AWS Marketplace payment option ..... 60

Modify the Deep Security Manager database ..... 60

Install Deep Security Manager ..... 61

Delete previous Deep Security Manager instances ..... 62

Check billing and usage for the Deep Security AMI from AWS Marketplace ..... 62

View usage data ..... 63

Export a usage data report ..... 63

What's new? ..... 63

Deep Security 11.1 ..... 63

Before you install ..... 66

Feature releases ..... 66

Version numbers ..... 66

Feature release life cycle ..... 67

Platform support ..... 67

Support services ..... 68

About the Deep Security components ..... 69
System requirements ..... 69
Deep Security Manager ..... 70
Deep Security Agent ..... 72
Deep Security Notifier ..... 72
Deep Security Manager - Agent compatibility by platform ..... 73
Docker support ..... 75
Deep Security Agent Linux kernel support ..... 76
Supported features by platform ..... 77
Microsoft Windows (11.1 agent) ..... 78
Red Hat Enterprise Linux (11.1 agent) ..... 81
CentOS Linux (11.1 agent) ..... 82
Oracle Linux (11.1 agent) ..... 83
SUSE Linux (11.1 agent) ..... 84
Ubuntu Linux (11.1 agent) ..... 85
Debian Linux (11.1 agent) ..... 85
Cloud Linux (11.1 agent) ..... 86
Amazon Linux (11.1 agents) ..... 87
Deep Security Virtual Appliance (NSX) (with embedded 11.1 agent) ..... 88
Sizing ..... 92
Deep Security Manager sizing ..... 92
Multiple server nodes ..... 93
Database sizing ..... 93
Disk space estimates ..... 94
Database sizing considerations ..... 95
Deep Security Agent and Relay sizing ..... 96
Port numbers ..... 96
Deep Security Manager ports ..... 98
Incoming (listening ports) ..... 98

Outgoing ..... 99
Deep Security Relay ports ..... 105
Incoming (listening) ..... 105
Outgoing ..... 106
Deep Security Agent ports ..... 106
Incoming (listening ports) ..... 106
Outgoing ..... 107
Prepare a database for Deep Security Manager on AWS ..... 114
Hardware recommendations ..... 116
Microsoft SQL Server ..... 116
Oracle Database ..... 117
Oracle RAC (Real Application Clusters) support ..... 117
Connection settings used during Deep Security Manager installation ..... 117
PostgreSQL recommendations ..... 118
General requirements ..... 118
Tuning PostgreSQL settings ..... 118
Logging settings ..... 119
Lock management ..... 120
Maximum connections ..... 120
Shared buffers ..... 120
Work memory and maintenance work memory ..... 120
Effective cache size ..... 121
Checkpoints ..... 121
Write-ahead log (WAL) ..... 121
Autovacuum settings ..... 121
High availability ..... 122
Backup and recovery ..... 122
Linux recommendations ..... 122
Transparent Huge Pages (Linux) ..... 122

Strengthen host-based authentication (Linux) 122
Set up authentication for SQL Server 123
Active Directory 123
The Deep Security Manager computer 124
Windows 124
Linux 125
Microsoft SQL Server 125
Synchronize system clocks 126
Microsoft SQL Server Express considerations 126
Supported versions 126
Limited number of hosts 127
Security module limitations 127
Minimize the agent size 127
Database pruning 127
Configure the IAM role for the Deep Security AMI from AWS Marketplace 127
IAM role requirements 128
Deploy Deep Security 128
Deploy the Deep Security AMI from AWS Marketplace 128
Run Deep Security Manager on multiple nodes 130
Add a node 131
Remove a node 131
Viewing node statuses 132
Network Map with Activity Graph 132
Jobs by Node 133
Jobs by Type 134
Total jobs by node and type 135
Deep Security Manager performance features 136
Performance profiles 136
Low disk space alerts 137

Low disk space on the database host ..... 137
Low disk space on the manager host ..... 137
Update the load balancer's certificate ..... 138
Set up a multi-tenant environment ..... 140
Multi-tenancy requirements ..... 141
Enable multi-tenancy ..... 142
Create a tenant ..... 143
Examples of messages sent to tenants ..... 144
Email Confirmation Link: Account Confirmation Request ..... 144
Email Generated Password ..... 144
Scalability guidelines ..... 145
Multi-tenancy tips ..... 146
Reconnaissance IP list ..... 146
Use multiple database servers ..... 146
Tenant pending deletion state ..... 146
Multi-tenant options under System Settings ..... 146
Managing tenants ..... 147
Tenant Properties ..... 147
General ..... 147
Modules ..... 147
Features ..... 148
Statistics ..... 148
Agent Activation ..... 148
What does the tenant see? ..... 149
Agent-Initiated Activation ..... 150
Tenant diagnostics ..... 151
Usage monitoring ..... 151
Multi-tenant Dashboard ..... 151
Multi-tenant reports ..... 152

Security Module Usage Cumulative Report ..... 152
Security Module Usage Report ..... 153
Tenant Report ..... 154
Configure database user accounts ..... 154
Configuring database user accounts ..... 154
SQL Server ..... 155
Oracle ..... 163
PostgreSQL ..... 165
Configuring multiple database servers ..... 166
Removing or changing secondary databases ..... 166
APIs ..... 167
Upgrade ..... 167
Supporting tenants ..... 168
Load balancers ..... 168
Multi-tenant settings ..... 171
Database servers ..... 173
New tenant template ..... 173
Protection usage monitoring ..... 175
Configure SMTP settings for email notifications ..... 176
Install the agents ..... 177
Get Deep Security Agent software ..... 177
Download agent software packages into Deep Security Manager ..... 177
Automatically import software updates ..... 177
Manually import software updates ..... 178
Export the agent installer ..... 178
Delete a software package from the Deep Security database ..... 179
Deleting agent packages in single-tenancy mode ..... 180
Deleting agent packages in multi-tenancy mode ..... 180
Deleting kernel support packages ..... 180

Manually install the Deep Security Agent ..... 180
Install a Windows agent ..... 181
Installation on Amazon WorkSpaces ..... 182
Installation on Windows 2012 Server Core ..... 182
Install a Red Hat, SUSE, Oracle Linux, or Cloud Linux agent ..... 182
Install an Ubuntu or Debian agent ..... 183
Install the agent on a Microsoft Azure VM ..... 184
Generate and run a deployment script ..... 184
Add a custom script extension to an existing virtual machine ..... 184
Install the agent on Amazon EC2 and WorkSpaces ..... 185
Add your AWS accounts to Deep Security Manager ..... 185
Set the communication direction ..... 186
Configure the activation type ..... 186
Open ports ..... 188
Which ports should be opened? ..... 189
Deploy agents to your Amazon EC2 instances and WorkSpaces ..... 190
Verify that the agent was installed and activated properly ..... 190
Assign a policy ..... 191
Bake the agent into your AMI or WorkSpace bundle ..... 192
Add your AWS account to Deep Security Manager ..... 193
Set the communication direction ..... 193
Configure the activation type ..... 193
Launch a 'master' Amazon EC2 instance or Amazon WorkSpace ..... 193
Deploy an agent on the master ..... 193
Verify that the agent was installed and activated properly ..... 194
(Recommended) Set up policy auto-assignment ..... 194
Create an AMI or custom WorkSpace bundle based on the master ..... 195
Use the AMI ..... 195
Configure communication between components ..... 196

Agent-manager communication ..... 196
Configure the heartbeat ..... 196
Configure communication directionality ..... 198
Supported cipher suites for agent-manager communication ..... 200
SSL implementation and credential provisioning ..... 201
Use agent-initiated communication with cloud accounts ..... 202
Enable agent-initiated communication on the policy ..... 202
Assign the policy to a deployment script ..... 203
Connect agents behind a proxy ..... 203
Requirements ..... 203
Register the proxy in Deep Security Manager ..... 204
Connect agents, appliances, and relays to security updates via proxy ..... 204
Connect agents to security services via proxy ..... 204
Connect agents to a relay via proxy ..... 205
Connect agents to a relay's private IP address ..... 205
Remove a proxy setting ..... 206
Windows ..... 206
Linux ..... 206
Subsequent agent deployments ..... 206
Configure agents that have no Internet access ..... 207
Solutions ..... 207
Use a proxy ..... 207
Install a Smart Protection Server locally ..... 208
Install a relay and supporting components in your DMZ or Internet-ready area ..... 209
Disable the features that use Trend Micro security services ..... 211
Proxy protocols supported by Deep Security ..... 214
Proxy settings ..... 214
Proxy server use ..... 215
Proxy servers ..... 216

Manage trusted certificates ..... 216
Import trusted certificates ..... 217
View trusted certificates ..... 217
Remove trusted certificates ..... 218
If I have disabled the connection to the Smart Protection Network, is any other information sent to Trend Micro? ..... 219
Activate the agent ..... 219
Deactivate the agent ..... 221
Stop or start the agent ..... 221
Stop or start the appliance ..... 222
Diagnose problems with agent deployment (Windows) ..... 222
Configure teamed NICs ..... 222
Agent settings ..... 223
Hostnames ..... 223
Agent-Initiated Activation ..... 223
Data Privacy ..... 225
Agentless vCloud Protection ..... 225
Linux Secure Boot support for agents ..... 225
Deploy a Smart Protection Server in AWS ..... 228
Create an Azure app for Deep Security ..... 232
Record the Azure Active Directory ID ..... 232
Create the Azure app ..... 233
Record the Azure app ID and password ..... 233
Record the Subscription ID ..... 233
Assign the Azure app a reader role and add it to your Azure Subscription ..... 234
Distribute security and software updates with relays ..... 234
How relays work ..... 235
Determine the number of relays to use ..... 235
Geographic region of agents ..... 236

Network configuration ..... 236
Network bandwidth usage ..... 236
Sizing recommendations ..... 236
Configure one or more relays ..... 237
Create one or more relay groups ..... 237
Enable one or more relays ..... 239
Assign agents to a relay group ..... 239
Configure relay settings for security and software updates ..... 240
Security updates ..... 240
Software updates ..... 241
Remove relay functionality from an agent ..... 241
10.2 or later ..... 241
10.1 or earlier ..... 242
DevOps, automation and scaling ..... 243
Command-line basics ..... 244
Deep Security Agent ..... 244
dsa_control ..... 244
Usage ..... 245
Agent-initiated activation ("dsa_control -a") ..... 246
Agent-initiated activation over a private network via proxy ..... 247
Agent-initiated heartbeat command ("dsa_control -m") ..... 248
Activate an agent ..... 256
Windows ..... 257
Linux ..... 257
Configure a proxy for anti-malware and rule updates ..... 257
Windows ..... 257
Linux ..... 257
Configure a proxy for connections to the manager ..... 258
Windows ..... 258

Linux ..... 258
Force the agent to contact the manager ..... 258
Windows ..... 258
Linux ..... 258
Initiate a manual anti-malware scan ..... 258
Windows ..... 258
Linux ..... 259
Create a diagnostic package ..... 259
Windows ..... 259
Linux ..... 259
Reset the agent ..... 259
Windows ..... 259
Linux ..... 260
dsa_query ..... 260
Usage ..... 260
Check CPU usage and RAM usage ..... 261
Windows ..... 261
Linux ..... 261
Check that ds_agent processes or services are running ..... 261
Windows ..... 261
Linux ..... 261
Restart an agent on Linux ..... 261
Use the Deep Security API to automate tasks ..... 261
Legacy REST and SOAP APIs ..... 262
Enable the Status Monitoring API (optional) ..... 262
Create a Web Service user account ..... 262
Schedule Deep Security to perform tasks ..... 263
Create scheduled tasks ..... 263
Enable or disable a scheduled task ..... 265

Set up recurring reports ..... 266
Automatically perform tasks when a computer is added or changed ..... 266
Create an event-based task ..... 266
Edit or stop an existing event-based task ..... 266
Events that you can monitor ..... 267
Conditions ..... 268
Actions ..... 270
Order of execution ..... 271
Temporarily disable an event-based task ..... 271
AWS Auto Scaling and Deep Security ..... 271
Pre-install the agent ..... 271
Install the agent with a deployment script ..... 272
Delete instances from Deep Security as a result of Auto Scaling ..... 274
Azure virtual machine scale sets and Deep Security ..... 274
Step 1: (Recommended) Add your Azure account to Deep Security Manager ..... 275
Step 2: Prepare a deployment script ..... 275
Step 3: Add the agent through a custom script extension to your VMSS instances ..... 276
Example 1: Create a new VMSS that includes the agent ..... 276
Example 2: Add the agent to an existing VMSS ..... 279
Use deployment scripts to add and protect computers ..... 281
Enable agent-initiated activation ..... 282
Generate a deployment script ..... 282
Troubleshooting and tips ..... 284
Automatically assign policies by AWS instance tags ..... 285
Integrate Deep Security with AWS Elastic Beanstalk ..... 287
For more information ..... 287
Deep Security Smart Check ..... 287
**Protect ..... 287**
Intrusion Prevention ..... 288

Anti-Malware ..... 288
Firewall ..... 289
Web Reputation ..... 289
Integrity Monitoring ..... 289
Log Inspection ..... 289
Application Control ..... 290
Manage protected computers ..... 290
Add computers and other resources to Deep Security Manager ..... 290
Add computers to the manager ..... 290
Group computers ..... 291
Export your computers list ..... 292
Delete a computer ..... 292
Add local network computers ..... 292
Agent-initiated activation ..... 292
Manually add a computer ..... 293
Discover computers ..... 294
Add AWS cloud accounts ..... 295
Method: Manager instance role and cross-account role ..... 297
Configure the AWS DSM account ..... 298
Configure AWS Account A ..... 300
Add the AWS accounts to Deep Security Manager ..... 302
Method: Manager instance role (single AWS account) ..... 303
Method: AWS access keys ..... 305
Edit a cloud account ..... 308
Remove a cloud account from the manager ..... 308
Add Amazon WorkSpaces ..... 308
Protect Amazon WorkSpaces if you already added your AWS account ..... 309
Protect Amazon WorkSpaces if you have not yet added your AWS account ..... 310
How do I migrate to the new cloud connector functionality? ..... 310

Add a Microsoft Azure account to Deep Security ....311
Configure a proxy setting for the Azure account ....312
Add virtual machines from a Microsoft Azure account to Deep Security ....312
Quick ....312
Advanced ....313
Manage Azure classic virtual machines with the Azure Resource Manager connector ....314
Remove an Azure account ....314
Create an Azure app for Deep Security ....315
Record the Azure Active Directory ID ....315
Create the Azure app ....315
Record the Azure app ID and password ....316
Record the Subscription ID ....316
Assign the Azure app a reader role and add it to your Azure Subscription ....316
Why should I upgrade to the new Azure Resource Manager connection functionality? ....317
Add virtual machines hosted on VMware vCloud ....318
Proxy setting for cloud accounts ....318
Create a VMware vCloud Organization account for the manager ....318
Import computers from a VMware vCloud Organization Account ....319
Import computers from a VMware vCloud Air data center ....320
Configure software updates for cloud accounts ....320
Remove a cloud account ....321
Add computer groups from Microsoft Active Directory ....321
Additional Active Directory options ....322
Remove Directory ....322
Synchronize Now ....323
Server certificate usage ....323
Filter Active Directory objects ....323
Import users and contacts ....324
Keep Active Directory objects synchronized ....325

Disable Active Directory synchronization 325
Remove computer groups from Active Directory synchronization 326
Delete Active Directory users and contacts 326
Protect Docker containers 326
Deep Security protection for the Docker host 328
Deep Security protection for Docker containers 328
Limitation on intrusion prevention recommendation scans 328
Computer and agent statuses 328
Status column - computer states 329
Status column - agent or appliance states 329
Task(s) column 330
Computer errors 333
Protection module status 334
Perform other actions on your computers 335
Computers icons 339
Status information for different types of computers 340
Ordinary computer 340
Relay 340
Docker hosts 341
Using Deep Security with iptables 341
Rules required by Deep Security Manager 342
Rules required by Deep Security Agent 342
Prevent Deep Security from automatically adding iptables rules 343
Enable or disable agent self-protection 343
Via Deep Security Manager 344
Via command line 344
Are "Offline" agents still protected by Deep Security? 345
Deep Security Notifier 345
How the notifier works 345

Create policies to protect your computers and other resources 349
Create a new policy 350
Other ways to create a policy 351
Edit the settings for a policy or individual computer 352
Assign a policy to a computer 352
Disable automatic policy updates 353
Send policy changes manually 353
Export a policy 354
Policies, inheritance, and overrides 354
Inheritance 355
Overrides 356
Override object properties 357
Override rule assignments 358
View the overrides on a computer or policy at a glance 358
Manage and run recommendation scans 359
What gets scanned? 359
Scan limitations 360
Run a recommendation scan 361
Create a scheduled task to regularly run recommendation scans 362
Configure an ongoing scan 363
Manually run a recommendation scan 363
Cancel a recommendation scan 363
Exclude a rule or application type from recommendation scans 364
Automatically implement recommendations 364
Check scan results and manually assign rules 365
Configure recommended rules 367
Implement additional rules for common vulnerabilities 367
Troubleshooting: Recommendation Scan Failure 368
Communication 368

Server resources ..... 369
Timeout values ..... 369
Detect and configure the interfaces available on a computer ..... 369
Configure a policy for multiple interfaces ..... 369
Enforce interface isolation ..... 370
Overview section of the computer editor ..... 371
General tab ..... 371
Computer status ..... 372
Protection module status ..... 373
VMware virtual machine summary ..... 374
Actions tab ..... 375
Activation ..... 375
Policy ..... 375
Agent Software ..... 375
Support ..... 376
TPM tab ..... 376
System Events tab ..... 377
Overview section of the policy editor ..... 377
General tab ..... 377
General ..... 377
Inheritance ..... 377
Modules ..... 378
Computer(s) Using This Policy tab ..... 378
Events tab ..... 378
Network engine settings ..... 378
Define rules, lists, and other common objects used by policies ..... 389
Rules ..... 389
Lists ..... 389
Other ..... 390

Create a firewall rule ..... 390
Add a new rule ..... 390
Select the behavior and protocol of the rule ..... 391
Select a Packet Source and Packet Destination ..... 393
Configure rule events and alerts ..... 394
Alerts ..... 395
Set a schedule for the rule ..... 395
Assign a context to the rule ..... 395
See policies and computers a rule is assigned to ..... 395
Export a rule ..... 395
Delete a rule ..... 396
Configure intrusion prevention rules ..... 396
See the list of intrusion prevention rules ..... 397
See information about an intrusion prevention rule ..... 397
General Information ..... 397
Details ..... 397
See the list of intrusion prevention rules ..... 398
General Information ..... 398
Identification (Trend Micro rules only) ..... 399
See information about the associated vulnerability (Trend Micro rules only) ..... 399
Assign and unassign rules ..... 399
Automatically assign updated required rules ..... 400
Configure event logging for rules ..... 401
Generate alerts ..... 402
Setting configuration options (Trend Micro rules only) ..... 402
Schedule active times ..... 403
Exclude from recommendations ..... 403
Set the context for a rule ..... 404
Override the behavior mode for a rule ..... 404

Override rule and application type configurations ..... 405
Export and import rules ..... 405
Create an integrity monitoring rule ..... 406
Add a new rule ..... 407
Enter integrity monitoring rule information ..... 407
Select a rule template and define rule attributes ..... 407
Registry Value template ..... 407
File template ..... 408
Custom (XML) template ..... 408
Configure Trend Micro integrity monitoring rules ..... 409
Configure rule events and alerts ..... 409
Real-time event monitoring ..... 410
Alerts ..... 410
See policies and computers a rule is assigned to ..... 410
Export a rule ..... 410
Delete a rule ..... 410
Define a log inspection rule for use in policies ..... 410
Create a new log inspection rule ..... 411
Decoders ..... 413
Subrules ..... 414
Groups ..... 414
Rules, ID, and Level ..... 415
Description ..... 416
Decoded As ..... 417
Match ..... 417
Conditional Statements ..... 418
Hierarchy of Evaluation ..... 419
Restrictions on the Size of the Log Entry ..... 420
Composite Rules ..... 421

Real world examples ..... 422
Log inspection rule severity levels and their recommended use ..... 431
strftime() conversion specifiers ..... 432
Examine a log inspection rule ..... 433
Log inspection rule structure and the event matching process ..... 433
Duplicate Sub-rules ..... 436
Create a list of directories for use in policies ..... 437
Import and export directory lists ..... 440
See which policies use a directory list ..... 440
Create a list of file extensions for use in policies ..... 440
Import and export file extension lists ..... 441
See which malware scan configurations use a file extension list ..... 441
Create a list of files for use in policies ..... 441
Import and export file lists ..... 443
See which policies use a file list ..... 444
Create a list of IP addresses for use in policies ..... 444
Import and export IP lists ..... 444
See which rules use an IP list ..... 445
Create a list of ports for use in policies ..... 445
Import and export port lists ..... 445
See which rules use a port list ..... 446
Create a list of MAC addresses for use in policies ..... 446
Import and export MAC lists ..... 446
See which policies use a MAC list ..... 447
Define contexts for use in policies ..... 447
Configure settings used to determine whether a computer has internet connectivity ..... 447
Define a context ..... 447
Define stateful firewall configurations ..... 448
Add a stateful configuration ..... 449

Enter stateful configuration information ..... 449
Select packet inspection options ..... 449
IP packet inspection ..... 450
TCP packet inspection ..... 450
FTP Options ..... 452
UDP packet inspection ..... 452
ICMP packet inspection ..... 453
Export a stateful configuration ..... 453
Delete a stateful configuration ..... 454
See policies and computers a stateful configuration is assigned to ..... 454
Define a schedule that you can apply to rules ..... 454
Lock down software with application control ..... 454
Key concepts ..... 455
How does application control work? ..... 456
A tour of the application control interface ..... 457
Application Control: Software Changes (Actions) ..... 458
Application Control Rulesets ..... 459
Security Events ..... 460
Decision Logs ..... 461
What does application control detect as a software change? ..... 461
Differences in how Deep Security Agent 10.x and 11.x compare files ..... 462
Set up application control ..... 463
Turn on application control ..... 463
Monitor new and changed software ..... 464
Tips for handling changes ..... 466
Turn on maintenance mode when making planned changes ..... 467
Application control tips and considerations ..... 468
Verify that application control is enabled ..... 469
Monitor application control events ..... 471

Choose which application control events to log ....471
View application control event logs ....472
Interpret aggregated security events ....472
Monitor application control alerts ....473
View and change application control rulesets ....474
View application control rulesets ....475
Security Events ....476
Change the action for an application control rule ....476
Delete an individual application control rule ....478
Delete an application control ruleset ....478
Reset application control after too much software change ....478
Use the API to create shared and global rulesets ....479
Create a shared ruleset ....482
Change from shared to computer-specific allow and block rules ....483
Deploy application control shared rulesets via relays ....484
Single tenant deployments ....484
Considerations when using relays with share rulesets ....485
Protect against malware ....486
Types of malware scans ....487
Real-time scan ....487
Manual scan ....487
Scheduled scan ....488
Quick scan ....488
Scan objects and sequence ....488
Malware scan configurations ....489
Malware events ....489
SmartScan ....490
Predictive Machine Learning ....490
Malware types ....491

Virus ..... 491
Trojans ..... 491
Packer ..... 492
Spyware/grayware ..... 492
Cookie ..... 493
Other threats ..... 494
Possible malware ..... 494
Enable and configure anti-malware ..... 494
Turn on the anti-malware module ..... 495
Select the types of scans to perform ..... 495
Configure scan exclusions ..... 495
Ensure that Deep Security can keep up to date on the latest threats ..... 496
Configure malware scans ..... 497
Create or edit a malware scan configuration ..... 497
Scan for specific types of malware ..... 498
Scan for spyware and grayware ..... 499
Scan for compressed executable files (real-time scans only) ..... 499
Scan process memory (real-time scans only) ..... 499
Scan compressed files ..... 500
Scan embedded Microsoft Office objects ..... 500
Specify the files to scan ..... 501
Inclusions ..... 501
Exclusions ..... 502
Syntax for directory lists ..... 502
Syntax of file lists ..... 504
Syntax of file extension lists ..... 506
Syntax of process image file lists (real-time scans only): ..... 506
Scan a network directory (real-time scan only) ..... 506
Specify when real-time scans occur ..... 506

Configure how to handle malware 507
Customize malware remedial actions 507
ActiveAction actions 508
Generate alerts for malware detection 508
Identify malware files by file hash digest 509
Configure notifications on the computer 509
Performance tips for anti-malware 510
Minimize disk usage 510
Optimize CPU usage 511
Optimize RAM usage 512
Disable Windows Defender after installing Deep Security anti-malware on Windows Server 2016 512
Installing the Anti-Malware module when Windows Defender is already disabled 513
Detect emerging threats using Predictive Machine Learning 513
Ensure Internet connectivity 513
Enable Predictive Machine Learning 514
Enhanced anti-malware and ransomware scanning with behavior monitoring 514
How does enhanced scanning protect you? 515
How to enable enhanced scanning 516
What happens when enhanced scanning finds a problem? 517
What if my agents can't connect to the Internet directly? 522
Smart Protection in Deep Security 522
Anti-malware and Smart Protection 522
Enable Smart Scan 522
Smart Protection Server for File Reputation Service 523
Web Reputation and Smart Protection 524
Smart Feedback 525
Handle malware 525
View and restore identified malware 526
See a list of identified files 526

Working with identified files ....527
Search for an identified file ....528
Restore quarantined files ....530
Create a scan exclusion for the file ....530
Restore the file ....533
Manually restore quarantined files ....533
Create anti-malware exceptions ....533
Create an exception from an anti-malware event ....534
Manually create an anti-malware exception ....535
Exception strategies for spyware and grayware ....535
Scan exclusion recommendations ....536
Increase debug logging for anti-malware in protected Linux instances ....536
Block exploit attempts using intrusion prevention ....537
Intrusion prevention rules ....537
Application types ....538
Rule updates ....538
Recommendation scans ....539
Use behavior modes to test rules ....539
Override the behavior mode for rules ....540
Intrusion prevention events ....540
Support for secure connections ....541
Contexts ....541
Interface tagging ....541
Set up intrusion prevention ....541
Enable intrusion prevention in Detect mode ....542
Test intrusion prevention ....544
Apply recommended rules ....545
Monitor your system ....547
Monitor system performance ....547

Check intrusion prevention events ..... 547
Enable 'fail open' for packet or system failures ..... 547
Switch to prevent mode ..... 547
Implement best practices for specific rules ..... 548
HTTP Protocol Decoding rule ..... 548
Cross-site scripting and generic SQL injection rules ..... 548
Configure intrusion prevention rules ..... 549
See the list of intrusion prevention rules ..... 550
See information about an intrusion prevention rule ..... 550
General Information ..... 550
Details ..... 551
See the list of intrusion prevention rules ..... 551
General Information ..... 551
Identification (Trend Micro rules only) ..... 552
See information about the associated vulnerability (Trend Micro rules only) ..... 552
Assign and unassign rules ..... 553
Automatically assign updated required rules ..... 553
Configure event logging for rules ..... 554
Generate alerts ..... 555
Setting configuration options (Trend Micro rules only) ..... 555
Schedule active times ..... 556
Exclude from recommendations ..... 556
Set the context for a rule ..... 557
Override the behavior mode for a rule ..... 557
Override rule and application type configurations ..... 558
Export and import rules ..... 559
Configure an SQL injection prevention rule ..... 559
What is an SQL injection attack? ..... 560
What are common characters and strings used in SQL injection attacks? ..... 560

How does the Generic SQL Injection Prevention rule work? 562
Examples of the rule and scoring system in action 564
Example 1: Logged and dropped traffic 564
Example 2: No logged or dropped traffic 565
Configure the Generic SQL Injection Prevention rule 566
Character encoding guidelines 569
Application types 571
See a list of application types 571
General Information 572
Connection 572
Configuration 573
Options 573
Assigned To 573
Inspect SSL or TLS traffic 573
Configure SSL inspection 574
Change port settings 575
Use Intrusion Prevention when traffic is encrypted with Perfect Forward Secrecy (PFS) 575
Special considerations for Diffie-Hellman ciphers 576
Supported ciphers 577
Supported protocols 578
Configure anti-evasion settings 578
Performance tips for intrusion prevention 581
Maximum size for configuration packages 582
Control endpoint traffic using the firewall 583
Firewall rules 583
Set up the Deep Security firewall 584
Test firewall rules before deploying them 585
Test in Tap mode 586
Test in Inline mode 586

Enable 'fail open' behavior ..... 587
Turn on firewall ..... 588
Default firewall rules ..... 589
Default Bypass rule for Deep Security Manager Traffic ..... 590
Restrictive or permissive firewall design ..... 590
Restrictive firewall ..... 590
Permissive firewall ..... 591
Firewall rule actions ..... 591
Firewall rule priorities ..... 592
Allow rules ..... 592
Force Allow rules ..... 592
Bypass rules ..... 593
Recommended firewall policy rules ..... 593
Reconnaissance scans ..... 593
Stateful inspection ..... 595
Example ..... 595
Important things to remember ..... 596
Create a firewall rule ..... 597
Add a new rule ..... 598
Select the behavior and protocol of the rule ..... 598
Select a Packet Source and Packet Destination ..... 601
Configure rule events and alerts ..... 602
Alerts ..... 602
Set a schedule for the rule ..... 602
Assign a context to the rule ..... 603
See policies and computers a rule is assigned to ..... 603
Export a rule ..... 603
Delete a rule ..... 603
Allow trusted traffic to bypass the firewall ..... 603

Create a new IP list of trusted traffic sources ..... 604
Create incoming and outbound firewall rules for trusted traffic using the IP list ..... 604
Assign the firewall rules to a policy used by computers that trusted traffic flows through ..... 605
Firewall rule actions and priorities ..... 605
Firewall rule actions ..... 605
More about Allow rules ..... 606
More about Bypass rules ..... 606
Default Bypass rule for Deep Security Manager traffic ..... 607
More about Force Allow rules ..... 608
Firewall rule sequence ..... 608
A note on logging ..... 609
How firewall rules work together ..... 610
Rule Action ..... 610
Rule priority ..... 611
Putting rule action and priority together ..... 612
Firewall settings ..... 612
General ..... 613
Firewall ..... 613
Firewall Stateful Configurations ..... 613
Port Scan (Computer Editor only) ..... 613
Assigned Firewall Rules ..... 614
Interface Isolation ..... 615
Interface Isolation ..... 615
Interface Patterns ..... 615
Reconnaissance ..... 615
Reconnaissance Scans ..... 615
Advanced ..... 618
Events ..... 618
Events ..... 618

Firewall settings with Oracle RAC ..... 618
Add a rule to allow communication between nodes ..... 619
Add a rule to allow UDP port 42424 ..... 619
Allow other RAC-related packets ..... 621
Ensure that the Oracle SQL Server rule is assigned ..... 624
Ensure that anti-evasion settings are set to "Normal" ..... 624
Define stateful firewall configurations ..... 625
Add a stateful configuration ..... 626
Enter stateful configuration information ..... 626
Select packet inspection options ..... 626
IP packet inspection ..... 626
TCP packet inspection ..... 627
FTP Options ..... 628
UDP packet inspection ..... 629
ICMP packet inspection ..... 629
Export a stateful configuration ..... 630
Delete a stateful configuration ..... 630
See policies and computers a stateful configuration is assigned to ..... 630
Scan for open ports ..... 631
Monitor for system changes with integrity monitoring ..... 632
Set up integrity monitoring ..... 632
How to enable Integrity Monitoring ..... 632
Turn on Integrity Monitoring ..... 633
Run a Recommendation scan ..... 634
Apply the Integrity Monitoring rules ..... 635
Build a baseline for the computer ..... 637
Periodically scan for changes ..... 637
When Integrity Monitoring scans are performed ..... 637
Integrity Monitoring scan performance settings ..... 638

Limit CPU usage ..... 638
Change the content hash algorithm ..... 639
Enable a VM Scan Cache configuration ..... 639
Integrity Monitoring event tagging ..... 639
Create an integrity monitoring rule ..... 640
Add a new rule ..... 641
Enter integrity monitoring rule information ..... 641
Select a rule template and define rule attributes ..... 642
Registry Value template ..... 642
File template ..... 642
Custom (XML) template ..... 643
Configure Trend Micro integrity monitoring rules ..... 643
Configure rule events and alerts ..... 644
Real-time event monitoring ..... 644
Alerts ..... 644
See policies and computers a rule is assigned to ..... 644
Export a rule ..... 644
Delete a rule ..... 644
Integrity monitoring rules language ..... 645
Entity Sets ..... 646
Hierarchies and wildcards ..... 647
Syntax and concepts ..... 648
Include tag ..... 649
Exclude tag ..... 650
Case sensitivity ..... 650
Entity features ..... 651
ANDs and ORs ..... 653
Order of evaluation ..... 654
Entity attributes ..... 654

Shorthand attributes ..... 655
onChange attribute ..... 656
Environment variables ..... 656
Environment variable overrides ..... 657
Registry values ..... 657
Use of ".." ..... 658
Best practices ..... 658
DirectorySet ..... 659
Tag Attributes ..... 659
Entity Set Attributes ..... 660
Short Hand Attributes ..... 661
Meaning of "Key" ..... 661
Sub Elements ..... 661
FileSet ..... 662
Tag Attributes ..... 662
Entity Set Attributes ..... 662
Short Hand Attributes ..... 664
Drives Mounted as Directories ..... 664
Alternate Data Streams ..... 664
Meaning of "Key" ..... 665
Sub Elements ..... 665
Special attributes of Include and Exclude for FileSets: ..... 666
GroupSet ..... 666
Tag Attributes ..... 666
Entity Set Attributes ..... 666
Short Hand Attributes ..... 667
Meaning of "Key" ..... 667
Include and Exclude ..... 667
InstalledSoftwareSet ..... 667

Tag Attributes ....668
Entity Set Attributes ....668
Short Hand Attributes ....669
Meaning of "Key" ....669
Sub Elements ....669
Special attributes of Include and Exclude for InstalledSoftwareSets: ....669
PortSet ....670
Tag Attributes ....670
Entity Set Attributes ....670
Meaning of "Key" ....671
IPV6 ....671
Matching of the Key ....671
Sub Elements ....672
Special attributes of Include and Exclude for PortSets: ....672
ProcessSet ....673
Tag Attributes ....673
Entity Set Attributes ....673
Short Hand Attributes ....674
Meaning of "Key" ....674
Sub Elements ....675
Special attributes of Include and Exclude for ProcessSets: ....675
RegistryKeySet ....676
Tag Attributes ....676
Entity Set Attributes ....677
Short Hand Attributes ....677
Meaning of "Key" ....677
Sub Elements ....677
RegistryValueSet ....678
Tag Attributes ....678

Entity Set Attributes ..... 678
Short Hand Attributes ..... 679
Meaning of "Key" ..... 679
Default Value ..... 679
Sub Elements ..... 680
ServiceSet ..... 680
Tag Attributes ..... 680
Entity Set Attributes ..... 681
Short Hand Attributes ..... 682
Meaning of "Key" ..... 682
Sub Elements ..... 682
Special attributes of Include and Exclude for ServiceSets: ..... 683
UserSet ..... 683
Tag Attributes ..... 683
Entity Set Attributes ..... 683
Common Attributes ..... 683
Windows-only Attributes ..... 684
Linux-only Attributes ..... 685
Short Hand Attributes ..... 685
Meaning of "Key" ..... 686
Sub Elements ..... 686
Include and Exclude ..... 686
Special attributes of Include and Exclude for UserSets ..... 686
WQLSet ..... 687
Entity Set Attributes ..... 689
Meaning of Key ..... 691
Include Exclude ..... 691
Analyze logs with log inspection ..... 691
Set up log inspection ..... 692

Turn on the log inspection module ..... 693
Run a recommendation scan ..... 693
Apply the recommended log inspection rules ..... 694
Configure log inspection event forwarding and storage ..... 695
Define a log inspection rule for use in policies ..... 696
Create a new log inspection rule ..... 696
Decoders ..... 698
Subrules ..... 700
Groups ..... 700
Rules, ID, and Level ..... 701
Description ..... 702
Decoded As ..... 702
Match ..... 703
Conditional Statements ..... 704
Hierarchy of Evaluation ..... 704
Restrictions on the Size of the Log Entry ..... 706
Composite Rules ..... 706
Real world examples ..... 708
Log inspection rule severity levels and their recommended use ..... 717
strftime() conversion specifiers ..... 718
Examine a log inspection rule ..... 719
Log inspection rule structure and the event matching process ..... 719
Duplicate Sub-rules ..... 722
Block access to malicious URLs with web reputation ..... 723
Turn on the web reputation module ..... 724
Switch between inline and tap mode ..... 724
Enforce the security level ..... 725
To configure the security level: ..... 725
Create exceptions ..... 726

To create URL exceptions: 726
Configure the Smart Protection Server 727
Smart Protection Server Connection Warning 728
Edit advanced settings 728
Blocking Page 728
Alert 729
Ports 729
Deep Security Best Practice Guide 729
**Maintain 730**
Check your license information 730
Licensing for Deep Security from AWS Marketplace 730
Back up and restore your database 731
Microsoft SQL Server Database 731
Restore the database only 732
Restore both the Deep Security Manager and the database 732
Export objects in XML or CSV format 733
Import objects 734
Restart the Deep Security Manager 734
Linux 734
Windows 735
Windows desktop 735
Command prompt 735
PowerShell 735
Upgrade Deep Security 735
About upgrades 735
How agents validate the integrity of updates 736
How Deep Security Manager checks for software updates 737
Update the Deep Security Agent 738
Update available notifications 738

Initiate an agent update ..... 739
Manually upgrade the agent ..... 739
Windows ..... 740
Linux ..... 740
Upgrade the Deep Security Manager AMI ..... 740
Upgrade Deep Security Manager AMI 11.0 or later ..... 741
Manually upgrade your Deep Security Manager AMI ..... 741
Error: The installer could not establish a secure connection to the database server ..... 742
Get and distribute security updates ..... 743
Configure a security update source and settings ..... 745
Perform security updates ..... 746
Special case: configure updates on a relay-enabled agent in an air-gapped environment ..... 746
Check your security update status ..... 747
See details about pattern updates ..... 747
See details about rule updates ..... 748
Use a web server to distribute software updates ..... 749
Web server requirements ..... 749
Copy the folder structure ..... 749
Configure agents to use the new software repository ..... 751
Disable emails for New Pattern Update alerts ..... 752
Harden Deep Security ..... 752
Protect Deep Security Manager with an agent ..... 753
Protect Deep Security Agent ..... 755
Bind Deep Security Agent to a specific Deep Security Manager ..... 755
Replace the Deep Security Manager SSL certificate ..... 756
See your trusted certificates ..... 757
Replace the SSL certificate in a Windows environment ..... 758
Create a new .keystore file and add your certificates to the cacerts file ..... 758
Create a PKCS12 keychain file and import it into the new .keystore file ..... 759

Configure Deep Security Manager to use the new .keystore file ....760
Replace the SSL certificate in a Linux environment ....761
Create a new .keystore file and add your certificates to the cacerts file ....761
Create a PKCS12 keychain file and import it into the new .keystore file ....762
Configure the Deep Security Manager to use the new .keystore file ....763
Encrypt communication between the Deep Security Manager and the database ....763
Encrypt communication between the manager and database ....764
Microsoft SQL Server database (Linux) ....764
Microsoft SQL Server (Windows) ....765
Oracle Database ....766
PostgreSQL ....767
Running an agent on the database server ....768
Disable encryption between the manager and database ....768
Microsoft SQL Server database (Linux) ....768
Microsoft SQL Server (Windows) ....769
Oracle Database ....769
PostgreSQL ....769
Change the Deep Security Manager database password ....770
Change your Microsoft SQL Server password ....770
Change your Oracle password ....771
Change your PostgreSQL password ....771
Enable Content Security Policy and HTTP Public Key Pinning ....772
Add a content security policy or public key pin policy ....772
Reset your configuration ....773
Content security policy ....773
Public key pin policy ....773
Enforce user password rules ....773
Specify password requirements ....773
Use another identity provider for sign-on ....775

Add a message to the Deep Security Manager Sign In page ..... 775
Present users with terms and conditions ..... 775
Other Security settings ..... 775
Set up multi-factor authentication ..... 775
Enable multi-factor authentication ..... 776
Disable multi-factor authentication ..... 778
Supported multi-factor authentication (MFA) applications ..... 778
Troubleshooting MFA ..... 779
What if my MFA is enabled but not working? ..... 779
What if my MFA device is lost or stops working? ..... 779
Manage AWS regions ..... 780
Add an Amazon Web Services region ..... 780
Viewing your Amazon Web Services regions ..... 780
Removing an Amazon Web Services region ..... 781
Configure alerts ..... 781
View alerts in Deep Security Manager ..... 782
Configure alert settings ..... 783
Set up email notification for alerts ..... 783
Turn alert emails on or off ..... 784
Configure an individual user to receive alert emails ..... 785
Configure recipients for all alert emails ..... 785
Generate reports about alerts and other activity ..... 786
Set up a single report ..... 786
Set up a recurring report ..... 789
Customize the dashboard ..... 790
Date and time range ..... 791
Computers and computer groups ..... 791
Filter by tags ..... 792
Select dashboard widgets ..... 793

Change the layout ..... 793
Save and manage dashboard layouts ..... 794
Event collection in Deep Security ..... 795
Where are event logs on the agent? ..... 795
When are events sent to the manager? ..... 795
How long are events stored? ..... 796
System events ..... 796
Security events ..... 796
See the events associated with a policy or computer ..... 797
View details about an event ..... 797
Filter the list to search for an event ..... 798
Export events ..... 799
Improve logging performance ..... 799
Log and event storage best practices ..... 799
Troubleshooting ..... 801
Limit log file sizes ..... 802
Event logging tips ..... 803
Apply tags to identify and group events ..... 804
Manual tagging ..... 804
Auto-tagging ..... 805
Set the precedence for an auto-tagging rule ..... 806
Auto-tagging log inspection events ..... 806
Trusted source tagging ..... 807
Local trusted computer ..... 807
How does Deep Security determine whether an event on a target computer matches an event on a trusted source computer? ..... 808
Tag events based on a local trusted computer ..... 808
Tag events based on the Trend Micro Certified Safe Software Service ..... 809
Tag events based on a trusted common baseline ..... 809

Delete a tag ..... 810
Reduce the number of logged events ..... 810
Rank events to quantify their importance ..... 813
Web reputation event risk values ..... 813
Firewall rule severity values ..... 813
Intrusion prevention rule severity values ..... 813
Integrity monitoring rule severity values ..... 814
Log inspection rule severity values ..... 814
Asset values ..... 814
Forward Deep Security events to an external syslog or SIEM server ..... 814
Forward system events to a syslog or SIEM server ..... 815
Forward security events to a syslog or SIEM server ..... 816
Forward security events directly from agent computers to a syslog or SIEM server ..... 816
Forward security events from the agent computers via the Deep Security Manager ..... 817
Define a syslog configuration ..... 817
Troubleshooting ..... 820
"Failed to Send Syslog Message" alert ..... 820
Can't edit syslog configurations ..... 820
Can't see the syslog configuration sections of Deep Security Manager ..... 820
Syslog not transferred due to an expired certificate ..... 821
Syslog not delivered due to an expired or changed server certificate ..... 821
Syslog or SIEM servers used for testing ..... 821
Syslog message formats ..... 821
CEF syslog message format ..... 822
LEEF 2.0 syslog message format ..... 824
Events originating in the Manager ..... 824
System event log format ..... 824
Events originating in the agent ..... 825
Anti-malware event format ..... 825

Application control event format 839
Firewall event log format 845
Integrity monitoring log event format 849
Intrusion prevention event log format 852
Log inspection event format 858
Web reputation event format 860
Configure Red Hat Enterprise Linux to receive event logs 863
Set up a Syslog on Red Hat Enterprise Linux 6 or 7 863
Set up a Syslog on Red Hat Enterprise Linux 5 864
Access events with Amazon SNS 864
Create an AWS user 865
Create an Amazon SNS topic 866
Enable SNS 866
Create subscriptions 867
JSON SNS configuration 867
Version 867
Statement 867
Topic 868
Condition 868
Bool 869
Exists 869
IpAddress 870
NotIpAddress 871
NumericEquals 872
NumericNotEquals 872
NumericGreaterThan 873
NumericGreaterThanEquals 874
NumericLessThan 875
NumericLessThanEquals 875

StringEquals ..... 876
StringNotEquals ..... 877
StringEqualsIgnoreCase ..... 877
StringNotEqualsIgnoreCase ..... 878
StringLike ..... 878
StringNotLike ..... 878
Event Description ..... 880
Event Data Types ..... 880
Event Properties ..... 881
Example events in JSON format ..... 897
Example Configurations ..... 899
Send all critical intrusion prevention events to an SNS topic ..... 899
Send different events to different SNS topics ..... 899
Multiple statements vs. multiple conditions ..... 900
Multiple statements ..... 900
Multiple conditions ..... 901
DevOps, automation and scaling ..... 902
DevOps, automation and scaling ..... 902
Forward system events to a remote computer via SNMP ..... 903
Lists of events and alerts ..... 903
Predefined alerts ..... 903
Agent events ..... 914
System events ..... 918
Anti-malware events ..... 942
What information is displayed for anti-malware events? ..... 942
List of all anti-malware events ..... 944
Firewall events ..... 944
What information is displayed for firewall events? ..... 945
List of all firewall events ..... 946

Intrusion prevention events ....953
What information is displayed for intrusion prevention events? ....953
List of all intrusion prevention events ....955
Integrity monitoring events ....957
What information is displayed for integrity monitoring events? ....957
List of all integrity monitoring events ....958
Log inspection events ....960
What information is displayed for log inspection events? ....960
List of log inspection security events ....962
Web reputation events ....962
What information is displayed for web reputation events? ....962
Add a URL to the list of allowed URLs ....963
Troubleshoot common events, alerts, and errors ....963
Why am I seeing firewall events when the firewall module is off? ....964
Why am I getting "Unrecognized Client" events? ....964
Troubleshoot "Smart Protection Server disconnected" errors ....965
Check the error details ....965
Error: Activation Failed ....965
Activation Failed - Protocol Error ....966
Agent-initiated communication ....966
Bidirectional communication ....966
Activation Failed - Unable to resolve hostname ....966
Activation Failed - No Agent/Appliance ....967
Activation Failed - AWS Marketplace billing usage data has not been submitted in 48 hours ....967
Error: Agent version not supported ....967
Error: Installation of Feature 'dpi' failed: Not available: Filter ....967
Additional information ....968
Error: AWS Marketplace billing usage data has not been successfully submitted in over 48 hours ....968
Error: Interface out of sync ....969

Check the specific virtual computer interfaces ....970
Check the virtual computer interface information in vCenter ....970
Check the vmx file and the virtual computer interface information in Deep Security Manager ....970
Check the virtual computer interface information in the Deep Security Virtual Appliance ....971
Workaround Options ....971
Option 1 ....971
Option 2 ....972
Option 3 ....972
Further Troubleshooting ....972
Error: Integrity Monitoring Engine Offline and other errors occur after activating a virtual machine ....973
Error: Module installation failed (Linux) ....974
Error: There are one or more application type conflicts on this computer ....974
Resolution ....975
Consolidate ports ....975
Disable the inherit option ....976
Error: Unable to connect to the cloud account ....976
Your AWS account access key ID or secret access key is invalid ....976
The incorrect AWS IAM policy has been applied to the account being used by Deep Security ....977
NAT, proxy, or firewall ports are not open, or settings are incorrect ....977
Error: Unable to resolve instance hostname ....978
Error: Anti-malware engine offline ....978
Agent-based protection ....978
If your agent is Windows: ....979
If your agent is Linux: ....979
Agentless protection ....980
Error: Check Status Failed ....981
Error: Log Inspection Rules Require Log Files ....981
If the file's location is required: ....982
If the files listed do not exist on the protected machine: ....982

Alert: Integrity Monitoring information collection has been delayed ..... 983
Alert: The memory warning threshold of Manager Node has been exceeded ..... 983
Increase the allocated memory on a Windows server ..... 983
Increase the allocated memory on a Linux server ..... 984
Verify the memory allocation change ..... 984
Alert: Manager Time Out of Sync ..... 984
Event: Max TCP connections ..... 984
Warning: Census, Good File Reputation, and Predictive Machine Learning Service Disconnected ..... 985
Cause 1: The agent or relay-enabled agent doesn't have Internet access ..... 986
Cause 2: A proxy was enabled but not configured properly ..... 986
Warning: Reconnaissance Detected ..... 986
Types of reconnaissance scans ..... 987
Suggested actions ..... 987
Warning: Insufficient disk space ..... 988
Tips ..... 989
Create and manage users ..... 989
Synchronize with an Active Directory ..... 989
Filtering the Active Directory ..... 990
Add or edit an individual user ..... 991
Change a user's password ..... 994
Lock out a user or reset a lockout ..... 994
View system events associated with a user ..... 994
Delete a user ..... 994
Define roles for users ..... 995
Add or edit a role ..... 996
Default settings for full access, auditor, and new roles ..... 1002
Add users who can only receive reports ..... 1010
Add or edit a contact ..... 1010
Delete a contact ..... 1010

Create an API key for a user ..... 1011
Lock out an existing API key ..... 1011
Unlock a locked out user name ..... 1012
Unlock users as an administrator ..... 1012
Unlock administrative users from a command line ..... 1012
Implement SAML single sign-on ..... 1013
What are SAML and single sign-on? ..... 1013
How SAML single sign-on works in Deep Security ..... 1013
Establishing a trust relationship ..... 1013
Creating Deep Security accounts from user identities ..... 1014
Implement SAML single sign-on in Deep Security ..... 1015
Getting started with SAML single sign-on ..... 1015
Configure pre-set up requirements ..... 1016
Configure Deep Security as a SAML service provider ..... 1016
Configure SAML in Deep Security ..... 1018
Import your identity provider's SAML metadata document ..... 1018
Create Deep Security roles for SAML users ..... 1018
Provide information for your identity provider administrator ..... 1018
Download the Deep Security Manager service provider SAML metadata document ..... 1018
Send URNs and the Deep Security SAML metadata document to the identity provider administrator 1019
SAML claims structure ..... 1019
Deep Security user name (required) ..... 1019
Sample SAML data (abbreviated) ..... 1020
Deep Security user role (required) ..... 1020
Sample SAML data (abbreviated) ..... 1020
Maximum session duration (optional) ..... 1021
Sample SAML data (abbreviated) ..... 1021
Preferred language (optional) ..... 1021
Sample SAML data (abbreviated) ..... 1021

Test SAML single sign-on ..... 1022
Review the set-up ..... 1022
Create a Diagnostic Package ..... 1022
Service and identity provider settings ..... 1022
Navigate and customize Deep Security Manager ..... 1023
Group computers dynamically with smart folders ..... 1023
Create a smart folder ..... 1024
Edit a smart folder ..... 1026
Clone a smart folder ..... 1026
Focus your search using sub-folders ..... 1026
Automatically create sub-folders ..... 1027
Searchable Properties ..... 1028
General ..... 1028
AWS ..... 1030
Azure ..... 1032
vCenter ..... 1033
vCloud ..... 1033
Folder ..... 1034
Operators ..... 1034
View active Deep Security Manager nodes ..... 1036
Customize advanced system settings ..... 1038
Primary Tenant Access ..... 1038
Load Balancers ..... 1038
Multi-tenant Mode ..... 1039
Deep Security Manager Plug-ins ..... 1039
SOAP Web Service API ..... 1040
Status Monitoring API ..... 1040
Export ..... 1040
Whois ..... 1040

Licenses ..... 1041
Scan Cache Configurations ..... 1041
CPU Usage During Recommendation Scans ..... 1041
Logo ..... 1041
Manager AWS Identity ..... 1041
Application control ..... 1042
Accelerate compliance ..... 1047
Meet PCI DSS requirements with Deep Security ..... 1048
GDPR ..... 1048
FIPS 140-2 support ..... 1049
Differences when operating Deep Security in FIPS mode ..... 1050
System requirements for FIPS mode ..... 1051
Deep Security Manager requirements ..... 1051
Deep Security Agent requirements ..... 1052
Enable FIPS mode for your Deep Security Manager ..... 1052
Enable FIPS mode for a Deep Security Manager on Windows ..... 1052
Enable FIPS mode for a Deep Security Manager on Linux ..... 1052
Connect to external services when in FIPS mode ..... 1053
Enable FIPS mode for the operating system of the computers you are protecting ..... 1053
Enable FIPS mode for the Deep Security Agent on the computers you are protecting ..... 1054
Enable FIPS mode for a Windows 7 agent ..... 1054
Enable FIPS mode for an RHEL 7 or CentOS 7 agent ..... 1054
Using FIPS mode with a PostgreSQL database ..... 1054
Using FIPS mode with a Microsoft SQL Server database ..... 1057
Disable FIPS mode ..... 1059
Set up AWS Config Rules ..... 1059
Bypass vulnerability management scan traffic in Deep Security ..... 1060
Create a new IP list from the vulnerability scan provider IP range or addresses ..... 1060
Create firewall rules for incoming and outbound scan traffic ..... 1061

Assign the new firewall rules to a policy to bypass vulnerability scans ....1062
Use TLS 1.2 with Deep Security ....1062
Benefits of TLS 1.2 ....1064
TLS 1.2 architectures ....1064
Upgrade components to use TLS 1.2 ....1069
Verify and upgrade your Deep Security Manager ....1069
Verify your Deep Security Manager database ....1069
Verify your Deep Security Agents ....1070
Verify your Deep Security Relays ....1070
Enforce TLS 1.2 ....1071
Where can TLS 1.2 be enforced? ....1071
What happens when TLS 1.2 enforced? ....1071
Is TLS 1.2 enforced by default? ....1072
Under what circumstances is TLS 1.2 enforcement possible? ....1072
Enforce TLS 1.2 on Deep Security Manager ....1072
Enforce TLS 1.2 on the Deep Security Relay ....1073
Enforce TLS 1.2 on just the manager's GUI port (4119) ....1073
Test that TLS 1.2 is enforced ....1074
Re-enable early TLS (1.0) ....1075
Re-enable TLS 1.0 on Deep Security Manager and the Deep Security Relay ....1075
Re-enable TLS 1.0 on the manager's GUI port (4119) ....1076
Determine whether TLS 1.2 is enforced ....1076
Guidelines for deploying agents, and relays after TLS 1.2 is enforced ....1077
Guidelines for deploying agents, and relays when TLS 1.2 is enforced ....1077
Guidelines for using deployment scripts when TLS 1.2 is enforced ....1077
Workaround ....1078
Migrate a Microsoft SQL Server Express database to Enterprise ....1080
Uninstall Deep Security ....1081
Uninstall Deep Security Relay ....1081

Uninstall a relay (Windows) ..... 1082
Uninstall a relay (Linux) ..... 1082
Uninstall Deep Security Agent ..... 1083
Uninstall an agent (Windows) ..... 1083
Uninstall an agent (Linux) ..... 1083
Uninstall an agent (Solaris 9 or 10) ..... 1084
Uninstall an agent (Solaris 11) ..... 1084
Uninstall an agent (AIX) ..... 1084
Uninstall an agent (HP-UX) ..... 1085
Uninstall Deep Security Notifier ..... 1085
Uninstall Deep Security Manager ..... 1085
Uninstall the manager (Windows) ..... 1085
Uninstall the manager (Linux) ..... 1086
**FAQs ..... 1086**
Deep Security release life cycle and support policy ..... 1086
Support milestones for major releases ..... 1087
Major release support services ..... 1087
Why does my Windows machine lose network connectivity when I turn on protection? ..... 1088
How do I get news about Deep Security? ..... 1089
How do I migrate to a larger RDS database instance? ..... 1089
AWS GovCloud (US) support ..... 1090
Protecting GovCloud instances using a manager in a commercial AWS instance ..... 1091
How can I minimize heartbeat alerts for offline environments in an AWS Elastic Beanstalk environment? ..... 1091
Why can't I add my Azure server using the Azure cloud connector? ..... 1092
Why can't I view all of the VMs in an Azure subscription in Deep Security? ..... 1093
**Troubleshooting ..... 1094**
AWS Marketplace Quick Start ..... 1094
Check CloudFormation template stack events ..... 1094
AWS Marketplace terms were not accepted ..... 1095

A stack could not create the IAM role ..... 1095
A stack could not create the Deep Security Manager database ..... 1096
Gather stack information and contact Trend Micro support ..... 1096
"Activation Failed" agent status ..... 1096
"Offline" agent ..... 1097
Causes ..... 1097
Verify that the agent is running ..... 1098
Verify DNS ..... 1098
Allow outbound ports (agent-initiated heartbeat) ..... 1099
Allow inbound ports (manager-initiated heartbeat) ..... 1100
Allow ICMP on Amazon AWS EC2 instances ..... 1100
High CPU usage ..... 1101
Security update connectivity ..... 1101
Purple screen of death ..... 1102
Prevent MTU-related agent communication issues across Amazon Virtual Private Clouds (VPC) ..... 1103
Create a diagnostic package and logs ..... 1105
Deep Security Manager diagnostics ..... 1105
Create a diagnostic package for Deep Security Manager ..... 1105
Enable debug logs for Deep Security Manager ..... 1105
Deep Security Agent diagnostics ..... 1106
Create an agent diagnostic package via Deep Security Manager ..... 1106
Create an agent diagnostic package via CLI on a protected computer ..... 1107
Collect debug logs with DebugView ..... 1107

# Get Started

## Privacy and personal data collection disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Trend Micro Deep Security collects and provides detailed instructions on how to disable the specific features that feed back the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Skip To Main Content

- placeholder

Filter:

- All Files

Submit Search

# D
# eep Security Software

© 2020 Trend Micro Incorporated. All rights reserved.

# Buy Deep Security AMI from AWS Marketplace

With Deep Security AMI from AWS Marketplace you can deploy the Deep Security AMI to protect your physical, virtual or cloud resources using either an agent or a virtual appliance, and are only billed for the hours that your computers are protected.

For more information on pricing, purchasing, and requirements, see the AWS Marketplace page for Trend Micro Deep Security.

## Check Deep Security pricing and billing on AWS Marketplace

In this article, you can learn more about:

- "Deep Security pricing" below.
- "What Deep Security considers as a protection hour" on the next page.
- "When Deep Security considers a computer protected" on page 59.

### Deep Security pricing

Pricing for AWS Marketplace billing subscription, prepaid credit and credit card subscription or Azure Marketplace Deep Security Manager (BYOL) payment options are:

| Instance size | Example instance types | Cost of protected instance per hour (in USD) |
|---|---|---|
| Medium or smaller | Amazon EC2: C1, M1, M3, T1, T2<br>Amazon WorkSpaces<br>Azure: 1 core | $0.01 |

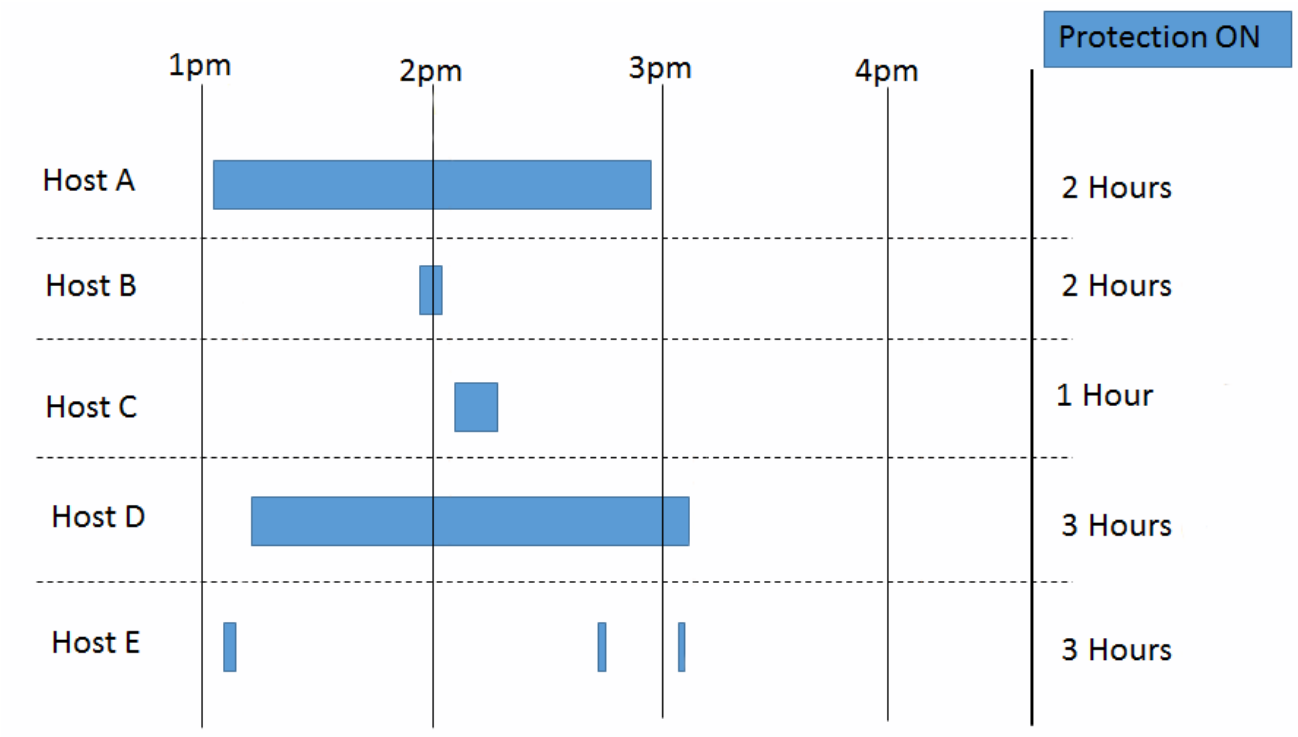
| Instance size | Example instance types | Cost of protected instance per hour (in USD) |
|---|---|---|
| Large | Amazon EC2: C3, C4, M1, M3, M4, R3, T2<br>Azure: 2 cores | $0.03 |
| xLarge and bigger | Amazon EC2: C1, C3, C4, CC2, CG1, CR1, D2, G2, HI1, HS1, I2, M1, M2, M3, M4, R3<br>Azure: 4 or more cores | $0.06 |
| Data Center | All non-cloud instances | $0.06 |

**Note:** If you are using the prepaid credit option, Trend Micro notifies you when you have 30 days left of credit, estimated based on your current usage. If your credit runs out before you have renewed, your protection remains active but you won't be able to activate any new agents and existing agents will no longer receive any updates.

## What Deep Security considers as a protection hour

With Deep Security AWS Marketplace billing, you pay for any hours during which your computers are protected. A computer that is protected for any part of an hour will be billed for the full hour.

You can see how this is calculated in the usage scenarios below:




## When Deep Security considers a computer protected

When a computer is considered to be protected by Deep Security depends on where it is hosted.

### Computers in a cloud

For computers added to Deep Security from a cloud service such as AWS, you are billed when the instance that the agent is protecting is powered on. This means that you will continue to be billed for agents in an "Offline" state if their instances are still powered on.

To avoid being billed for protection unnecessarily, if you are considering turning off an instance's Deep Security Agent, Trend Micro recommends that you power off that instance instead.

### Computers not in a cloud

For computers added to Deep Security that are not on a cloud service, you are billed when the agent is not "Offline". A computer will enter the "Offline" state if the agent protecting it misses one or more heartbeats from the Deep Security Manager.

# Change your Deep Security AMI from AWS Marketplace payment option

To change your Deep Security AMI from AWS Marketplace payment type, you need to perform the following steps:

1. "Modify the Deep Security Manager database" below.
2. "Install Deep Security Manager" on the next page.
3. "Delete previous Deep Security Manager instances" on page 62.

## Modify the Deep Security Manager database

**Note:** We strongly recommend that you back up your database before proceeding with the upgrade. Installations with embedded databases cannot be migrated from Pay Per Use (Deep Security (Classic)) to another payment type.

1. SSH into Deep Security Manager and run the following command:

   ```
   service dsm_s stop
   ```

2. Run the command from the table below that corresponds with the payment type you want to switch to:

| Payment type | Command |
|---|---|
| Pay Per Use | `sudo /opt/dsm/dsm_c -action changesetting -name com.trendmicro.ds.awsmarketplace:settings.configuration.productCode -value 997iokndd q6g16v8h8iqv5qg3` |
| AWS Marketplace Billing | `sudo /opt/dsm/dsm_c -action changesetting -name com.trendmicro.ds.awsmarketplace:settings.configuration.productCode -value cqcvf9f0ugw8rkbgmf1c9dtxu` |
| Bring Your Own License | `sudo /opt/dsm/dsm_c -action changesetting -name com.trendmicro.ds.awsmarketplace:settings.configuration.productCode -value 9sc4t8suhxrja5nkxqdrnuue5` |

3. Run the following command to verify that Deep Security Manager is using the correct

payment option:

```
sudo /opt/dsm/dsm_c -action viewsetting -name
com.trendmicro.ds.awsmarketplace:settings.configuration.productCode
```

## Install Deep Security Manager

1. Deploy a new instance of Deep Security Manager using the latest version from the AWS Marketplace.

   **Note:** If you are using Deep Security Marketplace metered billing, you cannot launch the new Deep Security AMI until you have configured the AWS Identity and Access Management (IAM) settings for the instance.

   **Warning:** The new instance of the Deep Security Manager must either be configured for load balancing or have the same network address or DNS host name as the previous Deep Security Manager instance.

2. Start the instance, go to `https://<host or IP>:8080`, enter the Instance ID, and click **Sign In**.

   The Deep Security setup page appears.

3. Read and accept the terms of the license agreement on the License Agreement tab and click **Next**.

4. Enter the configuration parameters of your existing Deep Security database on the Database tab and click **Next**.

5. Click **Upgrade** on the Previous Version Check tab and click **Next**.

6. On the Ports tab, type the host name or IP address of the computer you are installing Deep Security Manager on, and then click **Next**.

   **Note:** The Manager Address must be either a resolvable host name, a fully qualified domain name, or an IP address. If DNS is not available in your environment or if some computers are unable to use DNS, a fixed IP address should be used instead of a host

name. You can also change the default communication ports. See "Port numbers" on page 96.

7. Click **Next** on the Credentials tab.

   The existing credentials will stay the same.

8. Review the installation settings on the Review Settings tab to ensure that they are correct, and then click **Install**.

   The Deep Security Status page will show that the Deep Security Manager is being installed. When the installation is complete, Deep Security Manager will be displayed.

## Delete previous Deep Security Manager instances

1. Log in to Deep Security Manager and delete the computer records for any old Deep Security Manager installations by clicking the **Computers** tab, selecting the record, and clicking **Delete** on the toolbar.
2. Delete old manager nodes by going to the **Administration** tab in Deep Security Manager, selecting **Manager Nodes** in the left-hand navigation menu, opening the **Properties** dialog for each old manager node (Status: "Offline (Upgrade Required)"), and clicking **Decommission**.
3. Delete your old Deep Security Manager instances by right-clicking on the instance from the AWS console and selecting **Instance State > Terminate**.

# Check billing and usage for the Deep Security AMI from AWS Marketplace

After you have set up Deep Security from AWS Marketplace and deployed agents, you can view your hourly usage data per protected host by going to **Administration > AWS Billing Usage Data** in Deep Security Manager. From there, you can filter your usage data to show various periods of time and you can also export a usage report in CSV format. The Status column indicates if you were billed for the usage or not.

## View usage data

1. Go to **Administration > AWS Billing Usage Data**.
2. Select the period of time for which you want to view usage data from the **Period** list in the upper-left corner of the AWS Billing Usage Data page.
   -OR-
   Select **Custom Range** from the **Period** list and specify the start and end date in the **From** and **To** boxes.

## Export a usage data report

1. Go to **Administration > AWS Billing Usage Data**.
2. Click **Export** and select a report type depending on what usage data you want to export:

| Report | Rows | Columns |
|---|---|---|
| Export to CSV | All | Usage Data, Category, Instances, Status |
| Export Selected to CSV | User selected | Usage Data, Category, Instances, Status |
| Export to CSV (Computers View) | All | Usage Date, Computer Name, Instance Type, Category |
| Export Selected to CSV (Computers View) | User selected | Usage Date, Computer Name, Instance Type, Category |

# What's new?

## Deep Security 11.1

Below are major changes in the **feature release** Deep Security 11.1. For the support life cycle, see "Feature releases" on page 66. For a detailed change log, see the Deep Security release notes.

- **Simplified AMI upgrade:** If you are using Deep Security Manager AMI version 11.0 or later and see **A new version of Deep Security is available** in a banner at the top of the Deep Security Manager console, you can click **Upgrade Deep Security** in the banner to begin the upgrade process. For details, see "Upgrade the Deep Security Manager AMI" on page 740
- **New RESTful API:** Deep Security 11.1 provides a new RESTful API that enables you to automate the provisioning and maintenance of security via Deep Security. Go to the Deep Security Automation Center to download the SDKs in the language of your choice and learn how to use the API.

  The focus of the new API, which is continuously updated with new features and improvements, is on improving the functionality that exists in the SOAP API. When you start new automation projects, you should use the new API to benefit from continued support and maintenance in the long term.

  > **Note:** The REST and SOAP APIs that were provided before Deep Security 11.1 have not changed. They are still provided and function as usual. Support also has not changed for the older APIs. For details, see "Use the Deep Security API to automate tasks" on page 261.

- **Application control hash-based rules:** With Deep Security Agent 11.1, application control rules are based on a software file's SHA-256 has value, and not by file name and/or path. This enhancement greatly improves the coverage of each rule and reduces the operational overhead of creating and managing multiple rules for files with the same hash value. For example, if a file with a particular hash executes repeatedly on a machine but with a different file name each time, a single hash-based allow or block rule controls its execution. Previously, rules also evaluated the file name and file path, so a new rule would be needed each time the software was executed. For details, see "What does application control detect as a software change?" on page 461 Or, if you are using the Deep Security API to create shared rulesets, see "Use the API to create shared and global rulesets " on page 479.
- **Application control simplification:** The application control user interface has been simplified by removing the redundant decision log view. For information on how to reverse

an application control decision, see "View and change application control rulesets" on page 474.

- **Agent for Debian 9:** Deep Security Agent 11.1 supports Debian 9. For details, see "Supported features by platform" on page 77.
- **Alert improvement**: The 'Relay Update Service Unavailable' alert has been renamed to 'A Deep Security Relay cannot download security components' and now includes a more accurate description and solution.
- **Command improvement**: The `dsa_query`, and `dsa_control` commands now show the agent version and Deep Security protection module information. See "Command-line basics" on page 244 for details.
- **Smart Protection Server security improvement**: The Smart Protection Server CloudFormation Template in AWS now includes an HTTPS URL for the web reputation service. For details, see "Deploy a Smart Protection Server in AWS" on page 228.
- **TLS 1.2 change**: TLS 1.2 is now the default for all new Deep Security 11.1 deployments. If third-party applications or agents that do not support TLS 1.2 are used you'll need to re-enable TLS 1.0 to allow those applications to connect to Deep Security Manager. For backward compatibility, use of TLS 1.0 will be preserved on upgrades to Deep Security 11.1. See "Use TLS 1.2 with Deep Security" on page 1062 for details.
- **TLS 1.2 command addition**: The `dsm_c` command includes a new `-action` parameter called `settlsprotocol`. This parameter allows you to set and view the minimum TLS version accepted by Deep Security Manager. See "Command-line basics" on page 244 for details.
- **Trend Micro licensing and registration server security improvement**: As of Deep Security 11.1, all communication with the Trend Micro licensing and registration server must be secured using HTTPS. This will be the only supported configuration from this release forward. If you currently use HTTP, you must move to HTTPS as soon as possible.

**Note:** The Deep Security Agent for AIX and Solaris have not been tested for use with this feature release. The AIX and Solaris platforms continue to be fully supported using Deep Security Manager 11.0 and will continue to be supported in the next major release (Deep Security 12.0). If you have AIX and/or Solaris platforms in your deployment, please continue to use Deep Security Manager 11.0.

# Before you install

## Feature releases

Major releases of Deep Security Manager, such as Deep Security Manager 10.0, are made available on an annual basis, and include new functionality and enhancements for existing functionality. Feature releases are interim versions of Deep Security that provide early access to new functionality and are made available at regular intervals between major releases. This means that with feature releases you can immediately benefit from new functionality without having to wait for the next major release of Deep Security. Feature releases meet the same quality and release criteria as major releases, and are intended for use in production environments.

Feature releases are comprised of new versions of Deep Security Manager and Agent. The new manager is compatible with both the new and older versions of agent. However, new features in a feature release can require that both the new manager and the new agent are used. For information about which new features require an agent update, see "What's New".

While several feature releases may become available between major releases, the functionality of all feature releases is cumulative and is ultimately rolled into the next major release, which continue to be made available on an annual basis. For example, if you are now using the latest major release of Deep Security, you can obtain the Deep Security feature release to immediately take advantage of new functionality that it provides.

**Note:** If you are constrained to longer adoption cycles, wait for the next major release to benefit from the new functionality.

For more information about major releases and support services, see "Deep Security release life cycle and support policy" on page 1086.

## Version numbers

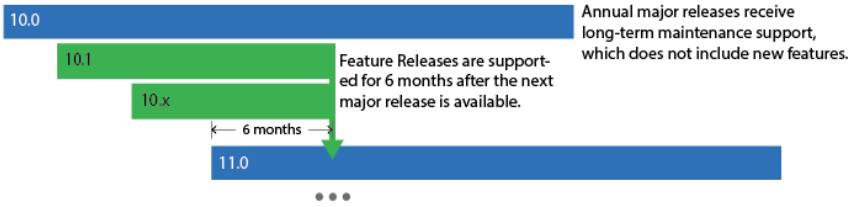
You can easily distinguish major releases and feature releases by the version number:

- Major releases use the x.0.z version pattern, for example the 10.0 GM version number is 10.0.3259, where 10 is the major version, 0 is the minor version, and 3259 is the build number:
  - Maintenance update versions are distinguished on the Deep Security Software page with a "U" suffix, for example 10.0_U1.
  - Maintenance updates have the build number incremented, for example the first maintenance update of 10.0 is 10.0.3271.
- Feature releases increment the minor version number, for example 10.1.z, or 10.2.z, where z is the build number.

You can obtain feature releases from the feature releases tab on the Deep Security Software page.

## Feature release life cycle

Deep Security feature releases have a shorter life cycle than major releases, and you should upgrade to the next major release when it becomes available. If you do not upgrade, you risk running an unsupported version of Deep Security. To ease the challenges of scheduling the upgrade in your production environment, support for feature releases is provided until 6 months after the next major release is available. The following diagram illustrates the timing of feature release availability and the support duration with respect to that of the major releases.




## Platform support

Feature releases support the same platforms that the next major release supports. Do not equate the platform support of the current major release with that of feature releases. To see a list of

older operating system versions and Deep Security Agents that are supported, see "Supported features by platform" on page 77.

## Support services

Most support items are provided for feature releases.

| Support item | Major release | Feature release | Delivery mechanism |
|---|---|---|---|
| Small enhancements (no change to core functionality) | ✔ | | Update |
| Linux kernel updates | ✔ | ✔ | Linux Kernel Package (LKP) |
| General bug fixes | ✔ | | Update |
| Critical bug fixes (system crash or hang, or loss of major functionality) | ✔ | ✔ | Update or Hot-fix |
| Critical and high vulnerability fixes | ✔ | ✔ | Update or Hot-fix |
| Medium and low vulnerability fixes | ✔ | | Update |
| Anti-Malware pattern updates | ✔ | ✔ | iAU (Active Update) |
| Intrusion prevention system, integrity monitoring, and log inspection rules updates | ✔ | ✔ | iAU |
| Support for Agents and Deep Security Manager on new versions of supported operating systems | ✔ | | Update |

Although updates that include small enhancements, general bug fixes, and support for new versions of operating systems are not provided for feature releases, these improvements are included in new feature release versions. For example, if you use 10.1, to benefit from any of these support items you need to obtain 10.2 when it is released. You should use the currently available feature release to benefit from these continual improvements.

## About the Deep Security components

Trend Micro Deep Security provides advanced server security for physical, virtual, and cloud servers. It protects enterprise applications and data from breaches and business disruptions without requiring emergency patching. This comprehensive, centrally managed platform helps you simplify security operations while enabling regulatory compliance and accelerating the ROI of virtualization and cloud projects.

For information on the protection modules that are available for Deep Security, see "Protect" on page 287.

Deep Security consists of the following set of components that work together to provide protection:

- **Deep Security Manager**, the centralized web-based management console that administrators use to configure security policy and deploy protection to the enforcement components: the Deep Security Virtual Appliance and the Deep Security Agent.
- **Deep Security Virtual Appliance** is a security virtual machine built for VMware vSphere environments that agentlessly provides anti-malware and integrity monitoring protection modules for virtual machines in a vShield environment. In an NSX environment, the anti-malware, integrity monitoring, firewall, intrusion prevention, and web reputation modules are available agentlessly.
- **Deep Security Agent** is a security agent deployed directly on a computer which provides application control, anti-malware, web reputation service, firewall, intrusion prevention, integrity monitoring, and log inspection protection to computers on which it is installed.
- The Deep Security Agent contains a **Relay** module. A relay-enabled agent distributes software and security updates throughout your network of Deep Security components.
- **Deep Security Notifier** is a Windows System Tray application that communicates information on the local computer about security status and events, and, in the case of relay-enabled agents, also provides information about the security updates being distributed from the local machine.

## System requirements

Each part of a Deep Security deployment has its own system requirements.

- "Deep Security Manager" below
- "Deep Security Agent" on page 72
- "Deep Security Notifier" on page 72

Requirements vary by version. For older versions of Deep Security Manager, agents, or relays, see their documentation:

- Deep Security 9.6 SP1 or earlier
- Deep Security 10.0
- Deep Security 10.1
- Deep Security 10.2
- Deep Security 10.3
- Deep Security 11.0

**Note:** If you plan to operate Deep Security in FIPS mode, see "FIPS 140-2 support" on page 1049 for additional requirements.

## Deep Security Manager

For a list of agents versions that are compatible with this version of Deep Security Manager, see "Deep Security Manager - Agent compatibility by platform" on page 73.

| System component | Requirements |
|---|---|
| Minimum memory (RAM) | Minimum RAM requirements depend on the number of agents that are being managed. See "Deep Security Manager sizing" on page 92.<br><br>**Note:**<br>On Linux, reserved system memory is separate from process memory. Therefore, although the installer's estimate might be similar, it will detect less RAM than the computer actually has. To verify the computer's actual total RAM, log in with a superuser account and enter:<br>`grep MemTotal /proc/meminfo` |

| System component | Requirements |
|---|---|
| Minimum disk space | 1.5 GB (200 GB recommended) |
| Database | • Microsoft SQL Server 2016<br>• Microsoft SQL Server 2014<br>• Microsoft SQL Server 2012<br>• Microsoft SQL Server 2008<br>• Microsoft SQL Server 2008 R2<br>• Oracle Database 12c<br>• Oracle Database 11g<br>• PostgreSQL 9.6.x (only Core or Amazon RDS distributions)<br>• Microsoft SQL RDS or Oracle RDS<br>• Azure SQL Database (SaaS) (multi-tenancy is not supported)<br><br>Disk space required varies by the size of the deployment, data retention, and frequency of logging. See "Sizing" on page 92.<br><br>Minimum free disk space = (2 x database size) + transaction log<br><br>For example, if your database plus transaction log is 40 GB, you must have 80 GB (40 x 2) of free disk space for database schema upgrades. To free disk space, delete any unnecessary event log data and transaction logs.<br><br>**Note:**<br>• Co-locate the database and all Deep Security Manager nodes in the same physical data center, with a 1 Gb link or better to ensure 2 ms latency or less between them.<br>• Microsoft SQL Server Express is supported in very limited deployments. See "Microsoft SQL Server Express considerations" on page 126 for important details.<br>• Trend Micro tests Deep Security with each Microsoft SQL Server service |

| System component | Requirements |
| --- | --- |
| | pack when it is released. Although not explicitly stated, the service packs for the Microsoft SQL versions listed above are also supported.<br>• Oracle Database Express (XE) is **not** supported.<br>• Oracle container database (CDB) configuration is **not** supported with Deep Security Manager multi-tenancy.<br>• Apache Derby, which provided an embedded database for proof-of-concept and testing in previous versions of Deep Security, is **not** supported anymore. |

## Deep Security Agent

Requirements vary by OS version and the features that you enable. See "Deep Security Agent and Relay sizing" on page 96.

For a list of all operating systems and agent versions that are compatible with Deep Security Manager 11.1, see "Deep Security Manager - Agent compatibility by platform" on the next page.

**Note:** Supported Deep Security features vary by platform.

**Note:** On supported versions of Microsoft Windows, you must have at least Powershell version 4.0 to run the agent deployment script.

## Deep Security Notifier

If installed, Deep Security Notifier appears in the Windows system tray. If anti-malware is licensed and enabled, it indicates the statuses of Deep Security Agent. Supported platforms include:

- Windows Server 2016 (64-bit)
- Windows Server 2012 or 2012 R2 (64-bit)
- Windows Server 2008 R2 (64-bit)

- Windows Server 2008 (32-bit and 64-bit)
- Windows 10 (32-bit and 64-bit)
- Windows 8.1 (32-bit and 64-bit)
- Windows 8 (32-bit and 64-bit)
- Windows 7 (32-bit and 64-bit)
- Windows XP (32-bit and 64-bit)

## Deep Security Manager - Agent compatibility by platform

Deep Security Manager 11.1 supports the Deep Security Agents in the table below.

**Note:** The Deep Security Agent for AIX and Solaris have not been tested for use with Deep Security Manager 11.1, which is a feature release. The AIX and Solaris platforms continue to be fully supported using Deep Security Manager 11.0 and will continue to be supported in the next major release (Deep Security 12.0). If you have AIX and/or Solaris platforms in your deployment, please continue to use Deep Security Manager 11.0. For more information on support for Solaris, see https://success.trendmicro.com/solution/1120706.

**Note:** The Deep Security Agent can be installed and is fully supported on any of the below platforms running in Amazon AWS or Microsoft Azure.

**Note:** Not all Deep Security features are available on all platforms. See "Supported features by platform" on page 77.

| Deep Security Agent Platform | Deep Security Agent Version | | | | |
|---|---|---|---|---|---|
| | 11.1 | 11.0 | 10.1, 10.2, or 10.3 Feature release (1) | 10.0 | 9.6 |
| Windows 2000 | | | | | ✔ (2) |
| Windows XP (32 and 64-bit) | | | | ✔ | ✔ |
| Windows Server 2003 SP1 (32 and 64-bit) | | | | ✔ | |
| Windows Server 2003 SP2 (32 and 64-bit) | | | | ✔ | |
| Windows Server 2003 R2 SP2 (32 and 64-bit) | | | | ✔ | ✔ |
| Windows 7 (32 and 64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |

| Deep Security Agent Platform | Deep Security Agent Version | | | | |
|---|---|---|---|---|---|
| | 11.1 | 11.0 | 10.1, 10.2, or 10.3 Feature release (1) | 10.0 | 9.6 |
| Windows Server 2008 (Full) (32 and 64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |
| Windows Server 2008 R2 (Full) (64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |
| Windows 8 (32 and 64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |
| Windows 8.1 (32 and 64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |
| Windows 10 (32 and 64-bit) (3) | ✔ | ✔ | ✔ | ✔ | ✔ |
| Windows Server (Full) 2012 (64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |
| Windows Server (Full or Core) 2012 R2 (64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |
| Windows Server 2016 (64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |
| Windows Server 2016 RS3 (64-bit) | ✔ | ✔ | | | |
| Red Hat Enterprise Linux 5 (32 and 64-bit) | | | | ✔ | ✔ |
| Red Hat Enterprise Linux 6 (32 and 64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |
| Red Hat Enterprise Linux 7 (64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |
| Ubuntu 10.04 LTS (64-bit) | | | | | ✔ |
| Ubuntu 12.04 LTS (64-bit) | | | | | ✔ |
| Ubuntu 14.04 LTS (64-bit) | | | | ✔ | ✔ |
| Ubuntu 16.04 LTS (64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |
| CentOS 5 (32 and 64-bit) | | | | ✔ | ✔ |
| CentOS 6 (32 and 64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |
| CentOS 7 (64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |
| Debian 6 (64-bit) | | | | | ✔ |
| Debian 7 (64-bit) | ✔ | ✔ | | ✔ | ✔ |
| Debian 8 (64-bit) | ✔ | ✔ | ✔ | ✔ (4) | |
| Debian 9 (64-bit) | ✔ | | | | |
| Amazon Linux (64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |
| Amazon Linux 2 (64-bit) | ✔ | ✔ | | ✔ (5) | |
| Oracle Linux 5 (32 and 64-bit) | | | | | ✔ |
| Oracle Linux 6 (32 and 64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |
| Oracle Linux 7 (64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |
| SUSE Linux Enterprise Server 10 SP3 & SP4 (32 and 64-bit) | | | | | ✔ |
| SUSE Linux Enterprise Server 11 SP1, SP2, SP3, SP4 (32 and 64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |
| SUSE Linux Enterprise Server 12 (64-bit) | ✔ | ✔ | ✔ | ✔ | ✔ |
| Cloud Linux 5 (32 and 64-bit) | | | | | ✔ |
| Cloud Linux 6 (32 and 64-bit) | | | | ✔ | ✔ |
| Cloud Linux 7 (64-bit) | | | ✔ | ✔ | ✔ |

(1) Support for the 10.1, 10.2, and 10.3 feature releases ends six months after the release of Deep Security 11.0. For details, see "Feature releases" on page 66.

(2) Requires Deep Security Agent 9.6 SP1 Patch 1 Update 17

(3) Microsoft releases regular, semi-annual releases for Microsoft Windows 10. For details about which specific releases are supported, see Deep Security Support for Windows 10.

(4) Requires Deep Security Agent 10.0 Update 1

(5) Requires Deep Security Agent 10.0 Update 8

## Docker support

You can use Deep Security 10.0 or later to protect Docker hosts and containers running on Linux distributions. Windows is not supported.

With each Deep Security release, Deep Security supports the last two stable releases of Docker Community Edition (CE) and Docker Enterprise Edition (EE). (See Announcing Docker Enterprise Edition.) We do not officially support Docker Edge releases, but strive to test against Docker Edge releases to the best of our ability.

Support for new stable Docker releases is introduced with each release of Deep Security. We recommend that you refrain from upgrading to the latest stable release of Docker until Trend Micro documents the support statements for the latest Deep Security release.

| Deep Security release | Supported Docker Releases |
|---|---|
| Deep Security 10.0 | Docker v1.12.x, v1.13.x |
| Deep Security 10.1 | Docker 17.03-ce, v1.13.x |
| Deep Security 10.2 | Docker 17.03, 17.06 |
| Deep Security 10.3 | Docker 17.03, 17.06 |
| Deep Security 11.0 | Docker 17.03-ee, 17.06-ee, 17.09-ce, 17.12-ce |
| Deep Security 11.1 | Docker 17.12-ce, 18.03-ce, 17.06-ee |

Before deploying Deep Security into your target environment, you should ensure that Docker supports your target environment and platform configuration.

## Deep Security Agent Linux kernel support

- Deep Security Agent 11.1 Linux kernel support
- Deep Security Agent 11.0 Linux kernel support
- Deep Security Agent 10.3 Linux kernel support
- Deep Security Agent 10.2 Linux kernel support
- Deep Security Agent 10.1 Linux kernel support
- Deep Security Agent 10.0 Linux kernel support
- Deep Security Agent 9.6 SP1 Linux kernel support
- Deep Security Agent 9.5 SP1 Linux kernel support

You can also use a JSON version of the complete list of the supported Linux kernels for Deep Security Agent 10.0 and higher with scripts and automated workflows.

# Supported features by platform

The tables below list the features available for each OS platform of **Deep Security Agent 11.1**:


- "Microsoft Windows (11.1 agent)" on the next page
- "Red Hat Enterprise Linux (11.1 agent)" on page 81
- "CentOS Linux (11.1 agent)" on page 82
- "Oracle Linux (11.1 agent)" on page 83
- "SUSE Linux (11.1 agent)" on page 84
- "Ubuntu Linux (11.1 agent)" on page 85
- "Debian Linux (11.1 agent)" on page 85
- "Cloud Linux (11.1 agent)" on page 86
- "Amazon Linux (11.1 agents)" on page 87


**Note:**
*Older* agents are compatible with other platforms (although they don't support new features on Deep Security Manager 11.1). See their "Deep Security Manager - Agent compatibility by platform" on page 73, Deep Security Agent release notes, and supported features lists:

- Deep Security Agent 10.0 (and newer) supported features: In the drop-down menu above, select that version of Deep Security.Deep Security Agent 10.0 (and newer) supported features
- Deep Security Agent 9.6 Service Pack 1 supported features

# Microsoft Windows (11.1 agent)

| | Anti-Malware | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | Integrity Monitoring | | | | | Log Inspection | Application Control | Recomm-endation Scan | Relay | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | On-demand | | | | | | Real-time | | On-demand | | | | | | | |
| | Feature set 1 | Feature set 2 | Feature set 1 | Feature set 2 | | | Unencrypted Traffic | SSL Encrypted Traffic | File and Directory Scans | Scans of Running Services, Processes, Listening Ports | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | |
| Windows 7 32 | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | ✔ | | |
| Windows 7 64 | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ |
| Windows Server 2008 32 | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | ✔ | | |
| Windows Server 2008 64 | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ |
| Windows Server 2008 R2 64 | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Windows 8 32 | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | ✔ | | |
| Windows 8 64 | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ |

## Trend Micro Deep Security for AWS Marketplace 11.1

| | Anti-Malware | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | Integrity Monitoring | | | | | Log Inspection | Application Control | Recomm-endation Scan | Relay | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | On-demand | | | | | | Real-time | | On-demand | | | | | | | |
| | Feature set 1 | Feature set 2 | Feature set 1 | Feature set 2 | | | Unencrypted Traffic | SSL Encrypted Traffic | File and Directory Scans | Scans of Running Services, Processes, Listening Ports | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | |
| Windows 8.1 32 | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | ✔ | | |
| Windows 8.1 64 | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ |
| Windows 10 32 ** | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | ✔ | | |
| Windows 10 64 ** | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ |
| Windows Server 2012 64 | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ |
| Windows Server 2012 R2 64 | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Windows Server Core 2012 64 | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |

## Trend Micro Deep Security for AWS Marketplace 11.1

| | Anti-Malware | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | Integrity Monitoring | | | | | Log Inspection | Application Control | Recomm-endation Scan | Relay | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | On-demand | | | | | | Real-time | | On-demand | | | | | | | |
| | Feature set 1 | Feature set 2 | Feature set 1 | Feature set 2 | | | Unencrypted Traffic | SSL Encrypted Traffic | File and Directory Scans | Scans of Running Services, Processes, Listening Ports | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | |
| Windows Server Core 2012 R2 64 | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Windows Server 2016 64 | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Windows Server 2016 RS3 64 | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |

# Red Hat Enterprise Linux (11.1 agent)

| | Anti-Malware | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | Integrity Monitoring | | | | | Log Inspection | Application Control | Recomm-endation Scan | Relay | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | On-demand | | | | | | Real-time | | On-demand | | | | | | | |
| | Feature set 1 | Feature set 2 | Feature set 1 | Feature set 2 | | | Unencrypted Traffic | SSL Encrypted Traffic | File and Directory Scans | Scans of Running Services, Processes, Listening Ports | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | |
| Red Hat Enterprise Linux 6 32 | ✔ | | ✔ | | | ✔ | ✔ | ✔ | | ✔ | ✔ | | ✔ | ✔ | | ✔ | | |
| Red Hat Enterprise Linux 6 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔* | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | |
| Red Hat Enterprise Linux 7 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔* | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |

# CentOS Linux (11.1 agent)

| | Anti-Malware | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | Integrity Monitoring | | | | | Log Inspection | Application Control | Recomm-endation Scan | Relay | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | On-demand | | | | | | Real-time | | On-demand | | | | | | | |
| | Feature set 1 | Feature set 2 | Feature set 1 | Feature set 2 | | | Unencrypted Traffic | SSL Encrypted Traffic | File and Directory Scans | Scans of Running Services, Processes, Listening Ports | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | |
| CentOS 6 32 | ✔ | | ✔ | | | ✔ | ✔ | ✔ | | ✔ | ✔ | | ✔ | ✔ | | ✔ | | |
| CentOS 6 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔* | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | |
| CentOS 7 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔* | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |

# Oracle Linux (11.1 agent)

| | Anti-Malware | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | Integrity Monitoring | | | | | Log Inspection | Application Control | Recomm-endation Scan | Relay | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | On-demand | | | | | | Real-time | | On-demand | | | | | | | |
| | Feature set 1 | Feature set 2 | Feature set 1 | Feature set 2 | | | Unencrypted Traffic | SSL Encrypted Traffic | File and Directory Scans | Scans of Running Services, Processes, Listening Ports | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | |
| Oracle Linux 6 32 | | | ✔ | | | ✔ | ✔ | ✔ | | ✔ | ✔ | | ✔ | ✔ | | ✔ | | |
| Oracle Linux 6 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔* | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | |
| Oracle Linux 7 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔* | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | |

## SUSE Linux (11.1 agent)

| | Anti-Malware | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | Integrity Monitoring | | | | | Log Inspection | Application Control | Recomm-endation Scan | Relay | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | On-demand | | | | | | Real-time | | On-demand | | | | | | | |
| | Feature set 1 | Feature set 2 | Feature set 1 | Feature set 2 | | | Unencrypted Traffic | SSL Encrypted Traffic | File and Directory Scans | Scans of Running Services, Processes, Listening Ports | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | |
| SUSE Linux Enterprise Server 11 32 | ✔ | | ✔ | | | ✔ | ✔ | ✔ | | ✔ | ✔ | | ✔ | ✔ | | ✔ | | |
| SUSE Linux Enterprise Server 11 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | ✔ | | ✔ | ✔ | | ✔ | ✔ | | ✔ | ✔ | |
| SUSE Linux Enterprise Server 12 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔* | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | |

## Ubuntu Linux (11.1 agent)

| | Anti-Malware | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | Integrity Monitoring | | | | | Log Inspection | Application Control | Recomm-endation Scan | Relay | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | On-demand | | | | | | Real-time | | On-demand | | | | | | | |
| | Feature set 1 | Feature set 2 | Feature set 1 | Feature set 2 | | | Unencrypted Traffic | SSL Encrypted Traffic | File and Directory Scans | Scans of Running Services, Processes, Listening Ports | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | |
| Ubuntu 16 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔* | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | |

## Debian Linux (11.1 agent)

| | Anti-Malware | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | Integrity Monitoring | | | | | Log Inspection | Application Control | Recomm-endation Scan | Relay | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | On-demand | | | | | | Real-time | | On-demand | | | | | | | |
| | Feature set 1 | Feature set 2 | Feature set 1 | Feature set 2 | | | Unencrypted Traffic | SSL Encrypted Traffic | File and Directory Scans | Scans of Running Services, Processes, Listening Ports | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | |
| Debian 7 64 | | | ✔ | | ✔ | ✔ | ✔ | ✔ | | ✔ | ✔ | | ✔ | ✔ | | ✔ | ✔ | |

### Trend Micro Deep Security for AWS Marketplace 11.1

| | Anti-Malware | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | Integrity Monitoring | | | | | Log Inspection | Application Control | Recomm-endation Scan | Relay | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | On-demand | | | | | | Real-time | | On-demand | | | | | | | |
| | Feature set 1 | Feature set 2 | Feature set 1 | Feature set 2 | | | Unencrypted Traffic | SSL Encrypted Traffic | File and Directory Scans | Scans of Running Services, Processes, Listening Ports | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | |
| Debian 8 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔* | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | |
| Debian 9 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔* | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | |

## Cloud Linux (11.1 agent)

| | Anti-Malware | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | Integrity Monitoring | | | | | Log Inspection | Application Control | Recomm-endation Scan | Relay | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | On-demand | | | | | | Real-time | | On-demand | | | | | | | |
| | Feature set 1 | Feature set 2 | Feature set 1 | Feature set 2 | | | Unencrypted Traffic | SSL Encrypted Traffic | File and Directory Scans | Scans of Running Services, Processes, Listening Ports | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | |
| Cloud Linux 7 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔* | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | |

# Amazon Linux (11.1 agents)

| | Anti-Malware | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | Integrity Monitoring | | | | | Log Inspection | Application Control | Recomm-endation Scan | Relay | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | On-demand | | | | | | Real-time | | On-demand | | | | | | | |
| | Feature set 1 | Feature set 2 | Feature set 1 | Feature set 2 | | | Unencrypted Traffic | SSL Encrypted Traffic | File and Directory Scans | Scans of Running Services, Processes, Listening Ports | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | |
| Amazon Linux 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔* | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | |
| Amazon Linux 2 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔* | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | |

## Deep Security Virtual Appliance (NSX) (with embedded 11.1 agent)

| | Anti-Malware | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | Integrity Monitoring | | | | | Log Inspection | Application Control | Recomm-endation Scan | Relay | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | On-demand | | | | | | Real-time | | On-demand | | | | | | | |
| | Feature set 1 | Feature set 2 | Feature set 1 | Feature set 2 | | | Unencrypted Traffic | SSL Encrypted Traffic | File and Directory Scans | Scans of Running Services, Processes, Listening Ports | File Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | |
| Windows 7 32 | ✔ | | ✔ | | ✔ | ✔ | ✔ | | | | ✔ | | | | | ✔ | | |
| Windows 7 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | | | | ✔ | | | | | ✔ | | |
| Windows Server 2008 32 | ✔ | | ✔ | | ✔ | ✔ | ✔ | | | | ✔ | | | | | ✔ | | |
| Windows Server 2008 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | | | | ✔ | | | | | ✔ | | |
| Windows Server 2008 R2 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | | | | ✔ | | | | | ✔ | | |
| Windows 8 32 | ✔ | | ✔ | | ✔ | ✔ | ✔ | | | | ✔ | | | | | ✔ | | |
| Windows 8 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | | | | ✔ | | | | | ✔ | | |

## Trend Micro Deep Security for AWS Marketplace 11.1

| | Anti-Malware | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | Integrity Monitoring | | | | | Log Inspection | Application Control | Recomm-endation Scan | Relay | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | On-demand | | | | | | Real-time | | On-demand | | | | | | | |
| | Feature set 1 | Feature set 2 | Feature set 1 | Feature set 2 | | | Unencrypted Traffic | SSL Encrypted Traffic | File and Directory Scans | Scans of Running Services, Processes, Listening Ports | File Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | |
| Windows 8.1 32 | ✔ | | ✔ | | ✔ | ✔ | ✔ | | | | ✔ | | | | | ✔ | | |
| Windows 8.1 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | | | | ✔ | | | | | ✔ | | |
| Windows Server 2012 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | | | | ✔ | | | | | ✔ | | |
| Windows Server 2012 R2 64 | ✔ | | ✔ | | ✔ | ✔ | ✔ | | | | ✔ | | | | | ✔ | | |
| Windows 10 32 ** | ✔ | | ✔ | | ✔ | ✔ | ✔ | | | | ✔ | | | | | ✔ | | |
| Windows 10 64 ** | ✔ | | ✔ | | ✔ | ✔ | ✔ | | | | ✔ | | | | | ✔ | | |
| Windows 2016 64 (with NSX 6.3.3) | ✔ | | ✔ | | ✔ | ✔ | ✔ | | | | ✔ | | | | | ✔ | | |
| Red Hat Enterprise Linux | | | | | ✔ | ✔ | ✔ | | | | | | | | | | | |

| | Anti-Malware | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | Integrity Monitoring | | | | | Log Inspection | Application Control | Recomm-endation Scan | Relay | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | On-demand | | | | | | Real-time | | On-demand | | | | | | | |
| | Feature set 1 | Feature set 2 | Feature set 1 | Feature set 2 | | | Unencrypted Traffic | SSL Encrypted Traffic | File and Directory Scans | Scans of Running Services, Processes, Listening Ports | File Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | |
| 6 32 | | | | | | | | | | | | | | | | | | |
| Red Hat Enterprise Linux 6 64 | | | | | ✔ | ✔ | ✔ | | | | | | | | | | | |
| Red Hat Enterprise Linux 7 64 | | | | | ✔ | ✔ | ✔ | | | | | | | | | | | |
| CentOS 6 32 | | | | | ✔ | ✔ | ✔ | | | | | | | | | | | |
| CentOS 6 64 | | | | | ✔ | ✔ | ✔ | | | | | | | | | | | |
| CentOS 7 64 | | | | | ✔ | ✔ | ✔ | | | | | | | | | | | |
| Oracle Linux 6 32 | | | | | ✔ | ✔ | ✔ | | | | | | | | | | | |
| Oracle Linux 6 64 | | | | | ✔ | ✔ | ✔ | | | | | | | | | | | |
| Oracle Linux 7 | | | | | ✔ | ✔ | ✔ | | | | | | | | | | | |

| | Anti-Malware | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | Integrity Monitoring | | | | | Log Inspection | Application Control | Recomm-endation Scan | Relay | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | On-demand | | | | | | Real-time | | On-demand | | | | | | | |
| | Feature set 1 | Feature set 2 | Feature set 1 | Feature set 2 | | | Unencrypted Traffic | SSL Encrypted Traffic | File and Directory Scans | Scans of Running Services, Processes, Listening Ports | File Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | |
| 64 | | | | | | | | | | | | | | | | | | |
| SUSE Linux Enterprise Server 11 32 | | | | | ✔ | ✔ | ✔ | | | | | | | | | | | |
| SUSE Linux Enterprise Server 11 64 | | | | | ✔ | ✔ | ✔ | | | | | | | | | | | |
| SUSE Linux Enterprise Server 12 64 | | | | | ✔ | ✔ | ✔ | | | | | | | | | | | |
| Ubuntu 16 LTS 64 | | | | | ✔ | ✔ | ✔ | | | | | | | | | | | |
| Debian 8 64 | | | | | ✔ | ✔ | ✔ | | | | | | | | | | | |
| Debian 9 64 | | | | | ✔ | ✔ | ✔ | | | | | | | | | | | |

**Feature set 1** includes signature-based file scanning, spyware scanning, and document exploit protection.

**Feature set 2** includes behavior monitoring, process memory scanning, and registry scanning.

***** This platform supports enhanced real-time integrity monitoring. It uses the application control driver to provide file monitoring and records information about *who* made changes to a monitored file.

**(**)** For details about which specific Windows 10 update releases are supported, see Deep Security Support for Windows 10.

# Sizing

Sizing guidelines for Deep Security deployments vary by the scale of your network, hardware, and software.

## Deep Security Manager sizing

The sizing recommendations for the Deep Security Manager computer depends on the number of agents that are being managed:

| Number of agents | Number of CPUs | RAM | JVM process memory | Number of manager nodes | Recommended disk space |
|---|---|---|---|---|---|
| <500 | 2 | 8 GB | 4 GB | 2 | 200 GB |
| 500-1000 | 4 | 8 GB | 4 GB | 2 | 200 GB |
| 1000-5000 | 4 | 12 GB | 8 GB | 2 | 200 GB |
| 5000-10000 | 8 | 16 GB | 12 GB | 2 | 200 GB |
| 10000-20000 | 8 | 24 GB | 16 GB | 2 | 200 GB |

- Two manager nodes are recommended to provide redundancy and ensure the availability of the manager services.
- To ensure adequate performance during concurrent operations, you should install Deep Security Manager and the database on separate, dedicated servers in the same physical location.
- Java Virtual machine (JVM) memory allocation is important for Deep Security Manager performance. To change the default allocated memory for the Deep Security Manager JVM process, see Configure Deep Security Manager memory usage.
- Recommendation scans are CPU-intensive for the Deep Security Manager. The performance impact to the Deep Security Manager should be taken into consideration when determining how often to run recommendation scans. For more information, see "Manage and run recommendation scans" on page 359.
- Resource spikes may occur if a large number of virtual machines are rebooted simultaneously and agents re-establish their connection with Deep Security Manager at the same time.

## Multiple server nodes

For better availability and scalability in larger deployments, use a load balancer, and install the same version of Deep Security Manager on multiple servers ("nodes"). Connect them to the same database storage.

**Tip:** To avoid high load on database servers, don't connect more than two Deep Security Manager nodes to each database server.

Each manager node is capable of all tasks. No node is more important than any of the others. You can log in to any node, and agents, appliances, and relays can connect with any node. If one node fails, other nodes can still provide service, and no data will be lost.

## Database sizing

Several variables affect database disk space requirements:

- Number of computers
- Number of events (logs) recorded per second
- How long events are retained

Event retention settings can be configured in the policy, the individual computer settings, or both. (See "Policies, inheritance, and overrides" on page 354.) To configure disk space usage, see "Limit log file sizes" on page 802, including which events are logged for stateful Firewall of TCP, UDP, and ICMP.See also "Deep Security Manager performance features" on page 136.

The database sizes in the following tables are suggestions for use with the default settings for log and event retention. (See "Log and event storage best practices" on page 799.) To estimate sizing for your database:

1. Identify the security features you are enabling and the number of agents that you are deploying.
2. Add the individual recommendations for each security feature to estimate the database size.
3. Compare this value with the Full Policy recommendation and provision the lesser of the two.

For example, you could deploy 750 agents with Deep Security Anti-Malware, Intrusion Prevention System and Integrity Monitoring. The total of the individual recommendations is 320 GB (20 + 100 + 200). However, the "Full Policy" recommendation is 300 GB. Therefore, you should provision 300 GB.

## Disk space estimates

| Number of agents | Anti-Malware | Web Reputation Service | Log Inspection | Firewall | Intrusion Prevention System | Application Control | Integrity Monitoring | Full Policy |
|---|---|---|---|---|---|---|---|---|
| 1-99 | 10 GB | 15 GB | 20 GB | 20 GB | 40 GB | 50 GB | 50 GB | 100 GB |
| 100-499 | 10 GB | 15 GB | 20 GB | 20 GB | 40 GB | 100 GB | 100 GB | 200 GB |
| 500-999 | 20 GB | 30 GB | 50 GB | 50 GB | 100 GB | 200 GB | 200 GB | 300 GB |
| 1000-9999 | 50 GB | 60 GB | 100 GB | 100 GB | 200 GB | 500 GB | 400 GB | 600 GB |

| Number of agents | Anti-Malware | Web Reputation Service | Log Inspection | Firewall | Intrusion Prevention System | Application Control | Integrity Monitoring | Full Policy |
|---|---|---|---|---|---|---|---|---|
| 10,000-20,000 | 100 GB | 120 GB | 200 GB | 200 GB | 500 GB | 750 GB | 750 GB | 1 TB |

## Database sizing considerations

- By default, data pruning is not performed on system events, which have a large impact on the database size. Adjust pruning settings according to your compliance requirements. (See "Log and event storage best practices" on page 799.)
- If you require long retention requirements for system events, use SIEM or Syslog servers for event forwarding. You can also use SEIM or Syslog servers for Security Control event forwarding. (See "Forward Deep Security events to an external syslog or SIEM server " on page 814.)

  **Note:** When system events and Security Control events are forwarded to SIEM or Syslog servers, they are not deleted from the database. To delete these events use data pruning.

- To conserve disk space, delete all agent configuration packages for each platform that are not in use. For more information, see "Delete a software package from the Deep Security database" on page 179. If you need to keep the configuration packages, add disk space accordingly. To help with estimating disk space requirements, consider a newly-installed Deep Security Manager with co-located relay that is assigned a policy that protects a Manager computer. When 29 agents (maximum 5 versions per agent platform) are added, the database size grows approximately 5 GB.
- The Rebuild Baseline, Scan for Integrity Changes, and Scan for Inventory Changes operations retain all records in the database and are never pruned or forwarded to external Syslog or SIEM systems. The Application Control and Integrity Monitoring security modules use these operations and therefore require more storage space than other security modules. Other types of operations, such as system or security events, are pruned or forwarded to external Syslog or SIEM systems.
- High-traffic environments that use the Firewall and Intrusion Prevention system modules can cause a large number of related events. Factors that influence the number of events are the number of applied Intrusion Prevention system rules and Firewall rule configuration. Because these events can require significant database storage, you should monitor these security events and use suitable data pruning.

- Intrusion Prevention rules are applied based on vulnerabilities assessed during a recommendation scan. You can reduce the number of rules assigned by regularly patching your system and keeping applications up to date.
- If you anticipate a significant number of Firewall events, consider disabling "Out of allowed policy" events. (See the "Advanced" on page 618 section in "Firewall settings" on page 612.)

## Deep Security Agent and Relay sizing

| Platform | Features enabled | RAM | Minimum disk space |
|---|---|---|---|
| Windows | All protection | 2 GB (4 GB recommended) | 1 GB |
| Windows | Relay only | 2 GB (4 GB recommended) | 30 GB |
| Linux | All protection | 1 GB (5 GB recommended) | 1 GB |
| Linux | Relay only | 1 GB (4 GB recommended) | 30 GB |

- Requirements vary by OS version, so some may require less RAM. Less RAM is also required if you are not enabling all of the Deep Security features.
- The Deep Security Relay must store packages for each of your agents' platforms. For more information, see "Get Deep Security Agent software" on page 177. If you have many different platforms, more disk space is required. For information on the number of relays you should use, see "Distribute security and software updates with relays" on page 234.

## Port numbers

If connecting Deep Security Manager, Relay, or Agents through a:

- firewall or AWS/Azure/NSX Security Group
- router
- proxy
- other network address translation (NAT) device

you'll need to know the required domain names or IP addresses, ports, and protocols.


- "Deep Security Manager ports" on the next page
  - "Incoming (listening ports)" on the next page
  - "Outgoing" on page 99
- "Deep Security Relay ports" on page 105
  - "Incoming (listening)" on page 105
  - "Outgoing" on page 106
- "Deep Security Agent ports" on page 106
  - "Incoming (listening ports)" on page 106
  - "Outgoing" on page 107


Firewall policies, proxies, and port forwarding often require this information. This is especially true for connections to services on the Internet, such as DNS, time servers, the Trend Micro Active Update servers, Trend Micro Smart Protection Network, and Deep Security as a Service. If a computer has other installed software that listens on the same ports, you must resolve the port conflict.

Default port numbers are in these tables. If the default port numbers don't work with your network or installation, you have a proxy, or if you require SSL or TLS secured versions of the traffic, the tables indicate if you can configure it.

## Deep Security Manager ports

### Incoming (listening ports)

| Transport Protocol | Destination Port Number | Service | Source | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| TCP | 443 | HTTPS | Trend Micro Control Manager, SOAP API client, or other REST API client | • WSDL access at: https://<manager FQDN or IP>:443/webservice/Manager?WSDL<br>• Status monitoring at: https://<manager FQDN or IP>:443/rest/status/manager/ping<br>• Control Manager uploads sandboxing results from Deep Discovery Analyzer with connected threat defense. | No | No |
| TCP | 443 | HTTPS | Web browser | Administrative connections to the Deep Security GUI or API. | No | No |
| TCP | 443 | HTTPS | Agent/Appliance | Deep Security Agent/Appliance installer downloads. | No | No |
| TCP | 4120 | HTTPS | Agent/Appliance | • Discovery and Agent/Appliance activation.<br>• Agent/Appliance to Manager heartbeat. Receives events and provides configuration updates to them. See also "Agent-manager communication" on page 196. | Yes | Yes |
| TCP | 8080 | HTTP | Web installer | Software installation via the web installer. Once Deep Security Manager installation is complete, or if you use the Quick Start instead, you can | No | No |

| Transport Protocol | Destination Port Number | Service | Source | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| | | | | block this port. | | |

## Outgoing

| Transport Protocol | Destination Port Number | Service | Destination | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| TCP | 25 | SMTP | E-mail server | Alerts for events.<br><br>**Tip:** AWS throttles (rate limits) e-mail on SMTP's IANA standard port number, port 25. If you use AWS Marketplace, you may have faster alerts if you use SMTP over STARTTLS (secure SMTP) instead. For more information, see: https://docs.aws.amazon.com/ses/latest/DeveloperGuide/smtp-connect.html https://docs.aws.amazon.com/ses/latest/DeveloperGuide/smtp-issues.html | Yes | No |
| UDP | 53 | DNS | DNS server | Domain name resolution of Trend Micro services, e-mail server, NTP server, and others. | Yes<br><br>(configure in the | Yes<br><br>(configure in the |

| Transport Protocol | Destination Port Number | Service | Destination | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| | | | | | operating system) | operating system) |
| TCP | 80 | HTTP | Trend Micro Smart Feedback<br>• deepsecurity1100-en.fbs25.trendmicro.com<br>• deepsecurity1100-jp.fbs25.trendmicro.com | Smart Protection feedback. | No | No |
| TCP | 80 | HTTP | Whois server<br>(could be http://reports.internic.net/cgi/whois?whois_nic=[IP]&type=nameserver) | Reverse name resolution of IP addresses into hostnames for event logs and computer discovery. | Yes | No |
| TCP | 443 | HTTPS | Trend Micro licensing and registration server<br>licenseupdate.trendmicro.com | Licensing and product registration. | No | Yes |
| TCP | 80 or 443 | HTTP or HTTPS | Trend Micro Active Update<br>• https://iaus.activeupdate.trendmicro.com/ | Security package updates.<br>Alternatively, use a relay. | Yes | Yes<br>SOCKS support |

| Transport Protocol | Destination Port Number | Service | Destination | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| | | | • https://ipv6-iaus.trendmicro.com | | | |
| TCP | 80 or 443 | HTTP or HTTPS | Trend Micro Download Center or web server<br>files.trendmicro.com | Deep Security Agent/Appliance installer downloads. | Yes<br>(append port number to URL) | No |
| TCP | 80 or 443 | HTTP or HTTPS | Trend Micro Certified Safe Software Service (CSSS)<br>• https://grid-global.trendmicro.com:443 | Automatic event tagging for integrity monitoring. | No | Yes |
| UDP | 123 | NTP | NTP server<br>(can be Trend Micro Control Manager server) | Accurate time for SSL or TLS connections, schedules, and event logs. | Yes<br>(configure in the operating system) | No |

| Transport Protocol | Destination Port Number | Service | Destination | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| UDP | 162 | SNMP | SNMP manager | Traps for events. | Yes | No |
| TCP | 389 | LDAP | Microsoft Active Directory server | • Discovery of and (optionally) synchronization of computer groups in the directory. | Yes | No |
| TCP | 389 | HTTPS | AWS Marketplace, Microsoft Azure Marketplace, and other clouds | Communication with cloud accounts to retrieve a list of computers. | No | Yes |
| TCP | 443 | HTTPS | news.deepsecurity.trendmicro.com | Deep Security news feed | No | Yes |
| TCP | 443 | HTTPS | NSX Manager | Communication to VMware NSX Manager. | Yes | No |
| TCP | 443 | HTTPS | vCenter server | Communication to VMware vCenter server. | Yes | No |
| TCP | 443 | HTTPS | ESXi server | Communication to VMware ESXi server. | No | |
| UDP | 514 | Syslog | SIEM or log server | External logging and reporting. | Yes | No |
| TCP | 636 | LDAPS | Microsoft Active Directory server | • Discovery and (optionally) synchronization of computer groups in the directory.<br>• Import and (optionally) synchronization of user groups, including contacts and passwords. | Yes | No |

| Transport Protocol | Destination Port Number | Service | Destination | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| TCP | 1433 | SQL | Microsoft SQL database | Deep Security Manager application to its storage.<br>Although it is not visible from the GUI, you can configure an encrypted database connection. | Yes | No |
| TCP | 1521 | SQL | Oracle database | Deep Security Manager application to its storage.<br>Although it is not visible from the GUI, you can configure an encrypted database connection. | Yes | No |
| TCP | 5432 | SQL | PostgreSQL database | Deep Security Manager application to its storage.<br>Although it is not visible from the GUI, you can configure an encrypted database connection. | Yes | No |
| TCP | 11000-11999, 14000-14999 | SQL | Azure SQL Database | If your Deep Security Manager runs inside the Azure cloud boundary, it uses a direct route to interact with the Azure SQL Database server. For more information, see https://docs.microsoft.com/en-us/azure/sql-database/sql-database-develop-direct-route-ports-adonet-v12.<br>This is only required when using Azure SQL Database with Deep Security Manager deployed on Azure, for | No | No |

| Transport Protocol | Destination Port Number | Service | Destination | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| | | | | example, the Deep Security Manager VM for Azure Marketplace. | | |
| TCP | 4118 | HTTPS | Agent/Appliance | Manager to Agent/Appliance heartbeat. Send events and get configuration updates from the Manager. See also "Agent-manager communication" on page 196.<br>Depending on your deployment type, you may be able to close port 4118, and only use agent-initiated heartbeats. | Yes | No |
| TCP | 4122 | HTTPS | Relay | Security package updates such as anti-malware engine and signatures via a Deep Security Relay. Alternatively, the Deep Security Manager can connect directly to the Trend Micro Active Update servers.<br>See also "Agent-manager communication" on page 196. | Yes | Yes |
| TCP<br>UDP | All | All | Agent/Appliance | Port scan to detect open (listening) ports on computers. | Yes | No |

## Deep Security Relay ports

Relays require all of the ports for an agent *and* these port numbers. (See "Deep Security Agent ports" on the next page.)

### Incoming (listening)

| Transport Protocol | Destination Port Number | Service | Source | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| TCP | 4122 | HTTPS | Manager, Agent, Appliance, or Relay | • Relay-to-Relay communication and Agent-to-Relay communication for synchronizing Deep Security Agent software installers and security package updates such as anti-malware engine and signatures.<br>• Manager, agent, or appliance downloading security package updates such as anti-malware engine and signatures from Relay.<br><br>See also "Agent-manager communication" on page 196. | Yes | Yes*<br>See Note. |
| TCP | 4123 | | Localhost Relay | Communication of Agent to its own integrated Relay.<br><br>This port should not be listening to connections from other computers, and you don't need to configure it in network firewall policies. But if you have a host firewall on the Deep Security Manager server itself, verify that it does not block this connection to itself. Also verify that other applications do not use the same port (a port conflict). | No | No |

### Outgoing

| Transport Protocol | Destination Port Number | Service | Destination | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| TCP | 80 or 443 | HTTP or HTTPS | Trend Micro Active Update<br>• https://iaus.activeupdate.trendmicro.com/<br>• https://ipv6-iaus.trendmicro.com | Security package updates such as anti-malware engine and signatures.<br>Alternatively, use another relay. | Yes | Yes<br>SOCKS support |
| TCP | 4122 | HTTPS | Relay | Relay-to-Relay communication for synchronizing Deep Security Agent software installers and security components such as anti-malware engine and signatures.<br>See also "Agent-manager communication" on page 196. | Yes | Yes*<br>See Note. |

## Deep Security Agent ports

### Incoming (listening ports)

| Transport Protocol | Destination Port Number | Service | Source | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| TCP | 22 | SSH | Manager, deployment tools such as RightScale, Chef, Puppet, | Remote installation of the agent (Linux only). | No | No |

| Transport Protocol | Destination Port Number | Service | Source | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| | | | Ansible and SSH | | | |
| TCP | 4118 | HTTPS | Manager | Manager to agent or appliance heartbeat. Send events and get configuration updates from the Manager. See also "Agent-manager communication" on page 196. | Yes | No |
| TCP | 3389 | RDP | Manager | Remote installation of the agent (Windows only). | No | No |
| TCP | 5985 | WinRM HTTP | deployment tools such as RightScale, Chef, Puppet, and Ansible | Remote installation of the agent (Windows only). | Yes (configure in the operating system) | Yes (configure in the operating system) |

## Outgoing

| Transport Protocol | Destination Port Number | Service | Destination | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| UDP | 53 | DNS | DNS server | Domain name resolution of the Deep Security Manager, Trend Micro Smart Protection Servers, and others. | Yes (configure in the | Yes (configure in the |

| Transport Protocol | Destination Port Number | Service | Destination | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| | | | | | operating system) | operating system) |
| TCP | 80 | HTTP | Good File Reputation Service<br>11.0 and 11.1<br>• deepsec11-en.gfrbridge.trendmicro.com<br>• deepsec11-jp.gfrbridge.trendmicro.com<br>10.2 and 10.3<br>• deepsec102-en.gfrbridge.trendmicro.com<br>• deepsec102-jp.gfrbridge.trendmicro.com<br>• deepsec102-cn.gfrbridge.trendmicro.com<br>10.1 and 10.0<br>• deepsec10-en.grid-gfr.trendmicro.com<br>• deepsec10-jp.grid-gfr.trendmicro.com<br>• deepsec10-cn.grid-gfr.trendmicro.com | Communicates with the Good File Reputation Service during file scans started by Behavior Monitoring. | No | Yes<br>SOCKS support |
| TCP | 80 | HTTP | File Census | Communicates with the Global Census Server during file scans started by Behavior Monitoring. | No | Yes |

| Transport Protocol | Destination Port Number | Service | Destination | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| | | | 11.0 and 11.1<br>• ds1100-en-census.trendmicro.com<br>• ds1100-jp-census.trendmicro.com<br>10.2 and 10.3<br>• ds1020-en-census.trendmicro.com<br>• ds1020-sc-census.trendmicro.com<br>• ds1020-jp-census.trendmicro.com<br>10.1 and 10.0<br>• ds1000-en.census.trendmicro.com<br>• ds1000-jp.census.trendmicro.com<br>• ds1000-sc.census.trendmicro.com<br>• ds1000-tc.census.trendmicro.com | | | SOCKS support |
| TCP | 80 or 443 | HTTP or HTTPS | Trend Micro Download Center or web server<br>files.trendmicro.com | Deep Security Agent/Appliance installer downloads. | Yes<br>(append port number to URL) | No |

| Transport Protocol | Destination Port Number | Service | Destination | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| TCP | 80 or 443 | HTTP or HTTPS | Trend Micro Active Update<br>• https://iaus.activeupdate.trendmicro.com/<br>• https://ipv6-iaus.trendmicro.com | Security package updates such as anti-malware engine and signatures.<br>Alternatively, use a relay. | Yes | Yes<br>SOCKS support |
| TCP | 80 or 443 | HTTP or HTTPS | Web server | Connectivity test to determine context (whether the computer is on the private network or not) for policies | Yes | No |
| TCP | 80 or 443 | HTTP or HTTPS | Predictive machine learning<br>11.0 and 11.1<br>• ds110-en-f.trx.trendmicro.com<br>• ds110-jp-f.trx.trendmicro.com<br>• ds110-sc-f.trx.trendmicro.com<br>10.2 and 10.3<br>• ds102-en-f.trx.trendmicro.com<br>• ds102-jp-f.trx.trendmicro.com<br>• ds102-sc-f.trx.trendmicro.com | Communicates with the Global Machine Learning Server during real-time file scans | No | Yes<br>SOCKS support |
| TCP | 80 or 443 | HTTP | Trend Micro Smart Protection Network | File reputation service and Smart Protection | Yes | Yes |

| Transport Protocol | Destination Port Number | Service | Destination | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| | | or HTTPS | 11.0 and 11.1<br>• ds110.icrc.trendmicro.com<br>• ds110-jp.icrc.trendmicro.com<br>10.2 and 10.3<br>• ds102.icrc.trendmicro.com<br>• ds102-jp.icrc.trendmicro.com<br>• ds102-sc.icrc.trendmicro.com.cn<br>10.1 and 10.0<br>• ds10.icrc.trendmicro.com<br>• ds10.icrc.trendmicro.com/tmcss/<br>• ds10-jp.icrc.trendmicro.com/tmcss/<br>• ds10-sc.icrc.trendmicro.com/tmcss/ | feedback.<br>Alternatively, you can connect to a Smart Protection Server on your local network, or a Smart Protection Server on AWS. | | |
| TCP | 80 or 443 | HTTP or HTTPS | Smart Protection Server | File reputation service.<br>You can connect to a Smart Protection Server on your local network, or a Smart Protection Server on AWS. | Yes | Yes |

| Transport Protocol | Destination Port Number | Service | Destination | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| UDP | 123 | NTP | NTP server<br>(can be Trend Micro Control Manager server) | Accurate time for SSL or TLS connections, schedules, and event logs. | Yes<br>(configure in the operating system) | No |
| TCP | 443 | HTTPS | Manager | • Discovery and Agent/Appliance activation.<br>• Agent or appliance to manager Manager heartbeat. Receives events and provides configuration updates to them. See also "Agent-manager communication" on page 196.<br>• Agent-to-relay communication for Deep Security Agent software installers and security package updates such as anti-malware engine and signatures. | Yes | Yes*<br>See Note. |

| Transport Protocol | Destination Port Number | Service | Destination | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| UDP | 514 | Syslog | SIEM or log server | External logging and reporting.<br><br>This is only used if you want the agents to send directly to an external SIEM, instead of uploading event logs to the Deep Security Manager. | Yes | No |
| TCP | 5274 | HTTPS | Trend Micro Smart Protection Network<br><br>11.0 and 11.1<br>• ds11-0-en.url.trendmicro.com<br>• ds11-0-jp.url.trendmicro.com<br><br>10.2 and 10.3<br>• ds10-2-en.url.trendmicro.com<br>• ds10-2-sc.url.trendmicro.com.cn<br>• ds10-2-jp.url.trendmicro.com<br><br>10.1 and 10.0<br>• ds100-en.url.trendmicro.com<br>• ds100-sc.url.trendmicro.com | Web reputation service.<br><br>Alternatively, you can connect to a Smart Protection Server on your local network, or a Smart Protection Server on AWS. | Yes | Yes |

| Transport Protocol | Destination Port Number | Service | Destination | Purpose | Configurable? | Proxy configurable? |
|---|---|---|---|---|---|---|
| | | | • ds100-jp.url.trendmicro.com | | | |
| TCP | 5274 | HTTPS | Smart Protection Server | Web reputation service.<br>You can connect to a Smart Protection Server on your local network, or a Smart Protection Server on AWS.. | Yes | No |

**Note:** In Deep Security Agent 10.0 GM and earlier, agents didn't have support for connections through a proxy to relays. You must either:

- update agents' software (see "Get Deep Security Agent software" on page 177), then configure the proxy (see "Connect agents behind a proxy" on page 203.)
- bypass the proxy
- change the application control rulesets relay setting as a workaround

## Prepare a database for Deep Security Manager on AWS

**Tip:** We recommend that you use the AWS Quick Start Deep Security on AWS to automatically deploy Deep Security on AWS. If you use that method, you can disregard the database preparation steps described here because the Quick Start takes care of database configuration for you. For information on the Quick Start, see "Deploy the Deep Security AMI from AWS Marketplace" on page 128.

If you are not using the Quick Start, you must install a database, create a database instance for Deep Security, and create a user account for Deep Security before you install Deep Security Manager. You can install your own database or you can use the Amazon RDS Management Console to create a database instance (Microsoft SQL RDS or Oracle RDS). Refer to the Amazon RDS Documentation for instructions, but keep the following considerations in mind for integration with Deep Security:

1. Check the "Hardware recommendations" on the next page.
2. Choose your database type. For a list of supported databases, see Database.
3. Depending on which database you choose, see "Microsoft SQL Server" on the next page, "Oracle Database" on page 117, or "PostgreSQL recommendations" on page 118 for database-specific considerations.

   **Note:** Microsoft SQL Server Express is supported only in certain limited deployments. For details, see "Microsoft SQL Server Express considerations" on page 126.

4. For high availability, the Deep Security database is compatible with database failover protection so long as no alterations are made to the database schema. For example, some database replication technologies add columns to the database tables during replication which can result in critical failures. For this reason, database mirroring is recommended over database replication.
5. The database time must be synchronized with the time on the Deep Security Manager computer. Ensure that the database and the manager use the same time zone and that they are synchronizing their time to the same time source.

   **Note:** By default, the AWS Marketplace AMI uses Coordinated Universal Time (UTC). We recommend that you also use UTC for your database. If you change this setting, be sure your manager and database match.

6. Allow communication from the Deep Security Manager computer to the database computer. See "Port numbers" on page 96.
7. During the Deep Security Manager installation, you will be asked for database connection details. Enter the database hostname under "Hostname" and the database that you created for Deep Security under "Database Name".

   The installation supports both SQL and Windows Authentication. When using Windows Authentication, the "Advanced" option is not available with the AWS Marketplace version of Deep Security Manager.

## Hardware recommendations

We recommend that you use an AWS RDS instance (Microsoft SQL RDS or Oracle RDS), but you can also use a stand-alone database server.

If you choose to use a stand-alone database server, keep these recommendations in mind:

- Many Deep Security Manager operations (such as updates and recommendation scans) require high CPU and memory resources. Trend Micro recommends that each manager node has four cores and sufficient RAM in high scale environments.
- The database should be installed on hardware that is equal to or better than the specifications of the best Deep Security Manager node. For the best performance, the database should have 8-16 GB of RAM and fast access to the local or network attached storage. Whenever possible, a database administrator should be consulted on the best configuration of the database server and a maintenance plan should be put in effect.

## Microsoft SQL Server

- You must create an empty database that will be used by Deep Security.
- The recommended transport protocol is **TCP**.
- Enable "Remote TCP Connections". (See https://msdn.microsoft.com/en-us/library/bb909712(v=vs.120).aspx)
- The AWS Marketplace version of Deep Security Manager does not support Named Pipes.
- The database account used by the Deep Security Manager must have **db_owner** rights.
- If using Multi-Tenancy, the database account used by the Deep Security Manager must have **dbcreator** rights. For information on multi-tenancy, see "Set up a multi-tenant environment" on page 140.
- It is important to have good database maintenance strategies in place. Refer to the Microsoft SQL Server documentation for guidelines, including Options in the Back Up Database Task for Maintenance Plan.

See also "Set up authentication for SQL Server" on page 123.

## Oracle Database

- Start the "Oracle Listener" service and make sure it accepts TCP connections.
- The database account used by the Deep Security Manager must be granted the **CONNECT** and **RESOURCE** roles and **UNLIMITED TABLESPACE**, **CREATE SEQUENCE**, **CREATE TABLE** and **CREATE TRIGGER** system privileges.
- If using multi-tenancy, the database account used by the Deep Security Manager must be granted the **CREATE USER**, **DROP USER**, **ALTER USER**, **GRANT ANY PRIVILEGE** and **GRANT ANY ROLE** system privileges.
- Avoid special characters for the database user name. Although Oracle allows special characters when configuring the database user object, if they are surrounded by quotes. Deep Security does not support special characters for the database user.

### Oracle RAC (Real Application Clusters) support

Deep Security supports:

- SUSE Linux Enterprise Server 11 SP3 with Oracle RAC 12c Release 1 (v12.1.0.2.0)
- Red Hat Linux Enterprise Server 6.6 with Oracle RAC 12c Release 1 (v12.1.0.2.0)

The default Linux Server Deep Security policy is compatible with the Oracle RAC environment, with the exception of Firewall settings. You can disable Firewall or customize the Firewall settings according to the instructions in "Firewall settings with Oracle RAC" on page 618.

## Connection settings used during Deep Security Manager installation

During the Deep Security Manager installation, you will be asked for Database connection details. Enter the Database hostname under "Hostname" and the pre-created database for Deep Security under "Database Name".

# PostgreSQL recommendations

Tuning recommendations that you should consider depend on your organization's needs (see "Tuning PostgreSQL settings" below).

## General requirements

- General database setup recommendations are located in "Prepare a database for Deep Security Manager on AWS" on page 114. For information on how to install and configure a PostgreSQL database specifically, refer to the PostgreSQL documentation.

  If you need additional help, PostgreSQL offers professional support.

- To prepare a PostgreSQL database for use with Deep Security Manager:

```
CREATE DATABASE "<database>";
```

```
CREATE ROLE "<username>" WITH PASSWORD '<password>';
```

```
GRANT ALL ON DATABASE "<database>" TO "<username>";
```

```
GRANT CONNECT ON DATABASE "<database>" TO "<username>";
```

- Based on your security requirements, consider using TLS to secure traffic between the Deep Security Manager and PostgreSQL. To turn on TLS after Deep Security Manager has been installed, see "Encrypt communication between the Deep Security Manager and the database" on page 763.

- If using multi-tenancy, users also need the right to create new databases and roles:

```
ALTER ROLE <username> CREATEDB CREATEROLE;
```

## Tuning PostgreSQL settings

To change the settings described in this section:

1. Open the `postgresql.conf` file. File locations depend on your PostgreSQL configuration.
2. Edit the parameters that you want to change.
3. Save and close the file.
4. Restart the PostgreSQL service.

## Logging settings

By default, PostgreSQL log files are not rotated, which can lead to the log files using a large amount of disk space. When using PostgreSQL with Deep Security, we recommend that you use these four parameters in the `postgresql.conf` file to configure log rotation:

- `log_filename`
- `log_rotation_age`
- `log_rotation_size`
- `log_truncate_on_rotation`

`log_rotation_age` and `log_rotation_size` control when a new log file is created. For example, setting `log_rotation_age` to 1440 will create a new log file every 1440 minutes (1 day), and setting `log_rotation_size` to 10000 will create a new log file when the previous one reaches 10 000 KB.

`log_filename` controls the name given to every log file. You can use time and date format conversion in the name. For a complete list, see http://pubs.opengroup.org/onlinepubs/009695399/functions/strftime.html.

When `log_truncate_on_rotation` is set to "on", it will overwrite any log file that has the same name as a newly created log file.

There are several combinations of parameters that you can use to achieve a log rotation to suit your requirements. Here is one example:

- `log_filename = 'postgresql-%a.log'` (every log file has the first 3 letters of the weekday in its name)
- `log_rotation_age = 1440` (a new log file is created daily)

- `log_rotation_size = 0`. (setting is disabled to prevent the overwriting of the daily log file every time this limit is exceeded)
- `log_truncate_on_rotation = on` (enable log file overwrite)

### Lock management

By default, the `deadlock_timeout` setting in the `postgresql.conf` file is configured to 1 second. This means every time a query waits on a lock for more than 1 second, PostgreSQL will launch a check for deadlock condition and will log an error if the logging setting has been configured that way (by default, it is). This can lead to performance degradation on bigger systems, where it can be normal for queries to wait for more than 1 second during load times. On large systems, consider increasing the `deadlock_timeout` setting. The PostgreSQL documentation contains this recommendation: "Ideally the setting should exceed your typical transaction time [...]".

### Maximum connections

The `max_connections` setting in the `postgresql.conf` file specifies the maximum number of open connections to the database. The default value is 100. We recommend increasing this value to 500.

### Shared buffers

The `shared_buffers` setting in the `postgresql.conf` file specifies how much memory PostgreSQL can use to cache data. A system with 1 GB of RAM must have one quarter of its memory value for shared buffer, which means the shared buffer should be set to 256 MB (the default is 32 MB).

### Work memory and maintenance work memory

The `work_mem` setting in the `postgresql.conf` file specifies the amount of memory that can be used by internal sort operations and hash tables before writing to temporary disk files. The default value is 1 MB, but it should be increased when running complex queries. The `maintenance_work_mem` setting determines the maximum amount of memory used for maintenance operations such as ALTER TABLE.

### Effective cache size

The `effective_cache_size` setting in the `postgresql.conf` file is used to estimate cache effects by a query. This setting only affects cost estimates during query planning and does not result in higher memory consumption. Consider increasing this setting.

### Checkpoints

Checkpoints are usually the main source of writes to data files. To get the smoothest performance, most checkpoints should be "timed" (triggered by checkpoint_timeout) and not "requested" (triggered by filling all the available WAL segments or by an explicit CHECKPOINT command). We strongly recommend that you make checkpoints less frequent.

| Setting | Default value | Recommended value |
|---|---|---|
| `checkpoint_timeout` | 5min | 15min |
| `checkpoint_completion_target` | 0.5 | 0.9 |
| `max_wal_size` | 1GB | 16GB |

### Write-ahead log (WAL)

The default value for the `wal_level` setting is 'minimal', which is appropriate when replication is not in place. Consider changing it if you plan to set up replicas.

### Autovacuum settings

PostgreSQL requires periodic maintenance called "vacuuming". Auto vacuuming is recommended in many cases, so there is no need to change the default setting: `autovacuum_max_workers = 3`.

### High availability

High availability (HA) is not set by default and was not enabled in our test environment, but it is highly recommended to ensure business continuity in the case of a database malfunction or server inaccessibility. Refer to your PostgreSQL documentation for information on how to enable and configure HA.

### Backup and recovery

Backup and recovery is not set by default, but it's absolutely essential in a production environment.

**Note:** Basic tools like pg_dump or pg_basebackup are not suitable for backups in an enterprise environment. Consider using other tools like Barman (https://www.pgbarman.org/index.html) for backup and recovery.

## Linux recommendations

### Transparent Huge Pages (Linux)

Transparent Huge Pages (THP) is a Linux memory management system that reduces the overhead of Translation Lookaside Buffer (TLB) lookups on machines with large amounts of memory by using larger memory pages. THP is enabled by default on Linux, but it is not recommended for computer running a database and should be disable if PostgreSQL is installed on a Linux computer. Refer to your OS vendor's documentation for details.

### Strengthen host-based authentication (Linux)

By default, Linux does not have restricted host-based authentication (HBA) for databases. Strengthening the HBA settings on a database appliance helps to prevent unauthorized access from external hosts. The HBA settings restrict access to an IP address range so that only hosts within that range have access. HBA settings were not used on our test environment and we do not recommend them.

# Set up authentication for SQL Server

When using Microsoft SQL Server as the Deep Security Manager database, you must use Kerberos as the authentication protocol. You must configure the following components to use Kerberos:

- "Active Directory" below
- "The Deep Security Manager computer" on the next page
- "Microsoft SQL Server" on page 125

You also need to make sure that system clocks are synchronized. See "Synchronize system clocks" on page 126.

## Active Directory

1. Ensure that Active Directory Domain Controller is installed.
2. Open Server Manager and ensure that the following services are running:
   - DNS Service
   - Kerberos Key Distribution Service
3. Ensure that the SQL Server computer has joined the domain.
4. Create an Active Directory user for Deep Security Manager to use to connect with SQL Server. Configure the account so that the password never expires.
5. To open ADSI Edit, type the following command in Command Prompt:
   `ADSIEdit.msc`
6. Right-click the SQL Server computer and select **Properties**.
7. Edit the **servicePrincipalNames** attribute and add the following strings, or ensure that existing strings use this format:
   - `MSSQLSvc/<SQL Server fully qualified name>`
   - `MSSQLSvc/<SQL Server fully qualified name>:<Port>`

## The Deep Security Manager computer

The configuration steps differ for Windows and Linux computers.

### Windows

1. To ensure that the DNS forward lookup and reverse lookup services resolve to the Active Directory and MS SQL computers, type the following commands in Command Prompt:
   - `nslookup <SQL Server IP address>`
   - `nslookup <Active Directory Controller IP address>`
   - `nslookup <SQL Server fully qualified domain name>`
   - `nslookup <Active Directory Controller fully qualified domain name>`
2. When you install Deep Security Manager, when you are specifying the database connection settings, specify the credentials of the user account that you created in Active Directory. In the Advanced options, specify the correct domain.

### Linux

1. Open the /etc/krb5.conf file in a text editor to configure Kerberos.
2. Add the following text to the `libdefaults` section:

```
default_realm = <DOMAIN>
[realms]
<DOMAIN> = {
kdc = <ACTIVE_DIRECTORY_CONTROLLER_FQDN>
admin_server = <ACTIVE_DIRECTORY_CONTROLLER_FQDN>
}
[domain_realm]
.<DOMAIN FQDN> = <DOMAIN>
<DOMAIN FQDN> = <DOMAIN>
```

3. Save and close the file.
4. To ensure that the DNS forward lookup and reverse lookup services resolve to the Active Directory and MS SQL computers, type the following commands in Terminal:
   - `nslookup <SQL Server IP address>`
   - `nslookup <Active Directory Controller IP address>`
   - `nslookup <SQL Server fully qualified domain name>`
   - `nslookup <Active Directory Controller fully qualified domain name>`

## Microsoft SQL Server

1. Add a Login for the Active Directory user that you created for Deep Security Manager (See https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008-r2/aa337562(v=sql.105)):

- Select Windows authentication.
- For Server Roles, select dbcreator. (The public role should be selected by default.)
- For User Mapping, map the db_owner role membership to the Deep Security Manager database.

2. Ensure that the DNS forward lookup and reverse lookup services resolve to the SQL Server computer. Type the following commands in Command Prompt:
   - `nslookup <SQL Server IP address>`
   - `nslookup <SQL Server fully qualified domain name>`

### Synchronize system clocks

Kerberos authentication requires that the system clocks of authenticating computers are within five minutes of the Active Directory system clock. Ensure that you synchronize the Active Directory and SQL Server system clocks.

## Microsoft SQL Server Express considerations

You can use Microsoft SQL Server Express as your Deep Security database in certain scenarios, but there are important limitations due to the 10 GB size limit for Microsoft SQL Server Express databases. If you think your deployment may exceed these limitations, use Microsoft SQL Server, Oracle database, or PostgreSQL instead.

**Warning:** If you exceed the 10 GB size limit, you will experience a service outage and you will need to upgrade to a paid version of Microsoft SQL Server.

### Supported versions

- Microsoft SQL Server Express 2008 R2
- Microsoft SQL Server Express 2012
- Microsoft SQL Server Express 2014

- Microsoft SQL Server Express 2016
- Amazon RDS SQL Server Express

### Limited number of hosts

Do not use Microsoft SQL Server Express if your deployment has more than 50 hosts.

### Security module limitations

Only the anti-malware and intrusion prevention modules are supported for use with Microsoft SQL Server Express, due to its database size limitation. If you require any other protection modules, use Microsoft SQL Server, Oracle, or PostgreSQL instead.

### Minimize the agent size

Remove any unneeded agent software packages from the Deep Security Manager to save disk space.

### Database pruning

Security updates and events require additional space in the database. Monitor your deployment on an ongoing basis to ensure that you stay below to 10 GB limit. For information on database pruning, see "Log and event storage best practices" on page 799. You may also choose to use the SQL Server settings described in Considerations for the "autogrow" and "autoshrink" settings in SQL Server.

## Configure the IAM role for the Deep Security AMI from AWS Marketplace

**Note:** An IAM role is only required if you are deploying with the Deep Security Marketplace metered billing AMI. If you are deploying with Deep Security Bring-Your-Own-License (BYOL) or if you are deploying from a CloudFormation template, you do not need to create the IAM role.

Before you can launch Deep Security AMI from AWS Marketplace, you must configure the AWS Identity and Access Management (IAM) permissions for the instance. The Deep Security Manager instance needs an IAM role with appropriate permissions and trust relationships associated with it to be able to authenticate to the AWS Marketplace Metering Service and record software usage. This means that your instance has to have an

- Internet connection to AWS services
- IAM role with appropriate permissions and trust relationships associated with it at the time of launch

## IAM role requirements

| | | |
|---|---|---|
| Required IAM permission | The IAM role you associate with the instance has to have the following IAM permission: **aws-marketplace:MeterUsage** | The recommended method for giving the IAM role this permission is to attach the AWS managed policy **AWSMarketplaceMeteringFullAccess** to the role. |
| Required trust relationship | The IAM role has to have a trust relationship with the **ec2.amazonaws.com** service. | For information on how to change which trusted principles can access an IAM role, see Modifying a Role (AWS Management Console). |

After you have created the IAM role and attached the AWSMarketplaceMeteringFullAccess policy to it and added ec2.amazonaws.com as a trusted service, make sure you select that role from the **IAM role** list on the Configure Instance Details page before you launch the instance.

For more information on IAM roles, see the AWS article IAM Roles for Amazon EC2.

# Deploy Deep Security

## Deploy the Deep Security AMI from AWS Marketplace

Instead of manually uploading and installing Deep Security software onto your own custom AMI, we recommend that you use the Quick Start Deep Security on AWS. This method uses AWS CloudFormation templates for quick deployment in about 1 hour. And if you're upgrading an existing Deep Security AMI, see "Upgrade the Deep

Security Manager AMI" on page 740 instead.

The default configuration protects instances in the Amazon Virtual Private Cloud (VPC) where your Deep Security Manager is deployed. After deployment, you can change this to protect instances across your entire AWS infrastructure.

The Deep Security AMI has two license models:

- Per Protected Instance Hour
- Bring your own License (BYOL)

The template includes an option for deploying in the AWS GovCloud (US) region.

Detailed step-by-step instructions for deploying the Quick Start are available in the AWS Quick Start deployment guide. Basic steps include:

1. If you're not familiar with AWS services, read the AWS Deep Security Overview.
2. Set up or identify an Amazon VPC that has two private subnets in different Availability Zones (AZ)and one public subnet with an Internet gateway.
3. Subscribe to Deep Security using one of the licensing models.
4. Launch the Quick Start template for the licensing model you selected: Per Protected Instance Hour Quick Start or BYOL Quick Start.
   When it finishes, a Deep Security management cluster has been deployed into the VPC that you have set up. This cluster includes Deep Security public and private elastic load balancers, Deep Security Manager instances, and a highly available multi-AZ RDS instance hosting the Deep Security database and its mirror.
5. Log in to the Manager console using the URL provided on the Outputs tab of the AWS CloudFormation stack.

   To connect via SSH to the Amazon Linux server where Deep Security Manager is running, see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html.

   **Note:** The user name for the Deep Security Manager instance is "trend", not "root" or "ec2-user".

6. Install the agent software on computers. There are multiple methods:

- **Manual deployment:** Run the install package on the computer, then activate it and assign a policy. For instructions, see "Manually install the Deep Security Agent" on page 180.
- **Deployment scripts:** Upload and then run the installer using Linux or Unix shell scripts or Microsoft PowerShell. For instructions, see "Use deployment scripts to add and protect computers" on page 281.
- **Ansible:** For Ansible recipes, see the Deep Security Ansible playbook on GitHub.
- **Chef:** For Chef recipes for deployment and management, see the Deep Security Chef cookbook on GitHub.
- **Puppet:** For Puppet manifests, see the Deep Security Puppet manifests repository on GitHub.
- **SCCM:** Microsoft System Center Configuration Manager (SCCM) can install an agent, activate it, and apply a policy. To use SCCM, go to **Administration > System Settings > Agents** and enable agent-initiated activation.
- **Template or Elastic Beanstalk:** Include the agent in your VM template. See "Bake the agent into your AMI or WorkSpace bundle" on page 192 and AWS Elastic Beanstalk scripts

7. "Activate the agent" on page 219.
8. "Assign a policy to a computer" on page 352.
9. Enable at least one agent to act as a Deep Security Relay. For details, see "Distribute security and software updates with relays" on page 234.

## Run Deep Security Manager on multiple nodes

Instead of running Deep Security Manager on *one* server, you can install Deep Security Manager on *multiple* servers ("nodes") and connect them to one shared database. This provides better:

- Reliability
- Availability

- Scalability
- Performance

You can log in to any node. Each node can do all types of tasks. No node is more important than any of the others. A node failure does not cause service downtime, and does not result in data loss. Deep Security Manager processes many concurrent activities in a distributed pool that all online nodes execute. All activity that does not happen due to user input is packaged as a job, and runs on any available manager (with some exceptions for "local" jobs that are executed on each node, like cache clearing).

**Each node must run the same Deep Security Manager software version.** When you upgrade, the first manager you upgrade will temporarily take over all duties and shut down the other nodes. On **Administration > System Information**, in the **Network Map with Activity Graph** of the **System Activity** area, other nodes' status will be "Offline" with an indication that an upgrade is required. Once upgrade, nodes will automatically return online and begin processing again.

## Add a node

Running multiple nodes requires either a Microsoft SQL Server or Oracle Database.

To add a Deep Security Manager node to the system, run the Deep Security Manager installer on a new computer. When prompted, type the location of and login credentials for the database. Once the installer connects to the database, you can continue to add the node.

**Warning:** Never run more than one instance of the installer at the same time. Doing so can lead to unpredictable results including corruption of the database.

**Note:** Set the system clock of each manager node to use the same time zone. The database must also use the same time zone. If the time zone is different, this causes Manager Time Out of Sync errors.

## Remove a node

Before you remove or replace a server, you should remove it from the pool of Deep Security Manager nodes.

1. Halt the service or uninstall Deep Security Manager on the node that you want to remove.

   Its status must change to "Offline".

2. Log into Deep Security Manager on another node.
3. Go to **Administration > Manager Nodes**.
4. Double-click the node that you want to remove.

   The node's Properties window should appear.

5. In the **Options** area, click **Decommission**.

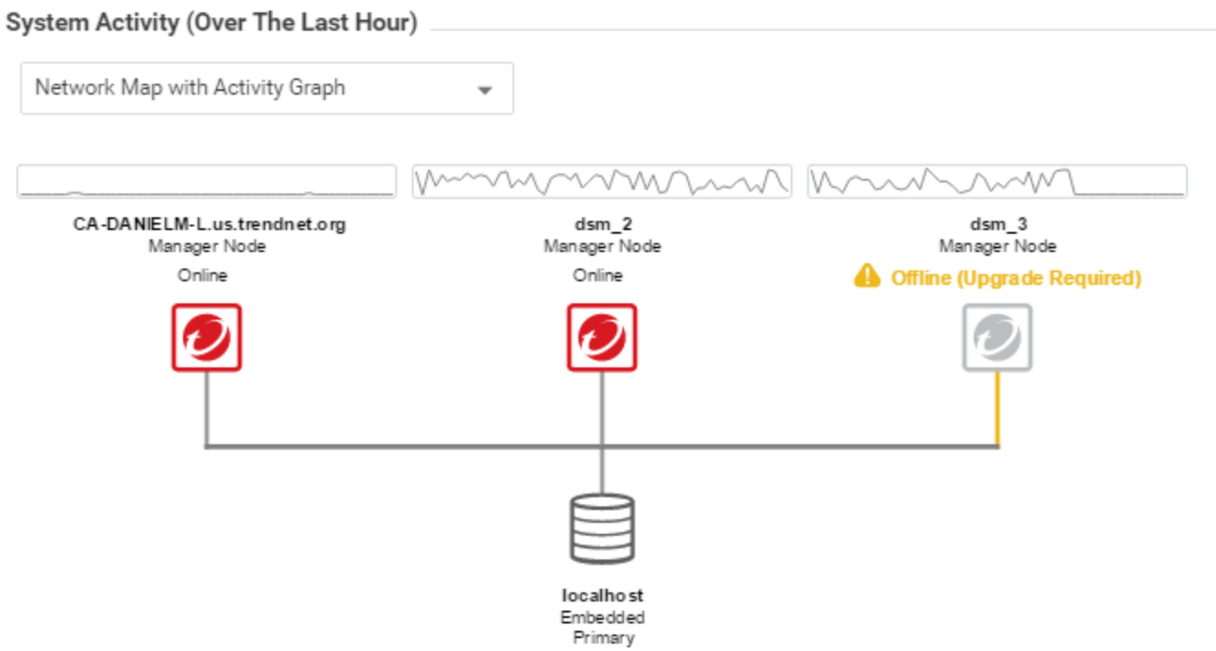
## Viewing node statuses

To display all Deep Security Manager nodes along with their status, combined activity, and jobs being processed, go to **Administration > System Information**. From the drop-down menu, select which graph you want to view.

### Network Map with Activity Graph

The **Network Map with Activity Graph** in the **System Activity** area displays a map of all installed manager nodes and their current status as well their relative activity over the last hour. The nodes can be in the following states:

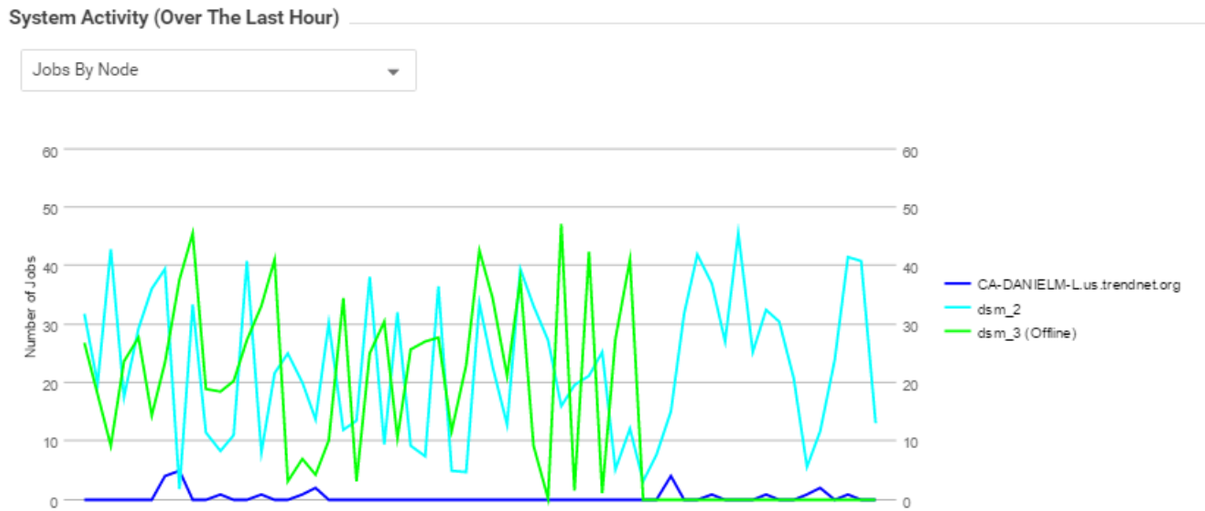
- **Online**
- **Offline**
- **Offline (Upgrade Required)**




**Note:** All Deep Security Manager nodes periodically check the health of all other nodes. If any manager node loses network connectivity for more than 3 minutes, it is considered offline. The remaining nodes assume its tasks.

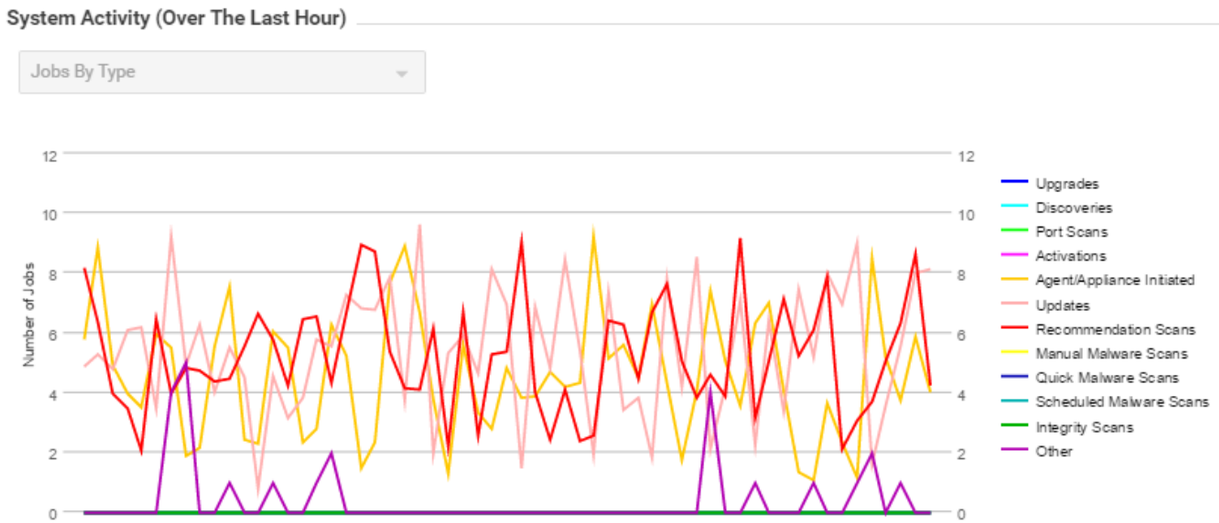
## Jobs by Node

This chart displays the number of jobs carried out over the last hour by each node.



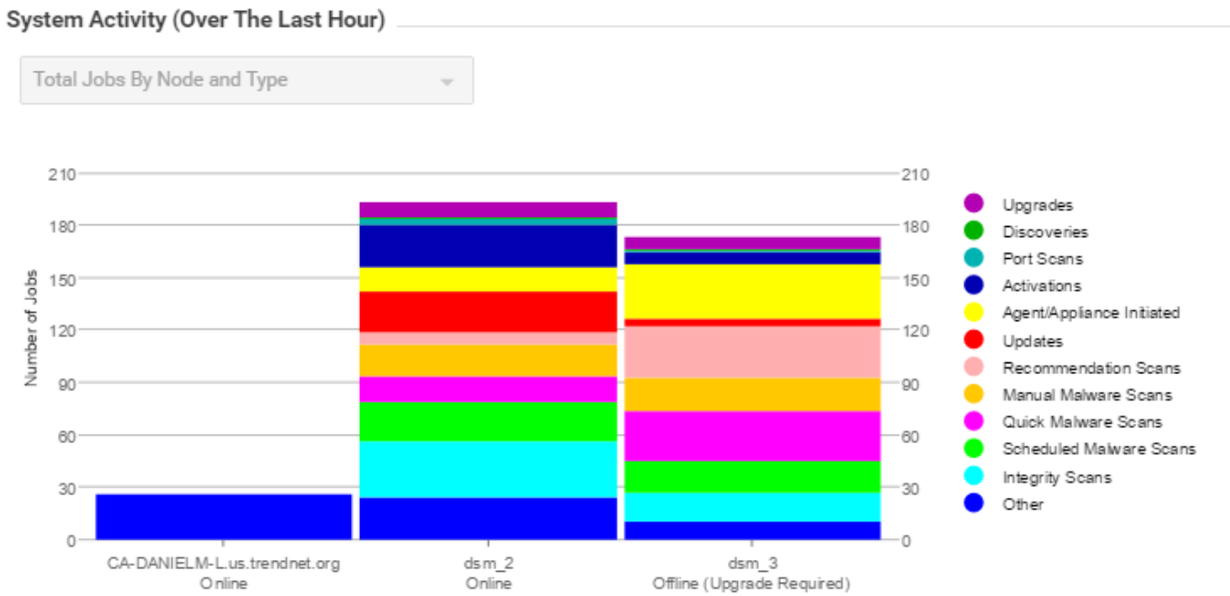

## Jobs by Type

This chart displays the jobs carried out over the last hour by type.




## Total jobs by node and type

This chart displays the number of job types for each node over the last hour.




# Deep Security Manager performance features

## Performance profiles

Deep Security Manager uses an optimized concurrent job scheduler that considers the impacts of each job on CPU, database and agents or appliances. By default, new installations use the "Aggressive" performance profile which is optimized for a dedicated manager. If the Deep Security Manager is installed on a system with other resource-intensive software it may be preferable to use the "Standard" performance profile. The performance profile can be changed by navigating to **Administration > Manager Nodes**. From this screen select a manager node and open the **Properties** window. From here the performance profile can be changed via the menu.

The performance profile also controls the number of agent- or appliance-initiated connections that the manager will accept. The default of each of the performance profiles effectively balances the amount of accepted, delayed and rejected heartbeats.

## Low disk space alerts

### Low disk space on the database host

If the Deep Security Manager receives a "disk full" error message from the database, it will start to write events to its own hard drive and will send an email message to all users informing them of the situation. This behavior is not configurable.

If you are running multiple manager nodes, the events will be written to whichever node is handling the event. (For more information on running multiple nodes, see "Run Deep Security Manager on multiple nodes" on page 130.)

Once the disk space issue on the database has been resolved, the manager will write the locally stored data to the database.

### Low disk space on the manager host

If the available disk space on the manager falls below 10%, the manager generates a Low Disk Space alert. This alert is part of the normal alert system and is configurable like any other. (For more information, see "Configure alerts" on page 781.)

If you are running multiple manager nodes, the node will be identified in the alert.

When the manager's available disk space falls below 5 MB, the manager will send an email message to all users and the manager will shut down. The manager cannot be restarted until the available disk space is greater than 5 MB.

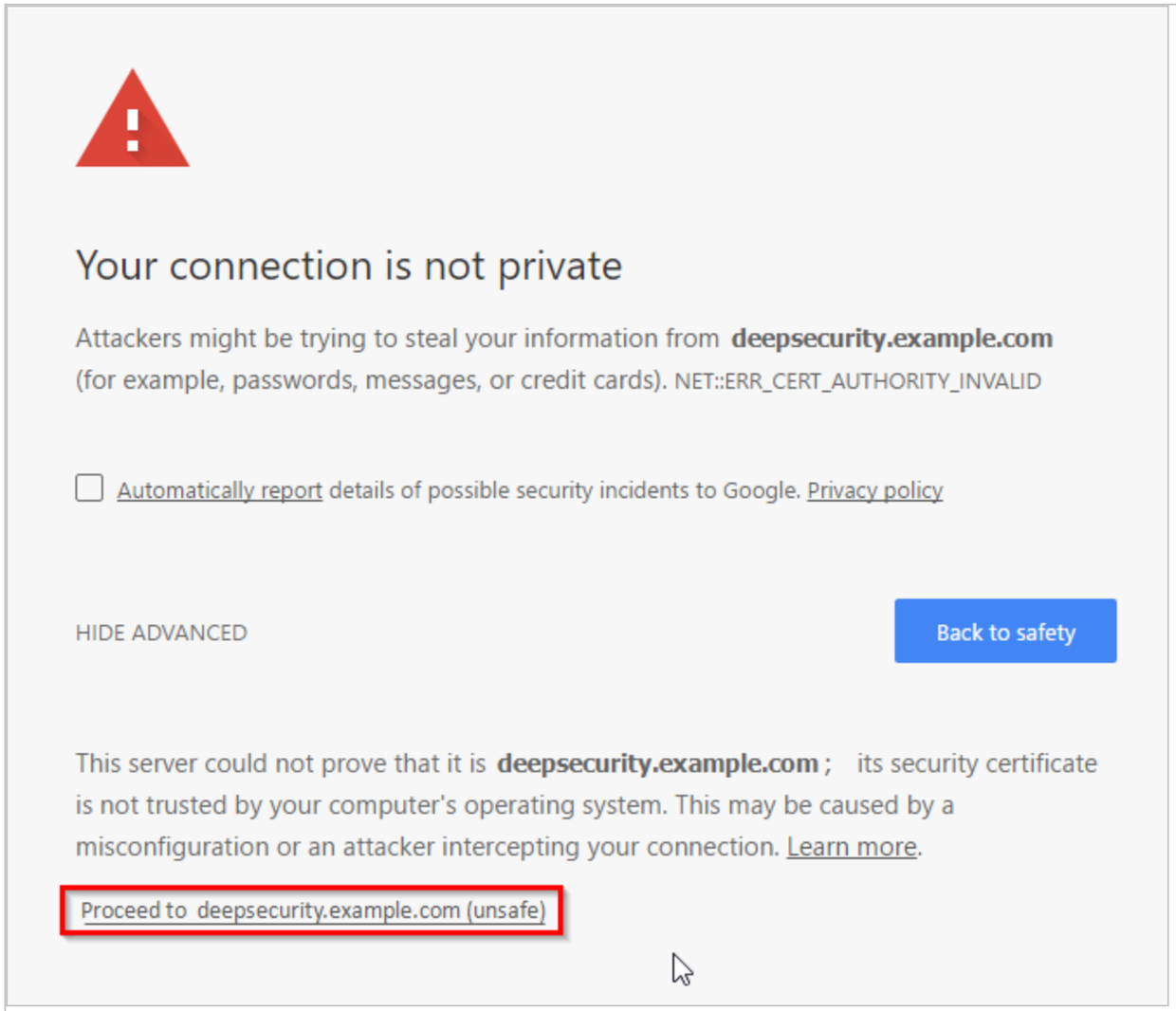
You must restart the manager manually.

If you are running multiple nodes, only the node that has run out of disk space will shut down. The other manager nodes will continue operating.

## Update the load balancer's certificate

Usually, your browser should warn you with a certificate validation error whenever you try to connect to a server with a self-signed certificate. This is because with any *self-*signed certificate, the browser cannot automatically validate the certificate's signature with a trusted *third party* certificate authority (CA), and therefore the browser doesn't know if the certificate was sent by an attacker or not. When installed, Deep Security Manager is initially configured to use a self-signed certificate for HTTPS connections (SSL or TLS), so you must manually verify that the server certificate fingerprint used to secure the connection belongs to your Deep Security server. This is normal until you replace the self-signed certificate with a CA-signed certificate.

The same error will occur if you have an AWS Elastic Load Balancer (ELB) or other load balancer, and it presents a self-signed certificate to the browser.


Your connection is not private
Attackers might be trying to steal your information from deepsecurity.example.com (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID
Automatically report details of possible security incidents to Google. Privacy policy
HIDE ADVANCED
Back to safety
This server could not prove that it is deepsecurity.example.com ; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.
Proceed to deepsecurity.example.com (unsafe)

You can still access Deep Security Manager if you ignore the warning and proceed (method varies by browser). However, this error will occur again each time you connect, unless you either:

- add the certificate to your computer's store of trusted certificates (not recommended) or
- replace the load balancer's certificate with one signed by a trusted CA (strongly recommended)

1. With a CA that is trusted by all HTTPS clients, register the fully qualified domain name (*not IP address*) that administrators, relays, and agents will use to connect to Deep Security Manager.

   Specify the sub-domain (for example, deepsecurity.example.com) that will uniquely identify Deep Security Manager. For nodes behind an SSL terminator load balancer, this certificate will be presented to browsers and other HTTPS clients by the load balancer, not by each Deep Security Manager node.

   When the CA signs the certificate, download both the certificate (with public key) and the private key.

   **Warning:** Store and transmit the private key securely. If file permissions or unencrypted connections allow a third party to access your private key, then all connections secured by that certificate and key are compromised. You must revoke that certificate, remove the key, and get a new certificate and key.

2. Add the certificate to your certificate store (optional if your computer trusts the CA that signed the certificate).
3. Update the DNS settings of the load balancer to use the new domain name.
4. Replace the SSL certificate of the load balancer.

## Set up a multi-tenant environment

**Note:** Multi-tenancy is only available for Deep Security from AWS Marketplace with the Bring your own License (BYOL) payment option.

The multi-tenancy feature in Deep Security lets you create separate management environments within a single Deep Security Manager. It allows tenants to each have their own settings and policies and to monitor their own events. This can be useful if you want to create separate staging and production environments or if you need to create separate environments for different business units in your organization. You can also use multi-tenancy to provision Deep Security to customers in a service model.

Once you enable multi-tenancy, you (as the "primary tenant") retain all of the capabilities of a regular installation of Deep Security Manager. However, the tenants you subsequently create can have their access to Deep Security functionality restricted to varying degrees, based on how you configure the system for them.

**Note:** FIPS mode is not supported in a multi-tenant environment, See "FIPS 140-2 support" on page 1049.

In this topic:


- "Multi-tenancy requirements" below
- "Enable multi-tenancy" on the next page
- "Create a tenant" on page 143
- "Scalability guidelines" on page 145
- "Multi-tenancy tips" on page 146
- "Managing tenants" on page 147
- "Set up a multi-tenant environment" on the previous page
- "Usage monitoring" on page 151
- "Configure database user accounts" on page 154
- "APIs" on page 167
- "Upgrade" on page 167
- "Supporting tenants" on page 168
- "Load balancers" on page 168


## Multi-tenancy requirements

You cannot set up multi-tenancy with:

- Any other license options for Deep Security from AWS Marketplace
- Deep Security Manager VM for Azure Marketplace
- Deep Security as a Service

You will need a separate activation code for multi-tenancy, and multi-tenancy has some extra database requirements in addition to the usual Deep Security Manager requirements. For details, see "Prepare a database for Deep Security Manager on AWS" on page 114 and "Configure database user accounts" on page 154.

To maximize scalability, we recommend that you use a multi-node Deep Security Manager (see "Run Deep Security Manager on multiple nodes" on page 130). All manager nodes process GUI, heartbeat, or job requests for any tenant. For background processing, each tenant is assigned a manager node that takes care of job queuing, maintenance, and other background tasks. Tasks are rebalanced across remaining nodes when manager nodes are added or taken offline.

When you enable multi-tenancy, your current installation of Deep Security Manager becomes the primary tenant (t0) and has special privileges, including the ability to create tenants. When you create tenants, they will be restricted from using certain features and will not see the UI for those features in Deep Security Manager. For example, tenants cannot create other tenants. For details, see "Set up a multi-tenant environment" on page 140

## Enable multi-tenancy

**Note:** Once you enable multi-tenancy, you cannot disable it or remove the primary tenant.

1. In the Deep Security Manager, go to **Administration > System Settings > Advanced**. In the Multi-Tenant Options area, click **Enable Multi-Tenancy**.
2. The Multi-Tenant Configuration wizard appears. Enter your multi-tenancy activation code and click **Next**.
3. Choose the license mode that you want to use:
   - **Inherit Licensing from Primary Tenant:** This option gives all tenants the same licenses that you (the primary tenant) have. This option is recommended if you are using multi-tenancy in a staging environment, or if you intend to set up tenancies for separate departments within your organization.
   - **Per Tenant Licensing:** This option is recommended if you are offering Deep Security as a service. With this configuration, you can use the Deep Security API to provide a license when you create a tenant, or the tenant can enter a license when they sign in to the Deep Security Manager for the first time.

4. Click **Next**. When the wizard closes, you'll be able to see a new **Administration > System Settings > Tenants** page, where you can configure multi-tenancy options. For information about the options on that page, click **Help** in the upper-right corner of Deep Security Manager.

## Create a tenant

**Tip:** You can automate tenant creation and configuration using the Deep Security API. For examples, see the Create and Manage Tenants guide.

Once multi-tenant mode is enabled, Tenants can be managed from the **Tenants** page that now appears in the **Administration** section.

For information about the database user account permissions that are required for adding tenants, see "Configure database user accounts" on page 154.

1. In the Deep Security Manager, go to **Administration > Tenants** and click **New**.
2. The New Tenant wizard appears. Enter a Tenant Account Name. The account name can be anything except "Primary", which is reserved for the primary tenant.
3. Enter an email address that will be used as a point of contact for the tenant.
4. Select the Locale. The Locale determines the language of the Deep Security Manager user interface for the tenant.
5. Select a Time Zone. All tenant-related events will be shown to the tenant users in the time zone that you specify here.
6. If your Deep Security installation is using more than one database, you will have the option to let Deep Security automatically select a database server on which to store the new tenant account ("Automatic -- No Preference") or you can specify a particular server.

   **Note:** This option will not appear if you have only one database. Database servers that are no longer accepting new tenants will not appear in the list.

7. Enter a user name for the first user of the new tenant account.
8. Select one of the three password options:
   - **No Email:** The tenant's first user's user name and password are defined here and no emails are sent.
   - **Email Confirmation Link:** You set the tenant's first user's password. However, the account is not active until the user clicks a link in a confirmation email that will be sent.
   - **Email Generated Password:** This allows you to generate a tenant without specifying the password.

> **Tip:**
> All three options are available via the REST API. The confirmation option provides a suitable method for developing public registration. A CAPTCHA is recommended to ensure that the tenant creator is a human not an automated bot.
>
> The email confirmation ensures that the email provided belongs to the user before they can access the account.

9. Click **Next** to finish with the wizard and create the tenant.

Tenant creation can take up to four minutes due to the creation of the schema and the population of the initial data. This ensures each new tenant has the most up- to-date configuration and removes the burden of managing database templates, especially between multiple database servers.

Each tenant database has an overhead of around 100 MB of disk space (due to the initial rules, policies and events that populate the system).

## Examples of messages sent to tenants

### Email Confirmation Link: Account Confirmation Request

```
Welcome to Deep Security! To begin using your account, click the following confirmation URL. You can then access the console using your chosen
password.
Account Name: AnyCo
User name: admin
Click the following URL to activate your account:
https://managerIP:portnumber/SignIn.screen?confirmation=1A16EC7A-D84F-D451-05F6-706095B6F646&tenantAccount=AnyCo&username=admin
```

### Email Generated Password

First email : Account and Username Notification

```
Welcome to Deep Security! A new account has been created for you. Your password will be generated and provided in a separate email.

Account Name: AnyCo
Username: admin
```

Trend Micro Deep Security for AWS Marketplace 11.1

```
You can access Deep Security using the following URL:
https://managerIP:portnumber/SignIn.screen? tenantAccount=AnyCo&username=admin
```

Second email: Password Notification

```
This is the automatically generated password for your Deep Security account. Your Account Name, Username, and a link to access Deep Security will follow in a separate email.

Password: z3IgRUQ0jaFi
```

## Scalability guidelines

Deployments of 50-100 tenants or more should follow these guidelines to avoid scalability issues:

- Create a maximum of 2000 tenants for a set of Deep Security Manager nodes
- Create a maximum of 300 tenants on a single database server
- Use a separate database server for the primary tenant, with no other tenants
- Limit the number of agents per tenant to 3000
- Limit the number of total agents to 20000
- Use a maximum of 2 Deep Security Manager nodes
- Do not use any co-located relays

Multi-tenancy relies on using multiple databases (if you are using Microsoft SQL) or multiple users (if you are using Oracle). To scale further, you can connect Deep Security Manager to multiple database servers and automatically distribute the new tenants across the available set of database servers. See "Configure database user accounts" on page 154.

# Multi-tenancy tips

## Reconnaissance IP list

In a multi-tenant environment, tenants may need to add the Deep Security Manager IP address to the "Ignore Reconnaissance IP" list found in **Policies > Common Objects > Lists > IP Lists**. This is to avoid getting a "Reconnaissance Detected: Network or Port Scan" warning.

## Use multiple database servers

Multi-tenancy relies on using multiple databases (if you are using Microsoft SQL) or multiple users (if you are using Oracle). To scale further, you can connect Deep Security Manager to multiple database servers and automatically distribute the new tenants across the available set of database servers. See "Configure database user accounts" on page 154.

## Tenant pending deletion state

Tenants can be deleted but the process is not immediate. Deep Security ensures that all the tenant-related jobs are finished before the records are deleted. The longest job runs every week, so the tenant will be in the "pending deletion" state for approximately seven days before the database is removed.

## Multi-tenant options under System Settings

Consider these options on the **Administration > System Settings > Tenants** page:

**Allow Tenants to use the Relays in my "Default Relay Group" (for unassigned Relays):** Gives tenants automatic access to relay-enabled agents set up in the primary tenant. This saves tenants the effort of setting up dedicated relay-enabled agents for security updates.

**Allow Tenants to use the "Run Script" Scheduled task:** Scripts present a potentially dangerous level of access to the system; however, the risk can be mitigated because scripts have to be installed on the Deep Security Manager using file-system access.

## Managing tenants

The **Tenants** page (**Administration > Tenants**) displays the list of all tenants. A tenant can be in any of the following **States**:

- **Created:** Created, but activation email has not been sent to the tenant user.
- **Confirmation Required:** Created, but the activation link in the confirmation email sent to the tenant user has not been clicked. (You can manually override this state.)
- **Active:** Fully online and managed.
- **Suspended:** No longer accepting sign-ins.
- **Pending Deletion:** Tenants can be deleted, however the process is not immediate. The tenant will be in the pending deletion state for approximately seven days before the database is removed.
- **Database Upgrade Failed:** For tenants that failed the upgrade path. The Database Upgrade button can be used to resolve this situation.

### Tenant Properties

Double-click on a tenant to view the tenant's **Properties** window.

### General

The Locale, Time zone and State of the tenant can be altered. Be aware that changing the time zone and locale does not affect existing tenant users. It will only affect new Users in that Tenancy and Events and other parts of the UI that are not user-specific.

The Database Name indicates the name of the database used by this tenancy. The properties of the tenant database can be accessed via the hyperlink.

### Modules

The **Modules** tab provides options for protection module visibility. The selected visibility can be used to tune which modules are visible for which tenants. By default all unlicensed modules are hidden. You can change this by deselecting **Always Hide Unlicensed Modules**. Alternatively, selected modules can be shown on a per-tenant

basis.

If you select **Inherit License from Primary Tenant**, all features that you (the primary tenant) are licensed for will be visible to all tenants. This means that even if you deselect **Always Hide Unlicensed Modules** all unlicensed modules will be hidden if you select this inheritance option.

If you are using the "per tenant" licensing, only the licensed modules for each tenant will be visible by default.

If you are evaluating Deep Security in a test environment and want to see what a full multi-tenancy installation looks like, you can enable "Multi-Tenancy Demo Mode". When in Demo Mode, the manager populates its database with simulated tenants, computers, Events, Alerts, and other data. Initially, seven days worth of data is generated but new data is generated on an ongoing basis to keep the manager's Dashboard, Reports and Events pages populated with data.

**Warning:** Demo Mode should **not** be used in a production environment.

## Features

As an Administrator, you have the ability to turn certain features on or off for specific tenants. These available features may change over time. Currently you can choose to enable **Extended Descriptions for Event Forwarding** to include the full description of events that are forwarded to Amazon SNS or a SIEM. Otherwise, the descriptions will be omitted. **SAML Identity Provider Integration**, **Amazon WorkSpaces Interagration**, and **Application** (Application Control), are enabled by default.

## Statistics

The Statistics tab shows information for the current tenant including database size, jobs processed, logins, security events and system events. The spark line show the last 24 hours at a glance.

## Agent Activation

The Agent Activation tab displays a command that can be run from the agent install directory of this tenant's computers which will activate the agent on the computer so that the tenant can assign policies and perform other configuration procedures from the Deep Security Manager.

## What does the tenant see?

When Multi-tenancy is enabled, the sign-in page has an additional **Account Name** text field.

Tenants are required to enter their account name in addition to their user name and password. The account name allows tenants to have overlapping user names. For example, if multiple tenants synchronize with the same Active Directory server.

> **Note:** When you (as the primary tenant) log in, leave the account name blank or use "Primary".

Some features in the Deep Security Manager UI are not available to tenant users. The following areas are hidden for tenants:

- Manager Nodes Widget
- Multi-Tenant Widgets
- Administration > System Information
- Administration > Licenses (If Inherit option selected)
- Administration > Manager Nodes
- Administration > Tenants
- Administration > System Settings:
  - Tenant Tab
  - Security Tab > Sign In Message
  - Updates Tab > Setting for Allowing Tenants to use Relays from the Primary Tenant
  - Advanced Tab > Load Balancers
  - Advanced Tab > Pluggable Section
- Some of the help content not applicable to tenants

- Some reports not applicable to tenants
- Other features based on the Multi-Tenant Options (discussed later)
- Some Alert Types will also be hidden from tenants:
  - Heartbeat Server Failed
  - Low Disk Space
  - Manager Offline
  - Manager Time Out Of Sync
  - Newer Version of Deep Security Manager available
  - Number of Computers Exceeds Database Limit
  - And when inherited licensing is enabled any of the license-related alerts

It is also important to note that tenants cannot see any of the multi-tenant features of the primary tenant or any data from any other tenant. In addition, certain APIs are restricted since they are only usable with primary tenant rights (such as creating other tenants).

For more information on what is and is not available to tenant users, see "Multi-tenant settings" on page 171.

All tenants have the ability to use Role-Based Access Control with multiple user accounts to further sub-divide access. Additionally, they can use Active Directory integration for users to delegate the authentication to the domain. The Tenant Account Name is still required for any tenant authentications.

## Agent-Initiated Activation

Agent-initiated activation is enabled by default for all tenants.

**Note:** Unlike agent-initiated activation for the primary tenant, a password and tenant ID are required to invoke the activation for other tenant users.

Tenants can see the arguments required for agent-initiated activation by clicking **Administration > Updates > Software > Local**, selecting the agent software and then clicking the **Generate Deployment Scripts** button. For example, the script for Agent-Initiated Activation on a Windows machine might look like this:

```
dsa_control -a dsm://<host or IP>:4120/ "tenantID:XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX" "token:XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"
```

### Tenant diagnostics

Tenants are not able to access manager diagnostic packages due to the sensitivity of the data contained within the packages. Tenants can still generate agent diagnostics by opening the Computer Editor and choosing **Agent Diagnostics** on the **Actions** tab of the **Overview** page.

## Usage monitoring

Deep Security Manager records data about tenant usage. This information is displayed in the **Tenant Protection Activity** widget on the Dashboard, the Tenant **Properties** window's **Statistics** tab, and reports. This information can also be accessed through the Status Monitoring REST API, which can be enabled or disabled by going to **Administration > System Settings > Advanced > Status Monitoring API**.

Use the Status Monitoring REST API to customize the type of tenant information that you would like to see, depending on your environment. For enterprises, this can be useful to determine the usage by each business unit. You can also use the information to monitor the usage of the overall Deep Security system and look for indicators of abnormal activity. For example, if a single tenant experiences a spike in security event activity, it might be under attack.

### Multi-tenant Dashboard

When multi-tenancy is enabled, primary tenant users have access to the following additional Dashboard widgets for monitoring tenant activity:

- Tenant Database Usage
- Tenant Job Activity
- Tenant Protection Activity
- Tenant Security Event Activity

- Tenant Sign-In Activity
- Tenant System Event Activity
- Tenants

The same information is available on the **Administration > Tenants** page (some in optional columns) and on the **Statistics** tab of a tenant's **Properties** window.

This information provides the ability to monitor the usage of the overall system and look for indicators of abnormal activity. For example, if a single tenant experiences a spike in **Security Event Activity**, they might be under attack.

## Multi-tenant reports

To generate reports that contain the information you require, go to **Event & Reports > Generate Reports** and choose the report you'd like to generate from the drop-down menu. The following are reports for multi-tenant environments, and the information they include:

### Security Module Usage Cumulative Report

- Tenant
- Hostname
- ID
- Anti-Malware hours
- Network hours
- System hours
- Enterprise hours

## Security Module Usage Report

- Tenant
- ID
- Hostname
- Display name
- Computer group
- Instance type
- Start date
- Start time
- Stop time
- Duration (seconds)
- Anti-malware
- Web Reputation
- Firewall
- Intrusion prevention
- Integrity monitoring
- Log Inspection
- Application Control

### Tenant Report

- Tenant name
- Database size
- Peak host count
- Protection hours
- Percentage of protected hours

## Configure database user accounts

The majority of each tenant's data is stored in a separate database. This database can co-exist on the same database server as other tenants, or it can be isolated onto its own database server. In all cases, some data only exists in the primary database (the one installed with Deep Security Manager). When multiple database servers are available, tenants are created on the database with the least amount of load.

The segmentation of each tenant's data into a database provides additional benefits:

- **Data destruction:** Deleting a tenant removes all traces of that tenant's data (supported in the product).
- **Backup:** Each tenant's data can be subject to different backup policies. This can be useful for something like tenancy being used for staging and production where the staging environment requires less stringent backups (backups are the responsibility of the administrator setting up Deep Security Manager).
- **Balancing:** The potential for future re-balancing to maintain an even load on all database servers.

### Configuring database user accounts

**Note:**
SQL Server, Oracle, and PostgreSQL use different terms for database concepts described below.

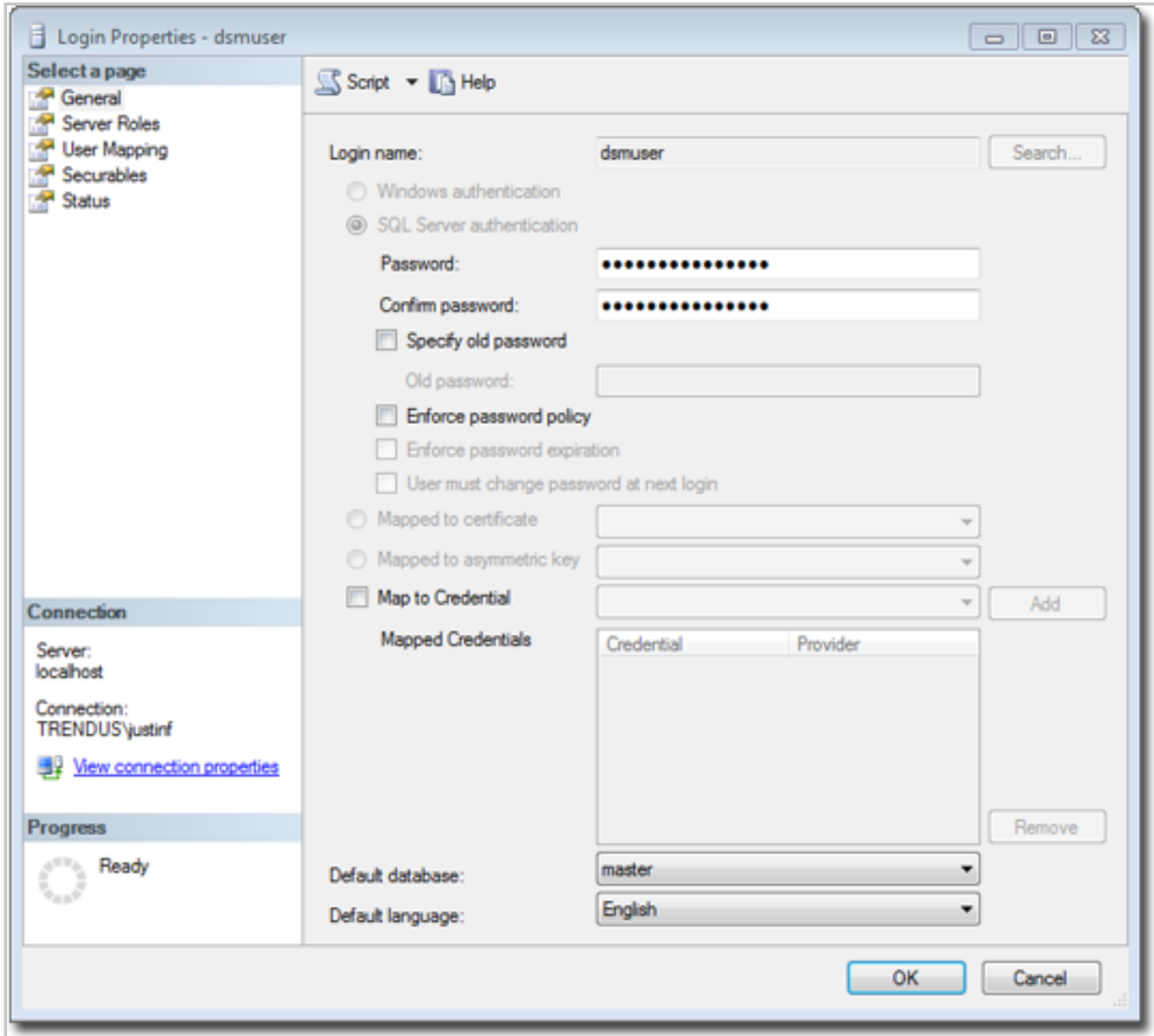
| Concept | SQL Server term | Oracle term | PostgreSQL term |
|---|---|---|---|
| **Process where multiple tenants execute** | Database Server | Database | Database Server |
| **One tenant's set of data** | Database | Tablespace/User | Database |

The following section uses the SQL Server terms for both SQL Server and Oracle.

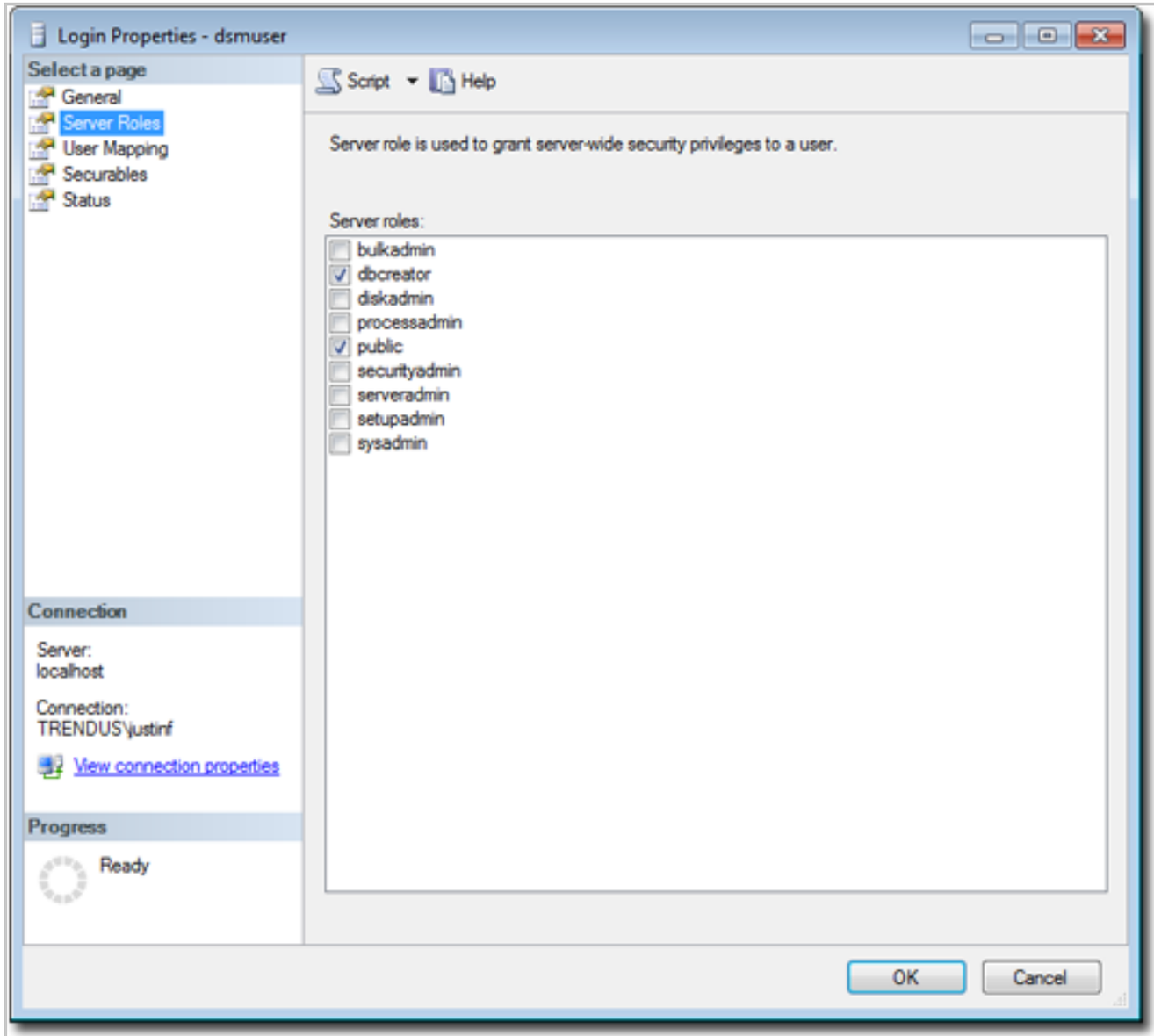
See also "Configure database user accounts" on the previous page.

## SQL Server

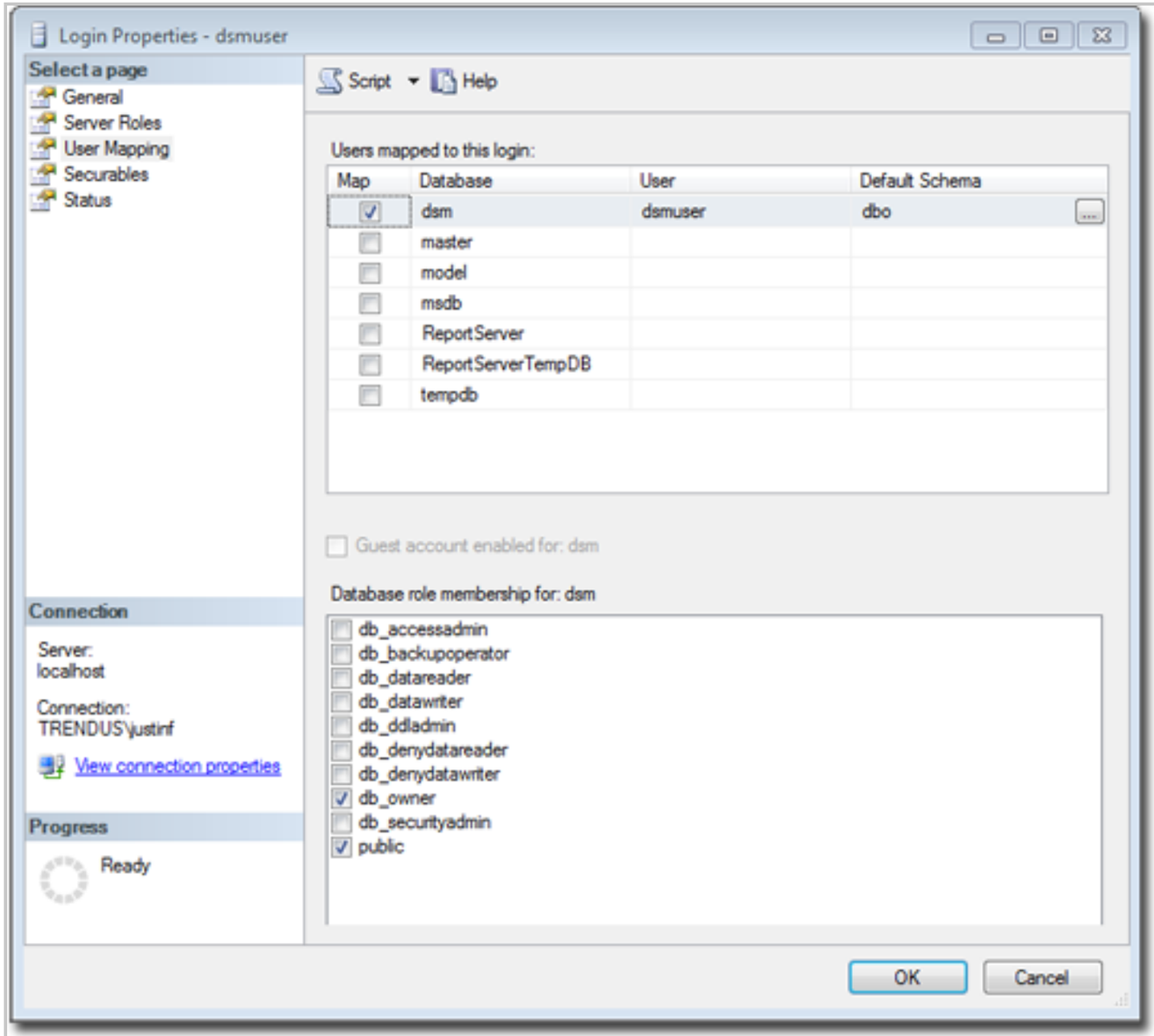
Since multi-tenancy requires the ability for the software to create databases, the **dbcreator** role is required on SQL Server:


Login Properties - dsmuser
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Login name:
dsmuser
Search...
Windows authentication
SQL Server authentication
Password:
Confirm password:
Specify old password
Old password:
Enforce password policy
Enforce password expiration
User must change password at next login
Mapped to certificate
Mapped to asymmetric key
Map to Credential
Add
Mapped Credentials
Credential
Provider
Remove
Connection
Server:
localhost
Connection:
TRENDUS\justinf
View connection properties
Progress
Ready
Default database:
master
Default language:
English
OK
Cancel

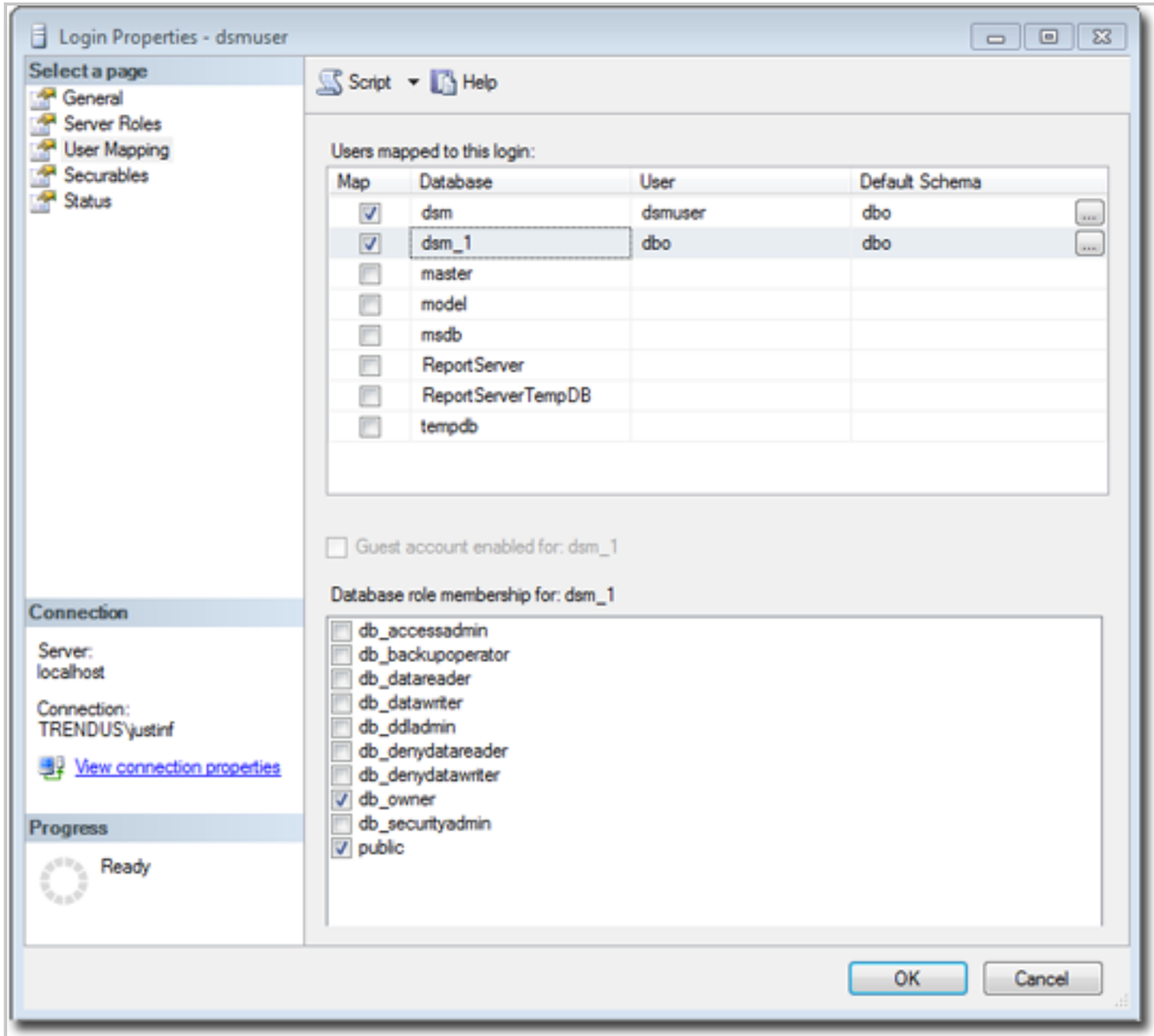
For the user role of the primary tenant, it is important to assign DB owner to the main database:


Login Properties - dsmuser
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Server role is used to grant server-wide security privileges to a user.
Server roles:
bulkadmin
dbcreator
diskadmin
processadmin
public
securityadmin
serveradmin
setupadmin
sysadmin
Connection
Server:
localhost
Connection:
TRENDUS\justinf
View connection properties
Progress
Ready
OK
Cancel

If desired, you can further refine the rights to include only the ability to modify the schema and access the data.


Login Properties - dsmuser
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Users mapped to this login:
Map
Database
User
Default Schema
dsm
dsmuser
dbo
master
model
msdb
ReportServer
ReportServerTempDB
tempdb
Guest account enabled for: dsm
Database role membership for: dsm
db_accessadmin
db_backupoperator
db_datareader
db_datawriter
db_ddladmin
db_denydatareader
db_denydatawriter
db_owner
db_securityadmin
public
Connection
Server:
localhost
Connection:
TRENDUS\justinf
View connection properties
Progress
Ready
OK
Cancel

With the **dbcreator** role, the databases created by the account will automatically be owned by the same user. For example, here are the properties for the user after the first tenant has been created:


Login Properties - dsmuser
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Users mapped to this login:
Map
Database
User
Default Schema
dsm
dsmuser
dbo
dsm_1
dbo
dbo
master
model
msdb
ReportServer
ReportServerTempDB
tempdb
Guest account enabled for: dsm_1
Database role membership for: dsm_1
db_accessadmin
db_backupoperator
db_datareader
db_datawriter
db_ddladmin
db_denydatareader
db_denydatawriter
db_owner
db_securityadmin
public
Connection
Server:
localhost
Connection:
TRENDUS\justinf
View connection properties
Progress
Ready
OK
Cancel

To create the first account on a secondary database server, only the **dbcreator** server role is required. No user mapping has to be defined.

### Oracle

Multi-tenancy in Oracle is similar to SQL Server but with a few important differences. Where SQL Server has a single user account per database server, Oracle uses one user account per tenant. The user that Deep Security was installed with maps to the primary tenant. That user can be granted permission to allocate additional users and tablespaces.

**Note:** Although Oracle allows special characters in database object names if they are surrounded by quotes, *Deep Security does not support special characters in database object names*. This page on Oracle's web site describes the allowed characters in non-quoted names: https://docs.oracle.com/cd/B28359_01/server.111/b28286/sql_elements008.htm#SQLRF00223#SQLRF0 0223

**Note:** Deep Security derives tenant database names from the main (primary tenant) Oracle database. For example, if the main database is "MAINDB", the first tenant's database name will be "MAINDB_1", the second tenant's database name will be "MAINDB_2", and so on. (Keeping the main database name short will make it easier to read the database names of your tenants.)

If multi-tenancy is enabled, the following Oracle permissions must be assigned:

## Roles

| Role | Admin Option | Default |
|---|---|---|
| CONNECT | N | Y |
| RESOURCE | N | Y |

## System Privileges

| System Privilege | Admin Option |
|---|---|
| ALTER USER | N |
| CREATE SEQUENCE | N |
| CREATE TABLE | N |
| CREATE TRIGGER | N |
| CREATE USER | N |
| DROP USER | N |
| GRANT ANY PRIVILEGE | N |
| GRANT ANY ROLE | N |
| UNLIMITED TABLESPACE | N |

## Object Privileges

| Object Privilege | Schema | Object | Grant Option |
|---|---|---|---|
| No items found | | | |

Tenants are created as users with long random passwords and given the following rights:

**Roles**

| Role | Admin Option | Default |
|---|---|---|
| CONNECT | N | Y |
| RESOURCE | N | Y |

**System Privileges**

| System Privilege | Admin Option |
|---|---|
| CREATE SEQUENCE | N |
| CREATE TABLE | N |
| CREATE TRIGGER | N |
| UNLIMITED TABLESPACE | N |

**Object Privileges**

| Object Privilege | Schema | Object | Grant Option |
|---|---|---|---|
| No items found | | | |

For secondary Oracle servers, the first user account (a bootstrap user account) must be created. This user will have an essentially empty tablespace. The configuration is identical to the primary user account.

### PostgreSQL

The user must have the right to create new databases and roles:

```
ALTER ROLE [username] CREATEDB CREATEROLE;
```

On a secondary database server, the hostname, username, and password are required. The username must have privileges to create additional users (roles) and databases.

## Configuring multiple database servers

By default, all tenants are created on the same database server that Deep Security Manager was installed with. In order to provide additional scalability, Deep Security Manager supports adding additional database servers (sometimes referred to as a secondary database). When you add a tenant, you will have the option to let Deep Security automatically select a database server on which to store the new tenant account or you can specify a particular server.

To configure additional databases, go to **Administration** > **System Settings** > **Tenants** and then click **View Database Servers** in the Database Servers section. Click **New** to add a database server.

For **SQL Server**, the secondary database server requires a hostname, user name and password (named instance and domain). The user (the Deep Security Manager) must have the following permissions:

- Create databases
- Delete databases
- Define schema

This account is used not only to create the database but to authenticate to the databases that are created.

**Oracle** multi-tenant uses a different model. The new database definition defines a user that is bound to a tablespace. That user is used to "bootstrap" the creation of additional users on Oracle.

## Removing or changing secondary databases

You can delete database servers (other than the primary database) if there are no tenants on the server.

If the hostname, user name, password or any details change for a secondary server, you can change these values in the Deep Security Manager console. To change values for the primary database, you must shut down all nodes of the Deep Security Manager and edit the dsm.properties file with the new details.

## APIs

Deep Security Manager includes a number of REST APIs for:

1. Enabling Multi-Tenancy
2. Managing Tenants
3. Accessing Monitoring Data
4. Accessing Chargeback (Protection Activity) Data
5. Managing Secondary Database Servers

In addition, the legacy SOAP API includes a new authenticate method that accepts the Tenant Account Name as a third parameter.

For more information on the REST APIs please see "Use the Deep Security API to automate tasks" on page 261.

## Upgrade

Upgrade is unchanged from previous versions. The installer is executed and detects an existing installation. It will offer an upgrade option. If upgrade is selected, the installer first informs other nodes to shutdown and then begins the process of upgrading.

The primary tenant is upgraded first, followed by the tenants in parallel (five at a time). Once the installer finishes, the same installer package should be executed on the rest of the manager nodes.

In the event of a problem during the upgrade of a tenant, the tenant's State (on the **Administration > Tenants** page) will appear as **Database Upgrade Failed (offline)**. The tenants interface can be used to force the upgrade process. If forcing the upgrade does not work, please contact support.

## Supporting tenants

In certain cases, a primary tenant might require access to a tenant's user interface. The tenants list and tenant properties pages provide an option to "Authenticate As" a given tenant, granting them immediate read-only access.

Users are logged in as a special account on the tenant using the prefix "support_". For example, if primary tenant user jdoe logs on as a tenant, an account is created called "support_jdoe" with the "Full Access" role. The user is deleted when the support user times out or signs out of the account.

The tenant can see this user account created, sign in, sign out and deleted along with any other actions in the System events.

Users in the primary tenant also have additional diagnostic tools available to them:

1. The **Administration > System Information** page contains additional information about tenant memory usage and the state of threads. This can be used directly or helpful to Trend Micro support.
2. The `server0.log` on the disk of the manager nodes contains additional information on the name of the tenant (and the user if applicable) that caused the log. This can be helpful in determining the source of issues.

In some cases, tenants will require custom adjustments not available in the GUI. This usually comes at the request of Trend Micro support. The command line utility to alter these settings accepts the argument:

```
-Tenantname "account name"
```

to direct the setting change or other command line action at a specific tenant. If omitted, the action is on the primary tenant.

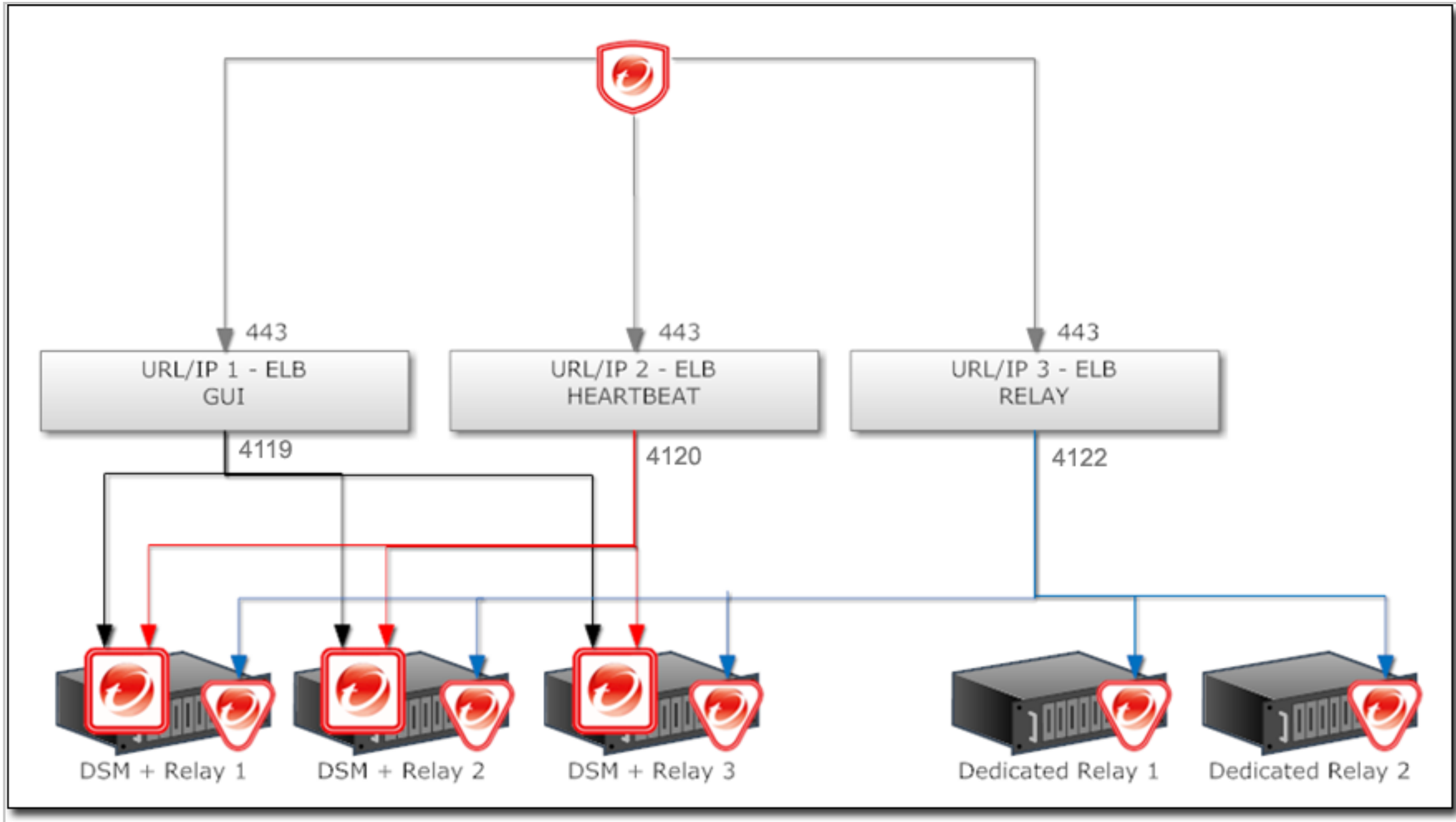
## Load balancers

By default, multi-node manager provides the address of all manager nodes to all agents and virtual appliances. The agents and virtual appliances use the list of addresses to randomly select a node to contact and continue to try the rest of the list until no nodes can be reached (or are all busy). If it can't reach any nodes, it waits until the next

heartbeat and tries again. This works very well in environments where the number of manager nodes is fixed and avoids having to configure a load balancer in front of the manager nodes for availability and scalability.

In multi-tenant environments, it may be desirable to add and remove manager nodes on demand (perhaps using auto-scaling features of cloud environments). In this case, adding and removing managers would cause an update of every agent and virtual appliance in the environment. To avoid this update, the load balancer setting can be used.

Load balancers can be configured to use different ports for the different types of traffic, or if the load balancer supports port re-direction it can be used to expose all of the required protocols over port 443 using three load balancers:


443
URL/IP 1 - ELB
GUI
443
URL/IP 2 - ELB
HEARTBEAT
443
URL/IP 3 - ELB
RELAY
4119
4120
4122
DSM + Relay 1
DSM + Relay 2
DSM + Relay 3
Dedicated Relay 1
Dedicated Relay 2

In all cases, the load balancer should be configured as TCP load balancer (not SSL Terminating). This ensures a given communication exchange will happen directly between the agent or virtual appliance and the manager from start to finish. The next connection may balance to a different node.

## Multi-tenant settings

**Note:** Multi-tenancy is only available for Deep Security from AWS Marketplace with the Bring your own License (BYOL) payment option.

The **Tenants** tab appears only if you have enabled multi-tenant mode.

- **Multi-Tenant License Mode:** The multi-tenant license mode can be changed after multi-tenant is setup, however it is important to note that switching from inherited to per-tenant will cause existing tenants to no longer have any licensed module.
- **Allow Tenants to use the "Run Script" Scheduled Task:** Scripts present a potentially dangerous level of access to the system, however the risk can be mitigated because scripts have to be installed on the Manager using file-system access.
- **Allow Tenants to run "Computer Discovery" (directly and as a Scheduled Task):** Determines if discovery is exposed. This may not be desirable in service provider environments where network discovery has been prohibited.
- **Allow Tenants to run "Port Scan" (directly and as a Scheduled Task):** Determines if port scans can be executed. This may not be desirable in service provider environments where network scan has been prohibited.
- **Allow Tenants to add VMware vCenters:** Determines for each tenant if vCenter connectivity should be exposed. If the deployment is intended through a public service (internet), this option should most likely be disabled since there will not be a secured route to the vCenter from a hosted service.
- **Allow Tenants to add with Cloud Accounts:** Determines if tenants can setup cloud sync. This is generally applicable to any deployment.
- **Allow Tenants to synchronize with LDAP Directories:** Determines if tenants can setup both User and Computer sync with Directories (LDAP or Active Directory for Computers, Active Directory only for users). If the deployment is intended to be made through a public service (internet), this option should most likely be disabled since there will not be a secure route to the directory from a hosted service.

- **Allow Tenants to configure SIEM settings (If not checked, all Tenants use the settings located on the SIEM tab for ALL event types and syslog is relayed via the Manager):** Displays the SIEM settings on the Event Forwarding tab.
- **Allow Tenants to configure SNS settings:** Displays the SNS settings on the Event Forwarding tab.
- **Allow Tenants to configure SNMP settings:** Allow tenants to forward System Events to a remote computer (via SNMP). If this option is not selected, all tenants use the settings located on the Event Forwarding tab for all event types and syslogs are relayed via the Deep Security Manager.
- **Show the "Forgot Password?" option:** Displays a link on the sign in screen which Users can access to reset their password. (Note that SMTP settings must be properly configured on the **Administration > System Settings > SMTP** tab for this option to work.)
- **Show the "Remember Account Name and Username" option:** Deep Security will remember the User's Account Name and Username and populate these fields when the sign in screen loads.
- **Allow Tenants to control access from the Primary Tenant:** By default, the primary tenant can sign in to a tenant's account by using the **Sign In As Tenant** option on the **Administration > Tenants** page. When the **Allow Tenants to control access from Primary Tenant** option is selected, tenants are given the option (under **Administration > System Settings > Advanced** in their ) to allow or prevent access by primary tenant to their Deep Security environment. (When this option is enabled, the default setting in the tenant's environment is to prevent access by the primary tenant.)

  Note: Whenever the primary tenant accesses a tenant's account, the access is recorded in the tenant's System Events.

- **Allow Tenants to use the Relays in my "Default Relay Group":** gives tenants automatic access to relays setup in the primary tenant. This saves tenants from having to setup dedicated Relays for Security Updates.

  Note: Tenants can reject the usage of "shared" relays by going to the **Updates** tab on the **Administration > System Settings** page and deselecting the **Use the Primary Tenant Relay Group as my Default Relay Group (for unassigned Relays)** option. If tenants deselect this setting they must set up dedicated Relays for themselves.

  Note: When relays are shared, it is the responsibility of the primary tenant to keep the relays up to date. This usually involves creating **Download Security Update** Scheduled Tasks for all relays at a regular intervals.

- **Enable the automatic download of Security Updates on new Tenants:** As soon as you create a new tenant account, it will check for and download the latest available security updates.

- **Lock and hide the following options (all Tenants will use the Primary Tenant's configurations):**
  - **Data Privacy options on the "Agents" Tab:** Allows the primary tenant to configure data privacy settings. (This setting only applies to "Allow Packet Data Capture on Encrypted Traffic (SSL)" in on the **Administration > System Settings > Agents** tab.)
  - **All options on the "SMTP" Tab:** Locks all settings on the **SMTP** tab.
  - **All options on the "Storage" Tab:** Locks all settings on the **Storage** tab.

## Database servers

By default, all tenants will be created on the same database server that Deep Security Manager was installed with. In order to provide additional scalability, Deep Security Manager supports adding additional database servers. For details, see "Set up a multi-tenant environment" on page 140.

## New tenant template

The tenant template feature provides a convenient way of creating a customized "out-of-the-box" experience for new tenants.

The process is as follows:

1. Create a new tenant.
2. Log in as that tenant.
3. Customize the example policies (adding, removing, or modifying) and the security update version (applying newer versions).
4. Return to the primary tenant and run the tenant template wizard.
5. Select the tenant to snapshot.

The following items are INCLUDED in the new template:

- Latest Security Update rules (Updates that have been applied to the template when created. This includes intrusion prevention rules provided by Trend Micro, change monitoring rules, security log monitoring rules)
- Policy Firewall rules
- IP list
- MAC list
- Directory listing
- File list
- File extension list
- Port list
- Contexts
- Schedule
- Firewall Stateful Configuration
- Malware scan settings

The following items are EXCLUDED from the new template:

- Custom Intrusion Prevention rules
- Custom Application Types
- Custom Integrity Monitoring rules
- Custom Log Inspection rules
- Custom Log Inspection Decoders
- Dashboard

- Alert settings
- System settings
- Scheduled tasks
- Event-based tasks
- Users
- Roles
- Contact information

This feature may be useful in service provider environments where some of the examples are not applicable, or special examples need to be created.

As always the examples are meant to be a starting point. Tenants are encouraged to create policies based on their unique needs.

**Note:** Creating a new template will not affect existing tenants.

## Protection usage monitoring

Deep Security collects information about protected computers. This information is visible on the dashboard in the tenants widget and the Tenant Protection Activity widget. The information is also provide in the Tenant report and is available via the REST API.

**Note:** In the most basic case, the monitoring can help determine the percentage usage of Deep Security Manager by hours of protection through the report or the API. Commonly called viewback or chargeback this information can be used in a variety of ways. In more advanced cases, this can be used for custom billing based on characteristics like tenant computer operating systems.

Use these options determine which additional tenant computer details are recorded.

# Configure SMTP settings for email notifications

Deep Security Manager can send emails to users when selected alerts are triggered (see "Configure alerts" on page 781). Before setting up the email notifications, you will need to give Deep Security Manager access to an SMTP mail server.

1. Go to **Administration > System Settings > SMTP**.
2. Type the IP address or host name of your SMTP e-mail server. Include the port number if it's not the default port number.

   **Tip:** AWS throttles (rate limits) e-mail on SMTP's IANA standard port number, port 25. If you use AWS Marketplace, you may have faster alerts if you use SMTP over STARTTLS (secure SMTP) instead. For more information, see: https://docs.aws.amazon.com/ses/latest/DeveloperGuide/smtp-connect.html.

3. Enter a "From" email address from which the emails should be sent.

   **Note:** If you are using Amazon SES, the sender email address must be verified. To learn how to verify your email address in Amazon SES and view a list of addresses you've already verified, see: https://docs.aws.amazon.com/ses/latest/DeveloperGuide/verify-email-addresses.html

4. Optionally, type a "bounce" address to which delivery failure notifications (DSN) should be sent if the alert emails can't be delivered to one or more users.
5. If your SMTP mail server requires outgoing authentication, type the user name and password credentials.
6. Select **STARTTLS** if your SMTP server supports the protocol. (STARTTLS is not supported in FIPS mode. See "FIPS 140-2 support" on page 1049.)
7. After you've entered the necessary information, click **Test SMTP Settings** to test the connection.

# Install the agents

## Get Deep Security Agent software

To install Deep Security Agent, you must download the agent installer and load packages for the agent's protection modules into Deep Security Manager. To view a list of software that has been imported into Deep Security Manager, go to **Administration > Updates > Software > Local**.

Deep Security is modular. Initially, Deep Security Agent only has core functionality. When you enable a protection module, then the agent downloads that plug-in and installs it. So before you activate any agents, first download the agent software packages into Deep Security Manager's database("import" them) so that they will be available to the agents and relays.

> **Warning:** Even if you use a third party deployment system, you **must** import all installed Deep Security Agent software into the Deep Security Manager's database. When a Deep Security Agent is first activated, it only installs protection modules that are currently enabled in the security policy. If you enable a new protection module later, Deep Security Agent will try to download its plug-in from Deep Security Manager. If that software is missing, the agent may not be able to install the protection module.

Once you import the agent installer package, depending on your preferred deployment method, you can then export and load the installers into a third party deployment system such as Ansible, Chef, or Puppet which will install it on your computers.

### Download agent software packages into Deep Security Manager

Even if you don't use Deep Security Manager to deploy agent updates, you should still import the software into the Deep Security Manager's database. You can do this manually or automatically.

#### Automatically import software updates

You can configure Deep Security Manager to automatically download any updates to software that you've already imported into Deep Security. To enable this feature, go to **Administration > System Settings > Updates** and select **Automatically download updates to imported software**.

**Note:** This setting will download the software to the Deep Security but will *not* automatically update your agent software. Continue with "Update the Deep Security Agent" on page 738.

### Manually import software updates

You can manually import software updates as they become available on the Download Center.

1. In Deep Security Manager, go to **Administration > Updates > Software > Download Center**.

   The Trend Micro Download Center displays the latest versions of agent software.

2. To download your agent software package to the manager's local storage, select the installer from the list, and then click **Import** .

   Deep Security Manager connects to the internet to download the software from Trend Micro. When the manager has finished, a green check mark will appear in the **Imported** column for that agent. Software packages will appear on **Administration > Updates > Software > Local**.

   If a package cannot be imported directly, a popup note will indicate that. For these packages, download them from the Trend Micro Download Center website to a local folder, then go to **Administration > Updates > Software > Local** and manually import them.

   **Tip:** Alternatively, if your Deep Security Manager is "air-gapped" (not connected to the Internet) and cannot connect *directly* to the Download Center web site, you can load them *indirectly*. Download the ZIP packages to your management computer first, and then log into the Deep Security Manager and upload them.

### Export the agent installer

You can download the agent installer from Deep Security Manager.

1. In Deep Security Manager, go to **Administration > Updates > Software > Local**.
2. Select your agent from the list.
3. Click **Export > Export Installer**.

If you have older versions, the latest version of the software will have a green check mark in the **Is Latest** column.

4. Save the agent installer. If you will install the agent manually, save it on the computer where you want to install Deep Security Agent. Otherwise, if you use a third party deployment system (such as Ansible, Chef, Puppet, PowerShell, or others), load the agent installer into that system.

**Tip:** To install Deep Security Agent, only use the exported agent installer (the .msi or the .rpm file) - *not* the full agent ZIP package. If you run the agent installer from the same folder that holds the other zipped agent components, all protection modules will be installed, even if you haven't enabled them on the computer. This consumes extra disk space. (For comparison, if you use the .msi or .rpm file, the agent will download and install protection modules *only if your configuration requires them*.)

**Tip:** Installing an agent, activating it, and applying protection with a security policy can be done using a command line script. For more information, see "Use deployment scripts to add and protect computers" on page 281.

## Delete a software package from the Deep Security database

To save disk space, Deep Security Manager will periodically remove unused packages from the Deep Security database. To configure the maximum number of old packages kept, go to **System Settings > Storage**.

**Note:** Deep Security Virtual Appliance uses protection module plug-ins in the 64-bit Red Hat Enterprise Linux Agent software package. Therefore if you have an activated Deep Security Virtual Appliance, and try to delete the 64-bit Red Hat Enterprise Linux Agent software package from the database, an error message will tell you that the software is in use.

There are two types of packages that can be deleted:

- agent
- kernel support

### Deleting agent packages in single-tenancy mode

In single tenancy mode, Deep Security automatically deletes agent packages (Agent-*platform*-*version*.zip) that are not currently being used by agents. Alternatively, you can manually delete unused agent packages. Only unused software packages can be deleted.

**Note:** For the Windows and Linux agent packages, only the currently used package (whose version is the same as the agent installer) cannot be deleted.

### Deleting agent packages in multi-tenancy mode

In multi-tenancy mode, unused agent packages (Agent-*platform*-*version*.zip) are **not** deleted automatically. For privacy reasons, Deep Security cannot determine whether software is currently in use by your tenants, even though you and your tenants share the same software repository in the Deep Security database. As the primary tenant, Deep Security does not prevent you from deleting software that is not currently running on any of your own account's computers, but before deleting a software package, be very sure that no other tenants are using it.

### Deleting kernel support packages

In both single and multi-tenancy mode, Deep Security automatically deletes unused kernel support packages (KernelSupport-*platform*-*version*.zip). A kernel support package can be deleted if both of these conditions are true:

- No agent package has the same group identifier.
- Another kernel support package has the same group identifier and a later build number.

You can also manually delete unused kernel support packages. For Linux kernel support packages, only the latest one cannot be deleted.

## Manually install the Deep Security Agent

**Tip:** For easier agent installation and activation, use a deployment script instead. For more information, see "Use deployment scripts to add and protect computers" on page 281.

Before installing the Deep Security Agent, you must import the software into Deep Security Manager and export the installer. See "Get Deep Security Agent software" on page 177.

After installation, the agent must be activated before it can protect its computer or be converted into a relay. See "Activate the agent" on page 219.

In this topic:


- "Install a Windows agent" below
- "Install a Red Hat, SUSE, Oracle Linux, or Cloud Linux agent" on the next page
- "Install an Ubuntu or Debian agent" on page 183


## Install a Windows agent

1. Copy the installer file to the computer.
2. Double-click the installation file (.MSI file) to run the installer package.

   **Note:** On Windows Server 2012 R2 Server Core, launch the installer using this command instead: `msiexec /i Agent-Core-Windows-11.1.x-xxxx.x86_64.msi`

3. At the Welcome screen, click **Next** to begin the installation.
4. **End-User License Agreement:** If you agree to the terms of the license agreement, select **I accept the terms of the license agreement** and click **Next**.
5. **Destination Folder:** Select the location where you would like Deep Security Agent to be installed and click **Next**.
6. **Ready to install Trend Micro Deep Security Agent:** Click **Install** to proceed with the installation.
7. **Completed:** when the installation has completed successfully, click **Finish**.

The Deep Security Agent is now installed and running on this computer, and will start every time the machine boots.

**Note:** When installing the agent on Windows 2012 Server Core, the notifier will not be included.

**Note:** During an install, network interfaces will be suspended for a few seconds before being restored. If you are using DHCP, a new request will be generated, potentially resulting in a new IP address for the restored connection.

### Installation on Amazon WorkSpaces

- If you are unable to install Deep Security Agent .msi file due to error code '2503' then you must do one of the following:
  - Edit your C:\Windows\Temp folder and allow the write permission for your user
    OR
  - Open the command prompt as an administrator and run the .msi file

**Note:** Amazon has fixed this issue for newly-deployed Amazon WorkSpaces.

### Installation on Windows 2012 Server Core

- Deep Security does not support switching the Windows 2012 server mode between Server Core and Full (GUI) modes after the Deep Security Agent is installed.
- If you are using Server Core mode in a Hyper-V environment, you will need to use Hyper-V Manager to remotely manage the Server Core computer from another computer. When the Server Core computer has the Deep Security Agent installed and Firewall enabled, the Firewall will block the remote management connection. To manage the Server Core computer remotely, turn off the Firewall module.
- Hyper-V provides a migration function used to move a guest VM from one Hyper-V server to another. The Deep Security Firewall module will block the connection between Hyper-V servers, so you will need to turn off the Firewall module to use the migration function.

## Install a Red Hat, SUSE, Oracle Linux, or Cloud Linux agent

1. Copy the installer file to the computer.
2. Install the agent.

```
# sudo rpm -i <package name>
```

```
Preparing... ########################################### [100%]
1:ds_agent ########################################### [100%]
Loading ds_filter_im module version ELx.x [ OK ]
Starting ds_agent: [ OK ]
```

To upgrade from a previous install, use "rpm -U" instead. This will preserve your profile settings.

The Deep Security Agent will start automatically upon installation.

## Install an Ubuntu or Debian agent

1. Go to **Administration > Updates > Software > Download Center**.
2. Import the agent package into Deep Security Manager.
3. , and then export the installer (.deb file).
4. Copy the installer file to the computer.
5. Install the agent.

```
sudo dpkg -i <installer file>
```

To start, stop, or reset the agent:

- Start: : `/etc/init.d/ds_agent start`
- Stop: `/etc/init.d/ds_agent stop`
- Reset: `/etc/init.d/ds_agent reset`
- Restart: `/etc/init.d/ds_agent restart`

## Install the agent on a Microsoft Azure VM

To install the agent on VM instances running in the Microsoft Azure cloud, you need to deploy Deep Security Agents to them. You can do this in multiple ways:

- "Generate and run a deployment script" below
- "Add a custom script extension to an existing virtual machine" below

### Generate and run a deployment script

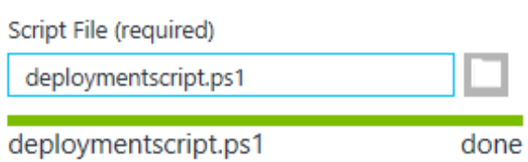
You can generate Deep Security deployment scripts for automatically deploying agents using deployment tools such as RightScale, Chef, Puppet, and SSH.

For more information on how to do so, see "Use deployment scripts to add and protect computers" on page 281.

### Add a custom script extension to an existing virtual machine

You can also add a custom script extension to an existing virtual machine to deploy and activate the Deep Security Agent. To do this, navigate to your existing virtual machine in the Azure management portal and follow the steps below to upload and execute the deployment script on your Azure VM.

1. Log in to the Azure portal.
2. Switch to the preview portal, and then click the virtual machine that you want to add the custom script to.
3. In the **Settings** blade, click **Extensions**, in the **Extensions** blade, click **Add extension**, in the **New Resource** blade, select **Custom Script**, and then click **Create**.
4. In the **Add Extension** blade under **Script File (required)**, click **upload**, select the saved .ps1 deployment script, and then click **OK**.



# Install the agent on Amazon EC2 and WorkSpaces

**Note:** The Deep Security Agent only supports Amazon WorkSpaces Windows desktops–it does not support Linux desktops.

Read this page if you want to protect *existing* Amazon EC2 instances and Amazon WorkSpaces with Deep Security.

If instead you want to:

- launch *new* Amazon EC2 instances and Amazon WorkSpaces with the agent 'baked in', see "Bake the agent into your AMI or WorkSpace bundle" on page 192.
- protect Amazon WorkSpaces after already protecting your Amazon EC2 instances, see instead "Protect Amazon WorkSpaces if you already added your AWS account" on page 309.

To protect your existing Amazon EC2 instances and Amazon WorkSpaces with Deep Security, follow these steps:

1. "Add your AWS accounts to Deep Security Manager" below
2. "Set the communication direction" on the next page
3. "Configure the activation type" on the next page
4. "Open ports" on page 188
5. "Deploy agents to your Amazon EC2 instances and WorkSpaces" on page 190
6. "Verify that the agent was installed and activated properly" on page 190
7. "Assign a policy" on page 191

## Add your AWS accounts to Deep Security Manager

You'll need to add your AWS account or accounts to Deep Security Manager. These AWS accounts contain the Amazon EC2 instances and Amazon WorkSpaces that you want to protect with Deep Security.

Follow the instructions in "Add AWS cloud accounts" on page 295 to add your AWS accounts.

After adding your AWS accounts:

- your existing Amazon EC2 instances and Amazon WorkSpaces appear in Deep Security Manager. If no agent is installed on them, they appear with a **Status** of **Unmanaged (Unknown)** and a grey dot next to them. If an agent was already installed, they appear with a **Status** of **Managed (Online)** and green dot next to them.
- any new Amazon EC2 instances or Amazon WorkSpaces that you launch through AWS under this AWS account are auto-detected by Deep Security Manager and displayed in the list of computers.

## Set the communication direction

You'll need to set the communication direction: either agent-initiated, manager-initiated, or bi-directional.

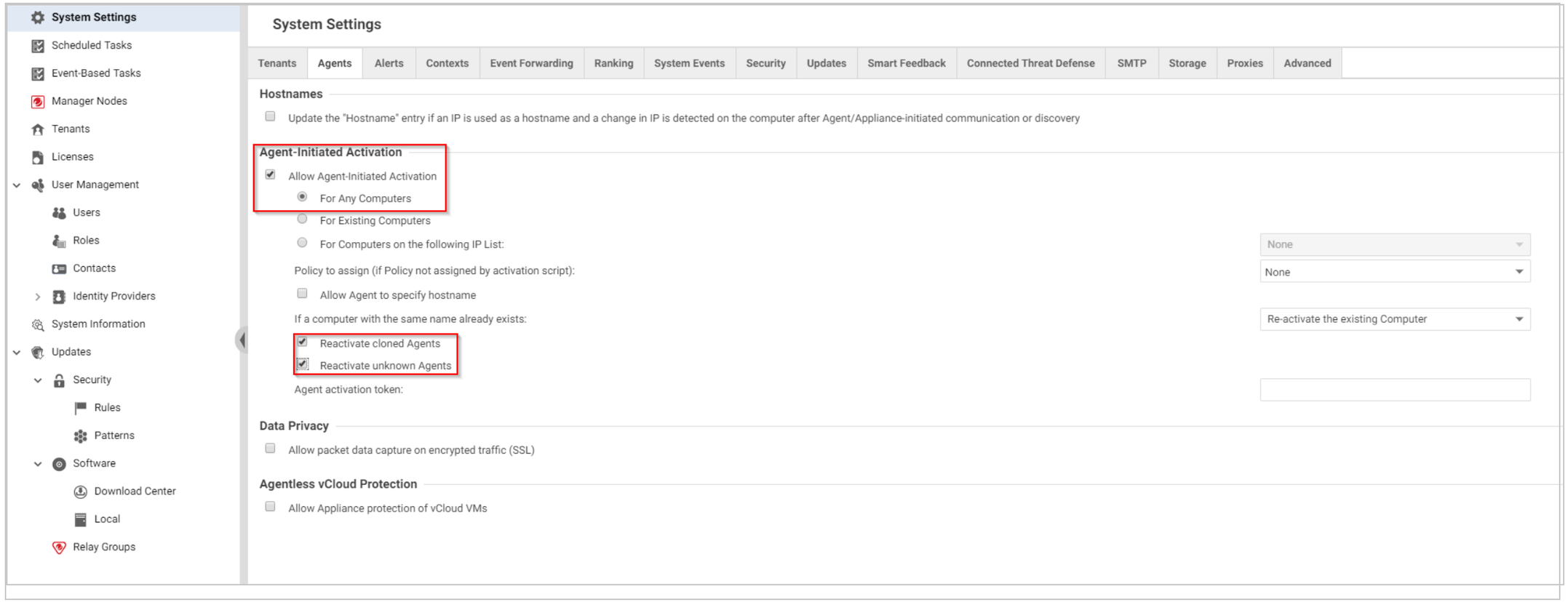
1. Log in to Deep Security Manager.
2. Set the communication direction following the instructions in "Configure communication directionality" on page 198. Follow these guidelines:
   - **Agent/Appliance Initiated** does not require you to open inbound ports on the Amazon EC2 instance or Amazon WorkSpace, while **Bidirectional** and **Manager-Initiated** do.
   - **Agent/Appliance Initiated** is the safest option since no inbound ports need to be opened on the Amazon EC2 instance or Amazon WorkSpace.
3. If you're using Amazon WorkSpaces, and you chose to set the communication direction to **Bidirectional** or **Manager-Initiated**, manually assign an elastic IP address to each WorkSpace before proceeding with further steps on this page. This gives the WorkSpace a public IP that can be contacted by the Deep Security Manager. This is not required for EC2 instances because they already use public IP addresses. WorkSpaces use private IP addresses.

## Configure the activation type

'Activation' is the process of registering an agent with a manager. You'll need to indicate whether you'll allow agent-initiated activation. If not, only manager-initiated activation is allowed.

1. Log in to Deep Security Manager.
2. Click **Administration** at the top.
3. On the left, click **System Settings**.

4. In the main pane, make sure the **Agents** tab is selected.
5. Select or deselect **Allow Agent-Initiated Activation**, noting that:
   - Agent-initiated activation does not require you to open up inbound ports to your Amazon EC2 instances or Amazon WorkSpaces, while manager-initiated activation does.
   - If agent-initiated activation is enabled, manager-initiated activation continues to work.
   - Agent-initiated activation works even if you set the communication direction to **Manager-Initated**.
6. If you selected **Allow Agent-Initiated Activation**, also select **Reactivate cloned Agents**, and **Enable Reactivate unknown Agents**. See "Agent settings" on page 223 for more information.
7. Click **Save**.
8. If you're using Amazon WorkSpaces, and you *didn't* allow agent-initiated activation, manually assign an elastic IP address to each WorkSpace now, before proceeding with further steps on this page. This gives each Amazon WorkSpace a public IP that can be contacted by other computers. This is not required for EC2 instances because they already use public IP addresses.




## Open ports

You'll need to make sure that the necessary ports are open to your Amazon EC2 instances or Amazon WorkSpaces.

To open ports:

1. Open ports to your Amazon EC2 instances, as follows:
   a. Log in to your Amazon Web Services Console.
   b. Go to **EC2 > Network & Security > Security Groups**.
   c. Select the security group that is associated with your EC2 instances, then select **Actions > Edit outbound rules**.
   d. Open the necessary ports. See "Which ports should be opened?" below below.
2. Open ports to your Amazon WorkSpaces, as follows:
   a. Go to the firewall software that is protecting your Amazon WorkSpaces, and open the ports listed above.

You have now opened the necessary ports so that Deep Security Agent and Deep Security Manager can communicate.

### Which ports should be opened?

Generally-speaking:

- agent-to-manager communication requires you to open the outbound TCP port (443 or 80, by default), while
- manager-to-agent communication requires you to open an inbound TCP port (4118).

More specifically:

- If you set the communication direction to **Agent/Appliance-Initiated**, you'll need to open the *outbound* TCP port (443 or 80, by default).
- If you set the communication direction to **Manager-Initiated**, you'll need to open the *inbound* TCP port of 4118.
- If you set the communication direction to **Bidirectional**, you'll need to open both the *outbound* TCP port (443 or 80, by default) AND the *inbound* TCP port of 4118.
- If you enabled **Allow Agent-Initiated Activation**, you'll need to open the *outbound* TCP port (443 or 80, by default) regardless of how you set the communication direction.
- If you disabled **Allow Agent-Initiated Activation**, you'll need to open the *inbound* TCP port of 4118 regardless of how you set the communication direction.

## Deploy agents to your Amazon EC2 instances and WorkSpaces

You'll need to deploy agents onto your Amazon EC2 instances and Amazon WorkSpaces. Below are a couple of options.

- **Option 1: Use a deployment script to install, activate, and assign a policy**

  Use Option 1 if you need to deploy agents to many Amazon EC2 instances and Amazon WorkSpaces.

  With this option, you must run a deployment script on the Amazon EC2 instances or Amazon WorkSpaces. The script installs and activates the agent and then assigns a policy. See "Use deployment scripts to add and protect computers" on page 281 for details.

  OR

- **Option 2: Manually install and activate**

  Use Option 2 if you only need to deploy agents to a few EC2 instances and Amazon WorkSpaces.

  a. Get the Deep Security Agent software, copy it to the Amazon EC2 instance or Amazon WorkSpace, and then install it. For details, see "Get Deep Security Agent software" on page 177, and "Manually install the Deep Security Agent" on page 180.
  b. Activate the agent. You can do so on the agent (if agent-initiated activation was enabled) or on the Deep Security Manager. For details, see "Activate the agent" on page 219

You have now installed and activated Deep Security Agent on an Amazon EC2 instance or Amazon WorkSpace. A policy may or may not have been assigned, depending on the option you chose. If you chose Option 1 (you used a deployment script), a policy was assigned to the agent during activation. If you chose Option 2 (you manually installed and activated the agent), then no policy has been assigned, and you will need to assign one following the instructions further down on this page.

## Verify that the agent was installed and activated properly

You should verify that your agent was installed and activated properly.

1. Log in to Deep Security Manager.
2. Click **Computers** at the top.
3. On the navigation pane on the left, make sure your Amazon EC2 instance or Amazon WorkSpace appears under **Computers** > *your_AWS_account* > *your_region* . (Look for WorkSpaces in a **WorkSpaces** sub-node.)
4. In the main pane, make sure your Amazon EC2 instances or Amazon WorkSpaces appear with a **Status** of **Managed (Online)** and a green dot next to them.

## Assign a policy

Skip this step if you ran a deployment script to install and activate the agent. The script already assigned a policy so no further action is required.

If you installed and activated the agent manually, you must assign a policy to the agent. Assigning the policy sends the necessary protection modules to the agent so that your computer is protected.

To assign a policy, see "Assign a policy to a computer" on page 352.

After assigning a policy, your Amazon EC2 instance or Amazon WorkSpace is now protected.

## Bake the agent into your AMI or WorkSpace bundle

Read this page if you want to launch *new* Amazon EC2 instances and Amazon WorkSpaces with the agent 'baked in'.

If instead you want to:

- protect *existing* Amazon EC2 instances and Amazon WorkSpaces with Deep Security, see "Install the agent on Amazon EC2 and WorkSpaces" on page 185.
- protect Amazon WorkSpaces after already protecting your Amazon EC2 instances, see instead "Protect Amazon WorkSpaces if you already added your AWS account" on page 309.

'Baking the agent' is the process of launching an EC2 instance based on a public AMI, installing the agent on it, and then saving this custom EC2 image as an AMI. This AMI (with the agent 'baked in') can then be selected when launching new Amazon EC2 instances.

Similarly, if you want to deploy the Deep Security Agent on multiple Amazon WorkSpaces, you can create a custom 'WorkSpace bundle' that includes the agent. The custom bundle can then be selected when launching new Amazon WorkSpaces.

To bake an AMI and create a custom WorkSpace bundle with a pre-installed and pre-activated agent, follow these steps:

1. "Add your AWS account to Deep Security Manager" on the next page
2. "Set the communication direction" on the next page
3. "Configure the activation type" on the next page
4. "Launch a 'master' Amazon EC2 instance or Amazon WorkSpace" on the next page
5. "Deploy an agent on the master" on the next page
6. "Verify that the agent was installed and activated properly" on page 194
7. "(Recommended) Set up policy auto-assignment" on page 194
8. "Create an AMI or custom WorkSpace bundle based on the master" on page 195
9. "Use the AMI" on page 195

### Add your AWS account to Deep Security Manager

You'll need to add your AWS accounts to Deep Security Manager. These are the AWS accounts that will contain the Amazon EC2 instances and Amazon WorkSpaces that you want to protect.

See "Add AWS cloud accounts" on page 295 for instructions.

### Set the communication direction

You'll need to set the communication direction: either agent-initiated, manager-initiated, or bidirectional.

See "Install the agent on Amazon EC2 and WorkSpaces" on page 185 > "Set the communication direction" on page 186 for instructions.

### Configure the activation type

You'll need to indicate whether you'll allow agent-initiated activation.

See "Install the agent on Amazon EC2 and WorkSpaces" on page 185 > "Configure the activation type" on page 186 for instructions.

### Launch a 'master' Amazon EC2 instance or Amazon WorkSpace

You'll need to launch a 'master' Amazon EC2 instance or Amazon WorkSpace. The master instance is the basis for the EC2 AMI or WorkSpace bundle that you will create later.

1. In AWS, launch an Amazon EC2 instance or Amazon WorkSpace. See the Amazon EC2 documentation and Amazon WorkSpaces documentation for details.
2. Call the instance 'master'.

### Deploy an agent on the master

You'll need to install and activate the agent on the master. During this process, you can optionally install a policy.

See "Install the agent on Amazon EC2 and WorkSpaces" on page 185 > "Deploy agents to your Amazon EC2 instances and WorkSpaces" on page 190 for instructions.

## Verify that the agent was installed and activated properly

You should verify that the agent was installed and activated properly on the master before proceeding.

See "Install the agent on Amazon EC2 and WorkSpaces" on page 185 > "Verify that the agent was installed and activated properly" on page 190 for instructions.

## (Recommended) Set up policy auto-assignment

You may need to set up policy auto-assignment depending on how you deployed the agent on the master:

- If you used a deployment script, then a policy has already been assigned, and no further action is required.
- If you manually installed and activated the agent, no policy was assigned to the agent, and one should be assigned now so that the master is protected. The Amazon EC2 instances and Amazon WorkSpaces that are launched based on the master will also be protected.

If you want to assign a policy to the master, as well as auto-assign a policy to future EC2 instances and WorkSpaces that are launched using the master, follow these instructions:

1. In Deep Security Manager, create an event-based task with these parameters:
   - Set the **Event** to **Agent-Initiated Activation**.
   - Set **Assign Policy** to the policy you want to assign.
   - (Optional) Set a condition to **Cloud Instance Metadata**, with
     - a **tagKey** of **EC2** and a **tagValue.*** of **True** (for an EC2 instance)
       OR
     - a **tagKey** of **WorkSpaces** and a **tagValue.*** of **True** (for WorkSpaces)

   The above event-based task says:
   *When an agent is activated, assign the specified policy, on condition that* `EC2=true` *or* `WorkSpaces=true` *exists in the Amazon EC2 instance or WorkSpace.*
   If that key/value pair does not exist in the EC2 instance or WorkSpace, then the policy is not assigned (but the agent is still activated). If you do not specify a condition, then

the policy is assigned on activation unconditionally.
For details on creating event-based tasks, see "Automatically assign policies by AWS instance tags" on page 285.

2. If you added a key/value pair in Deep Security Manager in the previous step, do the following:
   a. Go to AWS.
   b. Find your master EC2 instance or WorkSpace.
   c. Add tags to the master with a **Key** of **EC2** or **WorkSpaces** and a **Value** of **True**.
      For details, see this Amazon EC2 documentation on tagging, and this Amazon WorkSpace documentation on tagging.
      You have now set up policy auto-assignment. New Amazon EC2 instances and Amazon WorkSpaces that are launched using the master are activated automatically (since the agent is pre-activated on the master), and then auto-assigned a policy through the event-based task.
3. On the master EC2 instance or WorkSpace, reactivate the agent by re-running the activation command on the agent, or by clicking the **Reactivate** button in Deep Security Manager. For details, see "Activate the agent" on page 219
   The re-activation causes the event-based task to assign the policy to the master. The master is now protected.

You are now ready to bake your AMI or create a custom WorkSpace bundle.

## Create an AMI or custom WorkSpace bundle based on the master

- To create an AMI on Linux, see this Amazon documentation.
- To create an AMI on Windows, see this Amazon documentation.
- To create a custom WorkSpace bundle, see this Amazon documentation.

You now have an AMI or WorkSpace bundle that includes a pre-installed and pre-activated agent.

## Use the AMI

Now that you have a custom AMI or WorkSpace bundle, you can use it as the basis for future Amazon EC2 instances and Amazon WorkSpaces. With the custom AMI or bundle, Deep

Security Agent starts up automatically, activates itself, and applies the protection policy assigned to it. It appears in Deep Security Manager with a **Status** of **Managed** and a green dot next to it.

## Configure communication between components

Generally, communication-related settings only need to be configured once and then rarely changed.


- "Agent-manager communication" below
- "Use agent-initiated communication with cloud accounts" on page 202
- "Connect agents behind a proxy" on page 203
- "Proxy protocols supported by Deep Security" on page 214
- "Proxy settings" on page 214
- "Configure SMTP settings for email notifications" on page 176
- "Manage trusted certificates" on page 216


### Agent-manager communication

Deep Security Manager and the agent communicate using the latest mutually-supported version of TLS.

Topics in this article:


- "Configure the heartbeat" below
- "Configure communication directionality" on page 198
- "Supported cipher suites for agent-manager communication" on page 200


### Configure the heartbeat

A 'heartbeat' is a periodic communication between the Deep Security Manager and agent or appliance. During a heartbeat, the manager collects this information:

- the status of the drivers (on- or off-line)
- the status of the agent or appliance (including clock time)
- agent or appliance logs since the last heartbeat

- data to update counters
- a fingerprint of the agent or appliance security configuration (used to determine if it is up to date)

The heartbeat can be configured on a base or parent policy, on a sub-policy, or on an individual computer.

You can configure the following properties of the heartbeat:

- **Heartbeat Interval:** How much time passes between heartbeats.
- **Number of Heartbeats that can be missed before an alert is raised:** The number of consecutively missed heartbeats that triggers an alert. For example, a value of three causes the manager to trigger an alert on the fourth missed heartbeat.)

  **Note:** If the computer is a server, too many missed heartbeats in a row may indicate a problem with the agent/ or appliance or the computer itself. However if the computer is a laptop or any other system that is likely to experience a sustained loss of connectivity, this setting should be set to "unlimited".

- **Maximum change (in minutes) of the local system time on the computer between heartbeats before an alert is raised:** For agents that are capable of detecting changes to the system clock (Windows agents only) these events are reported to the manager as agent event 5004. If the change exceeds the clock change listed here then an alert is triggered. For agents that do not support this capability, the manager monitors the system time reported by the agent at each heartbeat operation and triggers an alert if it detects a change greater than the permissible change specified in this setting.

  **Note:** Once a **Computer-Clock-Changed** alert is triggered, it must be dismissed manually.

- **Raise Offline Errors For Inactive Virtual Machines:** Sets whether an offline error is raised if the virtual machine is stopped.

1. Open the **Policy editor**[1] or the **Computer editor**[2] for the policy or computer to configure.
2. Go to **Settings > General > Heartbeat.**
3. Change the properties as required.
4. Click **Save** .

### Configure communication directionality

Configure whether the agent or appliance or the manager initiates communication. 'Communication' includes the heartbeat and all other communications. The following options are available:

**Bidirectional:** By default, communications are bidirectional. The agent or appliance normally initiates the heartbeat and also listens on the agent's listening port number for connections from the Deep Security Manager. () The manager can contact the agent or appliance to perform required operations. The manager can apply changes to the security configuration of the agent or appliance.

> **Note:** The Deep Security Virtual Appliance can only operate in bidirectional mode. Changing this setting to any other mode for a virtual appliance will disrupt functionality.

- **Manager Initiated:** The manager initiates all communication with the agent or appliance. These communications include security configuration updates, heartbeat operations, and requests for event logs. If you choose this option, we strongly recommend that you "Protect Deep Security Agent" on page 755 so that it only accepts connections from known Deep Security Managers.
- **Agent/Appliance Initiated:** The agent or appliance does not listen for connections from the manager. Instead they contact the manager on the port number where the Manager listens for agent heartbeats. (See "Deep Security Manager ports" on page 98.) Once the agent or appliance has established a TCP connection with the manager, all normal communication takes place: the manager first asks the agent or appliance for its status and for any events. (This is the heartbeat operation.) If there are outstanding operations that need to be performed on the computer (for example, the policy needs to be updated), these operations

---

[1]To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

[2]To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

are performed before the connection is closed. Communications between the manager and the agent or appliance only occur on every heartbeat. If an agent or appliance's security configuration has changed, it is not updated until the next heartbeat.

**Note:** Before configuring an agent or appliance to initiate communication, ensure that the agent or appliance can reach the manager URL and heartbeat port. If the agent or appliance cannot resolve the manager URL or cannot reach the IP and port, agent- or appliance-initiated communications will fail for this agent or appliance. The Manager URL and the heartbeat port are listed in the **System Details** area in **Administration > System Information** .

**Note:** To enable communications between the Manager and the agents and appliances, the manager automatically implements a (hidden) firewall rule (priority four, Bypass) that opens the listening port number for heartbeats on the agents and appliances to incoming TCP/IP traffic. By default, it will accept connection attempts from any IP address and any MAC address. You can restrict incoming traffic on this port by creating a new priority 4, Force Allow or Bypass firewall rule that only allows incoming TCP/IP traffic from specific IP or MAC addresses, or both. This new firewall rule would replace the hidden firewall rule if the settings match these settings:

**action:** force allow or bypass
**priority:** 4 - highest
**packet's direction:** incoming
**frame type:** IP
**protocol:** TCP
**packet's destination port:** agent's listening port number for heartbeat connections from the Manager, or a list that includes the port number. (See agent listening port number.)

While these settings are in effect, the new rule will replace the hidden rule. You can then type packet source information for IP or MAC addresses, or both, to restrict traffic to the computer.

1. Open the **Policy editor**[1] or the **Computer editor**[2] for the policy or computer to configure.
2. Go to **Settings > General > Communication Direction.**
3. In the **Direction of Deep Security Manager to Agent/Appliance communication** menu, select one of the three options ("Manager Initiated", "agent/appliance Initiated", or "Bidirectional"), or choose "Inherited". If you select "Inherited", the policy or computer inherits the setting from its parent policy. Selecting one of the other options overrides the inherited setting.
4. Click **Save** to apply the changes.

**Note:** Agents and appliances look for the Deep Security Manager on the network by the Manager's hostname. Therefore the Manager's hostname **must** be in your local DNS for agent- or appliance-initiated or bidirectional communication to work.

### Supported cipher suites for agent-manager communication

Deep Security Manager and the agent communicate using the latest mutually-supported version of TLS.

The Deep Security Agent supports the following ciphers for communication with the manager. If you need to know the ciphers supported by the Deep Security Manager, contact Trend Micro.

The ciphers consist of a key exchange asymmetric algorithm, a symmetric data encryption algorithm and a hash function.

Deep Security Agent 9.5 supports these TLSv1.0 ciphers:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Deep Security Agent 9.6 supports these TLSv1.0 ciphers:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

---

[1]To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

[2]To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

Deep Security Agent 10.0 supports these TLSv1.2 ciphers:

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

Deep Security Agent 10.3 supports these TLSv1.2 ciphers:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

Deep Security Agent 11.0 supports these TLSv1.2 ciphers:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

## SSL implementation and credential provisioning

The Deep Security Agent may initiate communication to Deep Security Manager or it may be contacted by the manager if the computer object is set to operate in bi-directional mode. Deep Security Manager treats all connections to agents in a similar way. If the agent has not been activated, a limited set of interactions are possible. If the agent has been activated (either by an administrator or via the agent-initiated activation feature), the full set of interactions are enabled. The Deep Security Manager acts as an HTTP client in all cases, regardless of whether it was the client when forming the TCP connection. Agents cannot ask for data or initiate operations themselves. The manager requests information such as events and status, invokes operations, or pushes configuration to the agent. This security domain is highly controlled to ensure that agents have no access to Deep Security Manager or its host.

Both agent and manager use two different security contexts to establish the secure channel for HTTP requests:

1. Before activation, the agent accepts the bootstrap certificate to form the SSL or TLS channel.
2. After authentication, mutual authentication is required to initiate the connection. For mutual authentication, the manager's certificate is sent to the agent and the agent's certificate is sent to the manager. The agent validates that the certificates come from the same certificate authority (which is the Deep Security Manager) before privileged access is granted.

Once the secure channel is established, the agent acts as the server for the HTTP communication. It has limited access to the manager and can only respond to requests. The secure channel provides authentication, confidentiality through encryption, and integrity. The use of mutual authentication protects against man-in-the-middle (MiTM) attacks where the SSL communication channel is proxied through a malicious third party. Within the stream, the inner content uses GZIP and the configuration is further encrypted using PKCS #7.

## Use agent-initiated communication with cloud accounts

If any of the computers you are protecting with Deep Security are in cloud accounts, we recommend that you use agent-initiated communication to prevent communication issues between the Deep Security Manager and agents.

If you are using Deep Security as a Service, agent-initiated communication is enabled by default. The full list of Deep Security default communication direction settings is as follows:

| | |
|---|---|
| Deep Security | bidirectional |
| Deep Security AMI from AWS Marketplace | bidirectional |
| Deep Security as a Service | Agent-initiated |

To use agent-initiated communication, you must first enable it on a policy, and then assign that policy to a deployment script.

### Enable agent-initiated communication on the policy

You can enable agent-initiated communication by either modifying an existing policy or by creating a new one.

**Tip:** You can quickly create a new policy from an existing policy by right-clicking it and selecting **Duplicate**.

1. On the **Policies** page, double-click the policy.
2. Go to **Settings** > **General**.
3. Under Communication Direction, select **Agent/Appliance Initiated**.
4. Click **Save**.

### Assign the policy to a deployment script

1. In the upper-right corner, click **Support** > **Deployment Script**.
2. Select your platform from the list.
3. Select **Activate Agent automatically after installation**, and then select your policy from the list.
4. Click **Close**.

To learn how to use deployment scripts to apply protection to your computers, see "Use deployment scripts to add and protect computers" on page 281.

## Connect agents behind a proxy

To protect computers that require a proxy to access the Internet, Deep Security Manager, or relays, you need to configure Deep Security Manager with the proxy's address. It will give this information to agents. (Alternatively, you can use the CLI to configure proxy settings locally on the agent.)

In this topic:


- "Requirements" below
- "Register the proxy in Deep Security Manager" on the next page
- "Connect agents, appliances, and relays to security updates via proxy" on the next page
- "Connect agents to security services via proxy" on the next page
- "Connect agents to a relay via proxy" on page 205
- "Remove a proxy setting" on page 206
- "Subsequent agent deployments" on page 206


### Requirements

Deep Security Agent 10.0 or later (not GA) is required if connecting agents to a relay or manager via proxy (especially for application control rulesets).

### Register the proxy in Deep Security Manager

1. In Deep Security Manager, go to **Administration** > **System Settings** > **Proxies**.
2. In the **Proxy Servers** area, create a new HTTP proxy by clicking **New** in the menu bar.
3. Enter the protocol, IP Address, port number, user name and password.

### Connect agents, appliances, and relays to security updates via proxy

Alternatively, you can use the command line to configure proxy use instead.

1. Still on the **Proxies** tab, in the **Proxy Server Use** area, change the **Primary Security Update Proxy used by Agents, Appliances, and Relays** setting to point to the new proxy.
2. Click **Save**.

### Connect agents to security services via proxy

1. On Deep Security Manager, click **Policies** at the top.
2. On the left, click **Policies**.
3. In the main pane, double-click the policy that you use to protect computers that are behind the proxy.
4. Set up a proxy to the Global Census, Good File Reputation, and Predictive Machine Learning Services as follows:
   a. Click **Settings** on the left.
   b. In the main pane, click the **General** tab.
   c. In the main pane, look for the **Network Setting for Census and Good File Reputation Service, and Predictive Machine Learning** section.
   d. If the **Inherited** check box is selected, the proxy settings are inherited from the parent policy. To change the settings for this policy or computer, clear the check box.
   e. Select **When accessing Global Server, use proxy** and in the list, select your proxy, or select **New** to specify another proxy.
   f. Save your settings.
5. Set up a proxy to the Smart Protection Network for use with anti-malware:
   a. Click **Anti-Malware** on the left.
   b. In the main pane, click the **Smart Protection** tab.
   c. Under **Smart Protection Server for File Reputation Service**, if the **Inherited** check box is selected, the proxy settings are inherited from the parent policy. To change the settings for this policy or computer, clear the check box.

   d. Select **Connect directly to Global Smart Protection Service**.
   e. Select **When accessing Global Smart Protection Service, use proxy** and in the list, select your proxy or select **New** to specify another proxy.
   f. Specify your proxy settings and click **OK**.
   g. Save your settings.
6. Set up a proxy to the Smart Protection Network for use with web reputation:
   a. Click **Web Reputation** on the left.
   b. In the main pane, click the **Smart Protection** tab.
   c. Under **Smart Protection Server for Web Reputation Service**, set up your proxy, the same way you did under **Anti-Malware** in a previous step.
   d. With **Web Reputation** still selected on the left, click the **Advanced** tab.
   e. In the **Ports** section, select a group of port numbers that includes your proxy's listening port number, and then click **Save**. For example, if you're using a Squid proxy server, you would select the **Port List Squid Web Server**. If you don't see an appropriate group of port numbers, go to **Policies** > **Common Objects** > **Lists** > **Port Lists** and then click **New** to set up your ports.
   f. Save your settings.

Your agents can now connect to Trend Micro security services over the Internet through a proxy.

### Connect agents to a relay via proxy

1. In the top right-hand corner of Deep Security Manager, click **Support** > **Deployment Scripts**.
2. From **Proxy to contact Relay(s)**, select a proxy.
3. Copy the script or save it.
4. Run the script on the computer. You can either do this manually or with a third party deployment system such as Ansible, Chef, Powershell, or others.

## Connect agents to a relay's private IP address

If your relay has an elastic IP address, agents within an AWS VPC may not be able to reach the relay via that IP address. Instead, they must use the private IP address of the relay group.

1. Go to **Administration** > **System Settings**.
2. In the **System Settings** area, click the **Updates** tab.

3. Under **Software Updates**, in the window **Alternate software update distribution server(s) to replace Deep Security Relays** , type:

   ```
   https://<IP>:<port>/
   ```

   where `<IP>` is the private network IP address of the relay, and `<port>` is the relay port number

4. Click **Add**.
5. Click **Save**.

**Note:** If your relay group's private IP changes, you must manually update this setting. It will not be updated automatically.

### Remove a proxy setting

If you've installed an agent with a deployment script that adds proxy settings that you no longer require, you can remove the setting by entering the following commands in a command line:

## Windows

```
>C:\Program Files\Trend Micro\Deep Security\dsa_control -x ""
```

```
C:\Program Files\Trend Micro\Deep Security\dsa_control -y ""
```

## Linux

```
/opt/ds_agent/dsa_control -x ""
```

```
/opt/ds_agent/dsa_control -y ""
```

### Subsequent agent deployments

After your initial deployment, if you add more agents, modify their deployment scripts to use the proxy in the **Deployment Scripts Generator**.

## Configure agents that have no Internet access

If your agents or relays don't have access to the Internet (also called "air-gapped agents"), then they won't be able to access several of the security services provided by the Trend Micro Smart Protection Network. These security services are necessary for the full and successful operation of the Deep Security anti-malware and web reputation features.

These Trend Micro security services are:

| Service name | Required for these features |
|---|---|
| Smart Scan Service | Smart Scan |
| Web Reputation Service | web reputation |
| Global Census Service | behavior monitoring, predictive machine learning |
| Good File Reputation Service | behavior monitoring, predictive machine learning, process memory scans |
| Predictive Machine Learning Service | predictive machine learning |

If the above services can't be reached by the agent or relay-enabled agent, you have several solutions, described below.

### Solutions

- Solution 1: "Use a proxy" below
- Solution 2: "Install a Smart Protection Server locally " on the next page
- Solution 3: "Install a relay and supporting components in your DMZ or Internet-ready area" on page 209
- Solution 4: "Disable the features that use Trend Micro security services" on page 211

### Use a proxy

If your agents or relay-enabled agents can't connect to the Internet, you can install a proxy that can. Your Deep Security Agents and relays connect to the proxy, and the proxy then connects outbound to the Trend Micro security services in the Smart Protection Network.

**Note:** With a proxy, each Smart Scan or web reputation request goes out over the Internet to the Smart Protection Network. Consider instead using a Smart Protection Server inside your LAN to keep these requests within your network and reduce extranet bandwidth usage.

To use a proxy, see "Connect agents behind a proxy" on page 203

### Install a Smart Protection Server locally

If your agents and relay-enabled agents can't connect to the Internet, you can install a Smart Protection Server in your local area network (LAN) to which they *can* connect. The local Smart Protection Server periodically connects outbound over the Internet to the Smart Protection Network to retrieve the latest Smart Scan anti-malware patterns and web reputation information. This information is cached on the Smart Protection Server and disseminated to your agents and relay-enabled agents.

If you decide to use this solution, remember that:

- Only the Smart Scan and web reputation features are supported with a local Smart Protection Server.
- Use the proxy solution if you need the behavior monitoring, predictive machine learning, and process memory scanning features. See "Use a proxy" on the previous page above for details. If you decide not to use these features, you must disable them to prevent a query failure and to improve performance. For instructions on disabling these features, see "Disable the features that use Trend Micro security services" on page 211

To deploy a Smart Protection Server:

- install it manually. See the Smart Protection Server documentation for details.

  OR

- if your agents or relay-enabled agents are inside AWS, install it using an AWS CloudFormation template created by Trend Micro. See "Deploy a Smart Protection Server in AWS" on page 228 for details.

## Install a relay and supporting components in your DMZ or Internet-ready area

If your agents or relay-enabled agents can't connect to the Internet, you can install a relay-enabled Deep Security Agent, Deep Security Manager, and Deep Security Manager's database in your demilitarized zone (DMZ) or another area of your network where Internet access is available. These Deep Security components must be installed *in addition* to your existing air-gapped components.

Once all the components are installed, the relay-enabled agent automatically obtains the latest malware scan updates from the Update Server in the Smart Protection Network. These updates must be extracted to a .zip file, and then manually copied to your air-gapped relay or directly to your air-gapped agents, if you do not have an air-gapped relay. (Detailed instructions follow.)

If you decide to use this solution, remember that:

- The .zip file contains traditional (large) malware patterns, which give you basic anti-malware capabilities.
- The following advanced anti-malware features are *not* available: Smart Scan, behavior monitoring, predictive machine learning, process memory scans, and web reputation. These features all require access to Trend Micro security services.
- You should disable the advanced anti-malware features (Solution 4) since they cannot be used.
- You should have a plan in place to periodically update the .zip file on your air-gapped relay to ensure you always have the latest malware patterns.

To deploy this solution, follow these steps:

1. Install a Deep Security Manager and its associated database in your DMZ. We'll call these Internet-facing components the 'DMZ manager' and 'DMZ database'.
2. Install a Deep Security Agent in your DMZ and configure it as a relay. We'll call this agent the 'DMZ relay'. For information on setting up relays, see "Distribute security and software updates with relays" on page 234.

   The following items are now installed:

- a DMZ manager
- a DMZ database
- a DMZ relay
- an air-gapped manager
- an air-gapped database
- an air-gapped relay
- multiple air-gapped agents

3. On the DMZ relay, create a .zip file containing the latest malware patterns by running this command:

   ```
   dsa_control -b
   ```

   The command line output shows the name and location of the .zip file that was generated.

4. Copy the .zip file to the air-gapped relay, or, if you are not using an air-gapped relay, copy the .zip directly to each of your air-gapped agents. Place the file in the relay or agent's installation directory.
   - On Windows the default directory is `C:\Program Files\Trend Micro\Deep Security Agent`.
   - On Linux the default directory is `/opt/ds_agent`.

   > **Note:** Do not rename the .zip file.

5. On the air-gapped manager, initiate a security update download:
   a. Click **Computers** at the top.
   b. In the list of computers, find your air-gapped relay or agent where you copied the .zip file, right-click it and select **Download Security Update**.

      The air-gapped relay or agent checks its configured update source (typically the Update Server in the Trend Micro Smart Protection Network on the Internet). Since it can't connect to this server, it checks the .zip file in its installation directory. When it finds the .zip file, it extracts it and imports the updates. If an air-gapped relay is used, the updates are then disseminated to the air-gapped agents that are configured to connect to the relay.

   c. Delete the .zip file after the updates are imported to the air-gapped agent or relay.
6. Configure the air-gapped relay to connect to itself instead of the Trend Micro Update Server (to prevent connection error alerts):
   a. Log in to the air-gapped manager.
   b. Click **Administration** on the top.
   c. On the left, click **System Settings**.
   d. In the main pane, click the **Updates** tab.
   e. Under **Primary Security Update Source**, select **Other update source** and enter `https://localhost:[port]` where `[port]` is the configured port number for security updates, by default `4122`.
   f. Click **OK**.
      The air-gapped relay no longer tries to connect to the Update Server in the Trend Micro Smart Protection Network.
7. (Optional but recommended.) To improve performance, "Disable the features that use Trend Micro security services" below.
8. On a periodic basis, download the latest updates to your DMZ relay, zip them up, copy them to your air-gapped relay or agents, and initiate a security update download on the relay (if you're using one).

You have now deployed a Deep Security Manager, associated database and relay in your DMZ from which to obtain malware scan updates.

### Disable the features that use Trend Micro security services

You can disable the features that use Trend Micro security services. Doing so improves performance because the air-gapped agent no longer tries (and fails) to query the services.

> **Note:** Without Trend Micro security services, your malware detection is downgraded significantly, ransomware is not detected at all, and process memory scans are also affected. It is therefore strongly recommended that you use one of the other solutions to allow access to Trend Micro security services. If this is impossible, only then should you disable features to realize performance gains.

- To disable Smart Scans:
  a. Open the **Computer or Policy editor**[1] .
  b. On the left, click **Anti-Malware**.
  c. In the main pane, click **Smart Protection**.
  d. Under **Smart Scan**, deselect **Inherited** (if it is selected) and then select **Off**.
  e. Click **Save**.
- To disable web reputation:
  a. Open the **Computer or Policy editor**[2].
  b. On the left, click **Web Reputation**.
  c. In the main pane, make sure the **General** tab is selected.
  d. From the **Configuration** drop-down list, select **Off**.
  e. Click **Save**.
- To disable Smart Feedback:
  a. In Deep Security Manager, click **Administration** at the top.
  b. Click **System Settings** on the left.
  c. In the main pane, click the **Smart Feedback** tab.
  d. Deselect **Enable Trend Micro Smart Feedback (recommended)**.
  e. Click **Save**.

---

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

- To disable process memory scans:
  a. In Deep Security Manager, click **Policies** at the top.
  b. On the left, expand **Common Objects > Other** and then click **Malware Scan Configurations**.
  c. Double-click a malware scan configuration with a **SCAN TYPE** of **Real-Time**.
  d. On the **General** tab, under **Process Memory Scan**, deselect **Scan process memory for malware**.
  e. Click **OK**.
- To disable predictive machine learning:
  a. Make sure you still have a real-time malware scan configuration open.
  b. On the **General** tab, under **Predictive Machine Learning**, deselect **Enable Predictive Machine Learning.**
  c. Click **OK**.
- To disable behavior monitoring:
  a. Make sure you still have a real-time malware scan configuration open.
  b. On the **General** tab, under **Behavior Monitoring**, deselect both options, namely, **Detect suspicious activity and unauthorized changes (incl. ransomware)** and **Back up and restore ransomware-encrypted files**.
  c. Click **OK**.

Also disable the census and grid queries if you want performance gains. If you leave them enabled, a lot of unnecessary background processing takes place. To disable these queries:

1. Disable the census query:

```
dsm_c -action changesetting -name settings.configuration.enableCensusQuery -value false
```

2. Disable the grid query:

```
dsm_c -action changesetting -name settings.configuration.enableGridQuery -value false
```

## Proxy protocols supported by Deep Security

You can view and edit the list of proxy servers available to you on the Proxies tab on **Administration > System Settings**.

This table lists the proxy protocols supported by Deep Security.

| Traffic Originating From | To Service | HTTP Support | SOCKS4 Support | SOCKS5 Support |
|---|---|---|---|---|
| Manager | Software Updates, CSS, News Updates, Product Registration and Licensing | Yes | No | No |
| Manager | Smart Feedback | Yes | No | Yes |
| Manager | Cloud Accounts | Yes | No | No |
| Manager | Control Manager | Yes | No | No |
| Manager | Deep Discovery Analyzer | Yes | No | No |
| Agents or relays | Manager (activation and heartbeats) | Yes | No | No |
| Agents or relays | Relays (software and security updates) | Yes | Yes | Yes |
| Agents | Network Setting for Census, Good File Reputation, and Predictive Machine Learning | Yes | No | No |
| Agents | Global Smart Protection Server | Yes | No | No |

## Proxy settings

If your network uses a proxy, you can configure Deep Security to use it instead of the default port numbers. Proxy settings are in a few locations.

## Proxy server use

To view and edit the list of available proxies, go to **Administration > System Settings > Proxies**.

- **Primary Security Update Proxy used by Agents, Appliances, and Relays:** Select a proxy server that the Deep Security Relays will use to connect to the **Update Source** specified in the **Relays** area on the **Updates** tab (either a **Trend Micro Update Server** or **Other Update Source**).

  **Note:** By default, **agents and appliances**[1] download anti-malware components of their security updates from Deep Security Relays. However, if agents or appliances cannot connect to their assigned Relays, and the **Allow Agents/Appliances to download Security Updates from this source if Deep Security Relays are not available** option is selected, agents and appliances will also use this proxy.

  **Warning:** In Deep Security Agent 10.0 GM and earlier, agents didn't have support for connections through a proxy to relays. If a ruleset download fails due to a proxy, and if your agents require a proxy to access the relay or manager (including Deep Security as a Service), then you must either:

  - update agents' software (see "Get Deep Security Agent software" on page 177), then configure the proxy
  - bypass the proxy
  - change the application control rulesets relay setting as a workaround

- **Deep Security Manager (Software Updates, CSSS, Product Registration and Licensing):** Select a proxy that the Deep Security Manager will use to connect to Trend Micro to validate your Deep Security licenses, to connect to the Certified Safe Software Service (a feature of the Integrity Monitoring module), and for connecting to Amazon Web Services (AWS) and VMware vCloud Cloud Accounts.

  **Note:** Changes to the proxy settings for CSSS will not take effect until the Deep Security Manager and all Manager nodes are restarted. (You must restart the services manually.)

---

[1] The Deep Securty Agent and Deep Security Virtual Appliance are the components that enforce the Deep Security policies that you have defined. Agents are deployed directly on a computer. Appliances are used in VMware vSphere environments to provide agentless protection. They are not available with Deep Security as a Service.

- **Deep Security Manager (Cloud Accounts - HTTP Protocol Only):** Select a proxy for Deep Security Manager to use when connecting to cloud-based instances that have been added to Deep Security Manager using the "Add Cloud Account" procedure.

**Note:** After you select a proxy, restart agents that must use it.

### Proxy servers

Define the proxy servers that will be available for use by various Deep Security clients and services (for example, the proxy servers for Smart Protection on **Computer or Policy editor**[1] > **Anti-Malware > Smart Protection**).

The table lists the proxy protocols supported by the Deep Security services and clients:

| Service | Origin | HTTP Support | SOCKS4 Support | SOCKS5 Support |
|---|---|---|---|---|
| Software Updates, CSS, News Updates, Product Registration and Licensing | Manager | Yes | No | No |
| Smart Feedback | Manager | Yes | No | Yes |
| Cloud Accounts | Manager | Yes | No | No |
| Control Manager | Manager | Yes | No | No |
| Deep Discovery Analyzer | Manager | Yes | No | No |
| Manager (activation and heartbeats) | Agents/Relays | Yes | No | No |
| Relays (software and security updates) | Agents/Relays | Yes | Yes | Yes |
| Network Setting for Census, Good File Reputation, and Predictive Machine Learning | Agents | Yes | No | No |
| Global Smart Protection Server | Agents | Yes | No | No |

## Manage trusted certificates

Trusted certificates are used for code signing and SSL connections to external services such as a Microsoft Active Directory or VMware vCenter.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

## Import trusted certificates

**Note:** If you are importing a trusted certificate to establish trust with an Amazon Web Services region, you must use the `dsm_c` command-line tool.

**To import trusted certificates using the Deep Security Manager:**

1. In the Deep Security Manager, go to **Administration** > **System Settings** > **Security**.
2. Under **Trusted Certificates**, click **View Certificate List** to view a list of all security certificates accepted by Deep Security Manager.
3. Click **Import From File** to start the Import Certificate wizard.

**To import a trusted certificate using dsm_c:**

1. On the Deep Security Manager server, run the following command:

   ```
   dsm_c -action addcert -purpose PURPOSE -cert CERTFILE
   ```

   where the parameters are:

| Parameter | Description | Sample value |
|---|---|---|
| PURPOSE | What type of connections the certificate will be used for. This value must be selected from one of the sample values listed on the right. | `AWS` - Amazon Web Services |
| | | `DSA` - code signing |
| | | `SSL` - SSL connections |
| CERTFILE | The (user-defined) name of the file containing the certificate you want to import. | `/path/to/cacert.pem` |

**Note:** If you are running the Deep Security Manager in a Linux environment, you will need to run the `dsm_c` command as the root user.

## View trusted certificates

**Note:** To view trusted certificates for Amazon Web Services connections, you must use the `dsm_c` command-line tool.

**To view trusted certificates using the Deep Security Manager:**

1. In the Deep Security Manager, go to **Administration** > **System Settings** > **Security**.
2. Under **Trusted Certificates**, click **View Certificate List**.

**To view trusted certificates using dsm_c:**

1. On the Deep Security Manager server, run the following command:

   ```
   dsm_c -action listcerts [-purpose PURPOSE]
   ```

   The `-purpose PURPOSE` parameter is optional and can be omitted to see a list of all certificates. If you specify a value for `PURPOSE`, then only the certificates used for that purpose will be shown.

| Parameter | Description | Sample value |
|---|---|---|
| PURPOSE | What type of connections the certificate will be used for. | `AWS` - Amazon Web Services |
| | | `DSA` - code signing |
| | | `SSL` - SSL connections |

**Note:** If you are running the Deep Security Manager in a Linux environment, you will need to run the `dsm_c` command as the root user.

## Remove trusted certificates

**Note:** To remove trusted certificates for Amazon Web Services connections, you must use the `dsm_c` command-line tool.

**To remove a trusted certificate using the Deep Security Manager:**

1. In the Deep Security Manager, go to **Administration** > **System Settings** > **Security**.
2. Under **Trusted Certificates**, click **View Certificate List**.
3. Select the certificate you want to remove and click **Delete**.

**To remove a trusted certificate using dsm_c:**

1. Log in to Deep Security Manager .
2. Run the following command:

   ```
   dsm_c -action listcerts [-purpose PURPOSE]
   ```

   The `-purpose PURPOSE` parameter is optional and can be omitted to see a list of all

certificates. If you specify a value for `PURPOSE`, then only the certificates used for that purpose will be shown.

| Parameter | Description | Sample value |
|---|---|---|
| PURPOSE | What type of connections the certificate will be used for. | `AWS` - Amazon Web Services |
| | | `DSA` - code signing |
| | | `SSL` - SSL connections |

3. Find the `ID` value for the certificate you want to remove in the list.
4. Run the following command:

```
dsm_c -action removecert -id ID
```

The `ID` parameter value is required.

| Parameter | Description | Sample value |
|---|---|---|
| ID | The ID value assigned by Deep Security Manager for the certificate you want to delete. | `3` |

**Note:** If you are running the Deep Security Manager in a Linux environment, you will need to run the `dsm_c` commands as the root user.

### If I have disabled the connection to the Smart Protection Network, is any other information sent to Trend Micro?

When Smart Protection Network is disabled, the Deep Security Agents will not send any threat intelligence information to Trend Micro.

## Activate the agent

Before the installed agent can protect its computer or be converted to a relay, you must activate the agent with Deep Security Manager. Activation registers the agent with the manager during an initial communication. To do this, you can either:

- Activate the agent from the manager. Go to **Computers**, right-click the computer whose agent you want to activate or reactivate and select **Actions > Activate/Reactivate**.

(Alternatively, click **Activate** or **Reactivate** in the computer's **Details** window.)

- Activate the agent on the agent. Run this command:
  `dsa_control -a dsm://<dsm_host_or_IP>:<port>/`
  where:
  `<dsm_host_or_IP>` is replaced with the Deep Security Manager hostname or IP address, and
  `<port>` is replaced with the Deep Security Manager heartbeat port, which is 4120, by default.
  For details on this command, see "Command-line basics" on page 244.
- Activate the agent through a deployment script. See "Use deployment scripts to add and protect computers" on page 281 for details.
- Activate the agent through an event-based task ("Computer Created (by System)" event) to automatically activate computers when they connect to the manager or when the manager syncs with an LDAP directory, cloud account, or vCenter. For more information, see "Automatically perform tasks when a computer is added or changed" on page 266.

Before activation, the agent will have one of these statuses:

- **No Agent:** Indicates one of the following situations:
  - No agent is running or listening on the default port.
  - An agent is installed and running but is working with another manager and communications are configured as agent-initiated. In this case, the agent is not listening for this manager. To correct this situation, deactivate the agent from the computer.
- **Activation Required:** The agent is installed and listening, and is ready to be activated by the manager.
- **Reactivation Required:** The agent is installed and listening and is waiting to be reactivated by the manager.
- **Deactivation Required:** The agent is installed and listening, but has already been activated by another manager.
- **Unknown:** The computer has been imported (as part of an imported Computers list) without state information, or has been added by way of an LDAP directory discovery process.

After a successful activation, the agent state is Online. If the activation failed, the computer status is Activation Failed with the reason for the failure in brackets. Click this link to display the system event for more details on the reason for the activation failure.

**Note:** Although IPv6 traffic is supported by Deep Security 8.0 and earlier agents, it is blocked by default. To allow IPv6 traffic on Deep Security 8.0 Agents, open a **Computer or Policy editor**[1] and go to **Settings > Advanced > Advanced Network Engine Settings**. Set the **Block IPv6 for 8.0 and Above Agents** option to **No**.

## Deactivate the agent

If you want to transfer control of a computer from one Deep Security Manager installation to another, you must deactivate the agent with its current manager, and then re-activate it with the new manager.

You can normally deactivate the agent from the Deep Security Manager that is currently managing the agent. If the Deep Security Manager cannot communicate with the agent, you may have to perform the deactivation manually. To run the commands below, you must have administrator privileges on the local machine.

**To deactivate the agent on Windows:**

1. From a command line, change to the agent directory (Default is C:\Program Files\Trend Micro\Deep Security Agent)
2. Run the following: **dsa_control -r**

**To deactivate the agent on Linux:**

1. Run the following: **/opt/ds_agent/dsa_control -r**

## Stop or start the agent

**To start or stop the agent on Windows:**

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

- Stop: from the command line, run the following: **sc stop ds_agent**
- Start: from the command line, run the following: **sc start ds_agent**

**To start or stop the agent on Linux:**

- Stop: run the following: **/etc/init.d/ds_agent stop**
- Start: run the following: **/etc/init.d/ds_agent start**

### Stop or start the appliance

Stopping or starting the appliance can only be done locally on the host computer.

**To start or stop the appliance on Linux:**

## Diagnose problems with agent deployment (Windows)

If a Deep Security Agent on Windows fails to install or activate, look in the deployment logs to find the cause and troubleshoot it.

1. Log in to the computer where you were trying to install the agent.
2. Go to `%appdata%\Trend Micro\Deep Security Agent\installer`.
3. Examine:
    - **dsa_deploy.txt** - Log from the PowerShell script. Contains agent activation issues.
    - **dsa_install.txt** - Log from the MSI installer. Contains agent installation issues.

## Configure teamed NICs

"Teamed NICs" or "link aggregation" describes forming a network link on a computer by using multiple network interface cards (NICs) together. This is useful to increase the total network bandwidth, or to provide link redundancy.

You can configure teamed NICs on Windows so that they are compatible with Deep Security Agent.

On Windows, when you team NICs, it creates a new master virtual interface. This virtual interface adopts the MAC address of its first teamed physical interface.

By default, during installation or upgrade, the Windows Agent will bind to *all* virtual and physical interfaces. This includes the virtual interface created by NIC teaming. However, Deep Security Agent doesn't function properly if multiple interfaces have the same MAC address, which happens with NIC teaming on Windows

To avoid that, bind the agent *only* to the teamed virtual interface - *not* the physical interfaces.

**Note:** NIC teaming with Deep Security Agent requires Windows 2003 requires SP 2 or later.

**Warning:** Don't add or remove network interfaces from a teamed NIC *except* immediately before running the installer. If you do that, network connectivity may fail or the host computer may not be correctly detected. The agent's network driver is bound to network interfaces when you install or upgrade; the agent does not continuously monitor for changes after.

## Agent settings

Agent settings are located on **Administration > System Settings > Agents**.

**Tip:** You can automate Agent-related system setting changes using the Deep Security API. For examples, see the Configure Policy, Computer, and System Settings guide.

### Hostnames

**Update the "Hostname" entry if an IP is used as a hostname and a change in IP is detected on the computer after Agent/Appliance-initiated communication or discovery:** Updates the IP address displayed in the computer's "Hostname" property field if an IP change is detected.

**Note:** The Deep Security Manager always identifies computers by using a unique fingerprint, not their IP addresses or hostnames.

### Agent-Initiated Activation

**Note:** For more information on Agent-Initiated Activation, see Command-Line Utilities and "Use deployment scripts to add and protect computers" on page 281.

**Allow Agent-Initiated Activation**

- **For Any Computers:** Any computers, whether they are already listed on the Deep Security Manager's **Computers** page or not.
- **For Existing Computers:** Only computers already listed on the **Computers** page.
- **For Computers on the following IP List:** Only computers whose IP address has a match on the specified IP List.

**Policy to assign (if Policy not assigned by activation script):** The security policy to assign to the computer if no policy has been specified in the activation script.

> **Note:** If an event-based task exists which assigns policies to computers where activation is agent-initiated, the policy specified in the event-based task will override the policy assigned here or in the activation script.

**Allow Agent to specify hostname**: Select this option to allow the agent to specify the hostname by providing it to the Deep Security Manager during the agent activation process.

**If a computer with the same name already exists:** If a computer, VMware virtual machine, AWS instance, or Azure VM with the same Agent GUID or certificate is already listed on the **Computers** page, you can configure the Deep Security Manager to take the following actions:

- **Do not allow activation**: The computer object will not be activated.
- **Activate a new Computer with the same name**: The Deep Security Manager will create a new computer object with a new name.
- **Re-activate the existing Computer**: The existing computer object will be re-activated.

**Reactivate cloned Agents:** When a new computer (computer, VMware virtual machine, AWS instance, or Azure VM) that is running an already activated Deep Security Agent sends a heartbeat to the Deep Security Manager, the Deep Security Manager will recognize it as a clone. It will be reactivated as a new computer without the policies or rules of the original computer .

**Reactivate unknown Agents:** Select this setting to allow activated computers that were deleted from Deep Security Manager to reactivate if they reconnect.

> **Note:** When a removed computer reconnects, it will not have a policy, and will be added as a new computer. Any direct links to the computer will be removed from the Deep Security Manager event data.

**Agent activation token:** When a value is specified here, the same value must be provided when agents activate themselves in the Deep Security Manager. You can provide this agent activation secret in the **token** parameter in the agent activation script. For example, the script for agent-initiated activation on a Linux machine might look like this:

```
/opt/ds_agent/dsa_control -a dsm://172.31.2.247:4120/ "token:secret"
```

> **Note:** In a multi-tenant environment, the **Agent activation token** setting applies only to the primary tenant.

### Data Privacy

**Allow packet data capture on encrypted traffic (SSL):** The Intrusion Prevention module allows you to record the packet data that triggers Intrusion Prevention Rules. This setting lets you turn on data capture when Intrusion Prevention rules are being applied to encrypted traffic.

### Agentless vCloud Protection

**Allow Appliance protection of vCloud VMs:** Allow virtual machines in a vCloud environment to be protected by a Deep Security Virtual Appliance and let the security of those virtual machines be managed by tenants in a multi-tenancy Deep Security environment.

## Linux Secure Boot support for agents

When Linux Secure Boot is enabled on a Deep Security Agent computer, the Linux kernel performs a signature check on kernel modules before they are installed. These Deep Security features install kernel modules:

- anti-malware
- web reputation
- firewall
- intrusion prevention
- application control

> **Note:** The Deep Security Agent is only compatible with Secure Boot on RHEL 7.

If you intend to use any of those modules on a Linux computer where Secure Boot is enabled, you must enroll the Trend Micro public key for RHEL 7 (provided during install as DS11.der) into the Linux computer's firmware so that it recognizes the Trend Micro kernel module's signature. Otherwise, the kernel module can't be installed.

**Note:** Deep Security refreshes the kernel module signing key in every major release (for example, 10.0 and 11.0). To keep security features functioning when you upgrade a Deep Security Agent to a new major release, you must enroll the new public key into any Linux computers that have Secure Boot enabled. You may see "Engine Offline" error message in the Deep Security Manager console because the operating system will not load the upgraded kernel module until the new public key is enrolled.

Use the Unified Extensible Firmware Interface (UEFI) Secure Boot feature to enroll the public key. If you are protecting VMware virtual machines, the Secure Boot feature is available for VMware vSphere 6.5 or newer. For instructions on how to enable it, see Enable or Disable UEFI Secure Boot for a Virtual Machine on the VMware Docs site.

**Note:** The Secure Boot feature is not available for AWS instances and Azure VMs.

To enroll the Trend Micro public key:

1. On the RHEL 7 computer that you want to protect, install the Deep Security Agent, if it isn't installed already.

   After installation, the Trend Micro public key is in `/opt/ds_agent/DS10.der`.

2. Install the Machine Owner Key (MOK) facility, if it isn't already installed

   ```
   yum install mokutil
   ```

3. Add the public key, `DS10.der`, to the MOK list:

   ```
   mokutil --import DS10.der
   ```

   **Note:** For details about manually adding the public key to the MOK list, see the Red Hat documentation.

4. When prompted, enter a password that you will use later in this procedure.
5. Reboot the system.

6. After the computer restarts, the Shim UEFI key management console opens:

7. Press any key to get started.
8. On the **Perform MOK management** screen, select **Enroll MOK**.
9. On the **Enroll MOK** screen, select **View key 0**.
10. On the **Enroll the key(s)?** screen, select **Yes** and then enter the password you set in step 4, above.
11. On the **The system must now be rebooted** screen, select **OK** to confirm your changes and reboot.
12. Next, use the `keyctl` utility to check that key is on the system key ring. If the `keyctl` utility is not already installed, use this command to install it:

    ```
    yum install keyutils
    ```

13. To list the keys that are on the system key ring:

    ```
    keyctl list %:.system_keyring
    ```

    You should see the Trend Micro signing key listed.

# Deploy a Smart Protection Server in AWS

If you have Deep Security Agents in AWS, and you want them to be able to access Trend Micro's Smart Protection Network, then you must allow them to connect to the Internet on port 80 (HTTP) or 443 (HTTPS). (See "Port numbers" on page 96.) If this is not possible, you can deploy your own Smart Protection Server (SPS) within your Virtual Private Network (VPC) in AWS, or another VPC. The Smart Protection Server connects outbound to the Smart Protection Network to retrieve the latest anti-malware, file reputation, and web reputation information and then passes this information along to your agents.

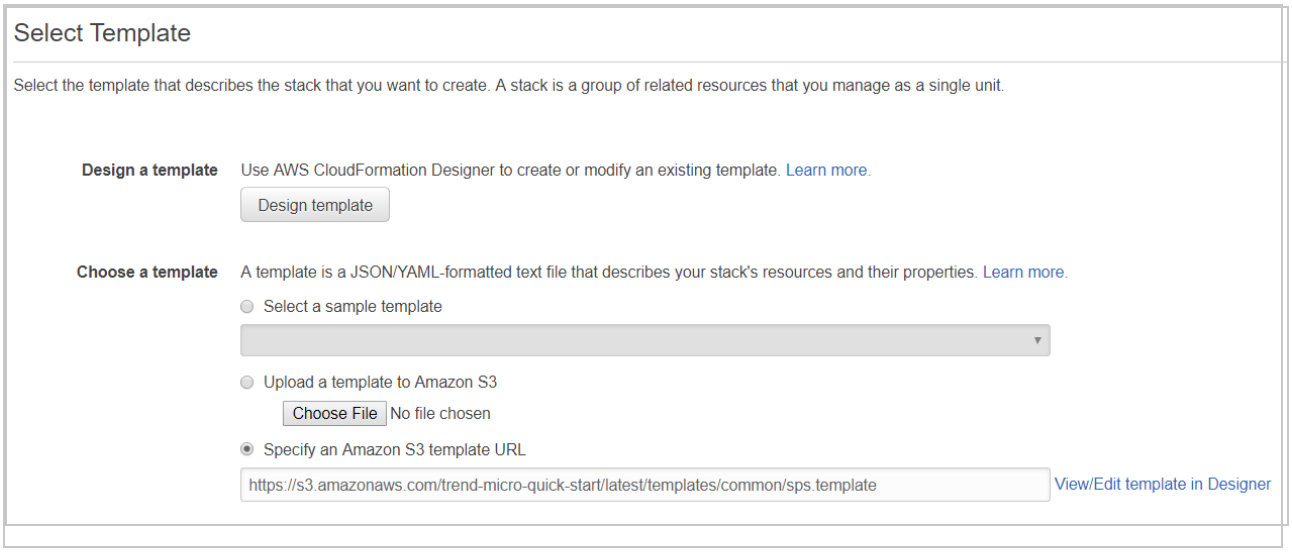
To deploy a Smart Protection Server in AWS, you can either:

- use an AWS CloudFormation template created by Trend Micro . This is the easiest way to deploy the server because the configuration is automated.
- install it manually. See the Smart Protection Server documentation for details.

The instructions below describe how to deploy the Smart Protection Server using the CloudFormation template.

1. In AWS, at the top, click **Services** and search for the **CloudFormation** service.
2. On the **CloudFormation** service page, click **Create Stack**.

   The **Select Template** page appears.



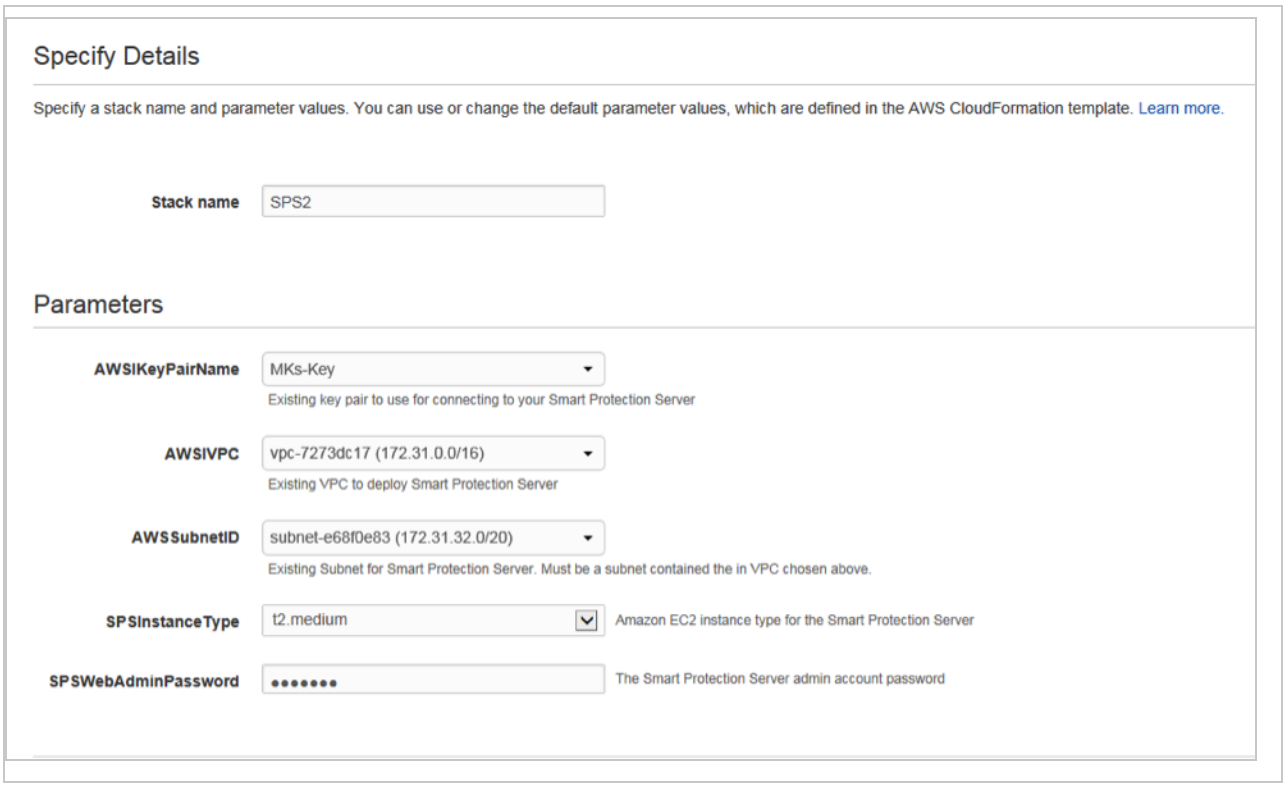
3. Select **Specify an Amazon S3 template URL** and enter this URL into the underlying field:

   `https://s3.amazonaws.com/trend-micro-quick-start/latest/templates/common/sps.template`

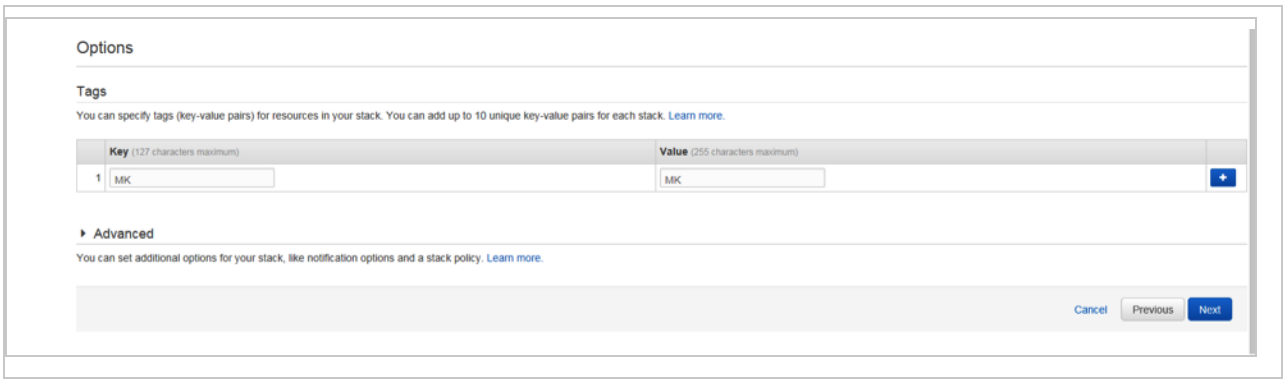
4. Click **Next**.

   Finish entering settings in the template. Choose the AWS key pairs you would like to use to authenticate to the server, the VPC and subnet where the Smart Protection Server will reside, and an administrator password. The password cannot contain special characters such as: !@#$%^&*()

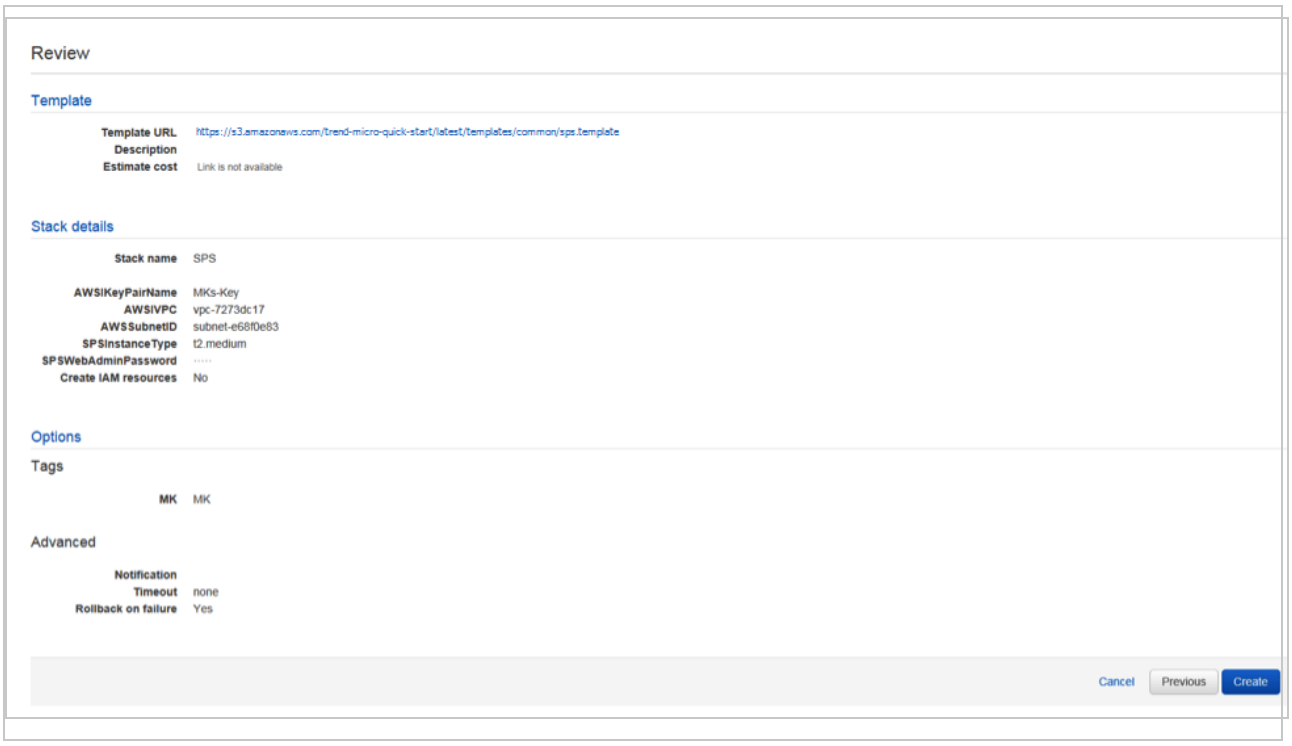
   **Warning:** Do not enter a password that contains dictionary words. It should be at least 8 characters in length. Failure to do this will result in a weak password that is vulnerable to guessing and brute force attacks, and could compromise the security of your network.



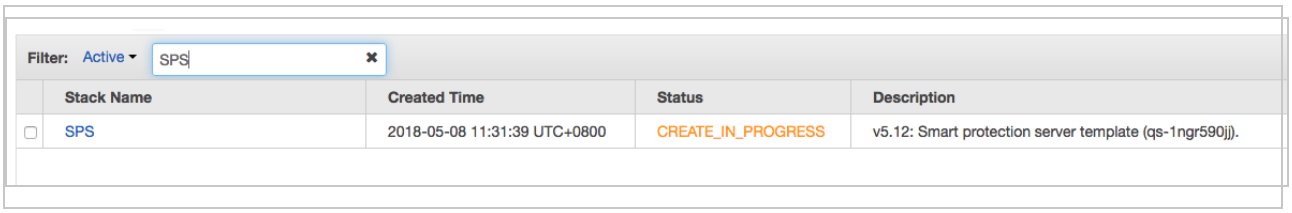

5. Click **Next**.
6. Optionally, create any tags that you would like to associate with this server, then click **Next**.

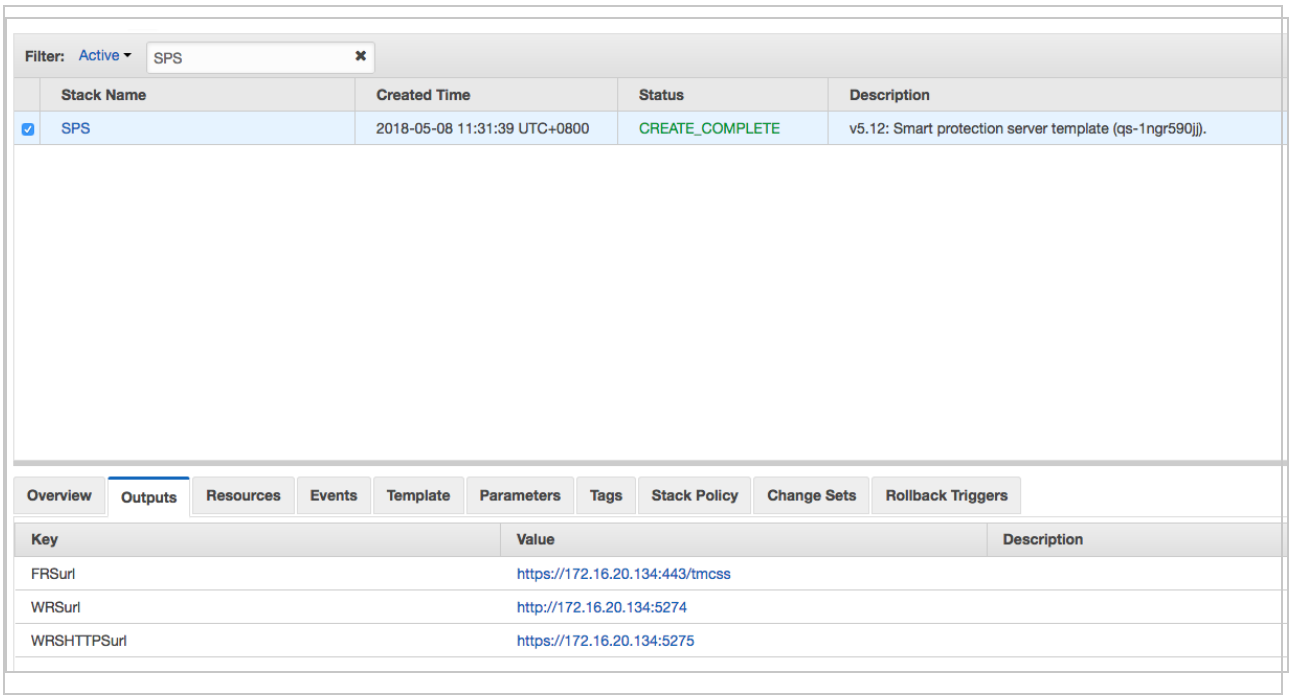



7. Review your settings, and then click **Create**.




While your server is being installed, the screen will indicate progress. To verify that the process has completed, you may need to click **Refresh** at the top of the screen.




8. After it is done creating, click the **Outputs** tab at the bottom of the screen. You see three URLS. In the Deep Security Manager's GUI, you must configure your computers to use the Smart Protection Server.
9. Log in to Deep Security Manager.
10. At either the policy level (recommended method) or at the computer level, go to the anti-malware section.
11. Click the Smart Protection tab at the top. Toward the bottom of the screen, deselect **Inherited** under **Smart Protection Server for File Reputation Service**.
12. Select **Use locally installed Smart Protection Server**.
13. Enter in the URL from the **Outputs** screen in your AWS console labeled "FRSurl" and click **Add**.
14. Click **Save**.
15. Open the web reputation section of the policy or computer and click the **Smart Protection** tab at the top.

16. Deselect **Inherited** under **Smart Protection Server for Web Reputation Service**.
17. Select **Use locally installed Smart Protection Server**.
18. Add the URL from the **Outputs** screen in your AWS console labeled "WRSurl" or "WRSHTTPSurl" and click **Add**. You can use the HTTP or HTTPS URL, but HTTPS is only supported with 11.0 Deep Security Agents and up.
19. Click **Save**.
20. If you don't have your system set up to automatically send policies, you will need to manually send the policy from your Deep Security Manager.

# Create an Azure app for Deep Security

In your operating environment, it may not be desirable to allow the Deep Security Manager to access Azure resources with an account that has both the Global Administrator role for the Azure Active Directory and the Subscription Owner role for the Azure subscription. As an alternative, you can create an Azure app for the Deep Security Manager that provides read-only access to Azure resources.

**Note:** To create an Azure app, your account must have been assigned the User Administrator role for the Azure Active Directory and the User Access Administrator role for the Azure subscription.

To do this you will need to:

1. "Record the Azure Active Directory ID" below.
2. "Create the Azure app" on the next page.
3. "Record the Azure app ID and password" on the next page.
4. "Record the Subscription ID" on the next page.
5. "Assign the Azure app a reader role and add it to your Azure Subscription" on page 234.

## Record the Azure Active Directory ID

1. On the Hub menu, click **Azure Active Directory** and select your Azure Active Directory.
2. In the **Azure Active Directory** blade, click **Properties**.
3. Record the **Directory ID**.

## Create the Azure app

1. In the **Azure Active Directory** blade, click **App registrations**.
2. Click **Add**.
3. Enter a **Name** (for example, Deep Security Azure Connector).
4. For the **Application Type**, select **Web app/API**.
5. Enter a **Sign-on URL**. The URL can be any value, but it must begin with the `http` prefix.

   **Note:** You must enter a URL in the **Sign-on URL** field, even though it is not used by Deep Security Azure integration. The value does not need to resolve to a valid address.

6. Click **Create**.The **Deep Security Azure Connector** app will appear in the **App registrations** list.

## Record the Azure app ID and password

1. In the **App registrations** list, click on the **Deep Security Azure Connector**.
2. Record the **Application ID**.
3. Click on **All settings**.
4. On the **Settings** blade, click **Keys**.
5. Enter a **Description** for the key.
6. Select an appropriate **Duration**.
7. Click **Save**.

   The key **Value** will appear.

8. Record the key **Value**. This will be used as the Application Password when registering the Azure app with Deep Security.

## Record the Subscription ID

1. On the Hub menu, go to **All Services** and click **Subscriptions**, then select the subscription you added the Deep Security Azure Connector app to.
2. Record the **Subscription ID**.

### Assign the Azure app a reader role and add it to your Azure Subscription

1. In the **Subscriptions** blade, click on **Access Control (IAM)**.
2. Click **Add**.
3. Click on the **Reader** role.
4. Select the **Deep Security Azure Connector** app. If it is not already in the list, enter it in the search field and select it when it appears.
5. Click **OK**.

You can now continue configuring Deep Security to add Azure virtual machines by following the remaining steps of the Advanced procedure in "Add a Microsoft Azure account to Deep Security" on page 311.

## Distribute security and software updates with relays

To ensure maximum protection for your Deep Security deployment, there are two components that you must periodically update. **Software updates** add new features and improvements to the Deep Security Agent, while **security updates** provide immediate protection against emerging threats.

Deep Security **relays** help to optimize the distribution of these updates. A relay is an agent that is capable of distributing the software and security updates to other agents . Relays can:

- Reduce WAN bandwidth costs by shaping update traffic.
- Provide redundancy to update distribution.

> **Note:** Relays are a mandatory part of aDeep Security deployment. Your deployment must include at least 1 relay.

First learn about "How relays work" on the next page, then how to "Determine the number of relays to use" on the next page, and finally how to "Configure one or more relays" on page 237.

You can also "Remove relay functionality from an agent" on page 241 if needed.

## How relays work

Relays download security updates from the Trend Micro Active Update servers directly through your WAN connection, and software updates from the Deep Security Manager. When you use relays, security and software updates only need to be downloaded once through your WAN connection. Relays then function as update distribution centers and the security and software updates are downloaded by other agents when they are directed to do so by the Deep Security Manager.

**Note:** If a relay cannot connect to a Deep Security Manager to download updates, it will download them directly from the Deep Security Download Center.

For more detailed information on security updates and how relays distribute them, see "Get and distribute security updates" on page 743.

Relays are organized into **relay groups**. Organizing relays into groups ensures that the update load is distributed across multiple relays, and also adds redundancy to your Deep Security deployment.

Relay groups can also be part of a distribution hierarchy. By creating distribution hierarchies for your relay groups, you can further improve performance and bandwidth usage by specifying:

- Which relay groups an agent should download security and software updates from.
- The order that relay groups should download security and software updates from each other.

## Determine the number of relays to use

Although a Deep Security deployment requires a minimum of 1 relay, as a baseline Trend Micro recommends using at least 2 relays for your deployment. However, you may need to use additional relays depending on:

- "Geographic region of agents " on the next page.
- "Network configuration " on the next page.
- "Network bandwidth usage " on the next page.

### Geographic region of agents

Trend Micro recommends that agents download updates from a relay group in the same geographic region. If you have agents in multiple regions, each region should have its own relay group with at least one relay.

### Network configuration

Your network configuration may include a low bandwidth WAN connection, routers, firewalls, or proxies between the network segments of agents and a remote Deep Security Manager or Trend Micro Active Update server. These configurations may cause bottlenecks that slow down the distribution of software and security updates. To reduce the impact of these configurations, you should place a relay inside each network segment.

### Network bandwidth usage

The download of security and software updates to the agents can be network intensive. You can use relays to shape how your network bandwidth is used to distribute updates. By placing a relay inside a network segment, it becomes the single download source for security and software updates for that segment. Agents will then update from the local relay, reducing the overall bandwidth required to download updates from the WAN connection to the local internal connection.

## Sizing recommendations

**Note:** Before you enable more relays, check that the computers that you want to enable as relays meet the requirements in "Deep Security Agent and Relay sizing" on page 96. Also check that the agent you are using supported the relay feature (see "Supported features by platform" on page 77).

In most deployments, Trend Micro recommends deploying a minimum of 2 relays for redundancy, which can be co-located with a Deep Security Manager. However, as noted above, you should also consider factors such as geographical location, network configuration and network bandwidth when determining how many relays to deploy. If your deployment has a large number of agents (more than 10,000), relays should be deployed on a dedicated system.

You might also want to add more relays if:

- The network configuration of your environment has changed.
- You want to provide additional redundancy to update distribution.

**Warning:** You should **only use as many relays as is necessary**, because deploying unneeded relays on your network will actually decrease performance. A relay requires more system resources than an ordinary agent.

## Configure one or more relays

To configure a relay, you need to:

1. "Create one or more relay groups" below.
2. "Enable one or more relays" on page 239.
3. "Assign agents to a relay group" on page 239.
4. "Configure relay settings for security and software updates" on page 240.

### Create one or more relay groups

Every relay must belong to a relay group. If you installed the Deep Security Relay during the Deep Security Manager installation, a default relay group will have been automatically created. You can also create additional relay groups.

**Note:** Each agent will try to download updates from a randomly arranged list of the relays in the group it is assigned to. If there's no response from a particular relay, the agent will try another from the list until it can successfully download the update. The list is random for each agent so that the update load is shared evenly across relays in a group.

1. Go to **Administration > Updates > Relay Management**.
2. On the Relay Management window, click **New Relay Group**. In the Relay Group Properties pane that appears, configure the settings for the relay group:
   - Enter a **Name** for the relay group.
   - Select an **Update Source**. The update source determines where the relay group will download and distribute security updates from. The update source can be either:
     - The Primary Security Update Source
       By default, the Primary Security Update Source is the Trend Micro Active Update

servers, but you can configure it to be a local mirror instead. A default relay group will always use the Primary Security Update Source. For more information, see "Configure a security update source and settings" on page 745.

- A parent relay group
  If you have already created other relay groups, you can configure a relay group to use one of them as the update source.

**Tip:** When selecting an update download source for a relay group, you should select the source that best matches your cost and speed requirements. Even if a relay group is part of a distribution hierarchy, it does not necessarily need to download updates from a relay in a parent group if downloading updates from the Primary Security Update Source would be cheaper or faster.

**Tip:** To improve performance in very large deployments, create multiple relay groups and arrange relays in a hierarchy: one or more first-level relay groups download updates directly from the Trend Micro Active Update servers, and then second-level relay groups download updates from the first-level group, and so on. However, each group level adds latency, and if there are too many levels of relay groups, the total latency can be greater than the bandwidth optimization provided by relays, resulting in decreased performance.

- Select the **Update Source Proxy** (if any) that relays must use to access the primary security update source.

  Every relay group can be configured to download security updates through a proxy server, except the Default Relay Group. The Default Relay Group uses the same proxy as Deep Security Manager. See "Connect agents behind a proxy" on page 203 and "Configure a proxy for anti-malware and rule updates" on page 257 (CLI).

  If the relay group is configured to use the Primary Security Update Source, relays will use this proxy. Otherwise, if this relay group is configured to download security updates from another relay group, relays won't use the proxy unless they can't connect to the parent relay group, and therefore are trying to connect to the Primary Security Update Source.

> **Warning:** Deep Security Agents version 10.0 and earlier do not have support for connections through a proxy to relays. If an application control ruleset download fails due to a proxy, and if your agents require a proxy to access the relay or manager (this includes Deep Security as a Service), then you must either:
>
> - update agents' software (See "Get Deep Security Agent software" on page 177) and then configure the proxy
> - bypass the proxy
> - change the application control rulesets relay setting as a workaround

3. Repeat the above steps if you need to create more relay groups.

## Enable one or more relays

1. Go to **Administration > Updates > Relay Management**.
2. Click on a relay group to select it.
3. Click **Add Relay**.
4. Select a computer from the Available Agents list and click **Enable Relay and Add to Group**. You can use the search field to filter the list of computers.

   The computer is added to the relay group, and displays a relay icon ().
5. If Windows Firewall or iptables is enabled on the computer, add a firewall rule that allows incoming connections to the relay's listening port number.
6. If relays must connect through a proxy, see "Connect agents, appliances, and relays to security updates via proxy" on page 204.

> **Note:** Newly activated relays will be automatically notified by the Manager to update their security update content.

## Assign agents to a relay group

You can either assign an agent to a relay group manually, or you can set up an event-based task to assign agents automatically.

1. In Deep Security Manager, go to **Computers**.
2. Right click the computer and select **Actions > Assign Relay Group**.

   To assign multiple computers, Shift-click or Ctrl-click computers in the list, and then select **Actions > Assign Relay Group**.
3. Select the relay group to use from the list, or from the Computer Details window, use **Download Updates From** to select the relay group.

## Configure relay settings for security and software updates

Deep Security Manager provides additional settings on the **Administration > System Settings > Updates** page that affect how relays are used to perform security and software updates.

### Security updates

- **Download Patterns for all Regions:** If you are operating in multi-tenancy mode and any of your tenants are in other regions, select this option. If this option is deselected, a relay will only download and distribute patterns for the region (locale) that Deep Security Manager was installed in.
- **Use the Primary Tenant Relay Group as my Default Relay Group (for unassigned Relays):** Use the Primary Tenant Relay group. By default, the primary tenant gives other tenants access to its relays. This way, tenants don't need to set up their own relays. If you don't want other tenants to share the primary tenant's relays, deselect this option and create separate relays for other tenants.

  **Note:** If this option is deselected, when you click **Administration** > **Updates** > **Relay Groups**, the relay group name will be "Default Relay Group" rather than "Primary Tenant Relay Group".

  **Note:** This setting appears only if you have enabled multi-tenant mode.

For information about other security update settings, see "Get and distribute security updates" on page 743.

### Software updates

- The **Allow Relays to download software updates from Trend Micro Download Center when Deep Security Manager is not accessible** option is useful when your Deep Security Manager is in an enterprise environment and you are managing computers in a cloud environment. If you enable this option and configure a relay in the cloud, the relay will be able to get software updates directly from the Download Center, removing the need for manual software upgrades or opening port numbers into your enterprise environment from the cloud.

For information about other software update settings, see "About upgrades" on page 735.

## Remove relay functionality from an agent

You might want to remove the relay functionality from a relay-enabled agent if:

- You are noticing communication delays because there are too many relay-enabled agents in your environment.
- The computer where the agent is installed does not meet the minimum system requirements for relay functionality.

**Note:** Deep Security uses relays to store data when a virtual machine protected by a Deep Security Virtual Appliance is being migrated by vMotion. If your deployment uses vMotion to migrate virtual machines, removing the relay functionality from a given agent may result in a loss of protection to the migrated virtual machine as well as loss of the security events of the virtual appliance .

The procedure for removing relay functionality differs depending on if the agent version is "10.2 or later" below or "10.1 or earlier" on the next page.

### 10.2 or later

1. Go to **Administration > Updates > Relay Management**.
2. Click the arrow next to the relay group with the computer you want to remove relay functionality from.

3. Click on the computer, and then click **Remove Relay**.

   The agent status will change to "Disabling" and the relay functionality will be removed from the agent.

   **Note:** It may take up to 15 minutes for the relay functionality to be removed from the agent. If the agent is in the "disabling" state for significantly longer than this, deactivate and reactivate the agent to finish removing relay functionality from the agent.

## 10.1 or earlier

**Note:** If you use multi-factor authentication with Deep Security Manager, you will need to temporarily disable it before proceeding. For information on how to do this, see "Set up multi-factor authentication" on page 775.

1. Go to **Administration > System Settings > Advanced** in the Deep Security Manager, click **Enabled - Access the WSDL at:** in the SOAP Web Service API section, and click **Save**.
2. Download the Disable Relay Tool: https://s3.amazonaws.com/customerscripts/Deep-Security-Disable-Relays.exe.
3. Run the tool on any Windows computer that can communicate with the computer where the Deep Security Manager is installed.
4. Enter the IP address and port of the Deep Security Manager and your administrator user name and password when prompted.
5. If you are using Deep Security as a Service or a multi-tenant Deep Security Manager, you also have to enter the tenant name.
6. Click **OK** when you have finished entering the information required for the tool to communicate with the Deep Security Manager.
7. Select all of the servers with relay-enabled agents that you want to downgrade from the list retrieved by the Disable Relay Tool and click **Disable Relay On Select Hosts** in the lower left corner.
8. Leave the tool open and click **Refresh Relay List** to monitor the progress of the downgrade. It can take up to 15 minutes to downgrade the agents on the servers you selected.
9. After a relay-enabled agent has been downgraded to a normal agent and no longer appears in the list of servers in the Disable Relay Tool, you should remove the relay files in

the following locations for that agent:

- Windows: `C:\ProgramData\Trend Micro\Deep Security Agent\relay`
- Linux: `/var/opt/ds_agent/relay`

# DevOps, automation and scaling

To support DevOps workflows, Deep Security offers APIs to automate, monitor, and manage security throughout the release lifecycle. (See "Use the Deep Security API to automate tasks" on page 261.)

To accelerate integration with popular DevOps tools, we've provided the following resources in Github for Chef, Puppet, and Ansible:

- https://github.com/deep-security/puppet
- https://github.com/deep-security/chef
- https://github.com/deep-security/ansible

These resources provide a starting point to integrate Deep Security with your specific deployment, including agent deployment and configuration and support for elastic workloads.

Deep Security also offers many other ways to speed up the protection of your computers and other resources:


- "Schedule Deep Security to perform tasks" on page 263
- "Automatically perform tasks when a computer is added or changed" on page 266
- "AWS Auto Scaling and Deep Security" on page 271
- "Use deployment scripts to add and protect computers" on page 281
- "Automatically assign policies by AWS instance tags" on page 285
- "Command-line basics" on the next page


In addition, Deep Security provides the ability to forward events to SIEMs such as Spunk, QRadar, ArcSight, as well as Amazon SNS. For details, see:

- "Forward Deep Security events to an external syslog or SIEM server " on page 814
- "Access events with Amazon SNS" on page 864


# Command-line basics

You can use the local command-line interface (CLI) to command both Deep Security Agents and the Deep Security Manager to perform many actions. The CLI can also configure some settings, and to display system resource usage.

**Tip:** You can also automate many of the CLI commands below using the Deep Security API. To get started with the API, see the First Steps Toward Deep Security Automation guide.

Below are command syntax and examples.

## Deep Security Agent

**Note:** On Windows, when self-protection is enabled (`-s <num>, --selfprotect=<num>` where 1 is enable, and 0 is disable), local users cannot uninstall, update, stop, or otherwise control the agent. Your CLI commands must include the authentication password.

### dsa_control

You can use `dsa_control` to configure some agent settings, and to manually trigger it to perform some actions such as an anti-malware scan or baseline rebuild.

In Windows:

- Open a Command Prompt as Administrator
- `cd C:\Program Files\Trend Micro\Deep Security Agent\`
- `dsa_control -m "AntiMalwareManualScan:true"`

In Linux:

- `/opt/ds_agent/dsa_control -m "AntiMalwareManualScan:true"`

## Usage

```
dsa_control [-a <str>] [-b] [-c <str>] [-d] [-g <str>] [-s <num>] [-m] [-p <str>] [-r] [-R <str>] [-t <num>] [-u <str>:<str>] [-w <str>:<str>] [-x dsm_proxy://<str>] [-y relay_proxy://<str>] [--buildBaseline] [--scanForChanges] [Additional keyword:value data to send to Manager during activation or heartbeat...]
```

- `-a <str>, --activate=<str>` Activate agent with Manager at specified URL. URL format must be:

  `dsm://<host or IP>:<port>/`

  where port is the manager's discovery and heartbeat port number.

- `-b, --bundle` Create update bundle.
- `-c <str>, --cert=<str>` Identify the certificate file.
- `-d, --diag` Generate an agent diagnostic package.
- `-g <str>, --agent=<str>` Agent URL. Defaults to:

  https://localhost:<port>/

  where port is the Manager's listening port number.

- `-m, --heartbeat` Ask the Agent to contact the Manager now.
- `-p <str>, --passwd=<str>` Authentication password. If you type the password directly into the command line, it will be displayed on screen. To hide the password with asterisks (*) while you type, enter the interactive form of the command, which will prompt you for the password:

  `dsa_control -p *`

- `-r, --reset` Reset agent configuration.
- `-R <str>, --restore=<str>` Restore quarantined file. (Deep Security)
- `-s <num>, --selfprotect=<num>` enable self-protection on the Agent by preventing local end-users from uninstalling, stopping, or otherwise controlling the Agent. Command-line instructions must include the authentication password when self-protection is enabled. (1:

enable, 0: disable). This is a Windows-only feature.

> **Note:** In Deep Security 9.0 and earlier, this option was `-H <num>, --harden=<num>`

- `-t <num>, --retries=<num>` If dsa_control cannot contact the Agent service to carry out accompanying instructions, this parameter instructs dsa_control to retry <num> number of times. There is a one second pause between retries.
- `-u <user>:<password>` If the agent connects through a proxy to the manager, provide the proxy user name and password, separated by a colon (:).
- `-w <user>:<password>` If the agent connects through a proxy to a relay for security updates and software, provide the proxy user name and password, separated by a colon (:).
- `-x dsm_proxy://<str>:<num>` If the agent connects through a proxy to the manager, provide the proxy's IP address or FQDN and port number, separated by a colon (:).
- `-y relay_proxy://<str>:<num>` If the agent connects through a proxy to a relay for security updates and software, provide the proxy's IP address or FQDN and port number, separated by a colon (:).
- `--buildBaseline` Build baseline for Integrity Monitoring
- `--scanForChanges` Scan for changes for Integrity Monitoring
- `--max-dsm-retries` Number of times to retry an activation. Valid values are 0 to 100, inclusive. The default value is 30.
- `--dsm-retry-interval` Approximate delay in seconds between retrying activations. Valid values are 1 to 3600, inclusive. The default value is 300.

## Agent-initiated activation ("dsa_control -a")

An Agent installed on a computer needs to be activated before the Manager can assign Rules and Policies to protect the computer. The activation process includes the exchange of unique fingerprints between the Agent and the Manager. This ensures that only one Manager (or one of its Manager Nodes) can send instructions to and communicate with the Agent.

You can manually activate an Agent from the Manager by right-clicking on the computer in the Computers screen and selecting **Actions > Activate/Reactivate**.

Agents can initiate the activation process using a locally-run command-line tool. This is useful when a large number of computers will be added to an installation and you want to write a script

to automate the activation process. To enabled agent-initiated activation, go to **Administration > System Settings > Agents** and select **Allow Agent-Initiated Activation**.

The minimum activation instruction contains the activation command and the Manager's URL (including the port number):

```
dsa_control -a dsm://<host>:<port>/
```

where:

- `-a` is the command to activate the Agent, and
- `dsm://<host>:<port>/` is the parameter that points the Agent to the Manager. (<host> could be the Manager's fully qualified domain name (FQDN), IPv4 address, or IPv6 address, and <port> is the Agent-to-Manager communication port number.) For example:

  ```
  dsa_control -a dsm://fe80::ad4a:af37:17cf:8937:4120
  ```

The host name is the only required parameter. Additional parameters are also available (see the table of available parameters below). They must be entered as key:value pairs (with a colon as a separator). There is no limit to the number of key:value pairs you can enter but the key:value pairs must be separated from each other by a space. For example:

```
dsa_control -a dsm://dsm-example-com:4120/ hostname:www12 "description:Long Description With Spaces"
```

(Quotation marks are only required if your value includes spaces or special characters.)

## Agent-initiated activation over a private network via proxy

Agents on a private network can perform agent-initiated communication with a manager through a proxy server.

1. In Deep Security Manager, go to **Administration > System Settings > Agents**.
2. In the **Agent-Initiated Activation** area:
   - Select **Allow Agent-Initiated Activation**.
   - Select **Allow Agent to specify hostname**.
   - In the **If a computer with the same name exists** list, select "Activate a new Computer with the same name".

3. Click **Save**.

Use the following command-line options to instruct the Agent to communicate with the Manager through a proxy server:

| Syntax | Notes |
|---|---|
| `dsa_control -x "dsm_proxy://<host or IP>/"` | Sets the address of the proxy server which the Agent uses to communicate with the Manager. |
| `dsa_control -x ""` | Clears the proxy server address. |
| `dsa_control -u "<username:password>"` | Sets the proxy user name and password. |
| `dsa_control -u ""` | Clears the proxy user name and password. |

**Examples**

| | |
|---|---|
| `dsa_control -x "dsm_proxy://172.21.3.184:808/"` | Proxy IPv4 address. |
| `dsa_control -x "dsm_proxy://squid:808/"` | Proxy host name. |
| `dsa_control -x "dsm_proxy://[fe80::340a:7671:64e7:14cc]:808/"` | Proxy IPv6 address. |
| `dsa_control -u "root:Passw0rd!"` | Proxy authentication is "root" and password is "Passw0rd!" (basic authentication only, digest and NTLM are not supported). |

When used in the context of agent-initiated activation, the proxy commands must be issued first, followed by the agent-initiated activation commands. The following example shows a complete sequence for setting a proxy address, setting proxy credentials, and activating the Agent:

```
dsa_control -x "dsm_proxy://172.21.3.184:808/"
dsa_control -u "root:Passw0rd!"
dsa_control -a "dsm://dsm.example.com:4120/"
Required Setting in Deep Security Manager
```

## Agent-initiated heartbeat command ("dsa_control -m")

The agent-initiated heartbeat command will instruct the agent to perform an immediate heartbeat operation to the manager. Although this may be useful on its own, like the activation command

above, the heartbeat command can be used to pass along a further set of parameters to the manager.

The following table lists the parameters that are available to the activation and heartbeat commands. Note that some parameters can only be used either during activation, or after activation during heartbeat exclusively.

| Parameter | Description | Example | Use during Activation | Use during Heartbeat |
|---|---|---|---|---|
| **AntiMalwareCancelManualScan** | Boolean.<br>Cancels an on-demand ("manual") scan that is currently occurring on the computer. | `"AntiMalwareCancelManualScan:true"` | no | yes |
| **AntiMalwareManualScan** | Boolean.<br>Initiates an on-demand ("manual") anti-malware scan on the computer. | `"AntiMalwareManualScan:true"` | no | yes |
| **description** | String.<br>Sets `description` value. Maximum length 2000 characters. | `"description:Extra information about the host"` | yes | yes |
| **displayname** | String. | `"displayname:the_name"` | yes | yes |

| Parameter | Description | Example | Use during Activation | Use during Heartbeat |
|---|---|---|---|---|
| | Sets `displayname` value. (Shown in parentheses next to the hostname.) Maximum length 2000 characters. | | | |
| **externalid** | Integer.<br>Sets the `externalid` value. This value can used to uniquely identify an Agent. The value can be accessed using the SOAP Web Service API. | `"externalid:123"` | yes | yes |
| **group** | String.<br>Sets the computers page `Group` | `"group:Zone A web servers"` | yes | yes |

| Parameter | Description | Example | Use during Activation | Use during Heartbeat |
|---|---|---|---|---|
| | the computer belongs in. Maximum length 254 characters per group name per hierarchy level.<br><br>The forward slash ("/") indicates a group hierarchy. The `group` parameter can read or create a hierarchy of groups. This parameter can only be used to add computers to standard groups under the main "Computers" root branch. It cannot be | | | |

| Parameter | Description | Example | Use during Activation | Use during Heartbeat |
|---|---|---|---|---|
| | used to add computers to groups belonging to Directories (MS Active Directory), VMware vCenters, or Cloud Provider accounts. | | | |
| **groupid** | Integer. | `"groupid:33"` | yes | yes |
| **hostname** | String.<br><br>Maximum length 254 characters.<br><br>The hostname can specify an IP address, hostname or FQDN that is best used to contact the computer in the **Computers** list in the Manager. | `"hostname:www1"` | yes | no |

| Parameter | Description | Example | Use during Activation | Use during Heartbeat |
|---|---|---|---|---|
| **IntegrityScan** | Boolean.<br><br>Initiates an integrity scan on the computer. | `"IntegrityScan:true"` | no | yes |
| **policy** | String.<br><br>Maximum length 254 characters.<br><br>The policy name is a case-insensitive match to the policy list. If the policy is not found, no policy will be assigned.<br><br>A policy assigned by an event-based task will override a policy assigned during agent- | `"policy:Policy Name"` | yes | yes |

| Parameter | Description | Example | Use during Activation | Use during Heartbeat |
|---|---|---|---|---|
| | initiated activation. | | | |
| **policyid** | Integer. | `"policyid:12"` | yes | yes |
| **relaygroup** | String.<br><br>Links the computer to a specific relay group. Maximum length 254 characters.<br><br>The relay group name is a case-insensitive match to existing relay group names. If the relay group is not found the default relay group will be used.<br><br>This does not affect relay groups | `"relaygroup:Custom Relay Group"` | yes | yes |

| Parameter | Description | Example | Use during Activation | Use during Heartbeat |
|---|---|---|---|---|
| | assigned during event-based tasks. Use either this option or event-based tasks, not both. | | | |
| **relaygroupid** | Integer. | `"relaygroupid:123"` | yes | yes |
| **relayid** | Integer. | `"relayid:123"` | yes | yes |
| **tenantID**and **token** | String.<br>If using agent-initiated activation as a tenant, both **tenantID** and **token** are required. The **tenantID** and **token** can be obtained from the deployment script generation tool. | `"tenantID:12651ADC-D4D5"`<br>`and`<br>`"token:8601626D-56EE"` | yes | yes |
| **RecommendationScan** | Boolean.<br>Initiate a recommendati | `"RecommendationScan:true"` | no | yes |

| Parameter | Description | Example | Use during Activation | Use during Heartbeat |
|---|---|---|---|---|
| | on scan on the computer. | | | |
| **UpdateComponent** | Boolean.<br>Instructs the Manager to perform a security update. | `"UpdateComponent:true"` | no | yes |
| **RebuildBaseline** | Boolean.<br>Rebuilds the integrity monitoring baseline on the computer. | `"RebuildBaseline:true"` | no | yes |
| **UpdateConfiguration** | Boolean.<br>Instructs the Deep Security Manager to perform a "Send Policy" operation. | `"UpdateConfiguration:true"` | no | yes |

## Activate an agent

To activate an agent from the command line, you need to know the tenant ID and password. You can get them from the deployment script.

1. In the top right-hand corner of Deep Security Manager, click **Support > Deployment Scripts**.
2. Select your platform.

3. Select **Activate Agent automatically after installation**.
4. In the deployment script, locate the strings for `tenantID` and `token`.

## Windows

In PowerShell:

```
& $Env:ProgramFiles"\Trend Micro\Deep Security Agent\dsa_control" -a <manager URL> <tenant ID> <token>
```

In cmd.exe:

```
C:\Windows\system32>"\Program Files\Trend Micro\Deep Security Agent\dsa_control" -a <manager URL> <tenant ID> <token>
```

## Linux

```
/opt/ds_agent/dsa_control -a <manager URL> <tenant ID> <token>
```

## Configure a proxy for anti-malware and rule updates

If the agent must connect to its relay through a proxy, you must configure the proxy connection.

## Windows

1. Open a command prompt (cmd.exe) as Administrator.
2. Enter these commands:

   ```
   cd C:\Program Files\Trend Micro\Deep Security Agent\
   ```

   ```
   dsa_control -w myUserName:MTPassw0rd
   ```

   ```
   dsa_control -y relay_proxy://squid.example.com:443
   ```

## Linux

```
/opt/ds_agent/dsa_control -w myUserName:MTPassw0rd
```

```
/opt/ds_agent/dsa_control -y relay_proxy://squid.example.com:443
```

### Configure a proxy for connections to the manager

If the agent must connect to its manager through a proxy, you must configure the proxy connection.

#### Windows

1. Open a command prompt (cmd.exe) as Administrator.
2. Enter these commands:

   ```
   cd C:\Program Files\Trend Micro\Deep Security Agent\
   ```

   ```
   dsa_control -u myUserName:MTPassw0rd
   ```

   ```
   dsa_control -x dsm_proxy://squid.example.com:443
   ```

#### Linux

```
/opt/ds_agent/dsa_control -u myUserName:MTPassw0rd
```

```
/opt/ds_agent/dsa_control -x dsm_proxy://squid.example.com:443
```

### Force the agent to contact the manager

#### Windows

In PowerShell:

```
& "\Program Files\Trend Micro\Deep Security Agent\dsa_control" -m
```

In cmd.exe:

```
C:\Windows\system32>"\Program Files\Trend Micro\Deep Security Agent\dsa_control" -m
```

#### Linux

```
/opt/ds_agent/dsa_control -m
```

### Initiate a manual anti-malware scan

#### Windows

1. Open a command prompt (cmd.exe) as Administrator.
2. Enter these commands:

```
cd C:\Program Files\Trend Micro\Deep Security Agent\
dsa_control -m "AntiMalwareManualScan:true"
```

### Linux

```
/opt/ds_agent/dsa_control -m "AntiMalwareManualScan:true"
```

## Create a diagnostic package

Deep Security Technical Support might ask you to create a diagnostic package to help them troubleshoot and diagnose your issue. The diagnostic package is created in a zip file which is downloaded locally on the endpoint in operation. From there you can send it to Technical Support. For more detailed instructions, see "Create a diagnostic package and logs" on page 1105.

> **Note:** You can produce a diagnostic package for a managed computer through the Deep Security Manager but if the computer is in agent-initiated activation (AIA) mode it cannot collect all of the required logs. So when Technical Support asks for a diagnostic package you need to run the command directly on the managed computer.

### Windows

In PowerShell:

```
& "\Program Files\Trend Micro\Deep Security Agent\dsa_control" -d
```

In cmd.exe:

```
C:\Windows\system32>"\Program Files\Trend Micro\Deep Security Agent\dsa_control" -d
```

### Linux

```
/opt/ds_agent/dsa_control -d
```

## Reset the agent

This command will remove the activation information from the target agent and deactivate it.

### Windows

In PowerShell:

```
& "\Program Files\Trend Micro\Deep Security Agent\dsa_control" -r
```

In cmd.exe:

```
C:\Windows\system32>"\Program Files\Trend Micro\Deep Security Agent\dsa_control" -r
```

### Linux

```
/opt/ds_agent/dsa_control -r
```

## dsa_query

You can use the `dsa_query` command to display agent information:

- License-status of each component
- Scan progress
- Version information of security update components

### Usage

```
dsa_query [-c <str>] [-p <str>] [-r <str]
```

- `-p,--passwd <string>`: authentication password. Required when agent self-protection is enabled.

  > **Note:** For some query-commands, authentication can be bypassed directly, in such case, password is not required.

- `-c,--cmd <string>`: execute query-command against the agent. The following commands are supported:
  - `GetHostInfo`: to query which identity is returned to the Manager during a heartbeat
  - `GetAgentStatus`: to query which protection modules are enabled and other miscellaneous information
  - `GetComponentInfo`: to query version information of anti-malware patterns and engines
  - `GetPluginVersion`: to query version information about the agent and protection modules
- `-r,--raw <string>`: returns the same query-command information as `"-c"` but in raw data format for third party software interpretation.

`pattern:` Wild card pattern to filter result. Optional.

**Example:**

```
dsa_query -c "GetComponentInfo" -r "au" "AM*"
```

### Check CPU usage and RAM usage

#### Windows

Use the Task Manager or procmon.

#### Linux

```
top
```

### Check that ds_agent processes or services are running

#### Windows

Use the Task Manager or procmon.

#### Linux

```
ps -ef|grep ds_agent
```

### Restart an agent on Linux

```
service ds_agent restart
```

or

```
/etc/init.d/ds_agent restart
```

Some actions require either a `-tenantname` parameter or a `-tenantid` parameter. If execution problems occur when you use the tenant name, try the command using the associated tenant ID.

## Use the Deep Security API to automate tasks

Deep Security 11.1 provides a new RESTful API that enables you to automate the provisioning and maintenance of security via Deep Security. Go to the Deep Security Automation Center to download the SDKs in the language of your choice and learn how to use the API:

- API Reference
- Task-oriented guides with ample code examples
- Support resources

The API is continuously updated with new features and improvements. When you start new automation projects, if the new API meets your needs you should use it to benefit from continued support and maintenance in the long term.

To get started with the API, see the First Steps Toward Deep Security Automation guide.

## Legacy REST and SOAP APIs

**Note:** The REST and SOAP APIs that were provided before Deep Security 11.1 have not changed. They have been deprecated, so new features will not be added but the existing API functionality will continue to function as usual.

Deep Security still includes the legacy REST and SOAP APIs. For guidance on using them, see the following guides on the Deep Security Automation Center:

- Transition From the SOAP API
- Use the Legacy REST API

The following tasks explain how to use Deep Security Manager to accomplish tasks that are related to using the SOAP and REST API. For more information about when you need to perform these tasks, see the guides listed above.

### Enable the Status Monitoring API (optional)

To use status monitoring with the legacy REST API, you must enable it. The API is disabled by default as it does not require authentication.

**Note:** On Deep Security as a Service, the status monitoring API is already enabled for the primary tenant (t0), so you don't need to enable it. It is not configurable for other tenants.

1. On Deep Security Manager, go to **Administration > System Settings > Advanced**.
2. In the Status Monitoring API section, select **Enabled**, then click **Save**.

### Create a Web Service user account

Create a role for Web Service-only access, and assign it to a new user.

1. On Deep Security Manager, go to **Administration** > **User Management** > **Roles** .
2. Click **New**.
3. Deselect the **Allow Access to Deep Security Manager User Interface** check box and select the **Allow Access to Web Service API check box**.
4. When all other configuration is complete, click **Save**.
5. Go to **Administration** > **User Management** > **Users** and click **New**.
6. Create a new user for use only with the Web Service API. Assign the new Role previously created to this user.
   *Make note of the new user account user name and password.*

# Schedule Deep Security to perform tasks

Deep Security has many tasks that you might want to perform automatically on a regular basis. Scheduled tasks are useful when deploying Deep Security in your environment and also later, to keep your system up to date and functioning smoothly. They are especially useful for running scans on a regular basis during off-peak hours.

**Tip:** You can automate scheduled task creation and configuration using the Deep Security API. For examples, see the Maintain Protection Using Scheduled Tasks guide.

## Create scheduled tasks

To set up a scheduled task in the Deep Security Manager, click **Administration** > **Scheduled Tasks** > **New**. This opens the "New Scheduled Task Wizard", which takes you through the steps to create a scheduled task.

**Backup:** Perform regular database backups. (This option is only available if you are using a Microsoft SQL Server database.)

**Check for Security Updates:** Regularly check for security updates and import them into Deep Security when they are available. For most organizations, performing this task once daily is ideal.

**Check for Software Updates:** Regularly check for Deep Security Agent software updates and download them when they are available.

**Discover Computers:** Periodically check for new computers on the network by scheduling a Discovery operation. You will be prompted for an IP range to check and asked to specify which computer group the new computer will be added to. This task is useful for discovering computers that are not part of your cloud connector.

**Generate and Send Report:** Automatically generate reports and optionally have them emailed to a list of users.

**Run Script:** If the Syslog options do not meet your event notification requirements, it may be possible for Trend Micro to provide a solution using custom-written scripts. Contact Trend Micro for more information.

**Scan Computers for Integrity Changes:** Causes the Deep Security Manager to perform an Integrity Scan to compare a computer's current state against its baseline.

**Scan computers for Malware:** Schedules a Malware Scan. The configuration of the scan is specified on the Policy or Computer Editor > Anti-Malware page for each computer. For most organizations, performing this task once weekly (or according to your organization's policies) is ideal. When you configure this task, you can specify a timeout value for the scan. The timeout option is available for daily, weekly, monthly, and once-only scans. It is not available for hourly scans. When a scheduled malware scan is running and the timeout limit has been reached, any tasks that are currently running or pending are canceled.

> **Tip:** When a **Scan Computers for Malware** task times out, the next scheduled scan starts over from the beginning (it does not start where the previous scan ended). The goal is to perform a complete scan, so consider making some configuration changes if your scans regularly reach the timeout limit. You can change the malware scan configuration to add some exceptions, or extend the timeout period.

**Scan Computers for Open Ports:** Schedule periodic port scans on one or more computers. You can specify individual computers or all computers belonging to a particular computer group. Deep Security Manager will scan the port numbers defined on the Scanning tab in the Policy or Computer Editor > Settings page.

**Scan Computers for Recommendations:** Causes the Deep Security Manager to scan the computer(s) for common applications and then make recommendations based on what is detected. Performing regular recommendation scans ensures that your computers are protected

by the latest relevant rule sets and that those that are no longer required are removed. If you have set the "Automatically implement Recommendations" option for each of the three protection modules that support it, Deep Security will assign and unassign rules that are required. If rules are identified that require special attention, an alert will be raised to notify you. For most organizations, performing this task once a week is ideal.

**Note:** Recommendation Scans can be CPU-intensive, so when scheduling Recommendation Scans, it is best practice to set the task by group (for example, per policy or for a group of computers, no more than 1,000 machines per group) and spread it in different days (for example, database server scans scheduled every Monday; mail server scans scheduled every Tuesday, and so on). Schedule Recommendation Scans more frequently for systems that change often.

**Send Outstanding Alert Summary:** Generate an email listing all outstanding (unresolved) alerts.

**Send Policy:** Regularly check for and send updated policies. Scheduled updates allow you to follow an existing change control process. Scheduled tasks can be set to update machines during maintenance windows, off hours, etc.

**Synchronize Cloud Account:** Synchronize the Computers list with an added cloud account. (only available if you have added a cloud account to the Deep Security Manager.)

**Synchronize Directory:** Synchronize the Computers list with an added LDAP directory. (Only available if you have added an LDAP directory to the Deep Security Manager.)

**Synchronize Users/Contact:** Synchronize the Users and Contacts lists with an added Active Directory. (Only available if you have added an Active Directory to the Deep Security Manager.)

## Enable or disable a scheduled task

Existing scheduled tasks can be enabled or disabled. For example, you might want to temporarily disable a scheduled task while you perform certain administrative duties during which you don't want any activity to occur. The control to enable or disable a scheduled task is on the General tab of the Task's Properties window.

### Set up recurring reports

Recurring Reports are simply scheduled tasks that periodically generate and distribute reports to users and contacts. Most of the options are identical to those for single reports, with the exception of the time filter.

**Tip:** To generate a report on specific computers from multiple computer groups, create a user who has viewing rights only to the computers in question and then either create a scheduled task to regularly generate an "All Computers" report for that user or sign in as that user and run an "All Computers" report. Only the computers to which that user has viewing rights will be included in the report.

## Automatically perform tasks when a computer is added or changed

**Note:** In this article, references to protecting virtual machines apply only to Deep Security On-Premise software installations.

Event-based tasks let you monitor protected computers for specific events and perform tasks based on certain conditions.

### Create an event-based task

In Deep Security Manager, click **Administration > Event-Based Tasks > New**. The wizard that appears will guide you through the steps of creating a new task. You will be prompted for different information depending on the type of task.

### Edit or stop an existing event-based task

To change the properties for an existing event-based task, go to click **Administration > Event-Based Tasks**. Select the event-based task from the list and click **Properties**.

## Events that you can monitor

- **Computer Created (by System):** A computer being added to the manager during synchronization with an Active Directory or Cloud Provider account, or the creation of a virtual machine on a managed ESXi server running a virtual appliance.
- **Computer Moved (by System):**A virtual machine being moved from one vApp to another within the same ESXi, or a virtual machine on an ESXi being move from one datacenter to another or from one ESXi to another (including from an unmanaged ESXi server to a managed ESXi server running a virtual appliance.)
- **Agent-Initiated Activation:** An agent is activated using agent-initiated activation.
- **IP Address Changed:** A computer has begun using a different IP.
- **NSX Security Group Changed:** The following situations will trigger this event (the event will be recorded on each affected VM):
  - A VM is added to a group that is (indirectly) associated with the NSX Deep Security Service Profile
  - A VM is removed from an NSX Group that is associated with the NSX Deep Security Service Profile
  - An NSX Policy associated with the NSX Deep Security Service Profile is applied to an NSX Group
  - An NSX Policy associated with the NSX Deep Security Service Profile is removed from an NSX Group
  - An NSX Policy is associated with the NSX Deep Security Service Profile
  - An NSX Policy is removed from the NSX Deep Security Service Profile
  - An NSX Group that is associated with an NSX Deep Security Service Profile changes name
- **Computer Powered On (by System)**: Enables users to trigger activation by the VMware Virtual Machine power on event.

> **Note:** The Computer Powered On event is only compatible with virtual machines hosted on ESX environments in VMWare. Use this event cautiously because if a large number of computers are turned on at the same time, this event could cause a slowdown.

## Conditions

You can require specific match conditions to be met in order for the task to be carried out. (Add additional conditions by pressing the "plus" button.) If you specify multiple conditions, each of the conditions must be met for the task to be carried out. (In other words, multiple conditions are "AND" conditions, not "OR".)

Use **Java regular expression syntax** (https://docs.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html) to match patterns in the following fields:

- **Cloud Instance Image ID**: AWS cloud instance AMI ID.

  **Note:** This match condition is only available for AWS cloud instances.

- **Cloud Instance Metadata:** The metadata being matched corresponds to AWS "tags" in the Amazon environment.

  **Note:** This match condition is only available for AWS cloud instances. Metadata currently associated with a computer is displayed on the **Overview** page in its editor window. To define the conditions to match for, you must provide two pieces of information: the metadata tag key and the metadata tag value. For example, to match a computer which has a metadata key named "**AlphaFunction**" that has a value of "**DServer**", you would enter "**AlphaFunction**" and "**DServer**" (without the quotes). If you wanted match more than one possible condition, you could use regular expressions and enter "**AlphaFunction**" and "**.*Server**", or "**AlphaFunction**" and "**D.***".

- **Cloud Instance Security Group Name**: The security group the cloud instance applies to.

  **Note:** This match condition is only available for AWS cloud instances.

- **Cloud Account Name**: The "Display Name" field in the Cloud Account properties window.
- **Computer Name**: The "Hostname" field in the computer properties window.
- **ESXi Name**: The "Hostname" field of the ESXi server on which the VM computer is hosted.
**ESXi Name**: The "Hostname" field of the ESXi server on which the VM computer is hosted.
- **Folder Name**: The name of the folder or directory in which the computer is located in its local environment.

> **Note:** This match condition looks for a match against the name of **any** parent folder of the computer, including the root datacenter for vCenter server integrations. If you add a "*" character to the beginning of the regular expression, the condition must match the name on **all** parent folders. This is particularly useful when combined with negation in a regular expression. For example, if you want to match computers in folders that do not include "Linux" in the folder name, you could use a regular expression like `*^((?!Linux).)*$`.

- **NSX Security Group Name:** The list of potential groups in this condition refers only to NSX Groups associated with NSX Policies associated with the NSX Deep Security Service Profile. The VM may be a member of other NSX Groups but for the purposes of this match, condition it is not relevant.
- **Platform**: The operating system of the computer.
- **vCenter name:** The "Name" field of the computer's vCenter properties that was added to Deep Security Manager.

**Java regular expression examples:**

| To match: | Use this: |
|---|---|
| any string (but not nothing) | .+ |
| empty string (no text) | ^$ |
| Folder Alpha | Folder\ Alpha |
| FIN-1234 | FIN-\d+<br>**or**<br>FIN-.* |
| RD-ABCD | RD-\w+<br>**or**<br>RD-.* |
| AB<br>**or**<br>ABC<br>**or**<br>ABCCCCCCCCCC | ABC* |
| Microsoft Windows 2003<br>**or**<br>Windows XP | .*Windows.* |
| Red Hat 7<br>**or**<br>Some_Linux123 | .*Red.*\|.*Linux.*\| |

These next two conditions match True or False conditions:

- **Appliance Protection Available:** A Deep Security Virtual Appliance is available to protect VMs on the ESXi on which the VM is hosted. The VM may or may not be in a "Activated" state.
- **Appliance Protection Activated**: A Deep Security Virtual Appliance is available to protect VMs on the ESXi on which the VM is hosted and the VM is "Activated".

The last condition option looks for matches to an IP in an IP list:

- **Last Used IP Address:** The current or last known IP address of the computer.

**Note:** Depending on the source of the new computer, some fields may not be available. For example, "Platform" would not be available for computers added as a result of the synchronization with an Active Directory.

## Actions

The following actions can be taken depending on which of the above events is detected:

- **Activate Computer:** Deep Security protection is activated on the computer.
  - **Delay activation by (minutes):** Activation is delayed by a specified number of minutes.

- **Note:** If the event-based task is intended to apply protection to a VM that is being vMotioned to an ESXi protected by a Deep Security Virtual Appliance, add a delay before activation to allow any pending VMware administrative tasks to complete. The amount of delay varies depending on your environment.

- **Deactivate Computer:**Deep Security protection is deactivated on the computer.
- **Assign Policy:** The new computer is automatically assigned a policy. (The computer must be activated first.)
- **Assign Relay Group:** The new computer is automatically assigned a relay group from which to receive security updates.
- **Assign to Computer Group:** The computer is placed in one of the computer groups on the Computers page.

### Order of execution

If multiple event-based tasks are triggered by the same condition, the tasks are executed in alphabetical order by task name.

### Temporarily disable an event-based task

To prevent an existing event-based task from running, right-click it and then click **Disable** . For example, you may want to temporarily disable an event-based task while you perform certain administrative duties during which you don't want any activity to occur.

To re-enable an event-based task, right-click it and then click **Enable**.

## AWS Auto Scaling and Deep Security

You can set up automatic protection in Deep Security for new instances created by AWS Auto Scaling.

Each instance created by Auto Scaling will need to have a Deep Security agent installed on it. There are two ways that you can do this: you can include a pre-installed agent in the EC2 instance used to create the AMI, or you install the agent by including a deployment script in the launch configuration for the AMI. There are pros and cons for each option:

- If you include a pre-installed agent, instances will spin up more quickly because there is no need to download and install the agent software.
- If you use a deployment script to install the agent, it will always get the latest version of the agent software from the Deep Security Manager. If you use a pre-installed agent, it will use the version included in the AMI.

### Pre-install the agent

If you have an EC2 instance already configured with a Deep Security Agent, you can use that instance to create the AMI for Auto Scaling. Before creating the AMI, you must deactivate the agent on the EC2 instance and stop the instance:

```
dsa_control -r
```

Each new EC2 instance created by Auto Scaling needs to have its agent activated and a policy applied to it, if it doesn't have one already. There are two ways to do this:

- You can create a deployment script that activates the agent and optionally applies a policy. Then add the deployment script to the AWS launch configuration so that it is run when a new instance is created. For instructions, see the "Install the Agent with a deployment script" section below, but omit the section of the deployment script that gets and installs the agent. You will only need the dsa_control -a section of the script.

  **Note:** For the deployment scripts to work, agent-initiated communication must be enabled on your Deep Security Manager. For details on this setting, see "Use agent-initiated communication with cloud accounts" on page 202

- You can set up an Event-Based Task in Deep Security Manager that will activate the agent and optionally apply a policy when an instance it launched and the "Computer Created (By System)" event occurs.

## Install the agent with a deployment script

Deep Security provides the ability to generate customized deployment scripts that you can run when EC2 instances are created. If the EC2 instance does not contain a pre-installed agent, the deployment script should install the agent, activate it, apply a policy, and optionally assign the machine to a computer group and relay group.

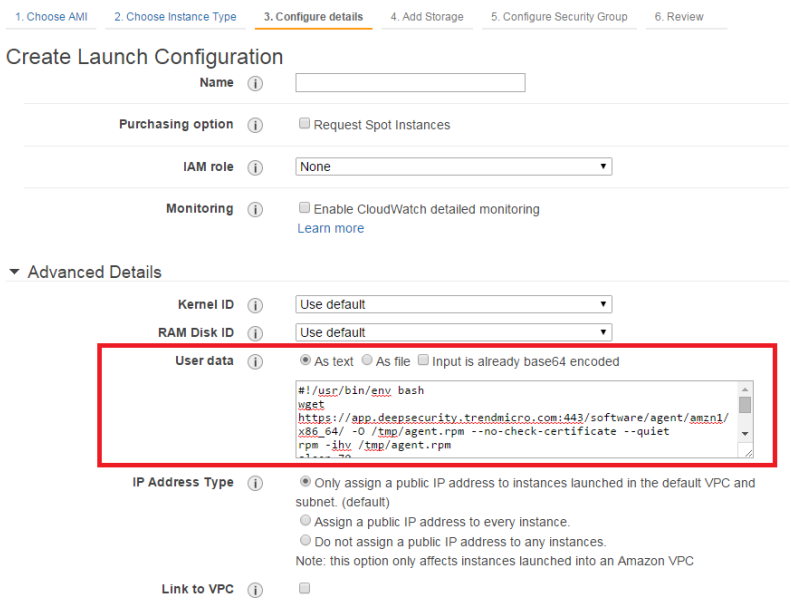
There are several ways to run the deployment script on your instances. The method described below is to add the deployment script to the launch configuration for the AMI but, alternatively, you could run it using an orchestration tool like Chef, Puppet, or Ansible. For Windows machines, you could also run it using Microsoft GPO or System Center.

In order for the deployment script to work:

- You must create AMIs from machines that are stopped.
- Agent-initiated communication must be enabled on your Deep Security Manager. For details on this setting, see "Use agent-initiated communication with cloud accounts" on page 202.

### To set up automatic protection for instances using a deployment script:

1. Sign in to the Deep Security Manager.
2. From **Support** menu in the top right-hand corner, select **Deployment Scripts**.
3. Select your platform.
4. Select **Activate Agent automatically after installation**.
5. Select the appropriate **Security Policy**, **Computer Group** and **Relay Group**.
6. Click **Copy to Clipboard.**
7. Go to the AWS launch configuration, expand **Advanced Details** and paste the deployment script into **User Data**.




**Note:** If you are encountering issues getting the PowerShell deployment script to run on a Microsoft Windows-based AMI, the issues may be caused by creating the AMI from a running instance. AWS supports creating AMIs from running instances, but this option disables ALL of the `Ec2Config` tasks that would run at start time on any instance created from the AMI. This behavior prevents the instance from attempting to run the PowerShell script.

**Note:** When you build an AMI on Windows, you need to re-enable user-data handling manually or as part of your image-building process. The user-data handling only runs in the first boot of the Windows base AMI unless it's explicitly told otherwise (it's disabled during the initial boot process), so instances built from a custom AMI won't run user-data unless the

feature is re-enabled. Configuring a Windows Instance Using the EC2Config Service has a detailed explanation and instructions for how to reset the feature or ensure it's not disabled on first boot. The easiest mechanism is to include `<persist>true</persist>` in your user data, providing that you have EC2Config version 2.1.10 or later.

### Delete instances from Deep Security as a result of Auto Scaling

After you have added an AWS Account in the Deep Security Manager, instances that no longer exist in AWS as a result of Auto Scaling will be automatically removed from the Deep Security Manager.

See "Add AWS cloud accounts" on page 295 for details on adding an AWS account.

## Azure virtual machine scale sets and Deep Security

Azure virtual machine scale sets (VMSS) provide the ability to deploy and manage a set of identical VMs. The number of VMs can increase or decrease automatically based on configurable scaling rules. For more information, see What are virtual machine scale sets in Azure?

You can set up your VMSS to include a base VM image that has the Deep Security Agent pre-installed and pre-activated. As the VMSS scales up, the new VM instances in the scale set automatically include the agent.

To add the agent to your VMSS:


- "Step 1: (Recommended) Add your Azure account to Deep Security Manager" on the next page
- "Step 2: Prepare a deployment script" on the next page
- "Step 3: Add the agent through a custom script extension to your VMSS instances" on page 276

## Step 1: (Recommended) Add your Azure account to Deep Security Manager

When you add your Azure account to Deep Security Manager, all the Azure instances created under that account are loaded into Deep Security Manager and appear under **Computers**. The instances appear regardless of whether they have an agent installed or not. The ones that do not include an agent have a **Status** of **No Agent**. After you install and activate the agent on them, their **Status** changes to **Managed (Online)**.

If the scale set is manually or automatically scaled up after adding your Azure account, Deep Security detects the new Azure instances and adds them to its list under **Computers**. Similarly, if the scale set is scaled down, the instances are removed from view. Thus, Deep Security Manager always shows the current list of available Azure instances in your scale set.

However, if you do not add your Azure account to Deep Security Manager, but instead add individual Azure instances using another method, then Deep Security does not detect any scaling down that might occur, and does not remove the non-existent Azure instances from its list. To prevent an ever-expanding list of Azure VMs in your Deep Security Manager, and to always show exactly which Azure instances are available in your scale set at any one time, it is highly recommended that you add your Azure account to Deep Security Manager.

For instructions on adding your Azure account, see "Add a Microsoft Azure account to Deep Security" on page 311.

## Step 2: Prepare a deployment script

In Deep Security Manager, prepare a deployment script from Deep Security Manager. For instructions, see "Use deployment scripts to add and protect computers" on page 281. This deployment script will be referenced in a custom script extension that you'll configure next.

**Note:** To run a custom script with the following VMSS script, the script must be stored in Azure Blob storage or in any other location accessible through a valid URL. For instructions on how to upload a file to Azure Blob storage, see Perform Azure Blob storage operations with Azure PowerShell.

## Step 3: Add the agent through a custom script extension to your VMSS instances

Below are a couple of examples on how to use PowerShell to add the agent.

- Example 1 shows how to create a new VMSS that includes the agent
- Example 2 shows how to add the agent to an existing VMSS

Both examples:

- use the Add-AzureRmVmssExtension cmdlet to add an extension to the VMSS
- use Azure PowerShell version 5.1.1

**Note:** For instructions on creating a new VMSS using PowerShell cmdlets, refer to this Microsoft tutorial. For the Linux platform, see https://github.com/Azure/custom-script-extension-linux.

### Example 1: Create a new VMSS that includes the agent

```
$resourceGroupName = <The resource group of the VMSS>
$vmssname = <The name of the VMSS>

# Create ResourceGroup
New-AzureRmResourceGroup -ResourceGroupName $resourceGroupName -Location EastUS

# Create a config object
$vmssConfig = New-AzureRmVmssConfig `
    -Location EastUS `
    -SkuCapacity 2 `
    -SkuName Standard_DS2 `
    -UpgradePolicyMode Automatic

# Define the script for your Custom Script Extension to run on the Windows Platform
```

```
$customConfig = @{
    "fileUris" = (,"A URL of your copy of deployment script, ex. deploymentscript.ps1");
    "commandToExecute" = "powershell -ExecutionPolicy Unrestricted -File deploymentscript.ps1"
}

# Define the script for your Custom Script Extension to run on the Linux Platform
#$customConfig = @{
# "fileUris" = (,"A URL of your copy of deployment script, ex. deploymentscript.sh");
# "commandToExecute" = "bash deploymentscript.sh"
#}

# The section is required only if deploymentscript has been located within Azure StorageAccount
$storageAccountName = <StorageAccountName if deploymentscript is locate in Azure Storage>
$key = (Get-AzureRmStorageAccountKey -Name $storageAccountName -ResourceGroupName $resourceGroupName).Value[0]
$protectedConfig = @{
    "storageAccountName" = $storageAccountName;
    "storageAccountKey" = $key
}

# Use Custom Script Extension to install Deep Security Agent (Windows)
Add-AzureRmVmssExtension -VirtualMachineScaleSet $vmssConfig `
    -Name "customScript" `
    -Publisher "Microsoft.Compute" `
```

```
    -Type "CustomScriptExtension" `
    -TypeHandlerVersion 1.8 `
    -Setting $customConfig `
    -ProtectedSetting $protectedConfig

# Use Custom Script Extension to install Deep Security Agent (Linux)
#Add-AzureRmVmssExtension -VirtualMachineScaleSet $vmssConfig `
# -Name "customScript" `
# -Publisher "Microsoft.Azure.Extensions" `
# -Type "customScript" `
# -TypeHandlerVersion 2.0 `
# -Setting $customConfig `
# -ProtectedSetting $protectedConfig

# Create a public IP address
# Create a frontend and backend IP pool
# Create the load balancer
# Create a load balancer health probe on port 80
# Create a load balancer rule to distribute traffic on port 80
# Update the load balancer configuration
# Reference a virtual machine image from the gallery
# Set up information for authenticating with the virtual machine
# Create the virtual network resources
# Attach the virtual network to the config object

# Create the scale set with the config object (this step might take a few minutes)
New-AzureRmVmss `
    -ResourceGroupName $resourceGroupName `
```

```
    -Name $vmssname `
    -VirtualMachineScaleSet $vmssConfig
```

## Example 2: Add the agent to an existing VMSS

```
$resourceGroupName = <The resource group of the VMSS>
$vmssname = <The name of the VMSS>

# Get the VMSS model
$vmssobj = Get-AzureRmVmss -ResourceGroupName $resourceGroupName -VMScaleSetName
$vmssname

# Show model data if you prefer
# Write-Output $vmssobj

# Define the script for your Custom Script Extension to run on the Windows platform
$customConfig = @{
    "fileUris" = (,"A URL of your copy of deployment script, ex.
deploymentscript.ps1");
    "commandToExecute" = "powershell -ExecutionPolicy Unrestricted -File
deploymentscript.ps1"
}

# Define the script for your Custom Script Extension to run on the Linux platform
#$customConfig = @{
# "fileUris" = (,"A URL of your copy of deployment script, ex.
deploymentscript.sh");
# "commandToExecute" = "bash deploymentscript.sh"
#}
```

```
# The section is required only if deploymentscript has been located within Azure StorageAccount
$storageAccountName = <StorageAccountName if deploymentscript is locate in Azure Storage>
$key= (Get-AzureRmStorageAccountKey -Name $storageAccountName -ResourceGroupName $resourceGroupName).Value[0]
$protectedConfig = @{
    "storageAccountName" = $storageAccountName;
    "storageAccountKey" = $key
}

# Use Custom Script Extension to install Deep Security Agent (Windows)
$newvmssobj = Add-AzureRmVmssExtension `
    -VirtualMachineScaleSet $vmssobj `
    -Name "customScript" `
    -Publisher "Microsoft.Compute" `
    -Type "CustomScriptExtension" `
    -TypeHandlerVersion 1.8 `
    -Setting $customConfig `
    -ProtectedSetting $protectedConfig

# Use Custom Script Extension to install Deep Security Agent (Linux)
#$newvmssobj = Add-AzureRmVmssExtension `
#    -VirtualMachineScaleSet $vmssobj `
#    -Name "customScript" `
#    -Publisher "Microsoft.Azure.Extensions" `
#    -Type "customScript" `
#    -TypeHandlerVersion 2.0 `
```

```
#    -Setting $customConfig `
#    -ProtectedSetting $protectedConfig

# Update the virtual machine scale set model
Update-AzureRmVmss -ResourceGroupName $resourceGroupName -name $vmssname -
VirtualMachineScaleSet $newvmssobj -Verbose

# Get Instance ID for all instances in this VMSS, and decide which instance you'd
like to update
# Get-AzureRmVmssVM -ResourceGroupName $resourceGroupName -VMScaleSetName $vmssname

# Now start updating instances
# If upgradePolicy is Automatic in the VMSS, do NOT execute the next command
Update-AzureRmVmssInstance. Azure will auto-update the VMSS.
# There's no PowerShell command to update all instances at once. But you could
refer to the output of Update-AzureRmVmss, and loop all instances into this
command.
Update-AzureRmVmssInstance -ResourceGroupName $resourceGroupName -VMScaleSetName
$vmssname -InstanceId 0
```

## Use deployment scripts to add and protect computers

Adding a computer to your list of protected resources in Deep Security and implementing protection is a multi-step process. Almost all of these steps can be performed from the command line on the computer and can therefore be scripted. The Deep Security Manager contains a deployment script writing assistant which can be accessed from the **Support** menu.

**Note:** If you want to deploy an agent to an early version of Windows or Linux that doesn't include PowerShell 4.0 or curl 7.3.4 at a minimum, you'll have to use a different deployment script from the one offered through the Deep Security Manager 10.1 and above. It is provided in this article. You can't use the one in Deep Security Manager 10.1+ because it includes a --

`tlsv1.2` (Linux) or `Tls12;` (Windows) tag. This tag enforces the use of TLS 1.2 communication between agent and manager, which is not supported by older operating systems.

## Enable agent-initiated activation

If your deployment script will automatically activate the Deep Security Agent after it is installed, you must configure Deep Security Manager to allow agent-initiated activation. For information on this setting, see "Use agent-initiated communication with cloud accounts" on page 202 and "Agent settings" on page 223.

1. Go to **Administration > System Settings > Agents**.
2. Select **Allow Agent-Initiated Activation.**

## Generate a deployment script

1. In the upper right corner of the Deep Security Manager console, click **Support > Deployment Scripts**.
2. Select the platform on which you are deploying the software.

   The platforms in the list correspond to the agent software that you have imported into Deep Security Manager. For information on importing Deep Security software, see "Get Deep Security Agent software" on page 177.

3. Select **Activate agent automatically after installation**.

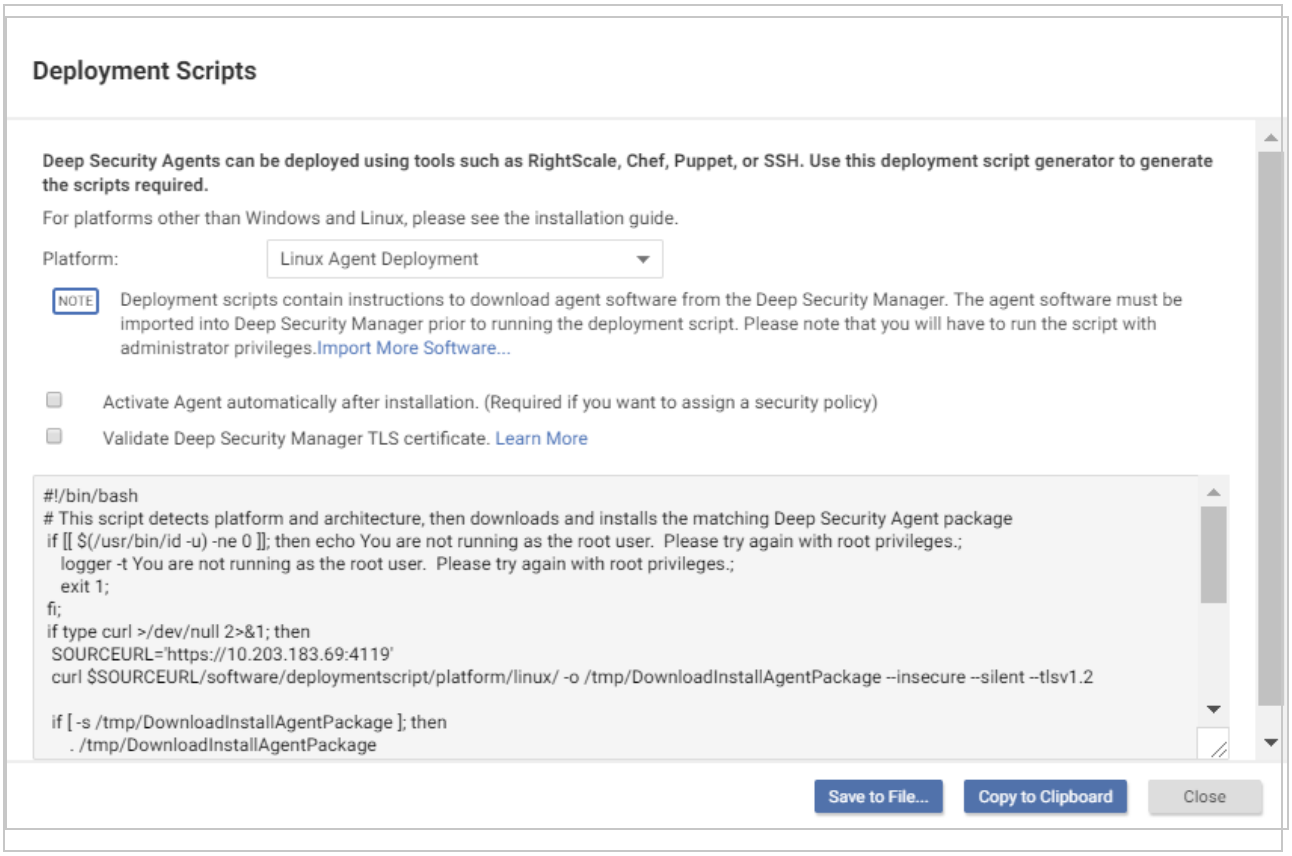
   Agents must be activated before you apply a policy to protect the computer. Activation registers the agent with the manager during an initial communication.

4. Optionally, select the **Security Policy**, **Computer Group**, **Relay Group**, **Proxy to contact Deep Security Manager**, and **Proxy to contact Relay(s)**.
5. Optionally (but highly recommended), select **Validate Deep Security Manager TLS certificate**.

   When this option is selected, it checks that Deep Security Manager is using a valid TLS certificate from a trusted certificate authority (CA) when downloading the agent software, which can help prevent a "man in the middle" attack. You can check whether Deep Security Manager is using a valid CA certificate by looking at the browser bar in the Deep

Security Manager console. By default, Deep Security Manager uses a self-signed certificate, which is not compatible with the **Validate Deep Security Manager TLS certificate** option. If your Deep Security Manager is not behind a load balancer, see "Replace the Deep Security Manager SSL certificate" on page 756 for instructions on replacing the default self-signed certificate with a certificate from a trusted certificate authority. If the manager is behind a load balancer, you will need to replace the load balancer's certificates.

6. The deployment script generator displays the script. Click **Copy to Clipboard** and paste the deployment script in your preferred deployment tool, or click **Save to File**.




**Note:** The deployment scripts generated by Deep Security Manager for Windows agent deployments require Windows PowerShell version 4.0 or later. You must run PowerShell as an Administrator and you may have to run the following command to be able to run scripts:
`Set-ExcecutionPolicy RemoteSigned`

**Note:** If you want to deploy an agent to an early version of Windows or Linux that doesn't include PowerShell 4.0 or curl 7.3.4 at a minimum, you'll have to use a different deployment script from the one offered through the Deep Security Manager. This deployment script is provided in this article. You can't use the one in Deep Security Manager because it includes a `--tlsv1.2` (Linux) or `Tls12;` (Windows) tag. This tag enforces the use of TLS 1.2 communication between agent and manager, which is not supported by older OSs.

If you are using Amazon Web Services and deploying new Amazon EC2, Amazon WorkSpace, or VPC instances, copy the generated script and paste it into the **User Data** field. This will let you launch existing Amazon Machine Images (AMIs) and automatically install and activate the agent at startup. The new instances must be able to access the URLs specified in the generated deployment script. This means that your Deep Security Manager must be either Internet-facing, connected to AWS via VPN or Direct Link, or that your Deep Security Manager be deployed on Amazon Web Services too.

When copying the deployment script into the **User Data** field for a **Linux** deployment, copy the deployment script as-is into the "User Data" field and CloudInit will execute the script with sudo. (If there are failures, they will be noted in `/var/log/cloud-init.log`.)

**Note:** The **User Data** field is also used with other services like CloudFormation. For more information, see:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-waitcondition.html

## Troubleshooting and tips

- If you are attempting to run a deployment script and see exit code 2 **"TLS certificate validation for the agent package download has failed. Please check that your Deep Security Manager TLS certificate is signed by a trusted root certificate authority. For more information, search for "deployment scripts" in the Deep Security Help Center."**, the deployment script was created with the **Validate Deep Security Manager TLS certificate** checkbox selected. This error appears if Deep Security Manager is using a certificate that is not publicly trusted (such as the default self-signed certificate) for the connection between Deep Security Manager and its agents, or if there is a problem with a

third-party certificate, such as a missing certificate in the trust chain between your certificate and the trusted CA. For information on certificates, see "Replace the Deep Security Manager SSL certificate" on page 756. As an alternative to replacing the trusted certificate, you can clear the **Validate Deep Security Manager TLS certificate** checkbox when generating a deployment script. Note that this is not recommended for security reasons.

- If you are attempting to deploy the agent from PowerShell (x86), you will receive the following error : `C:\Program Files (x86)\Trend Micro\Deep Security Agent\dsa_control' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.`

  The PowerShell script expects the environment variable for `ProgramFiles` to be set to "Program Files", not "Program Files (x86)". To resolve the issue, close PowerShell (x86) and run the script in PowerShell as an administrator.

- If you do not intend to enable anti-malware protection on your computers, you may want to prevent the installation of the anti-malware engine entirely. To do so, delete the string "ADDLOCAL=ALL" from the deployment script.
- On Windows computers, the deployment script will use the same proxy settings as the local operating system. If the local operating system is configured to use a proxy and the Deep Security Manager is accessible only through a direct connection, the deployment script will fail.

## Automatically assign policies by AWS instance tags

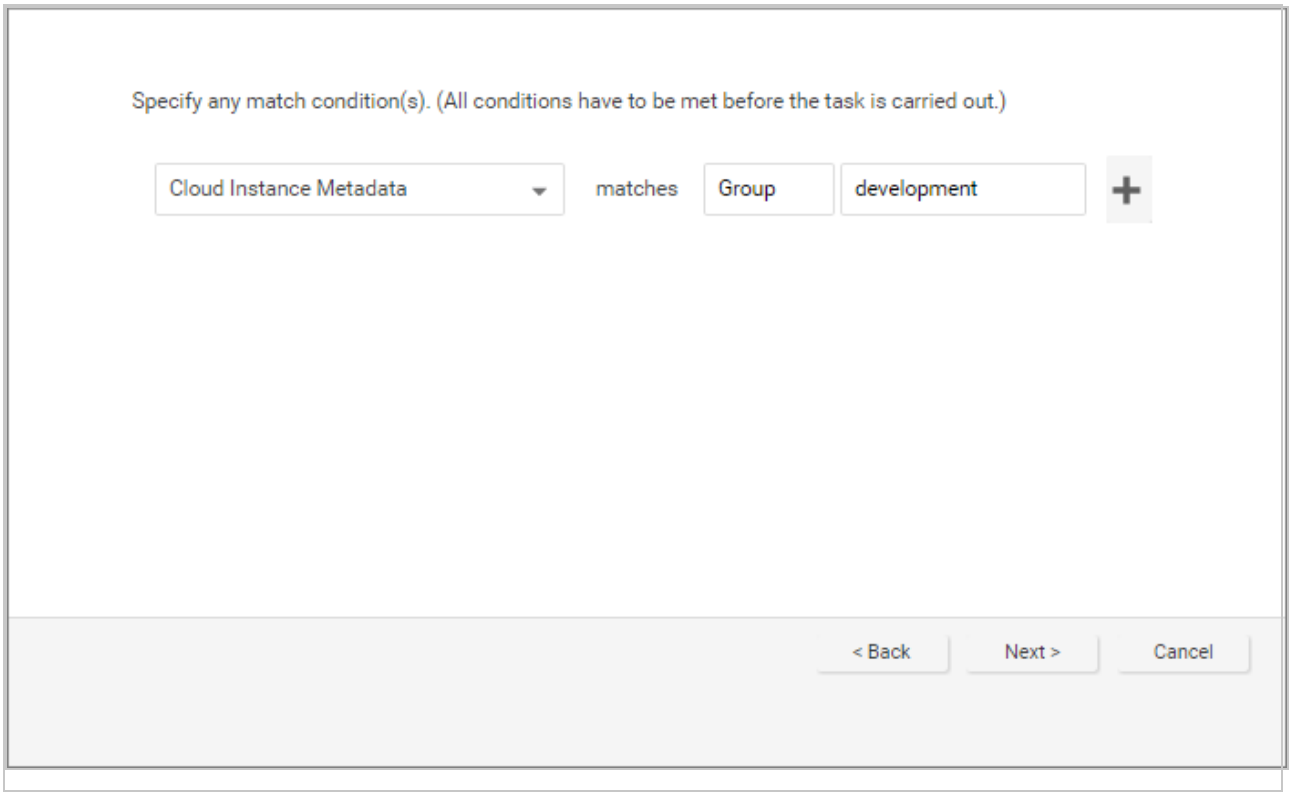
AWS tags allows you to categorize your resources by assigning metadata to AWS EC2 instances in the form of keys and values. You can also tag Amazon WorkSpaces with the similar key and value pair. Deep Security can use this metadata to trigger the automatic assigning of a policy to a Deep Security Agent when that agent is activated. This is done by creating an event-based task in Deep Security and defining the event, policy, and metadata. Event-based tasks are used to monitor protected resources for specific events and then perform tasks based on certain conditions: in this case the event is agent-initiated activation and a specific AWS instance tag is the condition.

This article describes how to do this using the following examples:

- Policy: AIA_Policy
- AWS tag key: Group
- AWS tag value: development

**Note:** The example below is based on the assumption that the policy AIA_Policy has already been created.

1. Go to **Administration** -> **Event-Based Tasks** in the Deep Security Manager console and click **New**.
2. Select **Agent-Initiated Activation** from the **Event** list and click **Next**.
3. Select the **Assign Policy** check box, select **AIA_Policy** from the list, and click **Next**.
4. Select **Cloud Instance Metadata** from the list, type **Group** and **development** into the key and value fields, and click **Next**.




5. Type and name for the event-based task and click **Finish** to save it.

You have now created an event-based task that will apply the AIA_Policy to an instance tagged with the key "Group" and the value "development" when the agent is activated on that instance.

## Integrate Deep Security with AWS Elastic Beanstalk

If you are using AWS Elastic Beanstalk to deploy and manage your applications in the AWS cloud, you can integrate Deep Security into your system so that services are scaled and your servers are automatically protected.

To help you integrate Deep Security Agent into your AWS Elastic Beanstalk configuration, we've provided extension configuration files in GitHub: deep-security/elastic-beanstalk. Follow the instructions in the repo's `README.md` file to edit and deploy the extension configuration files.

### For more information

- Customizing Software on Windows Servers - AWS Elastic Beanstalk
- Customizing Software on Linux Servers - AWS Elastic Beanstalk

## Deep Security Smart Check

Deep Security Smart Check is a container image scanner from Trend Micro. It performs pre-runtime scans of Docker images to detect OS vulnerabilities and malware, enabling you to fix issues before they reach the orchestration environment (for example, Kubernetes).

Deep Security Smart Check has two types of documentation:

- The Deployment Guide describes how Smart Check works and provides instructions on how to install and configure it.
- The API documentation provides information on using the Smart Check API.

# Protect

Trend Micro Deep Security has tightly integrated modules that easily expand your security capabilities:

- "Intrusion Prevention " below
- "Anti-Malware " below
- "Firewall " on the next page
- "Web Reputation " on the next page
- "Integrity Monitoring " on the next page
- "Log Inspection " on the next page
- "Application Control" on page 290


# Intrusion Prevention

The Intrusion Prevention module inspects incoming and outgoing traffic to detect and block suspicious activity. This prevents exploitation of known and zero-day vulnerabilities. Deep Security supports "virtual patching": you can use Intrusion Prevention rules to shield from known vulnerabilities until they can be patched, which is required by many compliance regulations. You can configure Deep Security to automatically receive new rules that shield newly discovered vulnerabilities within hours of their discovery.

The Intrusion Prevention module also protects your web applications and the data that they process from SQL injection attacks, cross-site scripting attacks, and other web application vulnerabilities until code fixes can be completed.

For more information, see "Set up intrusion prevention" on page 541.

# Anti-Malware

The Anti-Malware module protects your Windows and Linux workloads against malicious software, such as malware, spyware, and Trojans. Powered by the Trend Micro™ Smart Protection Network™, the Anti-Malware module helps you instantly identify and remove malware and block domains known to be command and control servers.

For more information, see "Enable and configure anti-malware" on page 494.

# Firewall

The Firewall Module is for controlling incoming and outgoing traffic and it also maintains firewall event logs for audits.

For more information, see "Set up the Deep Security firewall" on page 584.

# Web Reputation

The majority of today's attacks start with a visit to a URL that's carrying a malicious payload. The Web Reputation module provides content filtering by blocking access to malicious domains and known communication and control (C&C) servers used by criminals. The Web Reputation module taps into the Trend Micro Smart Protection Network, which identifies new threats quickly and accurately.

For more information, see "Block access to malicious URLs with web reputation" on page 723.

# Integrity Monitoring

The Integrity Monitoring module provides the ability to track both authorized and unauthorized changes made to an instance and enables you to receive alerts about unplanned or malicious changes. The ability to detect unauthorized changes is a critical component in your cloud security strategy because it provides visibility into changes that could indicate the compromise of an instance.

For more information, see "Set up integrity monitoring" on page 632.

# Log Inspection

The Log Inspection module captures and analyzes system logs to provide audit evidence for PCI DSS or internal requirements that your organization may have. It helps you to identify important security events that may be buried in multiple log entries. You can configure Log Inspection to forward suspicious events to an SIEM system or centralized logging server for correlation, reporting, and archiving.

For more information, see "Set up log inspection" on page 692.

# Application Control

The Application Control module monitors changes - "drift" or "delta" - compared to the computer's original software. Once application control is enabled, all software changes are logged and events are created when it detects new or changed software on the file system. When Deep Security Agent detects changes, you can allow or block the software, and optionally lock down the computer.

For more information, see "Verify that application control is enabled" on page 469.

# Manage protected computers

Perform the following tasks to protect and monitor computers using Deep Security:

- "Add computers and other resources to Deep Security Manager" below
- "Computer and agent statuses" on page 328
- "Connect agents behind a proxy" on page 203

## Add computers and other resources to Deep Security Manager

The **Computers** page in Deep Security Manager enables you to manage and monitor the computers you are protecting with Deep Security.

This page regularly refreshes itself to display the most current information. (You can modify the refresh rate on a per-user basis. Go to **Administration > User Management > Users** and then double-click on a user account to open its **Properties** window. On the **Settings** tab, in the **Refresh Rate** section, modify the page refresh rate.)

### Add computers to the manager

**Note:** After being installed on a computer, an agent must be activated by the Deep Security Manager. During activation, the Deep Security Manager sends a fingerprint to the agent, after

which the agent accepts instructions only from a manager with that unique fingerprint.

You can add computers in many different ways.

- "Add local network computers" on the next page
  If you are protecting computers on a locally accessible network you can add them individually by supplying their IP address or hostname or you can perform a Discovery operation to search for all computers visible to the Deep Security Manager.
- "Add computer groups from Microsoft Active Directory" on page 321
  You can import computer groups from Microsoft Active Directory or any other LDAP-based directory service.
- "Add virtual machines hosted on VMware vCloud" on page 318
- "Add AWS cloud accounts" on page 295
- "Add a Microsoft Azure account to Deep Security" on page 311
- "Bake the agent into your AMI or WorkSpace bundle" on page 192
  You can install a preactivated Deep Security Agent onto the instance that your Amazon Machine Image (AMI) is based on.
- "Use deployment scripts to add and protect computers" on page 281
  If you are going to be adding and protecting a large number of computers you may want to automate the process of installing and activating agents. You can use the Deep Security Manager's deployment script generator to generate scripts you can run on your computers which will install the agents and optionally perform subsequent tasks like activation and policy assignment. The scripts are also useful as a starting template to create your own customized scripts to execute various additional available commands.

## Group computers

Creating computer groups is useful from an organizational point of view and it speeds up the process of applying and managing policies. Groups are displayed in the tree structure on the left side of the Computers page. To create a new group, select the computer group under which you want to create the new computer group and then click **Add > Create Group(s)**.

To move a computer to a group, select the computer and click **Actions > Move to Group**. Keep in mind that policies are applied at the computer level, not the computer group level. Moving a

computer from one computer group to another has no effect on the policy assigned to that computer.

To remove a group, right-click it and click **Remove Group**. You can only remove a computer group if it contains no computers and has no sub-groups.

You can also "Group computers dynamically with smart folders" on page 1023.

## Export your computers list

You can click **Export** on the Computers page to export your computers list to an XML or CSV file. Exporting is useful when you want to back up your computer information, integrate it with other reporting systems, or to migrate computers to another Deep Security Manager. (If you export, you do not have to re-discover and scan computers from the new manager.)

> **Note:** The exported computers file does **not** include any assigned policies, firewall rules, firewall stateful configurations or intrusion prevention rules. To export this configuration information use the Policy export option in the **Policies** page.

## Delete a computer

If you delete a computer (by selecting it and clicking **Delete**), all information pertaining to that computer is deleted along with it. If you re-discover the computer, you will have to re-assign a policy and whatever rules were assigned previously.

## Add local network computers

### Agent-initiated activation

If the Deep Security Manager is hosted outside of your local network and cannot initiate communication with the computers on your network, you will need to instruct the computers to perform agent-initiated activation. With agent-initiated activation, you must install the Deep Security Agent on the computer and then run a set of command-line instructions which tell the Agent to communicate with the Deep Security Manager. During the communication, the Deep Security Manager activates the agent and can be further instructed to perform a number of other

actions such as assigning a security policy, making the computer a member of a computer group, and so on.

If you are going to add a large number of computers to the Deep Security Manager at one time, you can use the command-line instructions to create scripts to automate the process. For more information on agent-initiated activation, scripting, and command line options, see "Command-line basics" on page 244.

## Manually add a computer

You can manually add an individual computer by specifying its IP address or hostname.

1. Go to the **Computers** page and click **Add > Add Computer** in the toolbar to display the **New Computer** wizard.
2. Enter the new computer's IP address or hostname.
3. Select a policy to assign to it from the list.
4. Select a relay group from which the new computer will download security updates.
5. Click **Next** to begin the search for the computer.

If the computer is detected and an agent is installed and running on that computer, the computer will be added to your computers list and the agent will be activated.

> **Note:** "Activating" an agent means that the manager communicates with the agent sending it a unique "fingerprint". The agent will then use this fingerprint to uniquely identify the Deep Security Manager and will not accept instructions from any other managers that might try to contact it.

If a policy has been assigned to the computer, the policy will be deployed to the agent and the computer will be protected with all the rules and configurations that make up the policy.

By default, the security updates delivered by relay groups include new malware patterns. If you have enabled the **Support 9.0 (and earlier) agents** option (on the **Administration > System Settings > Updates** page), updates to the engines will also be included.

If the computer is detected but no Deep Security Agent is present, you will be told that the computer can still be added to your computers list but that you still have to install an agent on the computer. Once you install an agent on the computer, you will have to find the computer in your computers list, right-click it, and choose **Activate/Reactivate** from the context menu.

If the computer is not detected (not visible to the manager), you will be told that you can still add the computer but that when it becomes visible to the manager you will have to activate it as above.

## Discover computers

A discovery operation scans the network for visible computers. To initiate a discovery operation, go to the **Computers** page, click **Add > Discover**. The Discover Computers dialog will appear.

You are provided several options to restrict the scope of the scan. You can choose to perform a port scan of each discovered computer.

> **Note:** If you are discovering or scanning a large number of computers, a port scan can take time and reduce performance until it is complete.

When discovering computers, you can specify a computer group to which they should be added. Depending on how you have chosen to organize your computer groups, it may be convenient to create a computer group called "Newly Discovered Computers", or "Newly Discovered Computers on Network Segment X" if you will be scanning multiple network segments. You can then move your discovered computers to other computer groups based on their properties and activate them.

During discovery, the manager searches the network for any visible computers that are not already listed. When a computer is found, the manager attempts to detect whether an agent is present. When discovery is complete, the manager displays all the computers it has detected and displays their status in the **Status** column.

> **Note:** The Discovery operation only checks the status of newly-discovered computers. To update the status of already-listed computers, right-click the selected computer(s) and click **Actions > Check Status**.

After discovery operations, a computer can be in one of the following states:

- **Discovered (No Agent):** The computer has been detected but no agent is present. The computer may also be in this state if an agent is installed but has been previously activated and is configured for agent initiated communications. In this case, you will have to deactivate and then reactivate the agent. ("No Agent" will also be reported if the agent is

installed but not running.)

- **Discovered (Activation Required):** The agent is installed and listening, and has been activated, but is not yet being managed by the manager. This state indicates that this manager was at one point managing the agent, but the agent's public certificate is no longer in the manager's database. This may be the case if the if the computer was removed from the manager and then discovered again. To begin managing the agent on this computer, right-click the computer and select **Activate/Reactivate**. Once reactivated, the **Status** will change to "Online".
- **Discovered (Deactivation Required):** The agent is installed and listening, but it has already been activated by another manager. In this case, the agent must be deactivated (reset) prior to activation by this manager. Deactivating an agent can be done using the manager that originally activated it or it can be reset through the command line. To deactivate the agent from the manager, right-click the computer and choose **Actions > Deactivate**. To deactivate the agent from the command line, see "Reset the agent" on page 259.

The discovery operation will not discover computers running as virtual machines in a vCenter or computers in an LDAP directory or Active Directory.

**Note:** The Discovery operation does not discover computers running as virtual machines in a vCenter. The Discovery operation does not discover computers in a Microsoft Active Directory.

## Add AWS cloud accounts

You can add your AWS account to Deep Security. This imports all your Amazon EC2 instances into Deep Security Manager. Optionally, you can also "Add Amazon WorkSpaces" on page 308. They'll appear in one of the following locations:

- EC2 instances appear on the left under **Computers** > *your_AWS_account* > *your_region* > *your_VPC* > *your_subnet*
- Amazon WorkSpaces appear on the left under **Computers** > *your_AWS_account* > *your_region* > **WorkSpaces**

From there, you can manage them like any other computer.

You can add multiple AWS accounts if your Amazon EC2 instances and Amazon WorkSpaces are hosted under different AWS accounts.

**Note:** If you previously added Amazon EC2 instances or Amazon WorkSpaces as individual computers, and they are part of your AWS account, after importing the account, the instances are moved into the tree structure described above.

There are several ways to add AWS accounts to Deep Security Manager:

- "Method: Manager instance role and cross-account role" on the next page. Use this method if you want to add one or more AWS accounts that do not host Deep Security Manager. With this method, you assign a manager instance role to the EC2 instance that hosts Deep Security Manager. This role is then referenced in cross account roles under your other AWS accounts, enabling access to all of them.

  You can use this method with:

  - Deep Security as a Service
  - Deep Security AMI from AWS Marketplace
  - Deep Security on-premise, hosted inside AWS

- "Method: Manager instance role (single AWS account)" on page 303. Use this method if you want to add the AWS account where Deep Security Manager is hosted. With this method, you assign a manager instance role to the EC2 instance that hosts Deep Security Manager. Deep Security Manager then uses this role to access the AWS account.

  You can use this method with:

  - Deep Security AMI from AWS Marketplace
  - Deep Security on-premise, hosted inside AWS

- "Method: AWS access keys" on page 305. This method works with all deployment types, but is only recommended if your Deep Security Manager is hosted outside of AWS and you only have one AWS account to add, or if you have tried another method and it doesn't work.

  For all other scenarios, we recommend you use another method. Specifying access keys in Deep Security Manager is discouraged because the keys need to be updated

periodically (for security reasons), which creates management overhead. With this method, you log in to the AWS account that holds your Amazon EC2 instances and Amazon WorkSpaces and you create an IAM user and access keys. You then specify the access keys in Deep Security Manager, which uses them to access the IAM user and associated AWS account. You can repeat these steps for each AWS account you want to add.

You can use this method with:

- Deep Security as a Service
- Deep Security AMI from AWS Marketplace
- Deep Security on-premise
- Deep Security Manager VM for Azure Marketplace

### Method: Manager instance role and cross-account role

The instructions below assume you have two different AWS accounts, and both accounts contain Amazon EC2 instances and Amazon WorkSpaces that you want to protect...

- AWS DSM Account (where Deep Security Manager or Deep Security as a Service resides)
- AWS Account A

...and you want to protect the Amazon EC2 instances and Amazon WorkSpaces in both accounts with Deep Security.

Follow these high-level steps, which are described in detail below:

1. "Configure the AWS DSM account" on the next page (Skip if using Deep Security as a Service): Log in to the AWS DSM Account, create an IAM policy, create a manager instance role that references the IAM policy and attach it to the Deep Security Manager EC2 instance.
2. "Configure AWS Account A" on page 300: Log in to AWS Account A, configure an IAM policy, and create a cross account role that references the manager instance role.
3. "Add the AWS accounts to Deep Security Manager" on page 302: In Deep Security Manager, indicate that you're using a manager instance role, and then add AWS DSM Account and AWS Account A.

After completing these steps, Deep Security Manager can use the manager instance role to access AWS DSM Account and see its Amazon EC2 instances and Amazon WorkSpaces. Additionally, Deep Security Manager can access the resources under AWS Account A (indirectly) by way of the cross account roles that reference the manager instance role.

### Configure the AWS DSM account

Skip this section if you are using Deep Security as a Service. Deep Security as a Service already has an IAM policy and manager instance role that you can use.

First, log in to AWS DSM Account (the account under which your Deep Security Manager is located) and configure an IAM policy:

1. Log in to your Amazon Web Services Console and go to the **IAM** service.
2. In the left navigation pane, click **Policies**.

   **Note:** If this is your first time on this page, you'll need to click **Get Started**.

3. Click **Create policy**.
4. Select the **JSON** tab.
5. Copy the following JSON code into the text box:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "cloudconnector",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSecurityGroups",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaceBundles",
```

```
                "workspaces:DescribeTags",
                "iam:ListAccountAliases",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "sts:AssumeRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

**Note:** The `"sts:AssumeRole"` permission is required only if you are using cross account roles.

**Note:** The `"iam:GetRole"` and `"iam:GetRolePolicy"` permissions are optional, but recommended because they allow Deep Security to determine whether you have the correct policy when an update to the manager occurs that requires additional AWS permissions.

6. Click **Review policy**.
7. Give the policy a name and description. Example name: Deep_Security_Policy.
8. Click **Create policy**. Your policy is now ready to use.

Next, create an EC2 instance role for the EC2 instance where your Deep Security Manager is running:

1. Go to the **IAM** service.
2. Click **Roles**.
3. Click **Create role**.
4. Make sure the **AWS service** box is selected.
5. Click **EC2** from the list of services. More options are revealed.
6. Click **EC2 Allows EC2 instances to call AWS services on your behalf**. Click **Next: Permissions**.
7. Select the check box next to the IAM policy you just created. Click **Next: Review**.
8. Enter a **Role name** and **Role description**.
   Example role name: Deep_Security_Manager_Instance_Role
9. Click **Create role**.

10. Select the role in the list to reveal its details.
11. Look for the **Role ARN** field at the top of the page. Its value is similar to: arn:aws:iam::1234567890:role/Deep_Security_Manager_Instance_Role
12. Note the role's account ID in the ARN. It is the number (1234567890). You'll need it later.

Next, attach the manager instance role to the EC2 instance:

1. Go to the **EC2** service.
2. Click **Instances** on the left, and select the check box next to the EC2 instance that hosts your Deep Security Manager.
3. Click **Actions > Instance Settings > Attach/Replace IAM Role**.
4. From the **IAM role** drop-down list, select the manager instance role (Deep_Security_Manager_Instance_Role).
5. Click **Apply**.

You have now created a manager instance role with the correct IAM policy, and attached it to the Deep Security Manager's EC2 instance.

### Configure AWS Account A

First, log out of AWS and log back in using AWS Account A. This is the account under which some or all of your Amazon EC2 instances and Amazon WorkSpaces are located.

Next, while logged in to AWS Account A, configure an IAM policy for AWS Account A. It is the same as the policy for the AWS DSM account, except it does not require the `sts:AssumeRole` permission:

1. Log in to your Amazon Web Services Console and go to the **IAM** service.
2. In the left navigation pane, click **Policies**.

   **Note:** If this is your first time on this page, you'll need to click **Get Started**.

3. Click **Create policy**.
4. Select the **JSON** tab.
5. Copy the following JSON code into the text box:

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "cloudconnector",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSecurityGroups",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeTags",
                "iam:ListAccountAliases",
                "iam:GetRole",
                "iam:GetRolePolicy"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

**Note:** The `"iam:GetRole"` and `"iam:GetRolePolicy"` permissions are optional, but recommended because they allow Deep Security to determine whether you have the correct policy when an update to the manager occurs that requires additional AWS permissions.

6. Click **Review policy**.
7. Give the policy a name and description. Example name: Deep_Security_Policy_2.
8. Click **Create policy**. Your policy is now ready to use.

Next, create a cross account role that references the manager instance role:

1. Go to the **IAM** service.
2. In the left navigation pane, click **Roles**.
3. In the main pane, click **Create role**.
4. Click the **Another AWS account** box.

5. In the **Account ID** field, enter the account ID of the manager instance role.
   If you are using Deep Security as a Service, the manager instance role account ID is: 147995105371
   If you are using Deep Security AMI from AWS Marketplace or an on-premise version of Deep Security Manager inside AWS, you should have noted the manager instance role's account ID when you created it previously. In this example, it is: 1234567890
6. Next to **Options**, enable **Require external ID**. In the **External ID** field, enter a long, random secret string.
7. Note the external ID. You'll need this information later.
8. Click **Next: Permissions**.
9. Select the IAM policy that you just created (the example name was Deep_Security_Policy_2) and then click **Next: Review**.
10. On the **Review** page, enter a role name and description. Example role name: Deep_Security_Role_2.
11. On the main role page, search for the role you just created (Deep_Security_Role_2).
12. Click it.
13. Find the **Role ARN** field at the top and note the value. You'll need it later. It looks similar to: arn:aws:iam::1234567890:role/Deep_Security_Role

You now have a cross account role under AWS Account A that includes the correct policy and references the manager instance role.

### Add the AWS accounts to Deep Security Manager

First, indicate that you want to use a manager instance role:

1. In Deep Security Manager, click **Administration** at the top.
2. Click **System Settings** on the left.
3. Click the **Advanced** tab in the main pane.
4. Scroll to the bottom and look for the **Manager AWS Identity** section.
5. Make sure **Use Manager Instance Role** is selected.

   **Note:** If **Use Manager Instance Role** does not appear, make sure that you attached the role to the EC2 instance where Deep Security Manager is installed, and then "Restart the Deep Security Manager" on page 734. On restart, Deep Security detects the role of the

manager's EC2 instance and displays the **Use Manager Instance Role** option.

6. Click **Save**.

Next, add the AWS DSM Account:

1. In Deep Security Manager, click **Computers** at the top.
2. In the main pane, click **Add > Add AWS Account**.
3. Select **Use Manager Instance Role**.
4. If AWS DSM Account includes Amazon WorkSpaces, select **Include Amazon WorkSpaces** to include them with your Amazon EC2 instances. By enabling the check box, you ensure that your Amazon WorkSpaces appear in the correct location in the tree structure in Deep Security Manager and are billed at the correct rate.
5. Click **Next**.

Deep Security Manager uses the manager instance role that is attached to its Amazon EC2 instance to add AWS DSM Account's EC2 and WorkSpace instances to Deep Security Manager.

Finally, add AWS Account A using its cross account role:

1. Click **Computers** at the top.
2. Click **Add > Add AWS Account**.
3. Select **Use Cross Account Role**.
4. Enter AWS Account A's **Cross Account Role ARN** and **External ID**. You noted these earlier, when you created the cross account role.
5. If AWS Account A includes Amazon WorkSpaces, select **Include Amazon WorkSpaces** to include them with your Amazon EC2 instances. By enabling the check box, you ensure that your Amazon WorkSpaces appear in the correct location in the tree structure in Deep Security Manager and are billed at the correct rate.
6. Click **Next**.
   AWS Account A's Amazon EC2 instances and Amazon WorkSpaces are loaded.

You have now added AWS DSM Account and AWS Account A to Deep Security Manager.

## Method: Manager instance role (single AWS account)

First, log in to AWS using the account that holds your Deep Security Manager and configure an IAM policy:

1. Log in to your Amazon Web Services Console and go to the **IAM** service.
2. In the left navigation pane, click **Policies**.

   **Note:** If this is your first time on this page, you'll need to click **Get Started**.

3. Click **Create policy**.
4. Select the **JSON** tab.
5. Copy the following JSON code into the text box:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "cloudconnector",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSecurityGroups",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeTags",
                "iam:ListAccountAliases",
                "iam:GetRole",
                "iam:GetRolePolicy"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
```

```
    ]
}
```

**Note:** The `"iam:GetRole"` and `"iam:GetRolePolicy"` permissions are optional, but recommended because they allow Deep Security to determine whether you have the correct policy when an update to the manager occurs that requires additional AWS permissions.

6. Click **Review policy**.
7. Give the policy a name and description. Example name: Deep_Security_Policy_2.
8. Click **Create policy**. Your policy is now ready to use.

Next, create an IAM role that includes the IAM policy. This is called the 'manager instance role'.

Next, attach the manager instance role to the EC2 instance where Deep Security Manager is hosted:

1. Log in to AWS using the account that holds your Deep Security Manager.
2. Go to the **EC2** service.
3. Click **Instances** on the left, and select the check box next to the EC2 instance that hosts your Deep Security Manager.
4. Click **Actions > Instance Settings > Attach/Replace IAM Role**.
5. From the **IAM role** drop-down list, select the manager instance role.
6. Click **Apply**.

Finally, add your AWS account to Deep Security Manager:

1. In the Deep Security Manager, click **Computers** at the top.
2. Click **Add > Add AWS Account**
3. Select **Use Manager Instance Role**.

   **Note:** If **Use Manager Instance Role** does not appear, make sure that you attached the manager instance role to the EC2 instance where Deep Security Manager is installed, and then "Restart the Deep Security Manager" on page 734. On restart, Deep Security detects the role of the manager's EC2 instance and displays the **Use Manager Instance Role** option.

4. If your AWS account includes Amazon WorkSpaces, select **Include Amazon WorkSpaces** to include them with your Amazon EC2 instances. By enabling the check box, you ensure

that your Amazon WorkSpaces appear in the correct location in the tree structure in Deep Security Manager and are billed at the correct rate.

5. Click **Next**.

Your Amazon EC2 instances and Amazon WorkSpaces under your AWS account are loaded.

### Method: AWS access keys

First, log in to AWS using the account that holds the Amazon EC2 instances and Amazon WorkSpaces that you want to protect.

Next, configure an IAM policy:

1. Log in to your Amazon Web Services Console and go to the **IAM** service.
2. In the left navigation pane, click **Policies**.

   **Note:** If this is your first time on this page, you'll need to click **Get Started**.

3. Click **Create policy**.
4. Select the **JSON** tab.
5. Copy the following JSON code into the text box:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "cloudconnector",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSecurityGroups",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeTags",
```

```
                "iam:ListAccountAliases",
                "iam:GetRole",
                "iam:GetRolePolicy"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

**Note:** The `"iam:GetRole"` and `"iam:GetRolePolicy"` permissions are optional, but recommended because they allow Deep Security to determine whether you have the correct policy when an update to the manager occurs that requires additional AWS permissions.

6. Click **Review policy**.
7. Give the policy a name and description. Example name: Deep_Security_Policy_2.
8. Click **Create policy**. Your policy is now ready to use.

Next, create an IAM user account:

1. Go to the **IAM** service.
2. Click **Users**.
3. Click **Add user**.
4. Enter a user name. Example: Deep_Security_IAM_User.
5. For **Access type**, select **Programmatic access**.
6. Click **Next: Permissions**.
7. Click the **Attach existing policies directly** box.
8. Find the IAM policy you just created and select the check box next to it.
9. Click **Next: Review**.
10. Click **Create user**. Your access key ID and secret access key are shown in the table.
11. Copy the access key ID and secret access key to a safe location. You'll need them later.

Finally, add your AWS account to Deep Security:

1. In the Deep Security Manager, click **Computers** at the top.
2. In the main pane, click **Add > Add AWS Account.**
3. Select **Use AWS Access Keys**.

4. Specify the **Access Key ID** and **Secret Access Key** that you generated when you created the IAM user.
5. If your AWS account includes Amazon WorkSpaces, select **Include Amazon WorkSpaces** to include them with your Amazon EC2 instances. By enabling the check box, you ensure that your Amazon WorkSpaces appear in the correct location in the tree structure in Deep Security Manager and are billed at the correct rate.
6. Click **Next**.

Your Amazon EC2 instances and Amazon WorkSpaces under your AWS account are loaded.

## Edit a cloud account

You can edit a cloud account's settings in Deep Security Manager. You might need to do this if, for example, your AWS account needs to be configured to include Amazon WorkSpaces. To edit a cloud account:

1. Log in to Deep Security Manager.
2. Click **Computers** at the top.
3. On the left, right-click your cloud account name and select **Properties**.
4. Edit the settings and click **OK**.

## Remove a cloud account from the manager

Removing a cloud account from Deep Security Manager permanently removes the account from the Deep Security database as well as its underlying computers. Your account with your cloud provider is unaffected and any Deep Security Agents that were installed on the instances are still installed, running, and providing protection (although they will no longer receive security updates). If you decide to re-import computers from the cloud account, the Deep Security Agents download the latest security updates at the next scheduled opportunity.

1. In Deep Security Manager, click **Computers** at the top.
2. In the navigation panel, right-click the cloud account and select **Remove Cloud Account**.
3. Confirm that you want to remove the account.
   The account is removed from the Deep Security Manager.

## Add Amazon WorkSpaces

Amazon WorkSpaces are virtual cloud desktops that run in Amazon Web Services (AWS). You can protect them with Deep Security following the instructions in one of these sections:

- "Protect Amazon WorkSpaces if you already added your AWS account" on the next page
- "Protect Amazon WorkSpaces if you have not yet added your AWS account" on page 310

**Note:** The Deep Security Agent only supports Amazon WorkSpaces Windows desktops–it does not support Linux desktops.

After completing the steps in one of the above-mentioned sections:

- your Amazon WorkSpaces are displayed in Deep Security Manager on the left under **Computers** > *your_AWS_account* > *your_region* > **WorkSpaces**
- your Amazon WorkSpaces are billed at the appropriate rate, if you are using:
  - Deep Security AMI from AWS Marketplace hourly pricing
- your Amazon WorkSpaces are protected by the Deep Security Agent

### Protect Amazon WorkSpaces if you already added your AWS account

If you already added your AWS account to Deep Security Manager (to protect your Amazon EC2 instances), complete the steps in this section to configure Deep Security to work with Amazon WorkSpaces.

1. Upgrade Deep Security AMI from AWS Marketplace to version 10.3. See "Upgrade the Deep Security Manager AMI" on page 740.
2. Launch an Amazon WorkSpace, and then install and activate Deep Security Agent 10.2 or later on it. See "Install the agent on Amazon EC2 and WorkSpaces" on page 185 for details. Optionally, create a custom WorkSpace bundle so that you can deploy it to many people. See "Bake the agent into your AMI or WorkSpace bundle" on page 192 for details on installation, activation, and bundle creation.
3. Modify your IAM policy to include Amazon WorkSpaces permissions:
   a. Log in to AWS with the account that was added to Deep Security Manager.
   b. Go to the **IAM** service.

   c. Find the Deep Security IAM policy. You can find it under **Policies** on the left, or you can look for the Deep Security IAM role or IAM user that references the policy and then click the policy within it.
   d. Modify the Deep Security IAM policy to look like the one shown in "Add AWS cloud accounts" on page 295. The policy includes Amazon WorkSpaces permissions. If you added more than one AWS account to Deep Security, the IAM policy must be updated under all the AWS accounts.
4. In Deep Security Manager, edit your AWS account:
   a. On the left, right-click your AWS account and select **Properties**.
   b. Enable **Include Amazon WorkSpaces**.
   c. Click **Save**.

You have now added Amazon WorkSpaces to Deep Security.

### Protect Amazon WorkSpaces if you have not yet added your AWS account

If you have not yet added your AWS account to Deep Security Manager, complete the steps in one of the following sections:

- If you want to protect existing Amazon WorkSpaces, read "Install the agent on Amazon EC2 and WorkSpaces" on page 185
- If you want to be able to launch new Amazon WorkSpaces with the agent 'baked in', read "Bake the agent into your AMI or WorkSpace bundle" on page 192.

## How do I migrate to the new cloud connector functionality?

If you previously used the "Add Cloud Account" wizard to import Amazon Web Services resources into Deep Security Manager, those resources are organized by AWS region on **Computers**. You may have run the wizard more than once if you have multiple AWS regions.

The latest versions of Deep Security provide the ability to display your AWS instances under your AWS account name, organized in a hierarchy that includes the AWS Region, VPC, and subnet.

Before migrating your AWS resources, you will need to edit the policy that allows Deep Security to access your AWS account:

1. Log in to your Amazon Web Services Console and go to **Identity and Access Management (IAM)**.
2. In the left navigation pane, click **Policies**.
3. In the list of policies, select the policy that allows Deep Security to access your AWS account.
4. Go to the **Policy Document** tab and click **Edit**.
5. Edit the policy document to include this JSON code:

```
{
        "Version": "2012-10-17",
        "Statement": [
                {
                        "Sid": "cloudconnector",
                        "Effect": "Allow",
                        "Action": [
                                "ec2:DescribeImages",
                                "ec2:DescribeInstances",
                                "ec2:DescribeRegions",
                                "ec2:DescribeSubnets",
                                "ec2:DescribeTags",
                                "ec2:DescribeVpcs",
                                "iam:ListAccountAliases",
                                "sts:AssumeRole"
                        ],
                        "Resource": [
                                "*"
                        ]
                }
        ]
}
```

**Note:** The `"sts:AssumeRole"` permission is required only if you are using cross-account role access. For more information on IAM roles, see Tutorial: Delegate Access Across AWS Accounts Using IAM Roles.

6. Select **Save as default version**.

**To migrate your AWS resources in the Deep Security Manager:**

1. In the Deep Security Manager, go to the **Computers** page.
2. In the Computers tree, right-click an AWS region and select **Upgrade to Amazon Account**.
3. Click **Finish** and then **Close**. Your AWS instances will now appear under your AWS account name, organized in a hierarchy that includes the AWS Region, VPC, and subnet.

## Add a Microsoft Azure account to Deep Security

Once you've installed Deep Security Manager, you can add and protect Microsoft Azure virtual machines by connecting a Microsoft Azure account to the Deep Security Manager. Virtual machines appear on the Computers page, where you can manage them like any other computer.

**Note:** When FIPS mode is enabled, you cannot add a Microsoft Azure account to Deep Security. See "FIPS 140-2 support" on page 1049.

Topics in this article:


- "Configure a proxy setting for the Azure account" below
- " Add virtual machines from a Microsoft Azure account to Deep Security" below
- "Manage Azure classic virtual machines with the Azure Resource Manager connector" on page 314
- "Remove an Azure account" on page 314


### Configure a proxy setting for the Azure account

You can configure the Deep Security Manager to use a proxy server to access resources in Azure accounts.

1. Go to **Administration > System Settings > Proxies**.
2. In the **Proxy Server Use** section, select your proxy from the **Deep Security Manager (Cloud Accounts - HTTP Protocol Only)** list.

### Add virtual machines from a Microsoft Azure account to Deep Security

You can add virtual machines to the Deep Security Manager using either the Quick or Advanced method. The **Quick** method requires an Azure account that has been assigned the Global Administrator role for the Azure Active Directory and the Subscription Owner role for the Azure

subscription to access your Azure resources. The **Advanced** method involves creating an Azure app for the Deep Security Manager that provides read-only access to Azure resources.

1. On the Computers page, click **Add > Add Azure Account**.
2. Select either the **Quick** method or the **Advanced** method, and then click **Next**. Follow the corresponding procedure below:

### Quick

**Note:** Trend Micro recommends creating a dedicated Azure account for adding Azure resources into the Deep Security Manager. This allows you to change the user rights of the dedicated account independently of Azure accounts used to access and manage Azure resources.

1. Enter your Azure portal account credentials and click **Sign in**.

   **Note:** The account must have been assigned the Global Administrator role for the Azure Active Directory and the Subscription Owner role for the Azure subscription. These privileges are required for Deep Security to automate the provisioning of a Service Principal object in the Azure Active Directory. Deep Security uses the Service Principal object to authenticate itself to your Azure subscription so that it can invoke the necessary Azure APIs to synchronize your Azure virtual machines in the Deep Security Manager console. For information on creating a user with a Global Administrator role, see Microsoft's Add new users or users with Microsoft accounts to Azure Active Directory article.

2. On the Deep Security Azure Connector permissions page, click **Accept**.
3. Select the **Azure Active Directory** and **Subscription Name**, and then click **Next**.
4. Review the summary information, and then click **Finish**.

**Note:** If you have previously added virtual machines from this Azure account, they will be moved under this account in the Computers tree.

### Advanced

1. Log in to the Azure portal.
2. Follow the procedures in "Create an Azure app for Deep Security" on page 315 to create a new Azure app for the Deep Security Manager.

3. Enter a **Display name**, and then enter the following Azure access information you recorded in step 2:
   - **Active Directory ID**
   - **Subscription ID**
   - **Application ID**
   - **Application Password**

   **Note:** If you are upgrading from the Azure classic connector to the Azure Resource Manager connector, the Display name and the Subscription ID of the existing connector will be used.
4. Click **Next**.
5. Review the summary information, and then click **Finish**.

The Azure virtual machines will appear in the Deep Security Manager under their own branch on the Computers page.

**Tip:** You will see all the virtual machines in the account. If you'd like to only see certain virtual machines, use smart folders to limit your results. See "Group computers dynamically with smart folders" on page 1023 for more information.

**Note:** If you have previously added virtual machines from this Azure account, they will be moved under this account in the Computers tree.

## Manage Azure classic virtual machines with the Azure Resource Manager connector

You can also manage virtual machines that were added with the Azure classic connector with the Azure Resource Manager connector, allowing you to manage both your Azure classic and Azure Resource Manager virtual machines with a single connector.

For more information, see "Why should I upgrade to the new Azure Resource Manager connection functionality?" on page 317

1. On the **Computers** page, in the **Computers tree**, right-click the **Azure classic portal** and then click **Properties**.
2. Click **Enable Resource Manager connection**.

3. Select either the **Quick** method or the **Advanced** method, and then click **Next**. Follow the corresponding procedure above.

### Remove an Azure account

Removing an Azure account from the Deep Security Manager will permanently remove the account from the Deep Security database. This will not affect the Azure account. Virtual machines with Deep Security agents will continue to be protected, but will not receive security updates. If you later import these virtual machines from the same Azure account, the Deep Security agents will download the latest security updates at the next scheduled update.

1. Go to the **Computers** page, right-click on the Microsoft Azure account in the navigation panel, and select **Remove Cloud Account**.
2. Confirm that you want to remove the account.
3. The account is removed from the Deep Security Manager.

## Create an Azure app for Deep Security

In your operating environment, it may not be desirable to allow the Deep Security Manager to access Azure resources with an account that has both the Global Administrator role for the Azure Active Directory and the Subscription Owner role for the Azure subscription. As an alternative, you can create an Azure app for the Deep Security Manager that provides read-only access to Azure resources.

**Note:** To create an Azure app, your account must have been assigned the User Administrator role for the Azure Active Directory and the User Access Administrator role for the Azure subscription.

To do this you will need to:

1. "Record the Azure Active Directory ID" below.
2. "Create the Azure app" below.
3. "Record the Azure app ID and password" on the next page.
4. "Record the Subscription ID" on the next page.
5. "Assign the Azure app a reader role and add it to your Azure Subscription" on the next page.

## Record the Azure Active Directory ID

1. On the Hub menu, click **Azure Active Directory** and select your Azure Active Directory.
2. In the **Azure Active Directory** blade, click **Properties**.
3. Record the **Directory ID**.

## Create the Azure app

1. In the **Azure Active Directory** blade, click **App registrations**.
2. Click **Add**.
3. Enter a **Name** (for example, Deep Security Azure Connector).
4. For the **Application Type**, select **Web app/API**.
5. Enter a **Sign-on URL**. The URL can be any value, but it must begin with the `http` prefix.

   **Note:** You must enter a URL in the **Sign-on URL** field, even though it is not used by Deep Security Azure integration. The value does not need to resolve to a valid address.

6. Click **Create**.The **Deep Security Azure Connector** app will appear in the **App registrations** list.

## Record the Azure app ID and password

1. In the **App registrations** list, click on the **Deep Security Azure Connector**.
2. Record the **Application ID**.
3. Click on **All settings**.
4. On the **Settings** blade, click **Keys**.
5. Enter a **Description** for the key.
6. Select an appropriate **Duration**.
7. Click **Save**.

   The key **Value** will appear.

8. Record the key **Value**. This will be used as the Application Password when registering the Azure app with Deep Security.

## Record the Subscription ID

1. On the Hub menu, go to **All Services** and click **Subscriptions**, then select the subscription you added the Deep Security Azure Connector app to.

2. Record the **Subscription ID**.

### Assign the Azure app a reader role and add it to your Azure Subscription

1. In the **Subscriptions** blade, click on **Access Control (IAM)**.
2. Click **Add**.
3. Click on the **Reader** role.
4. Select the **Deep Security Azure Connector** app. If it is not already in the list, enter it in the search field and select it when it appears.
5. Click **OK**.

You can now continue configuring Deep Security to add Azure virtual machines by following the remaining steps of the Advanced procedure in "Add a Microsoft Azure account to Deep Security" on page 311.

## Why should I upgrade to the new Azure Resource Manager connection functionality?

The next time you try to add an Azure cloud account to Deep Security Manager you will be shown a message suggesting that you upgrade to the new Resource Manager connection functionality. Basically, this new functionality allows Deep Security to connect to Azure virtual machines using the Resource Manager interface. As an Azure user, you are probably aware that the new Azure deployment model Resource Manager is now the default deployment model, replacing the classic model. Since new resources are deployed using this model by default, Deep Security is only able to display these VM resources on the Computers page if it is able to communicate with the Resource Manager interface. So, if you allow Deep Security to upgrade to this new functionality then VM resources deployed with either the Resource Manager deployment model or the classic deployment model will be visible on the Computers page.

Three things to note:

- The account must be the owner of the Azure subscription and must have the Global Admin role in your Azure Active Directory. These privileges are required so that Deep Security can automate the provisioning of a Service Principal object in your Azure Active Directory. Deep Security uses that Service Principal object to authenticate itself to your Azure subscription so that it can invoke the necessary Azure APIs to synchronize your Azure

VMs in the Deep Security Manager console. For instructions on creating a user with global administrator rights, see Microsoft's Add new users or users with Microsoft accounts to Azure Active Directory.

- You can upgrade to this new functionality in Deep Security as a Service (DSaaS) and in Deep Security 10. It is already available in the new Deep Security Manager VM for Azure Marketplace console and no upgrade is needed.
- Until you perform this upgrade VMs deployed using Resource Manager are still being fully protected by Deep Security but for you to see them on the Computers page they have to be added as a computer object. For more information, see "Why can't I view all of the VMs in an Azure subscription in Deep Security?" on page 1093

## Add virtual machines hosted on VMware vCloud

To import cloud resources into their Deep Security Manager, Deep Security users must first have an account with which to access the cloud provider service resources. For each Deep Security user who will import a cloud account into the Deep Security Manager, Trend Micro recommends creating dedicated account for that Deep Security Manager to access the cloud resources. That is, users should have one account to access and control the virtual machines themselves, and a separate account for their Deep Security Manager to connect to those resources.

**Note:** Having a dedicated account for Deep Security ensures that you can refine the rights and revoke this account at any time. It is recommended to give Deep Security an access key or secret key with read-only rights at all times.

**Note:** The Deep Security Manager only requires read-only access to import the cloud resources and mange their security.

**Note:** When FIPS mode is enabled, you cannot add virtual machines hosted on VMware vCloud. See "FIPS 140-2 support" on page 1049.

### Proxy setting for cloud accounts

You can configure Deep Security Manager to use a proxy server specifically for connecting to instances being protected in cloud accounts. The proxy setting can be found in **Administration >**

**System Settings > Proxies > Proxy Server Use > Deep Security Manager (Cloud Accounts - HTTP Protocol Only)**.

## Create a VMware vCloud Organization account for the manager

1. Log in to VMware vCloud Director.
2. On the **System** tab, go to **Manage And Monitor**.
3. In the left navigation pane, click **Organizations**.
4. Double-click the Organization you wish to give the Deep Security user access to.
5. On the **Organizations** tab, click **Administration**.
6. In the left navigation pane, go to **Members > Users**.
7. Click the " plus " sign to create a new user.
8. Enter the new user's credentials and other information, and select **Organization Administrator** as the user's **Role**.

   Note: **Organization Administrator** is a simple pre-defined Role you can assign to the new user account, but the only privilege required by the account is **All Rights > General > Administrator View** and you should consider creating a new vCloud role with just this permission.

9. Click **OK** to close the new user's properties window.

The vCloud account is now ready for access by a Deep Security Manager.

Note: To import the VMware vCloud resources into the Deep Security Manager, users will be prompted for the **Address** of the vCloud, their **User name** , and their **Password** .

The **User name** must include "@orgName". For example if the vCloud account's username is **kevin** and the vCloud Organization you've given the account access to is called **CloudOrgOne**, then the Deep Security user must enter **kevin@CloudOrgOne** as their username when importing the vCloud resources.

(For a vCloud administrator view, use **@system**.)

## Import computers from a VMware vCloud Organization Account

1. In the Deep Security Manager, go to the **Computers** section, right-click **Computers** in the navigation panel and select **Add vCloud Account** to display the **Add vCloud Cloud**

**Account** wizard.

2. Enter a **Name** and **Description** of the resources you are adding. (These are only used for display purposes in the Deep Security Manager.)
3. Enter the vCloud **Address**. (The hostname of the vCloud Director host machine.)
4. Enter your **user name** and **Password**.

   **Note:** Your **user name** must be in the form **username@vcloudorganization**.

5. Click **Next**.
6. Deep Security Manager will verify the connection to the cloud resources and display a summary of the import action. Click **Finish**.

The VMware vCloud resources now appear in the Deep Security Manager under their own branch on the **Computers** page.

## Import computers from a VMware vCloud Air data center

1. In the Deep Security Manager, go to the **Computers** section, right-click **Computers** in the navigation panel and select **Add vCloud Account** to display the **Add vCloud Account** wizard.
2. Enter a **Name** and **Description** of the vCloud Air data center you are adding. (These are only used for display purposes in the Deep Security Manager.)
3. Enter the **Address** of the vCloud Air data center.

   **Note: To determine the address of the vCloud Air data center:**

   a. Log in to your vCloud Air portal.
   b. On the **Dashboard** tab, click on the data center you want to import into Deep Security. This will display the **Virtual Data Center Details** information page.
   c. In the Related Links section of the **Virtual Data Center Details** page, click on **vCloud Director API URL**. This will display the full URL of the vCloud Director API.
   d. Use the hostname only (not the full URL) as the Address of the vCloud Air data center that you are importing into Deep Security.

4. Enter your **user name** and **Password**.

   **Note:** Your **user name** must be in the form **username@virtualdatacenterid**.

5. Click **Next** .

6. Deep Security Manager will verify the connection to the vCloud Air data center and display a summary of the import action. Click **Finish**.

The VMware vCloud Air data center now appears in the Deep Security Manager under its own branch on the **Computers** page.

## Configure software updates for cloud accounts

Relays are modules within Deep Security Agents that are responsible for the download and distribution of Security and Software updates. Normally, the Deep Security Manager informs the relays when new updates are available, the relays get the updates and then the agents get their updates from the relays.

However, if your Deep Security Manager is in an enterprise environment and you are managing computers in a cloud environment, relays in the cloud may not be able to communicate with Deep Security Manager. You can solve this problem by allowing the relays to obtain software updates directly from the Trend Micro Download Center when they cannot connect to the Deep Security Manager. To enable this option, go to **Administration** > **System Settings** > **Updates** and under **Software Updates**, select **Allow Relays to download software updates from Trend Micro Download Center when Deep Security Manager is not accessible**.

## Remove a cloud account

Removing a cloud provider account from Deep Security Manager permanently removes the account from the Deep Security database. Your account with your cloud provider is unaffected and any Deep Security agents that were installed on the instances will still be installed, running, and providing protection (although they will no longer receive security updates.) If you decide to re-import computers from the Cloud Provider Account, the Deep Security Agents will download the latest Security Updates at the next scheduled opportunity.

1. Go to the **Computers** page, right-click on the Cloud Provider account in the navigation panel, and select **Remove Cloud Account**.
2. Confirm that you want to remove the account.
3. The account is removed from the Deep Security Manager.

## Add computer groups from Microsoft Active Directory

Deep Security can use an LDAP server such as Microsoft Active Directory for computer discovery and to create user accounts and their contacts. Deep Security Manager queries the server, and then displays computer groups according to the structure in the directory.

**Note:** If you are using Deep Security in FIPS mode, you must import the Active Directory's SSL certificate into Deep Security Manager before connecting the manager with the directory. See "Manage trusted certificates" on page 216.

1. Right-click **Computers** in the navigation panel and select **Add Active Directory**
2. Type a name and description for your imported directory (it doesn't have to match the directory's name in Active Directory), the IP and port number of the Active Directory server, and then your access method and credentials.

   **Note:** You must include your domain name with your username in the **User Name** field.

   **Note:** If you are using Deep Security in FIPS mode, click **Test Connection** in the Trusted Certificate section to check whether the Active Directory's SSL certificate has been imported successfully into Deep Security Manager.

   Click **Next** to continue.
3. Specify your directory's schema. (If you haven't customized the schema, you can use the default values for a Microsoft Active Directory server.)

   **Note:** The **Details** window of each computer in the Deep Security Manager has a "Description" field. To use an attribute of the "Computer" object class from your Active Directory to populate the "Description" field, type the attribute name in the **Computer Description Attribute** text box.

   Select **Create a Scheduled Task to Synchronize this Directory** if you want to automatically keep this structure in the Deep Security Manager synchronized with your Active Directory server. A **Scheduled Task** wizard will appear when you are finished adding the directory. (You can set this up later using the **Scheduled Tasks** wizard: **Administration > Scheduled Tasks**.)
4. Click **Next** to continue.

5. When the Manager has imported your directory, it will display a list of computers that it added. Click **Finish**.

   The directory structure will appear on the **Computers** page.

## Additional Active Directory options

Right-clicking an Active Directory structure gives you options that are not available for non-directory computer groups:

- **Remove Directory**
- **Synchronize Now**

### Remove Directory

When you remove a directory from the Deep Security Manager, you have these options:

- **Remove directory and all subordinate computers/groups from DSM:** Remove all traces of the directory.
- **Remove directory but retain computer data and computer group hierarchy:** Turn the imported directory structure into identically organized regular computer groups, no longer linked with the Active Directory server.
- **Remove directory, retain computer data, but flatten hierarchy:** Remove links to the Active Directory server, discards directory structure, and places all the computers into the same computer group.

### Synchronize Now

You can manually trigger Deep Security Manager to synchronize with the Active Directory server to refresh information on computer groups.

**Tip:** You can automate this procedure by creating a scheduled task.

## Server certificate usage

If it is not already enabled, enable SSL on your Active Directory server.

Computer discovery can use either SSL or TLS or unencrypted clear text, but importing user accounts (including passwords and contacts) requires authentication and SSL or TLS.

SSL or TLS connections require a server certificate on your Active Directory server. During the SSL or TLS handshake, the server will present this certificate to clients to prove its identity. This certificate can be either self-signed or signed by a certificate authority (CA). If you don't know if your server has a certificate, on the Active Directory server, open the Internet Information Services (IIS) Manager, and then select **Server Certificates**. If the server doesn't have a signed server certificate, you must install it.

## Filter Active Directory objects

When importing Active Directory objects, search filters are available to manage the objects that will be returned. By default the wizard will only show groups. You can add additional parameters to the filter to further refine the selections. For additional information about search filter syntax, refer to https://msdn.microsoft.com/en-us/library/aa746475(v=vs.85).aspx

## Import users and contacts

Deep Security can import user account information from Active Directory and create corresponding Deep Security users or contacts. This offers the following advantages:

- Users can use their network passwords as defined in Active Directory.
- Administrators can centrally disable accounts from within Active Directory.
- Maintenance of contact information is simplified (e.g., email, phone numbers, etc.) by leveraging information already in Active Directory.

Both users and contacts can be imported from Active Directory. Users have configuration rights on the Deep Security Manager. Contacts can only receive Deep Security Manager notifications. The synchronization wizard allows you to choose which Active Directory objects to import as users and which to import as contacts.

**Note:** To successfully import an Active Directory user account into Deep Security as a Deep Security user or contact, the Active Directory user account must have a **userPrincipalName** attribute value. (The **userPrincipalName** attribute corresponds to an Active Directory account holder's "User logon name".)

1. Click **Administration > User Management** and then click either **Users** or **Contacts**.

2. Click **Synchronize with Directory**.
   If this is the first time user or contact information is imported, the server information page is displayed. Otherwise, the Synchronize with Directory wizard is displayed.
3. Select the appropriate access options, provide logon credentials, and click **Next**.
4. Select the groups you want to synchronize by selecting them from the left column and clicking **>>** to add them to the right column and then click **Next**.

   Tip: You can select multiple groups by holding down shift or control while clicking on them.
5. Select whether to assign the same Deep Security role to all Directory group members or to assign Deep Security roles based on Directory Group membership and then select a default role from the list and click **Next**.
6. If you assigned Deep Security roles based on Directory Group membership, specify the synchronization options for each group and click **Next**.

   After synchronization, the wizard generates a report showing the number of objects imported.

   Tip: Before you finish the synchronization, you can choose to create a scheduled task to regularly synchronize users and contacts.
7. Click **Finish**.

Once imported, you will be able to tell the difference between organic (non-imported) Deep Security accounts and imported accounts because you will not be able to change any general information for these accounts.

## Keep Active Directory objects synchronized

Once imported, Active Directory objects must be continually synchronized with their Active Directory servers to reflect the latest updates for these objects. This ensures, for example, that computers that have been deleted in Active Directory are also deleted in Deep Security Manager. To keep the Active Directory objects that have been imported to the Deep Security Manager synchronized with Active Directory, it is essential to set up a scheduled task that synchronizes directory data. The host importation wizard includes the option to create these scheduled tasks.

It is also possible to create this task using the Scheduled Task wizard. On-demand synchronization can be performed using the **Synchronize Now** option for hosts and **Synchronize with Directory** button for users and contacts.

> **Note:** You do not need to create a scheduled task to keep users and contacts synchronized. At log in, Deep Security Manager checks whether the user exists in Active Directory. If the username and password are valid, and the user belongs to a group that has synchronization enabled, the user will be added to Deep Security Manager and allowed to log in.

## Disable Active Directory synchronization

You can stop Deep Security Manager from synchronizing with Active Directory for both computer groups and user accounts.

### Remove computer groups from Active Directory synchronization

1. Go to **Computers**.
2. Right-click the directory, and select **Remove Directory**.
3. Select a removal option:
   - **Remove directory and all subordinate computers/groups from Deep Security Manager**: All host records will be removed from the computers list
   - **Remove directory but retain computer data and group hierarchy**: The existing Active Directory structure will be retained, but this will no longer be synchronized with Active Directory. Since the structure is unaffected, user and role access to folders and hosts will be retained
   - **Remove directory, retain computer data, but flatten hierarchy**: Host records will be stripped of their original hierarchy, but will all be stored in a group named after the directory. User and role access to the directory will be transferred to the group so you can still access the hosts.
4. Confirm the action.

### Delete Active Directory users and contacts

Unlike when you remove directory queries for computer groups, if you delete the query for users and contacts, all those accounts will be deleted from Deep Security Manager. As a result, you

can't delete while logged into Deep Security Manager with a user account that was imported from the directory server. Doing so will result in an error.

1. On either **Users** or **Contacts**, click **Synchronize with Directory**.
2. Select **Discontinue Synchronization** then click **OK**.
3. Click **Finish**.

## Protect Docker containers

The benefits of a Docker deployment are real but so is the concern about the significant attack surface of the Docker host operating system (OS) itself. Like any well-designed software deployment, OS hardening and the use of best practices for your deployment, such as the Center for Internet Security (CIS) Docker Benchmark, provide a solid foundation as a starting point. Once you have a secure foundation in place, adding Deep Security to your deployment gives you access to Trend Micro's extensive experience protecting physical, virtual, and cloud workloads as well as to real-time threat information from the Trend Micro Smart Protection Network. Deep Security is supported for use in a wide range of container deployments that include, but is not restricted to, Amazon ECS, Docker Datacenter, Kubernetes, Docker Swarm, Rancher and more. Deep Security both protects your deployment as well as helps meet and maintain continuous compliance requirements. As you can see, Deep Security manages and protects both traditional and Docker workloads across physical, virtual, and cloud environments.

Deep Security protects your Docker hosts and containers running on Linux distributions:

- Identify, find, and protect Docker hosts within your deployment through the use of badges and smart folders
- Shield Docker hosts and containers from vulnerabilities to protect them against known and zero-day exploits by virtually patching new found vulnerabilities
- Provide real-time anti-malware detection for the file systems used on Docker hosts and within the containers
- Assert the integrity of the Docker host for continuous compliance and to protect your deployment using the following techniques:

- Prevent the unauthorized execution of applications on Docker hosts by helping you control which applications are allowed to run in addition to the Docker daemon
- Monitor Docker hosts for unexpected changes to system files
- Notify you of suspicious events in your OS logs

**Note:** Deep Security Docker protection controls work at the host system level and this means that the Deep Security Agent has to be installed on the Docker host system and not in the containers.

Beginning with Deep Security 10.1, Deep Security supports Docker in swarm mode while using an overlay network.

## Deep Security protection for the Docker host

- Virtual patching/ Intrusion prevention service (IPS)
- Anti-malware
- Integrity monitoring
- Log inspection
- Application control
- Firewall protection
- Web reputation

## Deep Security protection for Docker containers

- Virtual patching via the intrusion prevention module
- Anti-malware

## Limitation on intrusion prevention recommendation scans

Although Deep Security intrusion prevention controls work at the host level it will also protect container traffic on the exposed container port numbers. Since Docker allows multiple applications to run on the same Docker host, a single intrusion prevention policy will be applied

to all Docker applications. This means that recommendation scans should not be relied upon for Docker deployments.

## Computer and agent statuses

On the **Computers** page in Deep Security Manager:

- The **Status** column displays the state of the computer's network connectivity and the state (in parentheses) of the agent providing protection, if present. The status column might also display system or agent events. See "Status column - computer states" on the next pageand "Status column - agent or appliance states" on the next page
- The **Task(s)** column displays the state of the tasks. See "Task(s) column" on page 330.

For a list of the events, see "Agent events" on page 914 and "System events" on page 918.

Also on this page:

- "Computer errors" on page 333
- "Protection module status" on page 334
- "Perform other actions on your computers" on page 335
- "Computers icons" on page 339
- "Status information for different types of computers" on page 340

## Status column - computer states

| State | Description |
|---|---|
| Activated | The agent is activated. See "Perform other actions on your computers" on page 335. |
| Discovered | Computer has been added to the computers list via the discovery process. (See "Discover computers" on page 294.) |
| Managed | An agent is present and activated, with no pending operations or errors. |
| Multiple Errors | Multiple errors have occurred on this computer. See the computer's system events for details. |
| Multiple Warnings | Multiple warnings are in effect on this computer. See the computer's system events for details. |
| Reactivation Required | The agent is installed and listening and is waiting to be reactivated a Deep Security Manager. |
| Unmanaged | The computer's agent is not managed by this Deep Security Manager because it hasn't been activated. Deep Security Manager can't communicate with the agent until you activate it. |
| Upgrade | A newer version of the agent or appliance is available. An software upgrade is recommended. |

| State | Description |
|---|---|
| Recommended | |
| Upgrading Agent | The agent software on this computer is in the process of being upgraded to a newer version. |

## Status column - agent or appliance states

| State | Description |
|---|---|
| Activated | The agent has been successfully activated and is ready to be managed by the Deep Security Manager. |
| Activation Required | An unactivated agent has been detected on the target machine. It must be activated before it can be managed by the Deep Security Manager. |
| Deactivation Required | The manager has attempted to activate an agent that has already been activated by another Deep Security Manager. The original Deep Security Manager must deactivate the agent before it can be activated by the new manager. |
| No Agent | No agent was detected on the computer. |
| Offline | The agent has not connected to the manager for the number of heartbeats specified on **Computer or Policy editor**[1] > **Settings** > **General**.<br><br>This can occur when connectivity is interrupted by a network firewall or proxy, AWS security group, agent software update, or when a computer is powered down for repair.<br><br>Verify that firewall settings allow the required port numbers, and that the computer is powered on. If you use Deep Security as a Servicee, also see "Use agent-initiated communication with cloud accounts" on page 202. |
| Online | The agent is online and operating as expected. |
| Unknown | No attempt has been made to determine whether an agent is present. |

## Task(s) column

| State | Description |
|---|---|
| Activating | The manager is activating the agent. |
| Activating (Delayed) | The activation of the agent is delayed by the amount of time specified in the relevant event-based task. |

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| State | Description |
|---|---|
| Activation Pending | A command to activate the agent has been queued. |
| Agent Software Deployment Pending | An instruction to deploy the agent software is queued to be sent to the computer. |
| Agent Software Removal Pending | An instruction to remove the agent software is queued to be sent to the computer. |
| Application Control Inventory Scan In Progress | An application control inventory scan is being performed. |
| Application Control Inventory Scan Pending (Heatbeat) | An instruction to start an application control inventory scan will be sent from the manager during the next heartbeat. |
| Application Control Inventory Scan Pending (Offline) | The agent is currently offline. The manager will initiate an application control inventory scan when communication is reestablished. |
| Application Control Ruleset Update In Progress | The application control ruleset is being updated. |
| Application Control Ruleset Update Pending (Heartbeat) | An instruction to perform an application control ruleset update will be sent from the manager during the next heartbeat. |
| Application Control Ruleset Update Pending (Offline) | The agent is currently offline. The manager will initiate an application control ruleset update when communication is reestablished. |
| Baseline Rebuild In Progress | The Integrity Monitoring engine is currently rebuilding a system baseline. |
| Baseline Rebuild Paused | A baseline rebuild has been paused |
| Baseline Rebuild Pending | An instruction to rebuild a system baseline for Integrity Monitoring is queued to be sent. |
| Baseline Rebuild Pending (Offline) | The agent is currently offline. The Integrity Monitoring engine will rebuild a system baseline when communication between the manager and this computer is reestablished. |
| Baseline Rebuild Queued | The instruction to perform a baseline rebuild is queued. |
| Checking Status | The agent state is being checked. |
| Deactivate Pending (Heartbeat) | A deactivate instruction will be sent from the manager during the next heartbeat. |
| Deactivating | The manager is deactivating the agent. This means that the agent is available for activation and management by another Deep Security Manager. |
| Deploying Agent Software | Agent software is being deployed on the computer. |
| File Backup Cancellation In Progress | A file backup is being canceled. |
| File Backup Cancellation Pending | An instruction to cancel a file backup is queued to be sent. |
| File Backup Cancellation Pending (Offline) | The agent or appliance is currently offline. The manager will initiate the cancellation of the file backup when communication is reestablished. |
| File Backup In Progress | A file backup is being performed. |
| File Backup Pending | An instruction to start a file backup is queued to be sent. |
| File Backup Pending (Offline) | The agent or appliance is currently offline. The manager will initiate a file backup when communication is reestablished. |
| File Backup Queued | The instruction to perform a file backup is queued. |
| Getting Events | The manager is retrieving events from the agent. |
| Integrity Scan In Progress | An Integrity Scan is currently in progress. |
| Integrity Scan Paused | An integrity scan has been paused. |
| Integrity Scan Pending | A command to start an integrity scan is queued to be sent. |
| Integrity Scan Pending | The agent is currently offline. The manager will initiate an Integrity Scan when |

| State | Description |
|---|---|
| (Offline) | communication is reestablished. |
| Integrity Scan Queued | An instruction to start an integrity scan is queued to be sent. |
| Malware Manual Scan Cancellation In Progress | The instruction to cancel a manually-initiated Malware Scan has been sent. |
| Malware Manual Scan Cancellation Pending | The command to cancel a manually-initiated malware scan is queued to be sent. |
| Malware Manual Scan Cancellation Pending (Offline) | The appliance is offline. The instruction to cancel a manually-initiated Malware Scan will be sent when communication is reestablished. |
| Malware Manual Scan In Progress | A manually-initiated Malware Scan is in progress. |
| Malware Manual Scan Paused | A manually-initiated Malware Scan has been paused. |
| Malware Manual Scan Pending | The instruction to perform a manually-initiated Malware Scan has not yet been sent. |
| Malware Manual Scan Pending (Offline) | The agent is offline. The instruction to start a manually-initiated Malware Scan will be sent when communication is reestablished. |
| Malware Manual Scan Queued | The instruction to perform a manually-initiated Malware Scan is queued. |
| Malware Scheduled Scan Cancellation In Progress | The instruction to cancel a scheduled Malware Scan has been sent. |
| Malware Scheduled Scan Cancellation Pending | The instruction to cancel a scheduled Malware Scan is queued to be sent. |
| Malware Scheduled Scan Cancellation Pending (Offline) | The agent is offline. The instruction to cancel a scheduled Malware Scan will be sent when communication is reestablished. |
| Malware Scheduled Scan In Progress | A scheduled Malware Scan is in progress. |
| Malware Scheduled Scan Paused | A scheduled Malware Scan has been paused. |
| Malware Scheduled Scan Pending | The command to cancel a scheduled malware scan has not yet been sent. |
| Malware Scheduled Scan Pending (Offline) | The agent is offline. The instruction to start a scheduled Malware Scan will be sent when communication is reestablished. |
| Malware Scheduled Scan Queued | The instruction to cancel a scheduled Malware Scan is queued. |
| Quick Malware Scan Cancellation In Progress | A quick malware scan is being canceled. |
| Quick Malware Scan Cancellation Pending | An instruction to cancel a quick malware scan is queued to be sent. |
| Quick Malware Scan Cancellation Pending (Offline) | The agent is currently offline. The manager will initiate the cancellation of a quick malware scan when communication is reestablished. |
| Quick Malware Scan In Progress | A quick malware scan is being performed. |

| State | Description |
|---|---|
| Quick Malware Scan Paused | A quick malware scan has been paused. |
| Quick Malware Scan Pending | An instruction to start a quick malware scan is queued to be sent. |
| Quick Malware Scan Pending (Offline) | The agent is currently offline. The manager will initiate a quick malware scan when communication is reestablished. |
| Quick Malware Scan Queued | The instruction to perform a quick malware scan is queued. |
| Removing Agent Software | The agent software is being removed from the computer. |
| Rollback of Security Update In Progress | A security update is being rolled back. |
| Rollback of Security Update Pending | An instruction to roll back a security update is queued to be sent. |
| Rollback of Security Update Pending (Heartbeat) | An instruction to roll back a security update will be sent from the manager during the next heartbeat. |
| Rollback of Security Update Pending (Offline) | The agent is currently offline. The manager will initiate a rollback of the security update when communication is reestablished. |
| Scan for Recommendations Pending (Heartbeat) | The manager will initiate a recommendation scan at the next heartbeat. |
| Scan for Recommendations Pending (Offline) | The agent is currently offline. The manager will initiate a recommendation scan when communication is reestablished. |
| Scanning for Open Ports | The manager is scanning the computer for open ports. |
| Scanning for Recommendations | A recommendation scan is underway. |
| Security Update In Progress | A security update is being performed. |
| Security Update Pending | An instruction to perform a security update is queued to be sent. |
| Security Update Pending (Heartbeat) | An instruction to perform a security update will be sent from the manager during the next heartbeat. |
| Security Update Pending (Offline) | The agent is currently offline. The manager will initiate a security update when communication is reestablished. |
| Sending Policy | A policy is being sent to the computer. |
| Update of Configuration Pending (Heartbeat) | An instruction to update the configuration to match the policy changes will be sent from the manager during the next heartbeat. |
| Update of Configuration Pending (Offline) | The agent is currently offline. The manager will initiate the configuration update to match the policy changes when communication is reestablished. |
| Upgrading Software (In Progress) | A software upgrade is being performed. |
| Upgrading Software (Install Program Sent) | A software upgrade is being performed. The install program has been sent to the computer. |
| Upgrading Software (Pending) | An instruction to perform a software upgrade is queued to be sent. |
| Upgrading Software (Results Received) | A software upgrade is being performed. The results have been received. |
| Upgrading Software (Schedule) | A software upgrade will be performed once the computer's access schedule permits. |

## Computer errors

| State | Description |
|---|---|
| Communication error | General network error. |
| No route to computer | Typically the remote host cannot be reached because of an intervening firewall or if an intermediate router is down. |
| Unable to resolve hostname | Unresolved socket address. |
| Activation required | An instruction was sent to the agent when it was not yet activated. |
| Unable to communicate with Agent | Unable to communicate with agent. |
| Protocol Error | Communication failure at the IP, TCP, or HTTP layer.<br><br>For example, if the Deep Security Manager IP address is unreachable because the connection is being blocked by a firewall, router, or AWS security group, then it would cause a connection to fail. To resolve the error, verify that the activation port number is allowed and that a route exists. |
| Deactivation Required | The agent is currently activated by another Deep Security Manager. |
| No Agent | No agent was detected on the target. |
| No valid software version | Indicates that no installer can be found for the platform and version requested. |
| Send software failed | There was an error in sending a binary package to the computer. |
| Internal error | Internal error. Please contact your support provider. |
| Duplicate Computer | Two computers in the Deep Security Manager's computers list share the same IP address. |
| Unresolved software change limit reached | Software changes detected on the file system exceeded the maximum amount. Application control will continue to enforce existing rules, but will not record any more changes, and it will stop displaying any of that computer's software changes.<br><br>See "Reset application control after too much software change" on page 478. |

## Protection module status

When you hover over a computer name on the **Computers** page, the **Preview** icon ( ) is displayed. Click the icon to display the state of the computer's protection modules.

### On and Off States:

| State | Description |
|---|---|
| On | Module is configured in Deep Security Manager and is installed and operating on the Deep Security Agent. |
| Off | Module is either not configured in Deep Security Manager, not installed and operating on the Deep Security Agent, or both. |
| Unknown | Indicates an error with the protection modules. |

### Install state:

| State | Description |
|---|---|
| Not Installed | The software package containing the module has been downloaded in Deep Security Manager, but the module has not been turned on in Deep Security Manager or installed on the agent. |
| Installation Pending | Module is configured in the manager but is not installed on the agent. |
| Installation in Progress | Module is being installed on the agent. |
| Installed | Module is installed on the agent. This state is only displayed when the state of the module is "Off". (If the state is "On", the module has been installed on the agent.) |
| Matching Module Plug-In Not Found | The version of the software package containing the module imported into the manager does not match the version reported by the agent. |
| Not Supported/Update Not Supported | A matching software package was found on the agent, but it does not contain a module supported by the platform. "Not Supported" or "Update Not Supported" is displayed depending on whether there is already a version of this module installed on the agent. |

## Perform other actions on your computers

On the **Computers** page, the **Actions** button provides several actions that you can perform on the selected computers.

| Action | Description |
|---|---|
| Check Status | Checks the status of a computer without performing a scan or activation attempt. |
| Activate/Reactivate | Activates or reactivates the agent on the computer. See "Activate the agent" on page 219 |

| Action | Description |
| --- | --- |
| Deactivate | You may want to transfer control of a computer from one Deep Security Manager installation to another. If so, the agent has to be deactivated and then activated again by the new manager. |
| Assign Policy | Opens a window with a list that allows you to assign a policy to the computer. The name of the policy assigned to the computer will appear in the **Policy** column on the **Computers** page.<br><br>**Note:** If you apply other settings to a computer (for example, adding additional Firewall Rules, or modifying Firewall Stateful Configuration settings), the name of the policy will be in bold, indicating that the default settings have been changed. |
| Send Policy | When you use Deep Security Manager to change the configuration of an agent or appliance on a computer (apply a new intrusion prevention rule, change logging settings, etc.), the Deep Security Manager has to send the new information to the agent or appliance. This is a Send Policy instruction. Policy updates usually happen immediately but you can force an update by clicking **Send Policy**. |
| Download Security Update | Downloads the latest security update from the configured relay to the agent or appliance. See "Get and distribute security updates" on page 743. |
| Rollback Security Update | Rolls back the latest security update for the agent or appliance. |
| Get Events | Override the normal event retrieval schedule (usually every heartbeat) and retrieve the event logs from the computer(s) now. |
| Clear Warnings/Errors | Use this command to clear all warnings and errors for the computer. This command is useful in these situations:<br><br>• If the agent for the computer has been reset locally<br>• If the computer has been removed from the network before you had a chance to deactivate or delete it from the list of computers |

| Action | Description |
| --- | --- |
| Upgrade Agent Software | To upgrade an agent, you first need to import a newer version of the agent software package into the Deep Security Manager (see "About upgrades" on page 735). |
| Scan for Recommendations | Deep Security Manager can scan computers and then make recommendations for Security Rules. The results of a recommendation scan appear in the computer's **Details** window in the **Rules** pages. See "Manage and run recommendation scans" on page 359. |
| Clear Recommendations | Clears rule recommendations resulting from a recommendation scan on this computer. Clearing also removes the computer from those listed in an alert produced as a result of a recommendation scan.<br><br>**Note:** This action will not un-assign any rules that were assigned because of past recommendations. |
| Full Scan for Malware | Performs a full malware scan on the selected computers. The actions taken by a full scan depend on the **Malware Manual Scan Configuration** in effect on this computer. See "Configure malware scans" on page 497. |
| Quick Scan for Malware | Scans critical system areas for currently active threats. Quick Scan looks for currently-active malware but does not perform deep file scans to look for dormant or stored infected files. On larger drives, Quick Scan is significantly faster than a Full Scan.<br><br>**Note:** Quick Scan is only available on-demand. You cannot schedule a Quick Scan as part of a scheduled task. |

| Action | Description |
| --- | --- |
| Scan for Open Ports | Performs a port scan on all selected computers and checks the agent installed on the computer to determine whether its state is either Deactivation Required, Activation Required, Agent Reactivate Required, or Online. The scan operation, by default, scans ports 1-1024. This range can be changed in **Computer or Policy editor**[1] > **Settings** > **General**.<br><br>**Note:** The agent's listening port number for heartbeats is always scanned regardless of port range settings. When the Manager connects to communicate with the agent, it uses that port number. If communication direction is set to "Agent/Appliance Initiated" for a computer (**Computer or Policy editor**[2] > **Settings** > **General** > **Communication Direction**), however, that port number will not be open. For a list of ports used, see "Deep Security Agent ports" on page 106.<br><br>**Note:** New computers on the network will not be detected. To find new computers, use the **Discover** tool. |
| Cancel Currently Executing Port Scans | If you have initiated a set of port scans to a large number of computers or over a large range of ports and the scan is taking too long, use the **Cancel Currently Executing Port Scans** option to cancel the scans. |
| Scan for integrity | Integrity Monitoring tracks changes to a computer's system and files. It does by creating a baseline and then performing periodic scans to compare the current state of the computer to the baseline. For more information see "Set up integrity monitoring" on page 632. |
| Rebuild Integrity Baseline | Rebuilds a baseline for Integrity Monitoring on this computer. |

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| Action | Description |
| --- | --- |
| Assign Asset Value | Asset values allow you to sort computers and events by importance. The various security rules have a severity value. When rules are triggered on a computer, the severity values of the rules are multiplied by the asset value of the computer. This value is used to rank events in order of importance. See "Rank events to quantify their importance" on page 813. |
| Assign a Relay Group | To select a relay group for this computer to download updates from, right-click the computer and choose **Actions > Assign a Relay Group**. |

## Computers icons

Ordinary computer

Deep Security Relay (a computer with a Relay-enabled Agent)

Docker host (physical computer)

Azure virtual machine with Docker

Amazon EC2 with Docker

Amazon WorkSpace (started)

## Status information for different types of computers

### Ordinary computer

The preview pane for an ordinary computer displays the presence of an agent, its status, and the status of the protection modules.

| | Agent |
|---|---|
| | Managed (Online) |
| Anti-Malware | On, Real Time |
| Web Reputation | On |
| Firewall | On, 41 rules |
| Intrusion Prevention | **On, Prevent, 193 rules** |
| Integrity Monitoring | On, no rules |
| Log Inspection | On, 5 rules |
| Application Control | Off, not supported |

## Relay

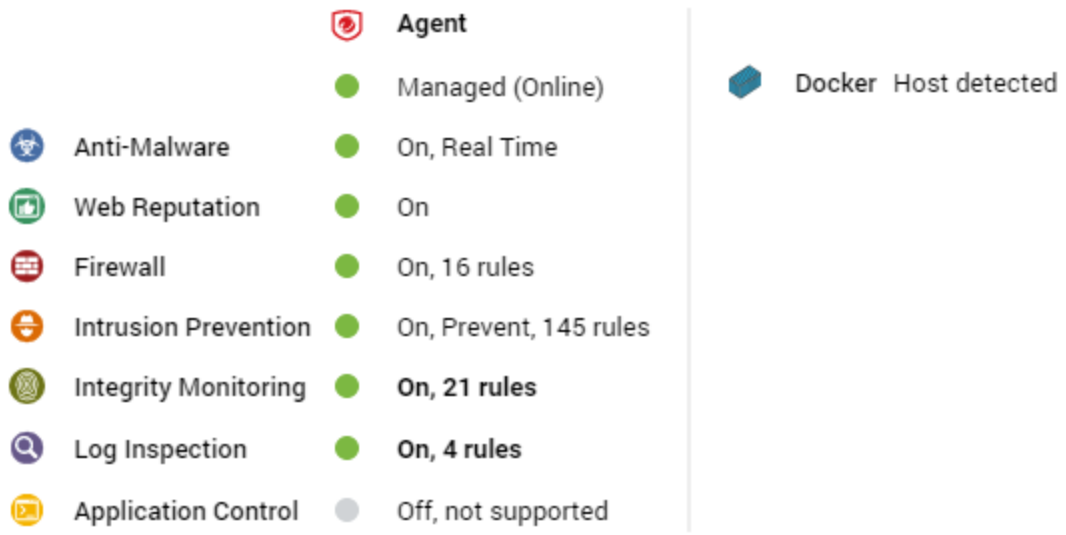
The preview pane for a Deep Security relay-enabled agent displays its status, the number of security update components it has available for distribution, and the status of the protection modules provided by its embedded Deep Security agent.

| | Agent |
|---|---|
| | Managed (Online) |
| Anti-Malware | On, Real Time |
| Web Reputation | **On** |
| Firewall | **On, 41 rules** |
| Intrusion Prevention | **On, Prevent, 316 rules** |
| Integrity Monitoring | **On, 30 rules** |
| Log Inspection | **On, 6 rules** |
| Application Control | Off, not supported |

**Relay** 192 components available

## Docker hosts

The preview pane for a docker host displays the presence of an agent and its status, the status of the protection modules, and the Docker status.




## Using Deep Security with iptables

When Deep Security Agent 10.1 or earlier was installed on Linux, it disabled the iptables service to avoid firewall conflicts unless you added a configuration file that prevented that change. However, the iptables service is used for more than just firewall (for example, Docker manages iptables rules as part of its normal operation), so disabling it sometimes had negative consequences.

With Deep Security 10.2 and higher (including Deep Security 11), the functionality around iptables has changed. Deep Security Agent no longer disables iptables. (If iptables is enabled, it stays enabled after the agent installation. If iptables is disabled, it stays disabled.) However, if the iptables service is running, Deep Security Agent and Deep Security Manager require certain iptables rules to enable communication, as described below.

### Rules required by Deep Security Manager

If iptables is enabled on the computer where Deep Security Manager is being installed, there are two required iptables rules. By default, these rules are added when Deep Security Manager starts up and removed when the manager is stopped or uninstalled. Alternatively, you can "Prevent Deep Security from automatically adding iptables rules" on the next page and add them manually instead:

- Allow incoming traffic on port 4119. This is required for access to the Deep Security Manager web UI and API.
- Allow incoming traffic on port 4120. This is required to listen for agent heartbeats.

**Note:** These are the default port numbers - yours may be configured differently. For a complete list of ports used in Deep Security, see "Port numbers" on page 96.

## Rules required by Deep Security Agent

If iptables is enabled on the computer where Deep Security Agent is being installed, iptables may require additional rules. By default, these rules when Deep Security Agent starts up and removed when the agent is stopped or uninstalled. Alternatively, you can "Prevent Deep Security from automatically adding iptables rules" on the next page and add them manually instead:

- Allow incoming traffic on port 4118. This is required when the agent uses manager-initiated or bidirectional communication. (For more information, see "Agent-manager communication" on page 196.)
- Allow incoming traffic on port 4122. This is required when the agent is acting as a relay, so that the relay can distribute software updates. (For more information, see "Distribute security and software updates with relays" on page 234.)

**Note:** These are the default port numbers - yours may be configured differently. For a complete list of ports used in Deep Security, see "Port numbers" on page 96.

## Prevent Deep Security from automatically adding iptables rules

You can prevent Deep Security Manager and Deep Security Agent from modifying iptables if you would rather add the required rules manually. To prevent the automatic modification of iptables, create the following file on the computers where you plan to install Deep Security Manager and Deep Security Agent:

```
/etc/do_not_open_ports_on_iptables
```

# Enable or disable agent self-protection

**Note:** The agent self-protection feature is only available for agents on Windows. It is not available on Linux.

To update or uninstall Deep Security Agent or Relay, or to create a diagnostic package for support (see "Create a diagnostic package and logs" on page 1105), you must temporarily disable agent self-protection.

Agent self-protection prevents local users from tampering with the agent. When enabled, if a user tries to tamper with the agent, the GUI will display a message such as "Removal or modification of this application is prohibited by its security settings".

**Note:** Anti-malware protection must be "On" to prevent users from stopping the agent, and from modifying agent-related files and Windows registry entries. It isn't required, however, to prevent uninstalling the agent.

You can configure agent self-protection using either the GUI for Deep Security Manager, or the command line on the agent's computer.

## Via Deep Security Manager

1. Open the **Computer or Policy editor**[1] where you want to enable agent self-protection.
2. Click **Settings > General**.
3. In the **Agent Self-Protection** section, for **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent**, select **Yes**.
4. To password-protect agent self protection, for **Local override requires password**, select **Yes** and type the password.
5. Click **Save**.
6. To disable the setting, select **No**. Click **Save**.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

## Via command line

1. Log in to the Windows computer locally.
2. Open the Command Prompt (`cmd.exe`) as Administrator.
3. Change the current directory to the Deep Security Agent installation folder. (The default install folder is shown below.)

   ```
   cd C:\Program Files\Trend Micro\Deep Security\Agent
   ```

4. Enter this command:

   ```
   dsa_control --selfprotect=1 --passwd=<password>
   ```

   where <password> is a password that will be required in order to override this setting. (See "Command-line basics" on page 244.) The password is optional, but strongly recommended.

   > **Warning:** Store this password in a safe location. If you lose or forget the password you will have to contact your support provider for assistance in overriding this protection.

5. To disable the setting, enter this command:

   dsa_control -s=0 -p "<password>"

# Are "Offline" agents still protected by Deep Security?

Agents showing as "Offline" in the Deep Security Manager are still being protected according to their last known configuration. However, they will not receive any software, security or policy updates until communication with the Deep Security Manager is restored.

For more information on how to bring an agent out of "Offline" status, see ""Offline" agent" on page 1097.

# Deep Security Notifier

The Deep Security Notifier is a Windows System Tray application that communicates the state of the Deep Security Agent and Deep Security Relay to client machines. The notifier displays

popup user notifications when the Deep Security Agent begins a scan, or blocks malware or access to malicious web pages.

The notifier has a small footprint on the client machine, requiring less than 1MB of disk space and 1MB of memory. When the notifier is running the notifier icon ( ) appears in the system tray. The notifier is automatically installed by default with the Deep Security Agent on Windows computers. Use the **Administration > Updates > Software > Local** page to import the latest version for distribution and upgrades.

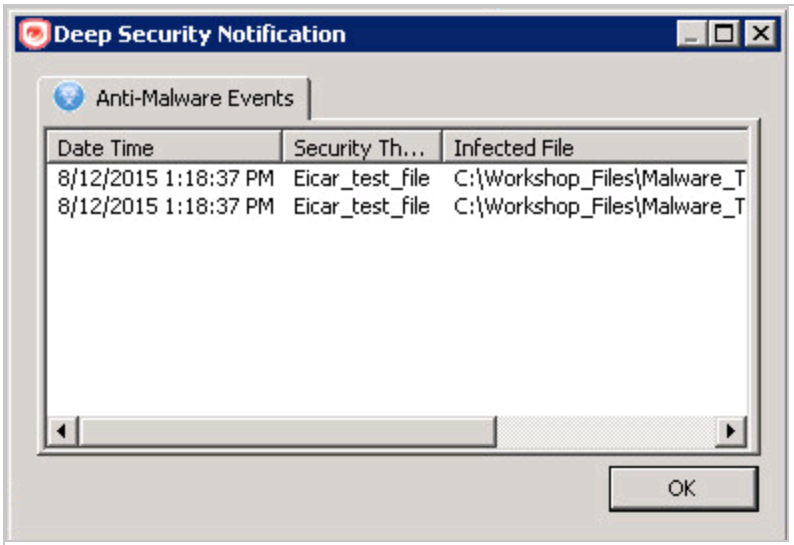
> **Note:** On computers running a relay-enabled agent, the notifier displays the components that are being distributed to agents or appliances, *not* which components are in effect on the local computer.

## How the notifier works

When malware is detected or a malicious site is blocked, the Deep Security Agent sends a message to the notifier, which displays a popup message in the system tray.

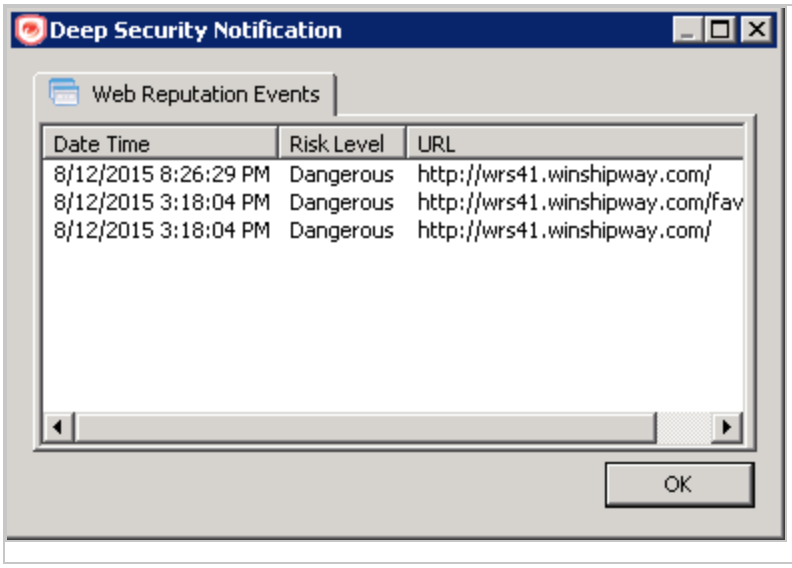
If malware is detected, the notifier displays a message in a system tray popup similar to the following:

If the user clicks on the message, a dialog box with detailed information about anti-malware events is displayed:

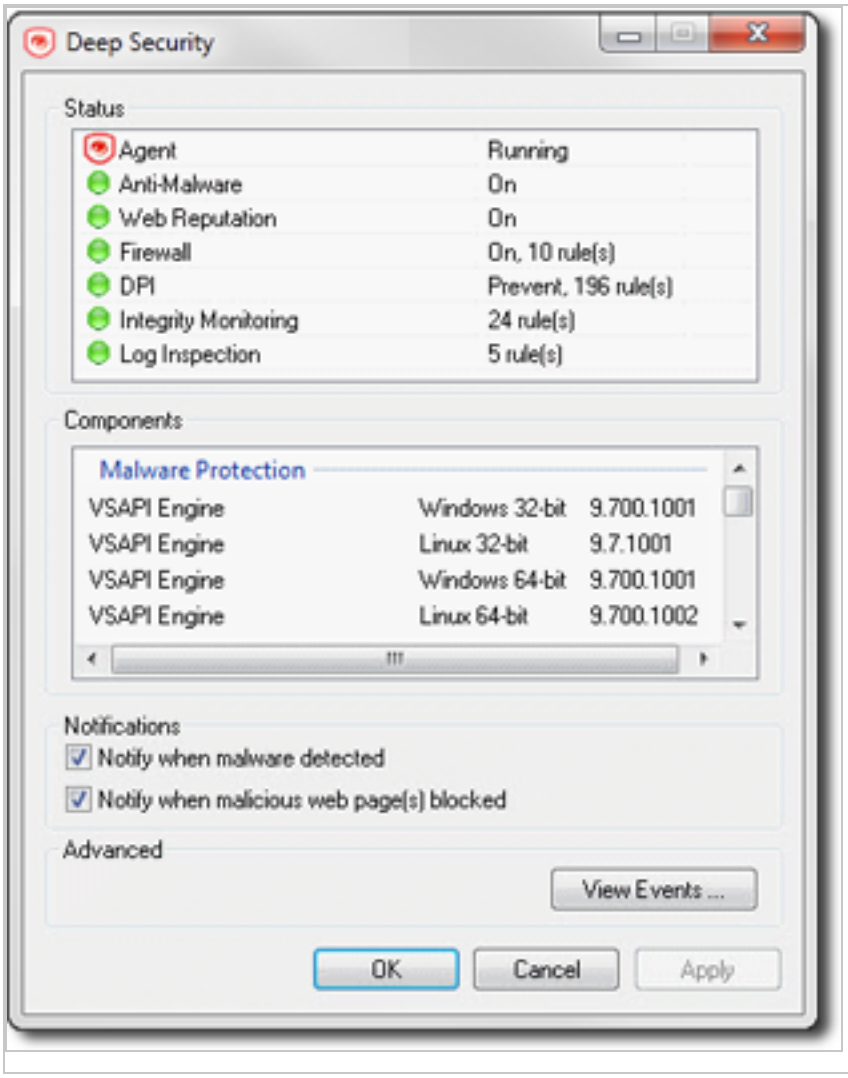



When a malicious web page is blocked, the notifier displays a message in a system tray popup similar to the following:

If the user clicks on the message, a dialog box with detailed information about web reputation events is displayed:

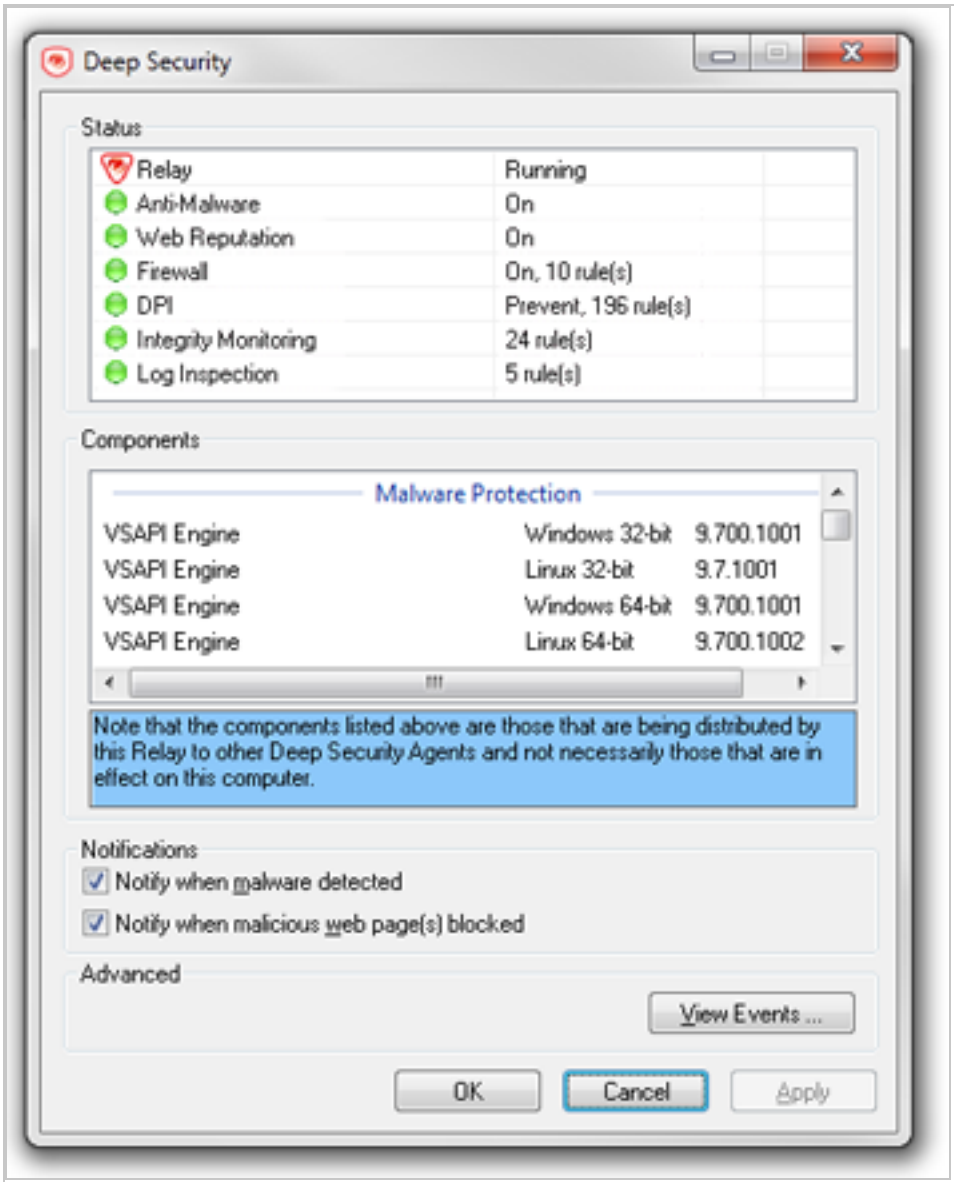


The notifier also provides a console utility for viewing the current protection status and component information, including pattern versions. The console utility allows the user to turn on and off the popup notifications and access detailed event information.




**Tip:** You can also turn off pop-up notifications for certain computers or for computers that are assigned a particular policy by going to the Deep Security Manager **Computer/Policy editor > Settings > General** and settings **Suppress all pop-up notifications on host** to **Yes**. The messages still appear as alerts or events in Deep Security Manager.

When the notifier is running on a computer hosting Deep Security Relay, the notifier's display shows the components being distributed by the relay and not the components that in effect on the computer.




# Create policies to protect your computers and other resources

Policies allow collections of rules and configuration settings to be saved for easier assignment to multiple computers. You can use the **Policy editor**[1] to create and edit policies that you can then

[1] To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

apply to one or more computers. You can also use the **Computer editor**[1] (which is very similar to the Policy editor) to apply settings to a specific computer, but the recommended method is to create specialized policies rather then edit the settings in the Computer editor.

> **Tip:** You can automate policy creation and configuration using the Deep Security API. For examples, see the Create and Configure Policies guide.

In this article:


- "Create a new policy" below
- "Other ways to create a policy" on the next page
- "Edit the settings for a policy or individual computer" on page 352
- "Assign a policy to a computer" on page 352
- "Disable automatic policy updates" on page 353
- "Send policy changes manually" on page 353
- "Export a policy" on page 354


## Create a new policy

1. Click **Policies > New > New Policy**.
2. Enter a name for the policy. If you want the new policy to inherit its settings from an existing policy, select a policy from the **Inherit from** list. Click **Next**.

   > **Tip:** For information on inheritance, see "Policies, inheritance, and overrides" on page 354.

3. Select whether you want to base this policy on an existing computer's configuration and then click **Next**.
4. If you selected **Yes** in step 3:
   a. Select a computer to use as the basis for the new policy and click **Next**.

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

   b. Specify which protection modules will be enabled for the new policy. If this policy is inheriting its settings from an existing policy, those settings will be reflected here. Click **Next**.
   c. On the next screen, select the properties that you want to carry into the new policy and click **Next**. Review the configuration and click **Finish**.
5. If you selected **No** in step 3, specify which protection modules will be enabled for the new policy. If this policy is inheriting its settings from an existing policy, those settings will be reflected here. Click **Finish**.
6. Click **Close**. Next, you can edit the settings for the policy, as described in "Edit the settings for a policy or individual computer" on the next page.

## Other ways to create a policy

There are several ways to create a policies on the **Policies** page:

- Create a new policy as described above.
- Click **New > Import From File** to import policies from an XML file.

> **Note:** When importing policies, ensure that the system where you created the policies and the system that will receive them both have the latest security updates. If the system that is receiving the policies is running an older security update, it may not have some of the rules referenced in the policies from the up-to-date system.

- Duplicate (and then modify and rename) an existing policy. To do so, right-click an existing policy you want to duplicate and then click **Duplicate**.
- Create a new policy based on a recommendation scan of a computer. To do so, go to the **Computers** page, right-click a computer and select **Actions > Scan for Recommendations**. When the scan is complete, return to the **Policies** page and click **New** to display the **New Policy** wizard. When prompted, choose to base the new policy on "an existing computer's current configuration". Then select "Recommended Application Types and Intrusion Prevention Rules", "Recommended Integrity Monitoring Rules", and "Recommended Log Inspection Rules" from among the computer's properties.

> **Note:** The Policy will consist only of recommended elements on the computer, regardless of what Rules are currently assigned to that computer.

## Edit the settings for a policy or individual computer

The **Policies** page shows your existing policies in their hierarchical tree structure. To edit the settings for a policy, select it and click **Details** to open the policy editor.

These sections are available in the **Computer or Policy editor**[1]:

- Overview (the "Overview section of the policy editor" on page 377 and "Overview section of the computer editor" on page 371 sections are different)
- "Configure malware scans" on page 497
- Web Reputation settings
- "Firewall settings" on page 612
- Intrusion Prevention
- Integrity Monitoring
- Log Inspection settings
- "Detect and configure the interfaces available on a computer" on page 369
- "Network engine settings" on page 378
- "Overrides" on page 356

## Assign a policy to a computer

1. Go to **Computers**.
2. Select your computer from the Computers list, right click and choose **Actions > Assign Policy**.
3. Select the policy from the hierarchy tree and click **OK**.

One of the following occurs:

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

- If you set the communication direction to **Manager Initiated** or **Bidirectional**, the policy is sent immediately to the agent computer.
- If you set the communication direction to **Agent/Appliance Initiated**, then the policy is sent when the next agent heartbeat occurs.

For more information on how child policies in a hierarchy tree can inherit or override the settings and rules of parent policies, see "Policies, inheritance, and overrides" on the next page.

After assigning a policy to a computer, you should still run periodic recommendation scans on your computer to make sure that all vulnerabilities on the computer are protected. See "Manage and run recommendation scans" on page 359 for more information.

## Disable automatic policy updates

By default, any changes to a security policy are automatically sent to the computers that use the policy. You can change this so automatic sending is disabled, and you must manually send the policy.

1. Open the **Policy editor**[1] for the policy to configure.
2. Go to **Settings > General > Send Policy Changes Immediately.**
3. Next to **Automatically send Policy changes to computers**, select **Yes** to allow automatic sending of policy changes. To disable automatic sending, and only allow manually sending, select **No**.
4. Click **Save** to apply the changes.

## Send policy changes manually

If you make a policy change and want to send the policy changes manually to a particular computer, follow the instructions below.

1. Go to **Computers** .
2. Double-click your computer from the Computers list.
3. In the navigation pane, make sure **Overview** is selected.

---

[1] To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

4. In the main pane, click the **Actions** tab.
5. Under **Policy**, click **Send Policy**.

One of the following occurs:

- If you set the communication direction to **Manager Initiated** or **Bidirectional**, the policy is sent immediately to the agent computer.
- If you set the communication direction to **Agent/Appliance Initiated**, then the policy is sent when the next agent heartbeat occurs.

## Export a policy

To export a policy to an XML file, select a policy from the policies tree and click **Export > Export Selected to XML (For Import)**.

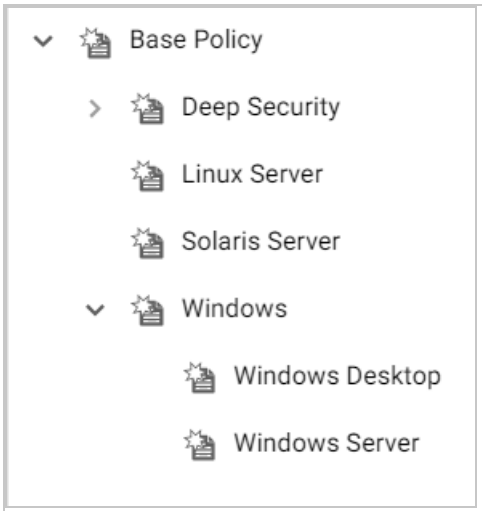
**Note:** When you export a selected policy to XML, any child policies that the policy may have are included in the exported package. The export package contains all the actual objects associated with the policy except: intrusion prevention rules, log inspection rules, integrity monitoring rules, and application types.

## Policies, inheritance, and overrides

Policies in Deep Security are intended to be created in a hierarchical structure. As an administrator, you begin with one or more base policies from which you create multiple levels of child policies that get progressively more granular in their detail. You can assign broadly applicable rules and other configuration settings at the top-level policies and then get more targeted and specific as you go down through levels of child policies, eventually arriving at rule and configuration assignments at the individual computer level.

As well as assigning more granular settings as you move down through the policy tree, you can also override settings from higher up the policy tree.

Deep Security provides a collection of policies that you can use as initial templates for the design of your own policies tailored to your environment:



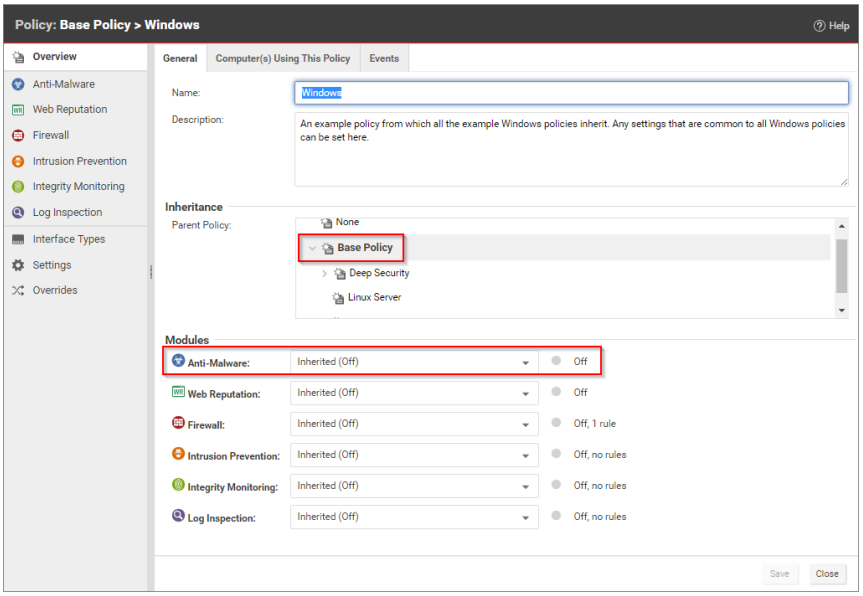

In this topic:


- "Inheritance" below
- "Overrides" on the next page
- "View the overrides on a computer or policy at a glance" on page 358


## Inheritance

Child policies inherit their settings from their parent policies. This allows you to create a policy tree that begins with a base parent policy configured with settings and rules that will apply to all computers. This parent policy can then have a set of child and further descendant policies which have progressively more specific targeted settings. Your policy trees can be built based on any kind of classification system that suits your environment. For example, the branch in the policy tree that comes with Deep Security has two child policies, one designed for a server hosting the Deep Security Manager and one designed for the Deep Security Virtual Appliance. This is a role-based tree structure. Deep Security also has three branches designed for specific operating systems, Linux, Solaris, and Windows. The windows branch has further child policies for various sub-types of Windows operating systems.

In the **Windows** policy editor on the **Overview** page, you can see that the **Windows** policy was created as a child of the **Base** policy. The policy's anti-malware setting is **Inherited (Off)**:

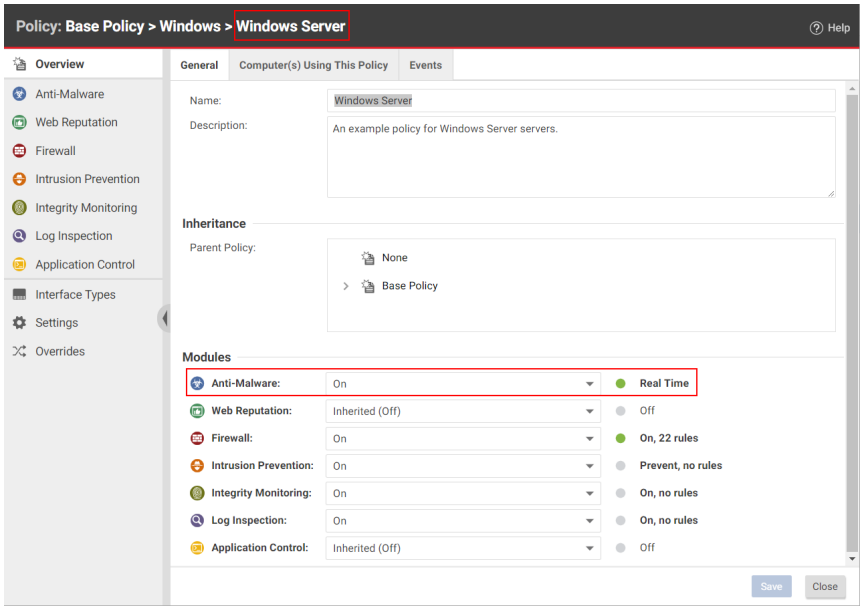



This means that the setting is inherited from the parent **Base** policy, and that if you were to change the anti-malware setting in the **Base** policy from **Off** to **On**, the setting would change in the **Windows** policy as well. (The **Windows** policy setting would then read **Inherited (On)**. The value in parentheses always shows you what the current inherited setting is.)

## Overrides

The **Overrides** page shows you how many settings have been overridden at this policy or specific computer level. To undo the overrides at this level, click the **Remove** button.

In this example, the **Windows Server** policy is a child policy of the **Windows** policy. Here, the anti-malware setting is no longer inherited; it is overridden and hard-set to **On**.




**Tip:** You can automate override checking, creation, and removal using the Deep Security API. For examples, see the Configure Computers to Override Policies guide.

## Override object properties

The intrusion prevention rules that are included in this policy are copies of the intrusion prevention rules stored by the Deep Security Manager which are available for use by any other policies. If you want to change the properties of a particular rule, you have two choices: modify the properties of the rule globally so that the changes you make apply to all instances where the rule is in use, or modify the properties locally so that the changes you make only apply locally. The default editing mode in a Computer or policy editor is **local**. If you click **Properties** on the **Assigned Intrusion Prevention Rules** area toolbar, any changes you make in the Properties window that appears will only apply locally. (Some properties like the rule name can't be edited locally, only globally.)

Right-clicking a rule displays a context menu which gives you the two Properties editing mode options: selecting **Properties** will open the local editor window and **Properties (Global)** will open the global editor window.

Most of the shared common objects in Deep Security can have their properties overridden at any level in the policy hierarchy right down to the individual computer level.

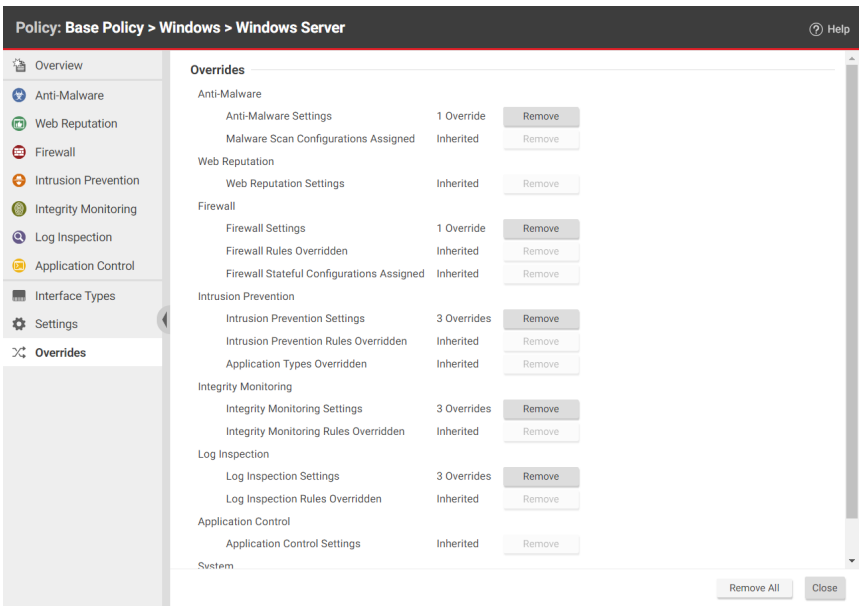
### Override rule assignments

You can always assign additional rules at any policy or computer level. However, rules that are in effect at a particular policy or computer level because their assignment is inherited from a parent policy cannot be unassigned locally. They must be unassigned at the policy level where they were initially assigned.

> **Tip:** If you find yourself overriding a large number of settings, you should probably consider branching your parent policy.

## View the overrides on a computer or policy at a glance

You can see the number of settings that have been overridden on a policy or a computer by going to the **Overrides** page in the computer or policy Editor:




Overrides are displayed by protection module. You can revert system or module overrides by clicking the **Remove** button.

# Manage and run recommendation scans

Deep Security can run recommendation scans on computers to help identify intrusion prevention, integrity monitoring, and log inspection rules that should be applied or removed.

> **Tip:** Recommendation scans provide a good starting point for establishing a list of rules that you should implement, but there are some important additional rules that are not identified by recommendation scans. You should implement those rules manually. See "Implement additional rules for common vulnerabilities" on page 367

You can configure recommendation scans and implement the recommended rules for individual computers or at the policy level. For large deployments, Trend Micro recommends managing recommendations through policies. This way, you can make all your rule assignments from a single source (the policy) rather than having to manage individual rules on individual computers. This can mean that some rules are assigned to computers on which they are not required; however, the minimal effect on performance is outweighed by the ease of management that results from using policies. If you enable recommendation scans in policies, use separate policies for scanning Windows and Linux computers, to avoid assigning Windows rules to Linux computers, and vice-versa.


- "What gets scanned?" below
- "Scan limitations" on the next page
- "Run a recommendation scan" on page 361
- "Automatically implement recommendations" on page 364
- "Check scan results and manually assign rules" on page 365
- "Configure recommended rules" on page 367
- "Implement additional rules for common vulnerabilities" on page 367
- "Troubleshooting: Recommendation Scan Failure" on page 368


## What gets scanned?

During a recommendation scan, Deep Security Agents scan the operating system for:

- installed applications
- the Windows registry
- open ports
- the directory listing
- the file system
- running processes and services
- environment variables
- users

## Scan limitations

Certain technical or logical limitations result in the rules for some types of software not being accurately recommended, or not recommended at all:

- On Unix/Linux systems, the recommendation scan engine might have trouble detecting software that is not installed through the operating system's default package manager, for example, Apache Struts, Wordpress, or Joomla. Applications installed using standard package managers are not a problem.
- On Unix/Linux systems, rules for desktop application vulnerabilities or local vulnerabilities (for example, browsers and media players) are not included in recommendation scans.
- Generic web application protection rules are not included in recommendation scans.
- Smart rules are generally not included in recommendation scans unless they address a major threat or a specific vulnerability. Smart rules address one or more known and unknown (zero-day) vulnerabilities. Rule lists in Deep Security Manager identify smart rules with "Smart" in the Type column.
- When dealing with rules related to a content management system (CMS), the recommendation scan cannot detect the CMS installation and installed version. It also cannot detect the plug-ins installed with a CMS and their versions. As a result, whenever a recommendation scan finds a web server installed and PHP installed or running on a system, all CMS-related intrusion prevention rules get recommended. This may result in the over-recommendation of rules, but balances the need for security vs. accuracy.

- The recommendations for the following web technologies may suggest more rules than necessary, so some tailoring may be required:
  - Red Hat JBoss
  - Eclipse Jetty
  - Apache Struts
  - Oracle WebLogic
  - WebSphere
  - Oracle Application Testing Suite
  - Oracle Golden Gate
  - Nginx
- OpenSSL rules are recommended on Windows only when OpenSSL is explicitly installed. If OpenSSL in being used internally by an application but it was not installed as a separate package, a recommendation scan does not detect it.
- On Linux systems, rules for Java-related vulnerabilities do not get recommended if web browsers are the only applicable vector.
- Recommendation scans cannot detect the Adobe Flash Player plug-in that is included in a default Chrome installation. Recommendations are based on the Chrome version, which means some unnecessary rules may be recommended.

## Run a recommendation scan

Because changes to your environment can affect which rules are recommended, it's best to run recommendation scans on a regular basis (the best practice is to perform recommendation scans on a weekly basis). Trend Micro releases new intrusion prevention rules on Tuesdays, so it's recommended that you schedule recommendation scans shortly after those releases. The use of system resources, including CPU cycles, memory, and network bandwidth, increases during a recommendation scan so it's best to schedule the scans at non-peak times.

There are several ways to run recommendation scans:

- **Scheduled task:** Create a scheduled task that runs recommendation scans according to a schedule that you configure. You can assign the scheduled task to all computers, one

individual computer, a defined computer group, or all computers protected by a particular policy. See "Create a scheduled task to regularly run recommendation scans" below.

- **Ongoing scans:** Configure a policy so that all computers protected by the policy are scanned for recommendations on a regular basis. You can also configure ongoing scans for individual computers. This type of scan checks the timestamp of the last scan that occurred and then and follows the configured interval thereafter to perform future scans. This results in recommendation scans occurring at different times in your environment. This setting is helpful in environments where an agent might not be online for more than a few days (for example, in cloud environments that are building and decommissioning instances frequently). See "Configure an ongoing scan" on the next page
- **Manual scans:** Run a single recommendation scan on one or more computers. A manual scan is useful if you've recently made significant platform or application changes and want to force a check for new recommendations instead of waiting for a scheduled task. See "Manually run a recommendation scan" on the next page.
- **Command line:** Initiate a recommendation scan via the Deep Security command-line interface. See "Command-line basics" on page 244.
- **API:** Initiate a recommendation scan via the Deep Security API. See "Use the Deep Security API to automate tasks" on page 261.

**Note:** Use either the scheduled tasks or ongoing scans, but not both.

Once a recommendation scan has run, alerts are raised on the all computers for which recommendations have been made.

## Create a scheduled task to regularly run recommendation scans

1. In the Deep Security Manager, go to the **Administration > Scheduled Tasks** page.
2. Click **New** on the toolbar and select **New Scheduled Task** to display the **New Scheduled Task** wizard.
3. In the **Type** list, select **Scan Computers for Recommendations** and then select how often you want the scan to occur. Click **Next**.
4. Depending on your choice in step 3, the next page lets you be more specific about the scan frequency. Make your selection and click **Next**.

5. Now select which computer(s) to scan and click **Next**.

   **Note:** You can select all computers, choose one individual computer, select a group of computers, or select computers that are assigned a particular policy. For large deployments, it's best to perform all actions, including recommendation scans, through policies.

6. Give a name to your new scheduled task, select whether or not to **Run Task on 'Finish'**, click **Finish**.

## Configure an ongoing scan

1. In the Deep Security Manager, open the **Computer or Policy editor**[1], depending on whether you want to configure the scan for an individual computer or for all computers that are using a policy.

   **Note:** For large deployments, it's best to perform all actions, including recommendation scans, through policies.

2. Click **Settings**. On the **General** tab, under **Recommendations**, the **Perform ongoing Recommendation Scans** setting enables or disables recommendation scans. The **Ongoing Scan Interval** setting specifies how often the scans occur. Both of those settings can be inherited from the computer or policy's parent (see "Policies, inheritance, and overrides" on page 354 for details about how inheritance works).

## Manually run a recommendation scan

1. In the Deep Security Manager, go to the **Computers** page.
2. Select the computer or computers you want to scan.
3. Click **Actions > Scan for Recommendations**.

## Cancel a recommendation scan

You can cancel a recommendation scan before it starts running.

---

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

1. In the Deep Security Manager, go to the **Computers** page.
2. Select the computer or computers where you want to cancel the scans.
3. Click **Actions > Cancel Recommendation Scan**.

### Exclude a rule or application type from recommendation scans

If you don't want a particular rule or application type to be included in recommendation scan results, you can exclude it from scans.

1. In the Deep Security Manager, open the **Computer or Policy editor**[1].

   **Note:** For large deployments, it's best to perform all actions, including recommendation scans, through policies.

2. Depending on which type of rule you want to exclude, go to the **Intrusion Prevention**, **Integrity Monitoring**, or **Log Inspection** page.
3. On the **General** tab, click **Assign/Unassign** (for rules) or **Application Types** (for application types).
4. Double-click the rule or application type that you want to exclude.
5. Go to the **Options** tab. For rules, set **Exclude from Recommendations** to "Yes" or "Inherited (Yes)". For application types, select the **Exclude from Recommendations** checkbox.

## Automatically implement recommendations

You can configure Deep Security to automatically implement recommendation scan results when it is appropriate to do so:

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

1. In the Deep Security Manager, open the **Computer or Policy editor**[1].

   **Note:** For large deployments, it's best to perform all actions, including recommendation scans, through policies.

2. Depending on which type of rules you want to implement automatically, go to the **Intrusion Prevention**, **Integrity Monitoring**, and/or **Log Inspection** pages. (You can change the setting independently for each protection module.)
3. On the **General** tab, under **Recommendations**, change the setting to "Yes" or "Inherited (Yes)".

Not all recommendations can be implemented automatically. The exceptions are:

- Rules that require configuration before they can be applied.
- Rules that are excluded from recommendation scans.
- Rules that have been automatically assigned or unassigned but that a user has overridden. For example, if Deep Security automatically assigns a rule and you subsequently unassign it, the rule is not reassigned after the next recommendation scan.
- Rules that have been assigned at a higher level in the policy hierarchy cannot be unassigned at a lower level. A rule assigned to a computer at the policy level must be unassigned at the policy level.
- Rules that Trend Micro has issued but which may pose a risk of producing false positives. (This will be addressed in the rule description.)

## Check scan results and manually assign rules

The results of the latest recommendation scan are displayed in the **Computer or Policy editor**[2], on the **General** tab of the protection module (**Intrusion Prevention**, **Integrity Monitoring**, and **Log**

---

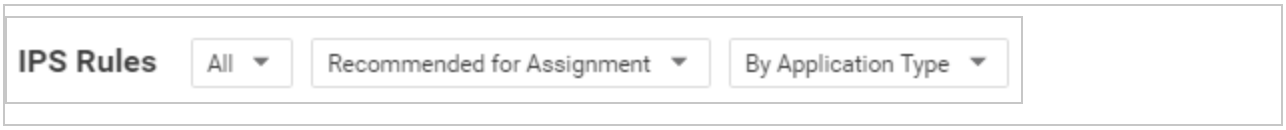
[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

**Inspection**).

The example below describes how to deal with intrusion prevention recommendation scan results via a policy:

1. Once a recommendation scan is complete, open the policy that is assigned to the computers you have just scanned.
2. Go to **Intrusion Prevention > General**. The number of unresolved recommendations (if any) is displayed in the **Recommendations** section.
3. Click **Assign/Unassign** to open the rule assignment window.
4. Sort the rules **By Application Type** and select **Recommended for Assignment** from the display filter menu:

   This displays a list of rules that are recommended for assignment but that have not been assigned.

5. To assign a rule to the policy, select the checkbox next to the rule name. Rules flagged with a icon have configuration options that you can set. Rules flagged with a icon have settings that **must** be configured before the rule is enabled.)

   Alternatively, to assign several rules at once, use the Shift or Control keys to select the rules, right-click the selection, and click **Assign Rule(s)**.

**Tip:** The results of a recommendation scan can also include recommendations to unassign rules. This can happen when applications are uninstalled, when security patches from a manufacturer are applied, or when unnecessary rules have been applied manually. To view rules that are recommended for unassignment, select **Recommended for Unassignment** from the display filter menu.

**Note:** Recommended rules are indicated by a full flag ( ) . A partial flag ( ) identifies an application type where only some of the rules that are part of the application type have been recommended.

## Configure recommended rules

Some rules require configuration before they can be applied. For example, some log inspection rules require that you specify the location of the log files to be inspected for change. If this is the case, an alert is raised on the computer on which the recommendation has been made. The text of the alert will contain the information required to configure the rule. In the policy or computer editor, rules flagged with a icon have configuration options that you can set. Rules flagged with a icon have settings that **must** be configured before the rule is enabled.

## Implement additional rules for common vulnerabilities

Recommendation scans provide a good starting point for establishing a list of rules that you should implement, but there are some additional rules for common vulnerabilities that are not identified by recommendation scans because they need to be carefully configured and tested before being implemented in "prevent" (block) mode. Trend Micro recommends that you configure and test these rules, then manually enable them in your policies (or for individual computers):

**Tip:** This list includes the most common of the additional rules you should configure. You can find others in Deep Security Manager by searching for rules whose type is "Smart" or "Policy".

| Rule name | Application type |
|---|---|
| 1007598 - Identified Possible Ransomware File Rename Activity Over Network Share | DCERPC Services |
| 1007596 - Identified Possible Ransomware File Extension Rename Activity Over Network Share | DCERPC Services |
| 1006906 - Identified Usage Of PsExec Command Line Tool | DCERPC Services |
| 1007064 - Executable File Uploaded On System32 Folder Through SMB Share | DCERPC Services |
| 1003222 - Block Administrative Share | DCERPC Services |
| 1001126 - DNS Domain Blocker | DNS Client |
| 1000608 - Generic SQL Injection Prevention<br>See "Configure an SQL injection prevention rule" on page 559 for details. | Web Application Common |

| Rule name | Application type |
|---|---|
| 1005613 - Generic SQL Injection Prevention - 2 | Web Application Common |
| 1000552 - Generic Cross Site Scripting (XSS) Prevention | Web Application Common |
| 1006022 - Identified Suspicious Image With Embedded PHP Code | Web Application Common |
| 1005402 - Identified Suspicious User Agent In HTTP Request | Web Application Common |
| 1005934 - Identified Suspicious Command Injection Attack | Web Application Common |
| 1006823 - Identified Suspicious Command Injection Attack - 1 | Web Application Common |
| 1005933 - Identified Directory Traversal Sequence In Uri Query Parameter | Web Application Common |
| 1006067 - Identified Too Many HTTP Requests With Specific HTTP Method | Web Server Common |
| 1005434 - Disallow Upload Of A PHP File | Web Server Common |
| 1003025 - Web Server Restrict Executable File Uploads | Web Server Common |
| 1007212 - Disallow Upload Of An Archive File | Web Server Common |
| 1007213 - Disallow Upload Of A Class File | Web Server Common |

## Troubleshooting: Recommendation Scan Failure

If you are receiving a Recommendation Scan Failure on your server, follow the steps below to resolve the issue. If the issue continues to persist after troubleshooting, create a diagnostic package from the agent and contact support.

### Communication

Typically for communication issues "protocol error" will appear in the body of the error message.

If you don't have open inbound firewall ports from the Deep Security Manger to the agent, open the ports or switch to agent-initiated communication. For more information, see "Use agent-initiated communication with cloud accounts" on page 202.

### Server resources

Monitor the CPU and memory resources on the server. If the memory or CPU is becoming exhausted during the scan, increase the resources.

### Timeout values

Increase the timeout values for the recommendation scan.

**Note:** dsm_c commands are not available on Deep Security as a Service.

1. Open the command prompt and navigate to the Deep Security Manager installation folder.
2. Enter the commands below (if this is a multi-tenant environment, add the tenant name):

```
dsm_c -action changesetting -name
settings.configuration.agentSocketTimeoutOverride -value 1200
```

```
dsm_c -action changesetting -name
settings.configuration.defaultSocketChannelTimeout -value 1200000
```

```
dsm_c -action changesetting -name
settings.configuration.recoScanKeepAliveTimeInterval -value 180000
```

## Detect and configure the interfaces available on a computer

The Computer and Policy editors contain an **Interfaces** (in the Computer editor) and **Interface Types** (in the Policy editor) section that displays the interfaces detected on the computer. If a policy with multiple interface assignments has been assigned to the computer, interfaces that match the patterns defined in the policy will be identified.

The **Interface Types** section of the Policy editor provides additional capabilities:

### Configure a policy for multiple interfaces

If you have computers with more than one interface, you can assign various elements of a policy (firewall rules, etc.) to each interface.

1. In the Policy editor, click **Interface Types**.
2. In the Network Interface Specificity section, select **Rules can apply to specific interfaces**
3. In the Interface Type sections that appear, type the names and pattern matching strings.

The interface type name is used only for reference. Common names include "LAN", "WAN", "DMZ", and "Wi-Fi", though any name can be used to map to your network's topology.

The matches define a wildcard-based interface name to auto map the interfaces to the appropriate interface type. Examples would be "Local Area Connection *", "eth*", or"Wireless *". When an interface cannot be mapped automatically, an alert is triggered. You can manually map it from the **Interfaces** page in the computer editor for a particular computer.

**Note:** If Deep Security detects interfaces on the computer that don't match any of these entries, the manager will trigger an alert.

## Enforce interface isolation

When Interface Isolation is enabled, the firewall will try to match the regular expression patterns to interface names on the local computer. To enforce interface isolation, click **Enable Interface Isolation** option on the **Policy or Computer Editor > Firewall > Interface Isolation** tab and enter string patterns that will match the names of the interfaces on a computer (in order of priority).

**Warning:** Before you enable Interface Isolation make sure that you have configured the interface patterns in the proper order and that you have removed or added all necessary string patterns. Only interfaces matching the highest priority pattern will be permitted to transmit traffic. Other interfaces (which match any of the remaining patterns on the list) will be "restricted". Restricted Interfaces will block all traffic unless an Allow Firewall Rule is used to allow specific traffic to pass through.

Selecting **Limit to one active interface** will restrict traffic to only a single interface even if more than one interface matches the highest priority pattern.

**Note:** Deep Security uses POSIX basic regular expressions to match interface names. For information on basic POSIX regular expressions, see http://pubs.opengroup.org/onlinepubs/009695399/basedefs/xbd_chap09.html#tag_09_03

# Overview section of the computer editor

The computer editor **Overview** page has the following tabbed sections:


- "General tab" below
- "Actions tab" on page 375
- "TPM tab" on page 376
- "System Events tab" on page 377


## General tab

- **Hostname:** Appears in the **Name** column on the **Computers** page. The name must be either the IP address of the computer or the hostname of the computer. Either a fully qualified hostname or a relative hostname can be used if a hostname is used instead of an IP address. You have to specify a hostname that can be resolved or a valid IP address that the Deep Security Manager can access. This is because the communication between the Deep Security Manager and the agent computers are based on the hostname. For relay-enabled agents, all of the computers within the relay group should be able to reach the specified IP address or hostname. If the Deep Security Manager cannot access the target computer the communication direction should be set to Agent/Appliance Initiated (Settings > Computer).
- **(Last IP Used: *<IP_address>*)**: The last IP used by the computer. **Last IP Used** may not always show the IP address of the Deep Security Agent's host. Instead, it could be the IP address of a proxy, load balancer, elastic load balancer (ELB), etc., that the agent uses to communicate with Deep Security Manager.
- **Display Name:** Appears in the Display Name column and in brackets next to the Hostname value.
- **Description:** a description of the computer.
- **Platform:** Details of the computer's OS will appear here.
- **Group:** The computer group to which the computer belongs appears in the list. You can reassign the computer to any other existing computer group.

- **Policy:** The policy (if any) that has been assigned to this computer.

  **Note:** Keep in mind that if you unassign a policy from a computer, rules may still be in effect on the computer if they were assigned independently of the policy.

- **Asset Importance:** Deep Security Manager uses a ranking system to quantify the importance of security events. Rules are assigned a severity level (high, medium, low, etc.), and assets (computers) are assigned an "asset importance" level. These levels have numerical values. When a rule is triggered on a computer the asset importance value and the severity level value are multiplied together. This produces a score which is used to sort events by importance. (Event ranking can be seen in the **Events** pages.) Use this **Asset Importance** list to assign an asset importance level to this computer. (To edit the numerical values associated with severity and importance levels, go to **Administration > System Settings > Ranking**.)
- **Download Security Updates From:** Use the dropdown list to select which relay group the agent/appliance on this computer will download security updates from. (not displayed if agent is acting as a relay.)

## Computer status

The Status area displays the latest available information about the computer and the protection modules in effect on it. Whether the computer is protected by an agent or an appliance (or both in the case of combined mode) is displayed in the top row.

- **Status:**
  - When the computer is unmanaged the status represents the state of the agent or appliance with respect to activation. The status will display either "Discovered" or "New" followed by the agent or appliance state in brackets ("No Agent/Appliance", "Unknown", "Reactivation Required", "Activation Required", or "Deactivation Required").
  - When the computer is managed and no computer errors are present, the status will display "Managed" followed by the state of the agent or appliance in brackets ("Online" or "Offline").

- When the computer is managed and the agent or appliance is in the process of performing an action (e.g. "Integrity Scan in Progress", "Upgrading Agent (Install Program Sent)", etc.) the task status will be displayed.
- When there are errors on the computer (e.g., "Offline", "Update Failed", etc.) the status will display the error. When more than one error is present, the status will display "Multiple Errors" and each error will be listed beneath.

## Protection module status

The software that implements Deep Security 9.5 or later protection modules is installed deployed to agents on an as-needed basis. Only core functionality is included when an agent is first installed. The software that implements Deep Security 9.5 or later protection modules is deployed to agents on an as-needed basis. Only core functionality is included when an agent is first installed.

The **Status** area provides information about the state of the Deep Security modules. The status reflects the state of a module on the agent as well as its configuration in Deep Security Manager. A status of "On" indicates that the module is configured in Deep Security Manager and is installed and operating on the Deep Security Agent.

A green status light is displayed for a module when it is "On" and working. In addition, modules that allow individual rule assignment must have at least one rule assigned before they will display a green light.

- **Anti-Malware:** Whether anti-malware protection is on or off and whether it is configured for real-time or on-demand scans.
- **Web Reputation:** Whether web reputation is on or off.
- **Firewall:** Whether the firewall is on or off and how many rules are in effect.
- **Intrusion Prevention:** Whether intrusion prevention is on or off and how many rules are in effect.
- **Integrity Monitoring:** Whether integrity monitoring is on or off and how many rules are in effect.
- **Log Inspection:** Whether log inspection is on or off and how many rules are in effect.
- **Application Control**: Whether application control is on or off.

- **Online:** Indicates whether the manager can currently communicate with the agent or appliance.
- **Last Communication:** The last time the manager successfully communicated with the agent or appliance on this computer.
- **Check Status:** This button allows you to force the manager to perform an immediate heartbeat operation to check the status of the agent or appliance. Check Status will not perform a security update of the agent or appliance. When manager to agent or appliance communications is set to "Agent/Appliance Initiated" the **Check Status** button is disabled. Checking status will not update the logs for this computer. To update the logs for this computer, go to the **Actions** tab.
- **Clear Warnings/Errors:** Dismisses any alerts or errors on this computer.
- **ESXi server:** If the computer is a virtual machine protected by a virtual appliance, the hosting ESXi server is displayed.
- **Appliance:** If the computer is a virtual machine protected by a virtual appliance, the protecting appliance is displayed.
- **ESXi Version:** If the computer is an ESXi server, the ESXi version number is displayed.
- **Filter Driver version:** If the computer is an ESXi server, the filter driver version number is displayed. If you are using DSVA 9.6 or later with ESXi 6.0 or later, "N/A" will be displayed because no filter driver is in use.
- **Guests:** If the computer is an ESXi server, the virtual appliance and guests are displayed.
- **Appliance Version:** If the computer is a virtual appliance, the appliance version number is displayed.
- **Protected Guests On:** If the computer is a virtual appliance, the IP of the ESXi server and the protected guest are displayed.

## VMware virtual machine summary

This section displays a summary of hardware and software configuration information about the virtual machine on which the agent or appliance is running (VMware virtual machines only).

# Actions tab

## Activation

A newly installed Deep Security agent or appliance needs to be "activated" by the Deep Security Manager before policies, rules, requests for event logs, etc. can be sent to it. The activation procedure includes the exchange of SSL keys which uniquely identify a manager (or one of its nodes) and an agent/appliance to each other. Once activated by a Deep Security Manager, an agent/appliance will only accept instructions or communicate with the Deep Security Manager which activated it (or one of its nodes).

An unactivated agent or appliance can be activated by any Deep Security Manager.

Agents and appliances can only be deactivated locally on the computer or from the Deep Security Manager which activated it. If an agent or appliance is already activated, the button in this area will read **Reactivate** rather than **Activate**. Reactivation has the same effect as activation. A reactivation will reset the agent or appliance to the state it was in after first being installed and initiate the exchange of a new set of SSL keys.

## Policy

When you change the configuration of an agent or appliance on a computer using the Deep Security Manager (apply a new intrusion prevention rule, change logging settings, etc.) the Deep Security Manager has to send the new information to the agent or appliance. This is a "Send Policy" instruction. Policy updates usually happen immediately but you can force an update by clicking the **Send Policy** button.

## Agent Software

This displays the version of the agent or appliance currently running on the computer. If a newer version of the agent or appliance is available for the computer's platform you can click the **Upgrade Agent** or **Upgrade Appliance** button to remotely upgrade the agent or appliance from the Deep Security Manager. You can configure the Deep Security Manager to trigger an alert if new versions of the agent or appliance software running on any of your computers by going to the **Administration > System Settings > Updates** tab.

**Note:** Before updating or uninstalling a Deep Security Agent or Relay on Windows, you must disable agent self-protection. To do this, on the Deep Security Manager, go to **Computer editor**[1] > **Settings** > **General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override.

### Support

The **Create Diagnostic Package** button creates a snapshot of the state of the agent or appliance on the computer. Your support provider may request this for troubleshooting purposes.

If you have lost communication with the computer, a diagnostics package can be created locally. For more information, see "Create a diagnostic package and logs" on page 1105.

## TPM tab

**Note:** The TPM tab will appear in place of the Actions tab for ESXi servers.

A Trusted Platform Module (TPM) is a type of chip that is used for hardware authentication. VMware uses the TPM with its ESXi hypervisors. During the boot sequence, an ESXi writes a SHA-1 hash of each hypervisor component to a set of registers as it loads. An unexpected change in these values from one boot sequence to the next can indicate a possible security issue worth investigating. Deep Security can monitor the TPM on an ESXi after every boot and raise an Alert if it detects any changes. If you select the option to enable TPM monitoring on an ESXi that doesn't support it, the option will be automatically disabled.

**Enable TPM Monitoring:** Select to enable Trusted Platform Module monitoring.

**Raise an alert when TPM Monitoring fails to obtain valid register values:** Select to have Deep Security raise an alert if the Trusted Platform Module fails to obtain valid register values for the hypervisor components during the ESXi boot sequence.

**TPM Register Data Imported:** Indicates whether the Trusted Protection Module data has been imported.

---

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

**TPM Last Checked:** Indicates when the Trusted Protection Module was last checked. You can click **Check Now** to start a check of the Trusted Platform Module.

**Note:** The minimum requirements for TPM monitoring are

- TPM/TXT installed and enabled on the ESXi (consult your VMware documentation for details)
- The Deep Security integrity monitoring and application control module must be properly licensed.

### System Events tab

For information about events, see "System events" on page 918.

## Overview section of the policy editor

The Overview section of the policy editor has the following tabbed sections:

- "General tab" below
- "Computer(s) Using This Policy tab" on the next page
- "Events tab" on the next page

### General tab

#### General

- **Name:** Appears in the Display Name column and in brackets next to the Hostname value.
- **Description:** a description of the computer.

#### Inheritance

Identifies the parent policy (if any) from which the current policy inherits its settings.

### Modules

- **Anti-Malware:** Whether anti-malware protection is on or off and whether it is configured for real-time or on-demand scans.
- **Web Reputation:** Whether web reputation is on or off.
- **Firewall:** Whether the firewall is on or off and how many rules are in effect.
- **Intrusion Prevention:** Whether intrusion prevention is on or off and how many rules are in effect.
- **Integrity Monitoring:** Whether integrity monitoring is on or off and how many rules are in effect.
- **Log Inspection:** Whether log inspection is on or off and how many rules are in effect.
- **Application Control:** Whether application control is on or off.

### Computer(s) Using This Policy tab

Lists computers to which this policy has been assigned.

### Events tab

For information about events, see "System events" on page 918.

## Network engine settings

To edit the network engine settings of a policy or computer, open the **Policy editor**[1] or the **Computer editor**[2] for the policy or computer to configure and click **Settings > Advanced** .

> **Note:** The **Advanced** tab also contains **Events** settings. For information on those settings, see "Limit log file sizes" on page 802. It also contains the **Generate an Alert when Agent**

---

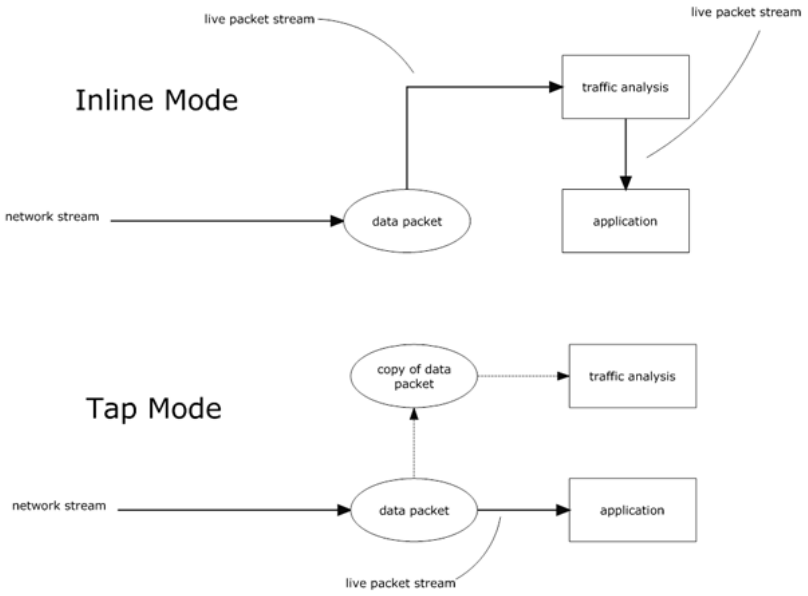
[1]To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

[2]To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

**configuration package exceeds maximum size** setting, which controls the display of the "Agent configuration package too large" setting.

The following settings are available:

- **Network Engine Mode** : The network engine is a component within the Intrusion Prevention, Firewall, and Web Reputation modules that decides whether to block or allow packets. For the Firewall and Intrusion Prevention modules, the network engine performs a packet sanity check and also makes sure each packet passes the firewall and intrusion prevention rules (called, rules matching). The network engine can operate Inline or in tap mode. When operating Inline, the packet stream passes through the network engine. Stateful tables are maintained, firewall rules are applied and traffic normalization is carried out so that intrusion prevention and firewall rules can be applied. When operating in tap mode, the packet stream is cloned and diverted from the main stream. In tap mode, the packet stream is not modified; all operations are carried out on the cloned stream.




- **Failure Response**: The settings here determine how the network engine behaves when it finds faulty packets. The default is to block them (Fail closed), but you can let some of them through (Fail open) for the reasons explained below.
  - **Network Engine System Failure**: This setting determines whether the network engine blocks or allows faulty packets that occur as a result of system failures on the network

engine host, such as out of memory failures, allocated memory failures, and network engine (DPI) decoding failures occur. The options are:

- **Fail closed** (default): The network engine blocks the faulty packet. It does not perform rules matching. This option provides the highest level of security.
- **Fail open**: The network engine allows the faulty packet through, does not perform rules matching, and logs an event. Consider using **Fail open** if your agent or virtual appliance frequently encounters network exceptions because of heavy loads or lack of resources.

- **Network Packet Sanity Check Failure**: This setting determines whether the network engine blocks or allows packets that fail the packet sanity checks. Examples of sanity check failures: firewall sanity check failures, network layer 2, 3, or 4 attribute check failures, TCP state check failures. The options are:
  - **Fail closed** (default): The network engine blocks the failed packet. It does not perform any rules matching. This option provides the highest level of security.
  - **Fail open**: The network engine allows the failed packet, does not perform any rules matching on it, and logs an event. Consider using **Fail open** if you want to disable the packet sanity checks, but preserve rules matching functionality.

- **Anti-Evasion Posture**: The anti-evasion setting controls the network engine handling of abnormal packets that may be attempting to evade analysis. For details, see "Configure anti-evasion settings" on page 578.

- **Advanced Network Engine Options**: If you deselect the **Inherited** check box, you can customize these settings:
  - **CLOSED timeout:** For gateway use. When a gateway passes on a "hard close" (RST), the side of the gateway that received the RST will keep the connection alive for this amount of time before closing it.
  - **SYN_SENT Timeout:** How long to stay in the SYN-SENT state before closing the connection.
  - **SYN_RCVD Timeout:** How long to stay in the SYN_RCVD state before closing the connection.

- **FIN_WAIT1 Timeout:** How long to stay in the FIN-WAIT1 state before closing the connection.
- **ESTABLISHED Timeout:** How long to stay in the ESTABLISHED state before closing the connection.
- **ERROR Timeout:** How long to maintain a connection in an Error state. (For UDP connections, the error can be caused by any of a variety of UDP problems. For TCP connections, the errors are probably due to packets being dropped by the firewall.)
- **DISCONNECT Timeout:** How long to maintain idle connections before disconnecting.
- **CLOSE_WAIT Timeout:** How long to stay in the CLOSE-WAIT state before closing the connection.
- **CLOSING Timeout:** How long to stay in the CLOSING state before closing the connection.
- **LAST_ACK Timeout:** How long to stay in the LAST-ACK state before closing the connection.
- **ACK Storm timeout:** The maximum period of time between retransmitted ACKs within an ACK Storm. In other words, if ACKs are being retransmitted at a lower frequency then this timeout, they will NOT be considered part of an ACK Storm.
- **Boot Start Timeout:** For gateway use. When a gateway is booted, there may already exist established connections passing through the gateway. This timeout defines the amount of time to allow non-SYN packets that could be part of a connection that was established before the gateway was booted to close.
- **Cold Start Timeout:** Amount of time to allow non-SYN packets that could belong to a connection that was established before the stateful mechanism was started.
- **UDP Timeout:** Maximum duration of a UDP connection.
- **ICMP Timeout:** Maximum duration of an ICMP connection.
- **Allow Null IP:** Allow or block packets with no source or destination IP address.
- **Block IPv6 on Agents and Appliances versions 8 and earlier:** Block or Allow IPv6 packets on older version 8.0 agents and appliances.

> **Note:** Deep Security Agents and Appliances versions 8.0 and older are unable to apply firewall or DPI rules to IPv6 network traffic and so the default setting for these older versions is to block IPv6 traffic.

**Block IPv6 on Agents and Appliances versions 8 and earlier:** Block or Allow IPv6 packets on older version 8.0 Agents and Appliances.

> **Note:** Deep Security Agents and Appliances versions 8.0 and older are unable to apply firewall or DPI Rules to IPv6 network traffic and so the default setting for these older versions is to block IPv6 traffic.

- **Block IPv6 on Agents and Appliances versions 9 and later:** Block or Allow IPv6 packets on agents and appliances that are version 9 or later.
- **Connection Cleanup Timeout:** Time between cleanup of closed connections (see next).
- **Maximum Connections per Cleanup:** Maximum number of closed connections to cleanup per periodic connection cleanup (see previous).
- **Block Same Src-Dest IP Address:** Block or allow packets with same source and destination IP address. (Doesn't apply to loopback interface.)
- **Maximum TCP Connections:** Maximum simultaneous TCP Connections.
- **Maximum UDP Connections:** Maximum simultaneous UDP Connections.
- **Maximum ICMP Connections:** Maximum simultaneous ICMP Connections.
- **Maximum Events per Second:** Maximum number of events that can be written per second.
- **TCP MSS Limit:** The MSS is the Maximum Segment Size (or largest amount of data) that can be sent in a TCP packet without being fragmented. This is usually established when two computers establish communication. However, in some occasions, the traffic goes through a router or switch that has a smaller MSS. In this case the MSS can change. This causes retransmission of the packets and the agent or appliance logs them as "Dropped Retransmit". In cases where there are large numbers of dropped retransmit event entries, you may wish to lower this limit and see if the volume is reduced.

- **Number of Event Nodes:** The maximum amount of kernel memory the driver will use to store log/event information for folding at any one time.

  Note: Event folding occurs when many events of the same type occur in succession. In such cases, the agent/appliance will "fold" all the events into one.

- **Ignore Status Code:** This option lets you ignore certain types of events. If, for example, you are getting a lot of "Invalid Flags" you can simply ignore all instances of that event.
- **Ignore Status Code:** Same as above.
- **Ignore Status Code:** Same as above.
- **Advanced Logging Policy:**
  - **Bypass:** No filtering of events. Overrides the "Ignore Status Code" settings (above) and other advanced settings, but does not override logging settings defined in the Deep Security Manager. For example, if firewall stateful configuration logging options set from a Firewall Stateful Configuration Properties window in the Deep Security Manager will not be affected.
  - **Normal:** All events are logged except dropped retransmits.
  - **Default:** Will switch to "Tap Mode" (below) if the engine is in tap mode, and will switch to "Normal" (above) if the engine is in inline mode.
  - **Backwards Compatibility Mode:** For support use only.
  - **Verbose Mode:** Same as "Normal" but including dropped retransmits.
  - **Stateful and Normalization Suppression:** Ignores dropped retransmit, out of connection, invalid flags, invalid sequence, invalid ack, unsolicited udp, unsolicited ICMP, out of allowed policy.
  - **Stateful, Normalization, and Frag Suppression:** Ignores everything that "**Stateful and Normalization Suppression**" ignores as well as events related to fragmentation.
  - **Stateful, Frag, and Verifier Suppression:** Ignores everything "**Stateful, Normalization, and Frag Suppression**" ignores as well as verifier-related events.
  - **Tap Mode:** Ignores dropped retransmit, out of connection, invalid flags, invalid sequence, invalid ack, max ack retransmit, packet on closed connection.

> **Note:** For a more comprehensive list of which events are ignored in **Stateful and Normalization Suppression; Stateful, Normalization, and Frag Suppression; Stateful, Frag, and Verifier Suppression; and Tap** modes, see "Reduce the number of logged events" on page 810.

- **Silent TCP Connection Drop:** When Silent TCP Connection Drop is on, a RST packet is only sent to the local stack. No RST packet is sent on the wire. This reduces the amount of information sent back to a potential attacker.

  > **Note:** If you enable the Silent TCP Connection Drop you must also adjust the DISCONNECT Timeout. Possible values for DISCONNECT Timeout range from 0 seconds to 10 minutes. This must be set high enough that the connection is closed by the application before it is closed by the Deep Security agent/appliance. Factors that will affect the DISCONNECT Timeout value include the operating system, the applications that are creating the connections, and network topology.

- **Enable Debug Mode:** When in debug mode, the agent/appliance captures a certain number of packets (specified by the setting below: Number of Packets to retain in Debug Mode). When a rule is triggered and debug mode is on, the agent/appliance will keep a record of the last X packets that passed before the rule was triggered. It will return those packets to the manager as debug events.

  > **Note:** Debug mode can very easily cause excessive log generation and should only be used under Client Services supervision.

- **Number of Packets to retain in Debug Mode:** The number of packets to retain and log when debug mode is on.
- **Log All Packet Data:** Record the packet data for events that are not associated with specific firewall or intrusion prevention rules. That is, log packet data for events such as "Dropped Retransmit" or "Invalid ACK".

  > **Note:** Events that have been aggregated because of event folding cannot have their packet data saved.

- **Log only one packet within period:** If this option is enabled and **Log All Packet Data** is not, most logs will contain only the header data. A full packet will be attached periodically, as specified by the **Period for Log only one packet within period** setting.
- **Period for Log only one packet within period:** When **Log only one packet within period** is enabled, this setting specifies how often the log will contain full packet data.
- **Maximum data size to store when packet data is captured:** The maximum size of header or packet data to be attached to a log.
- **Generate Connection Events for TCP:** Generates a firewall event every time a TCP connection is established.
- **Generate Connection Events for ICMP:** Generates a firewall event every time an ICMP connection is established.
- **Generate Connection Events for UDP:** Generates a firewall event every time a UDP connection is established.
- **Bypass CISCO WAAS Connections:** This mode bypasses stateful analysis of TCP sequence numbers for connections initiated with the proprietary CISCO WAAS TCP option selected. This protocol carries extra information in invalid TCP Sequence and ACK numbers that interfere with stateful firewall checks. Only enable this option if you are using CISCO WAAS and you are seeing connections with Invalid SEQ or Invalid ACK in the firewall logs. When this option is selected, TCP stateful sequence number checks are still performed for non WAAS enabled connections.
- **Drop Evasive Retransmit:** Incoming packets containing data that has already been processed will be dropped to avoid possible evasive retransmit attack techniques.
- **Verify TCP Checksum:** The segment's checksum field data will be used to assess the integrity of the segment.
- **Minimum Fragment Offset:** Defines the minimum acceptable IP fragment offset. Packets with offsets less than this will be dropped with reason "IP fragment offset too small". If set to 0 no limit is enforced. (default 60)
- **Minimum Fragment Size:** Defines the minimum acceptable IP fragment size. Fragmented packets that are smaller than this will be dropped with reason "First fragment too small" as potentially malicious. (default 120)

- **SSL Session Size:** Sets the maximum number of SSL session entries maintained for SSL session keys.
- **SSL Session Time:** Sets how long SSL session renewal keys are valid before they expire.
- **Filter IPv4 Tunnels:** Not used by this version of Deep Security.
- **Filter IPv6 Tunnels:** Not used by this version of Deep Security.
- **Strict Teredo Port Check:** Not used by this version of Deep Security.
- **Drop Teredo Anomalies:** Not used by this version of Deep Security.
- **Maximum Tunnel Depth:** Not used by this version of Deep Security.
- **Action if Maximum Tunnel Depth Exceeded:** Not used by this version of Deep Security.
- **Drop IPv6 Extension Type 0:** Not used by this version of Deep Security.
- **Drop IPv6 Fragments Lower Than minimum MTU:** Drop IPv6 fragments that do not meet the minimum MTU size specified by IETF RFC 2460.
- **Drop IPv6 Reserved Addresses**: Drop these reserved addresses:
  - IETF reserved 0000::/8
  - IETF reserved 0100::/8
  - IETF reserved 0200::/7
  - IETF reserved 0400::/6
  - IETF reserved 0800::/5
  - IETF reserved 1000::/4
  - IETF reserved 4000::/2
  - IETF reserved 8000::/2
  - IETF reserved C000::/3
  - IETF reserved E000::/4
  - IETF reserved F000::/5
  - IETF reserved F800::/6
- **Drop IPv6 Site Local Addresses:** Drop site local addresses FEC0::/10.

- **Drop IPv6 Bogon Addresses:** Drop these addresses:
  - "loopback ::1
  - "IPv4 compatible address", ::/96
  - "IPv4 mapped address" ::FFFF:0.0.0.0/96
  - "IPv4 mapped address", ::/8
  - "OSI NSAP prefix (deprecated by RFC4048)" 0200::/7
  - "6bone (deprecated)", 3ffe::/16
  - "Documentation prefix", 2001:db8::/32
- **Drop 6to4 Bogon Addresses:** Drop these addresses:
  - "6to4 IPv4 multicast", 2002:e000:: /20
  - "6to4 IPv4 loopback", 2002:7f00:: /24
  - "6to4 IPv4 default", 2002:0000:: /24
  - "6to4 IPv4 invalid", 2002:ff00:: /24
  - "6to4 IPv4 10.0.0.0/8", 2002:0a00:: /24
  - "6to4 IPv4 172.16.0.0/12", 2002:ac10:: /28
  - "6to4 IPv4 192.168.0.0/16", 2002:c0a8:: /32
- **Drop IP Packet with Zero Payload:** Drop IP packets that have a zero-length payload.
- **Drop Unknown SSL Protocol:** Drop connection if a client attempts to connect to the Deep Security Manager with the wrong protocol. By default, any protocol other than "http/1.1" will cause an error.
- **Force Allow DHCP DNS:** Controls whether the following hidden firewall rules are enabled:

| Rule type | Priority | Direction | Protocol | Source port | Destination port |
|---|---|---|---|---|---|
| Force Allow | 4 | Outgoing | DNS | Any | 53 |
| Force Allow | 4 | Outgoing | DHCP | 68 | 67 |
| Force Allow | 4 | Incoming | DHCP | 67 | 68 |

When the rules are enabled, agent computers can connect with the manager using the listed protocols and ports. The following values for this property are available:

- Inherited: Inherits the setting from the policy
- Turn off rules: Disables the rules. Note that this setting can cause agent computers to appear offline
- Allow DNS Query: Enable only the DNS-related rule
- Allow DNS Query and DHCP Client: Enable all 3 rules

- **Force Allow ICMP type3 code4:** Controls whether the following hidden firewall rules are enabled:

| Rule type | Priority | Direction | Protocol | Type | Code |
|---|---|---|---|---|---|
| Force Allow | 4 | Incoming | ICMP | 3 | 4 |

When enabled, these rules allow relay computers to connect with the manager so that the relay's heartbeat is transmitted. The following values are available:

- Inherited: Inherits the setting from the policy.
- Turn off rules: Disables the rule. This value can cause connection timeouts or "Destination cannot be reached" responses.
- Add Force Allow rule for ICMP type3 code4: Enables the rule.

- **Fragment Timeout:** If configured to do so, the intrusion prevention rules will inspect the content of a packet (or packet fragment) if that content is considered suspicious. This setting determines how long after inspecting to wait for the remaining packet fragments before discarding the packet.
- **Maximum number of fragmented IP packets to keep:** Specifies the maximum number of fragmented packets that Deep Security will keep.
- **Send ICMP to indicate fragmented packet timeout exceeded:** When this setting is enabled and the fragment timeout is exceeded, an ICMP packet is sent to the remote computer.

# Define rules, lists, and other common objects used by policies

The Common Objects pages (located under **Policies > Common Objects** in Deep Security Manager) provide a way to define objects once so that you can reuse them various policies and rules. When you use one of the common objects in the policy or computer editor, its settings can be overridden for that specific policy or computer. For more information on how common object properties can be inherited and overridden at the policy or computer level, see "Policies, inheritance, and overrides" on page 354.

**Tip:** You can automate common object creation and configuration using the Deep Security API. For examples, see the Create and Configure Common Objects for Policies and Computers guide.

## Rules

Some protection modules make use of rules:

- "Create a firewall rule" on page 597
- Configure an intrusion prevention rule for use in policies
- "Create an integrity monitoring rule" on page 640
- "Define a log inspection rule for use in policies" on page 696

## Lists

- "Create a list of directories for use in policies" on page 437
- "Create a list of file extensions for use in policies" on page 440
- "Create a list of files for use in policies" on page 441
- "Create a list of IP addresses for use in policies" on page 444
- "Create a list of MAC addresses for use in policies" on page 446
- "Create a list of ports for use in policies" on page 445

## Other


- "Define contexts for use in policies" on page 447
- "Define stateful firewall configurations" on page 625
- "Configure malware scans" on page 497
- "Define a schedule that you can apply to rules" on page 454


## Create a firewall rule

Firewall rules examine the control information in individual packets, and either block or allow them according to the criteria that you define. Firewall rules can be assigned to a policy or directly to a computer.

**Note:** This article specifically covers how to create a firewall rule. For information on how to configure the firewall module, see "Set up the Deep Security firewall" on page 584.

To create a new firewall rule, you need to:

1. "Add a new rule" below.
2. "Select the behavior and protocol of the rule" on the next page.
3. "Select a Packet Source and Packet Destination" on page 393.

When you're done with your firewall rule, you can also learn how to:

- "Configure rule events and alerts" on page 394
- "Set a schedule for the rule" on page 395
- "See policies and computers a rule is assigned to" on page 395
- "Assign a context to the rule " on page 395

### Add a new rule

There are three ways to add a new firewall rule on the **Policies** > **Common Objects** > **Rules** > **Firewall Rules** page. You can:

- Create a new rule. Click **New** > **New Firewall Rule**.
- Import a rule from an XML file. Click **New** > **Import From File**.

- Copy and then modify an existing rule. Right-click the rule in the Firewall Rules list and then click **Duplicate**. To edit the new rule, select it and then click **Properties**.

## Select the behavior and protocol of the rule

1. Enter a **Name** and **Description** for the rule.

   Tip: It is good practice to document all firewall rule changes in the Description field of the firewall rule. Make a note of when and why rules were created or deleted for easier firewall maintenance.

2. Select the **Action** that the rule should perform on packets. You can select from one of the following five actions:

   Note: Only one rule action is applied to a packet, and rules (of the same priority) are applied in the order of precedence listed below.

   - The rule can allow traffic to **bypass** the firewall. A bypass rule allows traffic to pass through the firewall and intrusion prevention engine at the fastest possible rate. Bypass rules are meant for traffic using media intensive protocols where filtering may not be desired or for traffic originating from trusted sources.

     Tip: For an example of how to create and use a bypass rule for trusted sources in a policy, see "Allow trusted traffic to bypass the firewall" on page 603.

     Note: Bypass rules are unidirectional. Explicit rules are required for each direction of traffic.

     Tip: You can achieve maximum throughput performance on a bypass rule with the following settings:
     - **Priority:** Highest
     - **Frame Type:** IP
     - **Protocol:** TCP, UDP, or other IP protocol. (Do not use the "Any" option.)
     - **Source and Destination IP and MAC:** all "Any"

- If the protocol is TCP or UDP and the traffic direction is "incoming", the destination ports must be one or more specified ports (not "Any"), and the source ports must be "Any".
- If the protocol is TCP or UDP and the traffic direction is "outgoing", the source ports must be one or more specified ports (Not "Any"), and the destination ports must be "Any".
- **Schedule:** None.

- The rule can **log only**. This action will make entries in the logs but will not process traffic.
- The rule can **force allow** defined traffic (it will allow traffic defined by this rule without excluding any other traffic.)
- The rule can **deny** traffic (it will deny traffic defined by this rule.)
- The rule can **allow** traffic (it will exclusively allow traffic defined by this rule.)

**Note:** If you have no allow rules in effect on a computer, all traffic is permitted unless it is specifically blocked by a deny rule. Once you create a single allow rule, all other traffic is blocked unless it meets the requirements of the allow rule. There is one exception to this: ICMPv6 traffic is always permitted unless it is specifically blocked by a deny rule.

3. Select the **Priority** of the rule. The priority determines the order in which rules are applied. If you have selected "force allow", "deny", or "bypass" as your rule action, you can set a priority of 0 (low) to 4 (highest). Setting a priority allows you to combine the actions of rules to achieve a cascading rule effect.

**Note:** **Log only** rules can only have a priority of **4**, and **Allow** rules can only have a priority of **0**.

**Note:** High priority rules get applied before low priority rules. For example, a port 80 incoming deny rule with a priority of 3 will drop a packet before a port 80 incoming force allow rule with a priority of 2 gets applied to it.

For detailed information on how actions and priority work together, see "Firewall rule actions and priorities" on page 605.

4. Select a **Packet Direction**. Select whether this rule will be applied to **incoming** (from the network to the host) or **outgoing**(from the host to the network) traffic.

   **Note:** An individual firewall rule only apply to a single direction of traffic. You may need to create incoming and outgoing firewall rules in pairs for specific types of traffic.

5. Select an Ethernet **Frame Type**. The term "frame" refers to Ethernet frames, and the available protocols specify the data that the frame carries. If you select "Other" as the frame type, you need to specify a frame number.

6. **Note:** **IP** covers both IPv4 and IPv6. You can also select **IPv4** or **IPv6** individually

   **Note:** Linux Agents will only examine packets with IP or ARP frame types. Packets with other frame types will be allowed through. Note that the Virtual Appliance does not have these restrictions and can examine all frame types, regardless of the operating system of the virtual machine it is protecting.

   If you select the Internet Protocol (IP) frame type, you need to select the transport **Protocol**. If you select "Other" as the protocol, you also need to enter a protocol number.

## Select a Packet Source and Packet Destination

Select a combination of **IP** and **MAC** addresses, and if available for the frame type, **Port** and **Specific Flags** for the Packet Source and Packet Destination.

**Tip:** You can use a previously created IP, MAC or port list.

Support for IP-based frame types is as follows:

| | IP | MAC | Port | Flags |
|---|---|---|---|---|
| Any | ✔ | ✔ | | |
| ICMP | ✔ | ✔ | | ✔ |

| | IP | MAC | Port | Flags |
|---|---|---|---|---|
| ICMPV6 | ✔ | ✔ | | ✔ |
| IGMP | ✔ | ✔ | | |
| GGP | ✔ | ✔ | | |
| TCP | ✔ | ✔ | ✔ | ✔ |
| PUP | ✔ | ✔ | | |
| UDP | ✔ | ✔ | ✔ | |
| IDP | ✔ | ✔ | | |
| ND | ✔ | ✔ | | |
| RAW | ✔ | ✔ | | |
| TCP+UDP | ✔ | ✔ | ✔ | ✔ |

**Note:** ARP and REVARP frame types only support using MAC addresses as packet sources and destinations.

You can select **Any Flags** or individually select the following flags:

- URG
- ACK
- PSH
- RST
- SYN
- FIN

## Configure rule events and alerts

When a firewall rule is triggered, it logs an event in the Deep Security Manager and records the packet data.

**Note:** Note that rules using the "Allow", "Force Allow" and "Bypass" actions will not log any events.

### Alerts

You can configure rules to also trigger an alert if they log an event. To do so, open the properties for a rule, click on **Options**, and then select **Alert when this rule logs an event**.

**Note:** Only firewall rules with an action set to "Deny" or "Log Only" can be configured to trigger an alert.

## Set a schedule for the rule

Select whether the firewall rule should only be active during a scheduled time.

For more information on how to do so, see "Define a schedule that you can apply to rules" on page 454.

## Assign a context to the rule

Rule contexts allow you to set firewall rules uniquely for different network environments. Contexts are commonly used to allow for different rules to be in effect for laptops when they are on and off-site.

For more information on how to create a context, see "Define contexts for use in policies" on page 447.

**Tip:** For an example of a policy that implements firewall rules using contexts, look at the properties of the "Windows Mobile Laptop" Policy.

## See policies and computers a rule is assigned to

You can see which policies and computers are assigned to a firewall rule on the **Assigned To** tab. Click on a policy or computer in the list to see their properties.

## Export a rule

You can export all firewall rules to a .csv or .xml file by clicking **Export** and selecting the corresponding export action from the list. You can also export specific rules by first selecting them, clicking **Export** and then selecting the corresponding export action from the list.

### Delete a rule

To delete a rule, right-click the rule in the Firewall Rules list, click **Delete** and then click **OK**.

**Note:** Firewall Rules that are assigned to one or more computers or that are part of a policy cannot be deleted.

## Configure intrusion prevention rules

Perform the following tasks to configure and work with intrusion prevention rules:


- "See the list of intrusion prevention rules" on the next page
- "See information about an intrusion prevention rule" on the next page
- "See information about the associated vulnerability (Trend Micro rules only)" on page 399
- "Assign and unassign rules" on page 399
- "Automatically assign updated required rules" on page 400
- "Configure event logging for rules" on page 401
- "Generate alerts" on page 402
- "Setting configuration options (Trend Micro rules only)" on page 402
- "Schedule active times" on page 403
- "Exclude from recommendations" on page 403
- "Set the context for a rule" on page 404
- "Override the behavior mode for a rule" on page 404
- "Override rule and application type configurations" on page 405
- "Export and import rules" on page 405
- "Configure an SQL injection prevention rule" on page 559


For an overview of the intrusion prevention module, see "Block exploit attempts using intrusion prevention" on page 537.

## See the list of intrusion prevention rules

The Policies page provides a list of intrusion prevention rules. You can search for intrusion prevention rules, and open and edit rule properties. In the list, rules are grouped by application type, and some rule properties appear in different columns.

> **Tip:** The "TippingPoint" column contains the equivalent Trend Micro TippingPoint rule ID. In the Advanced Search for intrusion prevention, you can search on the TippingPoint rule ID. You can also see the TippingPoint rule ID in the list of assigned intrusion prevention rules in the policy and computer editor.

To see the list, click **Policies**, and then below **Common Objects/Rules** click **Intrusion Prevention Rules**.

## See information about an intrusion prevention rule

The properties of intrusion prevention rules include information about the rule and the exploit against which it protects.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.

### General Information

- **Name:** The name of the intrusion prevention rule.
- **Description:** The description of the intrusion prevention rule.
- **Minimum Agent/Appliance Version:** The minimum version of the Deep Security **Agent or Appliance**[1] required to support this intrusion prevention rule.

### Details

Clicking **New** ( ) or **Properties** ( ) displays the **Intrusion Prevention Rule Properties** window.

---

[1]The Deep Securty Agent and Deep Security Virtual Appliance are the components that enforce the Deep Security policies that you have defined. Agents are deployed directly on a computer. Appliances are used in VMware vSphere environments to provide agentless protection. They are not available with Deep Security as a Service.

**Note:** Note the **Configuration** tab. Intrusion Prevention Rules from Trend Micro are not directly editable through Deep Security Manager. Instead, if the Intrusion Prevention Rule requires (or allows) configuration, those configuration options will be available on the **Configuration** tab. Custom Intrusion Prevention Rules that you write yourself will be editable, in which case the **Rules** tab will be visible.

## See the list of intrusion prevention rules

The Policies page provides a list of intrusion prevention rules. You can search for intrusion prevention rules, and open and edit rule properties. In the list, rules are grouped by application type, and some rule properties appear in different columns.

**Tip:** The "TippingPoint" column contains the equivalent Trend Micro TippingPoint rule ID. In the Advanced Search for intrusion prevention, you can search on the TippingPoint rule ID. You can also see the TippingPoint rule ID in the list of assigned intrusion prevention rules in the policy and computer editor.

To see the list, click **Policies**, and then below **Common Objects/Rules** click **Intrusion Prevention Rules**.

## General Information

- **Application Type:** The application type under which this intrusion prevention rule is grouped.

  **Tip:** You can edit application types from this panel. When you edit an application type from here, the changes are applied to all security elements that use it.

- **Priority:** The priority level of the rule. Higher priority rules are applied before lower priority rules.
- **Severity:** Setting the severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as sorting criteria when viewing a list of intrusion prevention rules. More importantly, each severity level is associated with a severity value; this value is multiplied by a computer's Asset Value to determine the Ranking of an Event. (See **Administration > System Settings > Ranking**.)

- **CVSS Score:** A measure of the severity of the vulnerability according the National Vulnerability Database.

### Identification (Trend Micro rules only)

- **Type:** Can be either Smart (one or more known and unknown (zero day) vulnerabilities), Exploit (a specific exploit, usually signature based), or Vulnerability (a specific vulnerability for which one or more exploits may exist).
- **Issued:** The date the rule was released. This does not indicate when the rule was downloaded.
- **Last Updated:** The last time the rule was modified either locally or during Security Update download.
- **Identifier:** The rule's unique identification tag.

## See information about the associated vulnerability (Trend Micro rules only)

Rules that Trend Micro provides can include information about the vulnerability against which the rule protects. When applicable, the Common Vulnerability Scoring System (CVSS) is displayed. (For information on this scoring system, see the CVSS page at the National Vulnerability Database.)

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Vulnerabilities** tab.

## Assign and unassign rules

To apply intrusion prevention rules during agent scans, you assign them to the appropriate policies and computers. When the rule is no longer necessary because the vulnerability has been patched you can unassign the rule.

If you cannot unassign intrusion prevention rules from a **Computer editor**[1], it is likely because the rules are currently assigned in a policy. Rules assigned at the policy level must be removed using the **Policy editor**[2] and cannot be removed at the computer level.

When you make a change to a policy, it affects all computers using the policy. For example, when you unassign a rule from a policy you remove the rule from all computers that are protected by that policy. To continue to apply the rule to other computers, create a new policy for that group of computers. (See "Policies, inheritance, and overrides" on page 354.)

**Tip:** To see the policies and computers to which a rule is assigned, see the Assigned To tab of the rule properties.

1. Go to the **Policies** page, right-click the policy to configure and click **Details**.
2. Click **Intrusion Prevention > General**.
   The list of rules that are assigned to the policy appear in the **Assigned Intrusion Prevention Rules** list.
3. Under **Assigned Intrusion Prevention Rules**, click **Assign/Unassign**.
4. To assign a rule, select the check box next to the rule.
5. To unassign a rule, deselect the check box next to the rule.
6. Click **OK**.

## Automatically assign updated required rules

Security updates can include new or updated application types and intrusion prevention rules which require the assignment of secondary intrusion prevention rules. Deep Security can automatically assign these rules if they are required. You enable these automatic assignments in the the policy or computer properties.

1. Go to the **Policies** page, right-click the policy to configure and click **Details**.
2. Click **Intrusion Prevention > Advanced**.
3. To enable the automatic assignments, in the **Rule Updates** area, select **Yes**.
4. Click **OK**.

---

[1]To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2]To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

## Configure event logging for rules

Configure whether events are logged for a rule, and whether to include packet data in the log.

> **Note:** Deep Security can display X-Forwarded-For headers in intrusion prevention events when they are available in the packet data. This information can be useful when the Deep Security Agent is behind a load balancer or proxy. The X-Forwarded-For header data appears in the event's Properties window. To include the header data, include packet data in the log. In addition, rule 1006540 " Enable X-Forwarded-For HTTP Header Logging" must be assigned.

Because it would be impractical to record all packet data every time a rule triggers an event, Deep Security records the data only the first time the event occurs within a specified period of time. The default time is five minutes, however you can change the time period using the "Period for Log only one packet within period" property of a policy's Advanced Network Engine settings. (See Advanced Network Engine Options.)

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on page 405.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. On the General tab, go to the Events area and select the desired options:
   - To disable logging for the rule, select **Disable Event Logging**.
   - To log an event when a packet is dropped or blocked, select **Generate Event on Packet Drop**.
   - To include the packet data in the log entry, select **Always Include Packet Data**.
   - To log several packets that precede and follow the packet that the rule detected, select **Enable Debug Mode**.Use debug mode only when your support provider instructs you to do so.

Additionally, to include packet data in the log, the policy to which the rule is assigned must allow rules to capture packet data:

1. On the Policies page, open the policy that is assigned the rule.
2. Click **Intrusion Prevention > Advanced**.

3. In the **Event Data** area, select **Yes**.

## Generate alerts

Generate an alert when an intrusion prevention rule triggers an event.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on page 405.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the Options tab, and in the **Alert** area select **On**.
4. Click **OK**.

## Setting configuration options (Trend Micro rules only)

Some intrusion prevention rules that Trend Micro provides have one or more configuration options such as header length, allowed extensions for HTTP, or cookie length. Some options require you to configure them. If you assign a rule without setting a required option, an alert is generated that informs you about the required option. (This also applies to any rules that are downloaded and automatically applied by way of a Security Update.)

Intrusion prevention rules that have configuration options appear in the Intrusion Prevention Rules list with a small gear over their icon .

> **Note:** Custom intrusion prevention rules that you write yourself include a **Rules** tab where you can edit the rules.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on page 405.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Configuration** tab.
4. Configure the properties and then click **OK**.

## Schedule active times

Schedule a time during which an intrusion prevention rule is active. Intrusion prevention rules that are active only at scheduled times appear in the Intrusion Prevention Rules page with a small clock over their icon .

> **Note:** With Agent-based protection, schedules use the same time zone as the endpoint operating system. With Agentless protection, schedules use the same time zone as the Deep Security Virtual Appliance. Agentless protection is not available with Deep Security as a Service.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on page 405.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Options** tab.
4. In the **Schedule** area, select **New** or select a frequency.
5. Edit the schedule as required.
6. Click **OK**.

## Exclude from recommendations

Exclude intrusion prevention rules from rule recommendations of recommendation scans.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on page 405.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Options**tab.
4. In the **Recommendations Options** area, select **Exclude from Recommendations**.
5. Click **OK**.

## Set the context for a rule

Set the context in which the rule is applied.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on the next page.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Options** tab.
4. In the **Context** area, select **New** or select a context.
5. Edit the context as required.
6. Click **OK**.

## Override the behavior mode for a rule

Set the behavior mode of an intrusion prevention rule to Detect when testing new rules. In Detect mode, the rule creates a log entry prefaced with the words "detect only:" and does not interfere with traffic. Some intrusion prevention rules are designed to operate only in Detect mode. For these rules, you cannot change the behavior mode.

> **Note:** If you disable logging for the rule, the rule activity is not logged regardless of the behavior mode.

For more information about behavior modes, see "Use behavior modes to test rules" on page 539.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on the next page.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Select **Detect Only**.

## Override rule and application type configurations

From a **Computer or Policy editor**[1] , you can edit an intrusion prevention rule so that your changes apply only in the context of the policy or computer. You can also edit the rule so that the changes apply globally so that the changes affect other policies and computers that are assigned the rule. Similarly, you can configure application types for a single policy or computer, or globally.

1. Go to the **Policies** page, right-click the policy to configure and click **Details**.
2. Click **Intrusion Prevention**.
3. To edit a rule, right-click the rule and select one of the following commands:
   - **Properties**: Edit the rule only for the policy.
   - **Properties (Global)**: Edit the rule globally, for all policies and computers.
4. To edit the application type of a rule, right-click the rule and select one of the following commands:
   - **Application Type Properties**: Edit the application type only for the policy.
   - **Application Type Properties (Global)**: Edit the application type globally, for all policies and computers.
5. Click **OK**.

**Tip:** When you select the rule and click Properties, you are editing the rule only for the policy that you are editing.

**Note:** You cannot assign one port to more than eight application types. If they are, the rules will not function on that port.

## Export and import rules

You can export one or more intrusion prevention rules to an XML or CSV file, and import rules from an XML file.

---

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

1. Click **Policies > Intrusion Prevention Rules**.
2. To export one or more rules, select them and click **Export > Export Selected to CSV** or **Export > Export Selected to XML**.
3. To export all rules, click **Export > Export to CSV** or **Export > Export to XML**.
4. To import rules, click **New > Import From File** and follow the instructions on the wizard.

## Create an integrity monitoring rule

Integrity monitoring rules describe how Deep Security Agents should scan for and detect changes to a computer's files, directories, and registry keys and values, as well as changes in installed software, processes, listening ports, and running services. Integrity monitoring rules can be assigned directly to computers or can be made part of a policy.

**Note:** This article specifically covers how to create an integrity monitoring rule. For information on how to configure the Integrity Monitoring module, see "Set up integrity monitoring" on page 632.

There are two types of integrity monitoring rules: those that you have created, and those that are issued by Trend Micro. For more information on how to configure rules issued by Trend Micro, see the "Configure Trend Micro integrity monitoring rules" on page 409 section.

To create a new integrity monitoring rule, you need to:

1. "Add a new rule" on the next page.
2. "Enter integrity monitoring rule information " on the next page.
3. "Select a rule template and define rule attributes" on the next page.

When you're done with your rule, you can also learn how to

- "Configure rule events and alerts" on page 409
- "See policies and computers a rule is assigned to" on page 410
- "Export a rule" on page 410
- "Delete a rule" on page 410

## Add a new rule

There are three ways to add an integrity monitoring rule on the **Policies** > **Common Objects** > **Rules** > **Integrity Monitoring Rules** page. You can:

- Create a new rule. Click **New** > **New Integrity Monitoring Rule**.
- Import a rule from an XML file. Click **New** > **Import From File**.
- Copy and then modify an existing rule. Right-click the rule in the Integrity Monitoring Rules list and then click **Duplicate**. To edit the new rule, select it and then click **Properties**.

## Enter integrity monitoring rule information

1. Enter a **Name** and **Description** for the rule.

   **Tip:** It is good practice to document all integrity monitoring rule changes in the Description field of the firewall rule. Make a note of when and why rules were created or deleted for easier maintenance.

2. Set the **Severity** of the rule.

   **Note:** Setting the severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as sorting criteria when viewing a list of integrity monitoring rules. More importantly, each severity level is associated with a severity value; this value is multiplied by a computer's Asset Value to determine the ranking of an event. (See **Administration > System Settings > Ranking**.)

## Select a rule template and define rule attributes

Go to the **Content** tab and select from one of the following three templates:

### Registry Value template

Create an integrity monitoring rule to specifically monitor changes to registry values.

**Note:** The Registry Value template is only for Windows-based computers .

1. Select the **Base Key** to monitor and whether or not to monitor contents of sub keys.
2. List **Value Names** to be included or excluded. You can use "?" and "*" as wildcard characters.
3. Enter **Attributes** to monitor. Entering "STANDARD" will monitor changes in registry size, content and type. For more information on Registry Value template attributes see the "RegistryValueSet" on page 678 documentation.

### File template

Create an integrity monitoring rule to specifically monitor changes to files.

1. Enter a **Base Directory** for the rule (for example, `C:\Program Files\MySQL`.) Select **Include Sub Directories** to include the contents of all subdirectories relative to the base directory.

2. Use the **File Names** fields to include or exclude specific files. You can use wildcards (" `?` " for a single character and " `*` " for zero or more characters.

   **Note:** Leaving the **File Names** fields blank will cause the rule to monitor all files in the base directory. This can use significant system resources if the base directory contains numerous or large files.

3. Enter **Attributes** to monitor. Entering "STANDARD" will monitor changes in file creation date, last modified date, permissions, owner, group, size, content, flags (Windows), and SymLinkPath (Linux). For more information on File template attributes see the "FileSet" on page 662 documentation.

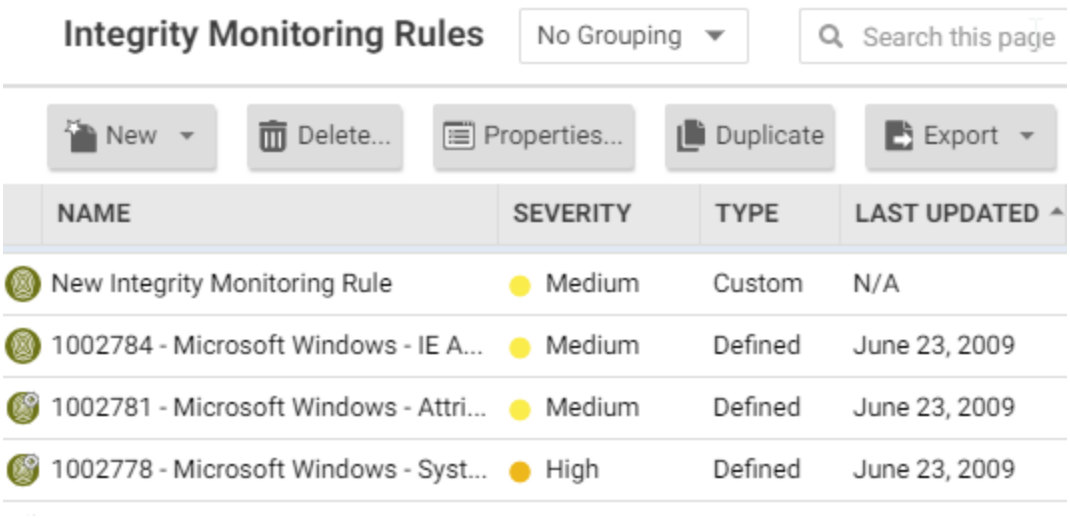
### Custom (XML) template

Create a custom integrity monitoring rule template to monitor directories, registry values, registry keys, services, processes, installed software, ports and files using the Deep Security XML-based "Integrity monitoring rules language" on page 645.

**Tip:** You can create your rule in your preferred text editor and paste it to the **Content** field when you are done.

## Configure Trend Micro integrity monitoring rules

Integrity monitoring rules issued by Trend Micro cannot be edited in the same way as the custom rules you create. Some Trend Micro rules cannot be modified at all, while other rules may offer limited configuration options. Both of these rule types will show as "Defined" under the "Type" column, but rules that can be configured will display a gear in the Integrity Monitoring icon ( ).




You can access the configuration options for a rule by opening the properties for the rule and clicking on the **Configuration** tab.

Rules issued by Trend Micro also show the following additional information under the **General** tab:

- When the rule was first issued and last updated, as well as a unique identifier for the rule.
- The minimum versions of the Agent and the Deep Security Manager that are required for the rule to function.

Although you cannot edit rules issued by Trend Micro directly, you can duplicate them and then edit the copy.

## Configure rule events and alerts

Any changes detected by an integrity monitoring rule is logged as an event in the Deep Security Manager.

### Real-time event monitoring

By default, events are logged at the time they occur. If you only want events to be logged when you manually perform a scan for changes, deselect **Allow Real Time Monitoring**.

### Alerts

You can also configure the rules to trigger an alert when they log an event. To do so, open the properties for a rule, click on **Options**, and then select **Alert when this rule logs an event**.

### See policies and computers a rule is assigned to

You can see which policies and computers are assigned to an integrity monitoring rule on the **Assigned To** tab. Click on a policy or computer in the list to see their properties.

### Export a rule

You can export all integrity monitoring rules to a .csv or .xml file by clicking **Export** and selecting the corresponding export action from the list. You can also export specific rules by first selecting them, clicking **Export** and then selecting the corresponding export action from the list.

### Delete a rule

To delete a rule, right-click the rule in the Integrity Monitoring Rules list, click **Delete** and then click **OK**.

> **Note:** Integrity monitoring rules that are assigned to one or more computers or that are part of a policy cannot be deleted.

## Define a log inspection rule for use in policies

The OSSEC log inspection engine is integrated into Deep Security Agents and gives Deep Security the ability to inspect the logs and events generated by the operating system and applications running on the computer. Deep Security Manager ships with a standard set of OSSEC log inspection rules that you can assign to computers or policies. You can also create custom rules if there is no existing rule that fits your requirements.

Log Inspection Rules issued by Trend Micro are not editable (although you can duplicate them and then edit them.)

**Note:** Log Inspection Rules that are assigned to one or more computers or that are part of a policy cannot be deleted.

To create log inspection rules, perform these basic steps:

- "Create a new log inspection rule" below
- "Decoders" on page 413
- "Subrules" on page 414
- "Real world examples" on page 422
- "Log inspection rule severity levels and their recommended use" on page 431
- "strftime() conversion specifiers " on page 432
- "Examine a log inspection rule" on page 433

For an overview of the log inspection module, see "Analyze logs with log inspection" on page 691.

## Create a new log inspection rule

1. In the Deep Security Manager, go to **Policies** > **Common Objects** > **Rules** > **Log Inspection Rules**.
2. Click **New** > **New Log Inspection Rule**.
3. On the **General** tab, enter a name and an optional description for the rule.
4. The **Content** tab is where you define the rule. The easiest way to define a rule is to select **Basic Rule** and use the options provided to define the rule. If you need further customization, you can select **Custom (XML)** to switch to an XML view of the rule that you are defining.

   **Note:** Any changes you make in the Custom (XML) view will be lost if you switch back to the Basic Rule view.

   For further assistance in writing your own log inspection rules using the XML-based language, consult the OSSEC documentation or contact your support provider.

These options are available for the Basic Rule template:

- **Rule ID:** The Rule ID is a unique identifier for the rule. OSSEC defines 100000 - 109999 as the space for user-defined rules. Deep Security Manager will pre-populate the field with a new unique Rule ID.
- **Level:** Assign a level to the rule. Zero (0) means the rule never logs an event, although other rules that watch for this rule may fire.
- **Groups:** Assign the rule to one or more comma-separated groups. This can be useful when dependency is used because you can create rules that fire on the firing of a rule, or a rule that belongs to a specific group.
- **Rule Description:** Description of the rule.
- **Pattern Matching:** This is the pattern the rule will look for in the logs. The rule will be triggered on a match. Pattern matching supports Regular Expressions or simpler String Patterns. The "String Pattern" pattern type is faster than RegEx but it only supports three special operations:
  - **^ (caret)**: specifies the beginning of text
  - **$ (dollar sign)**: specifies the end of text
  - **| (pipe)**: to create a "OR" between multiple patterns

  For information on the regular expression syntax used by the Log Inspection module, see https://www.ossec.net/docs/syntax/regex.html.
- **Dependency:** Setting a dependency on another rule will cause your rule to only log an event if the rule specified in this area has also triggered.
- **Frequency** is the number of times the rule has to match within a specific time frame before the rule is triggered.
- **Time Frame** is the period of time in seconds within which the rule has to trigger a certain number of times (the frequency, above) to log an event.

Note: The **Content** tab only appears for log inspection rules that you create yourself. Log inspection rules issued by Trend Micro have a **Configuration** tab instead that displays the log inspection rule's configuration options (if any).

1. On the **Files** tab, type the full path to the file(s) you want your rule to monitor and specify the type of file it is.
2. On the **Options** tab, in the **Alert** section, select whether this rule triggers an alert in the Deep Security Manager.

   The **Alert Minimum Severity** setting is only used if you have written "multiple rules" within your rule - something that cannot be done using the Basic template. However, if after creating your rule using the Basic template, you edit the XML of the rule and add additional rules to the XML that have different severity levels, you can use the **Alert Minimum Severity Level** setting to set the minimum severity from the multiple rules that will trigger an Alert.

3. The **Assigned To** tab lists the policies and computers that are using this log inspection rule. Because you are creating a new rule, it has not been assigned yet.
4. Click **OK**. The rule is ready to be assigned to policies and computers.

## Decoders

A log inspection rule consists of a list of files to monitor for changes and a set of conditions to be met for the rule to trigger. When the log inspection engine detects a change in a monitored log file, the change is parsed by a decoder. Decoders parse the raw log entry into the following fields:

- **log:** the message section of the event
- **full_log:** the entire event
- **location:** where the log came from
- **hostname:** hostname of the vent source
- **program_name:** Program name. This is taken from the syslog header of the event
- **srcip:** the source IP address within the event
- **dstip:** the destination IP address within the event
- **srcport:** the source port number within the event
- **dstport:** the destination port number within the event
- **protocol:** the protocol within the event
- **action:** the action taken within the event

- **srcuser:** the originating user within the event
- **dstuser:** the destination user within the event
- **id:** any ID decoded as the ID from the event
- **status:** the decoded status within the event
- **command:** the command being called within the event
- **url:** the URL within the event
- **data:** any additional data extracted from the event
- **systemname:** the system name within the event

Rules examine this decoded data looking for information that matches the conditions defined in the rule.

If the matches are at a sufficiently high severity level, any of the following actions can be taken:

- An alert can be raised. (Configurable on the **Options** tab of the Log Inspection Rule's **Properties** window.)
- The event can be written to syslog. (Configurable in the **SIEM** area on **Administration > System Settings > Event Forwarding** tab.)
- The event can be sent to the Deep Security Manager. (Configurable in the **Log Inspection Syslog Configuration** setting on the **Policy or Computer Editor > Settings > Event Forwarding** tab.)

## Subrules

A single log inspection rule can contain multiple subrules. These subrules can be of two types: atomic or composite. An atomic rule evaluates a single event and a composite rule examines multiple events and can evaluate frequency, repetition, and correlation between events.

### Groups

Each rule, or grouping of rules, must be defined within a **<group></group>** element. The attribute name must contain the rules you want to be a part of this group. In the following example we have indicated that our group contains the syslog and sshd rules:

```
<group name="syslog,sshd,">
</group>
```

**Note:** Notice the trailing comma in the group name. Trailing commas are required if you intend to use the **<if_group></if_group>** tag to conditionally append another sub-rule to this one.

**Note:** When a set of log inspection rules are sent to an agent, the log inspection engine on the agent takes the XML data from each assigned rule and assembles it into what becomes essentially a single long log inspection rule. Some group definitions are common to all log inspection rules written by Trend Micro. For this reason Trend Micro has included a rule called "Default Rules Configuration" which defines these groups and which always gets assigned along with any other Trend Micro rules. (If you select a rule for assignment and haven't also selected the "Default Rules Configuration" rule, a notice will appear informing you that the rule will be assigned automatically.) *If you create your own log inspection rule and assign it to a Computer without assigning any Trend Micro-written rules, you must either copy the content of the "Default Rules Configuration" rule into your new rule, or also select the "Default Rules Configuration" rule for assignment to the Computer.*

### Rules, ID, and Level

A group can contain as many rules as you require. The rules are defined using the **<rule></rule>** element and must have at least two attributes, the **id** and the **level**. The **id** is a unique identifier for that signature and the **level** is the severity of the alert. In the following example, we have created two rules, each with a different rule ID and level:

```
<group name="syslog,sshd,">
       <rule id="100120" level="5">
       </rule>
       <rule id="100121" level="6">
       </rule>
</group>
```

**Note:** Custom rules must have ID values of 100,000 or greater.

You can define additional subgroups within the parent group using the **<group></group>** tag. This subgroup can reference any of the groups listed in the following table:

| Group Type | Group Name | Description |
|---|---|---|
| Reconnaissance | connection_attempt<br>web_scan<br>recon | Connection attempt<br>Web scan<br>Generic scan |

| Group Type | Group Name | Description |
|---|---|---|
| Authentication Control | authentication_success<br>authentication_failed<br>invalid_login<br>login_denied<br>authentication_failures<br>adduser<br>account_changed | Success<br>Failure<br>Invalid<br>Login Denied<br>Multiple Failures<br>User account added<br>User Account changed or removed |
| Attack/Misuse | automatic_attack<br>exploit_attempt<br>invalid_access<br>spam<br>multiple_spam<br>sql_injection<br>attack<br>virus | Worm (nontargeted attack)<br>Exploit pattern<br>Invalid access<br>Spam<br>Multiple spam messages<br>SQL injection<br>Generic attack<br>Virus detected |
| Access Control | access_denied<br>access_allowed<br>unknown_resource<br>firewall_drop<br>multiple_drops<br>client_misconfig<br>client_error | Access denied<br>Access allowed<br>Access to nonexistent resource<br>Firewall drop<br>Multiple firewall drops<br>Client misconfiguration<br>Client error |
| Network Control | new_host<br>ip_spoof | New host detected<br>Possible ARP spoofing |
| System Monitor | service_start<br>system_error<br>system_shutdown<br>logs_cleared<br>invalid_request<br>promisc<br>policy_changed<br>config_changed<br>low_diskspace<br>time_changed | Service start<br>System error<br>Shutdown<br>Logs cleared<br>Invalid request<br>Interface switched to promiscuous mode<br>Policy changed<br>Configuration changed<br>Low disk space<br>Time changed |

**Note:** If event auto-tagging is enabled, the event will be labeled with the group name. Log inspection rules provided by Trend Micro make use of a translation table that changes the group to a more user-friendly version. So, for example, "login_denied" would appear as "Login Denied". Custom rules will be listed by their group name as it appears in the rule.

## Description

Include a **<description></description>** tag. The description text will appear in the event if the rule is triggered.

```
<group name="syslog,sshd,">
       <rule id="100120" level="5">
               <group>authentication_success</group>
               <description>SSHD testing authentication success</description>
       </rule>
       <rule id="100121" level="6">
               <description>SSHD rule testing 2</description>
       </rule>
</group>
```

### Decoded As

The **<decoded_as></decoded_as>** tag instructs the log inspection engine to only apply the rule if the specified decoder has decoded the log.

```
<rule id="100123" level="5">
       <decoded_as>sshd</decoded_as>
       <description>Logging every decoded sshd message</description>
</rule>
```

**Note:** To view the available decoders, go to the **Log Inspection Rule** page and click **Decoders.** Right-click on **1002791-Default Log Decoders** and select **Properties**. Go the **Configuration** tab and click **View Decoders**.

### Match

To look for a specific string in a log, use the **<match></match>**. Here is a Linux sshd failed password log:

```
 Jan 1 12:34:56 linux_server sshd[1231]: Failed password for invalid
       user jsmith from 192.168.1.123 port 1799 ssh2
```

Use the **<match></match>** tag to search for the "password failed" string.

```
<rule id="100124" level="5">
       <decoded_as>sshd</decoded_as>
       <match>^Failed password</match>
       <description>Failed SSHD password attempt</description>
</rule>
```

**Note:** Notice the regex caret ("^") indicating the beginning of a string. Although "Failed password" does not appear at the beginning of the log, the log inspection decoder will have broken up the log into sections. See "Decoders" on page 413 for more information. One of those sections is "log" which is the message part of the log as opposed to "full_log" which is the log in its entirety.

The following table lists supported regex syntax:

| Regex Syntax | Description |
|---|---|
| \w | A-Z, a-z, 0-9 single letters and numerals |
| \d | 0-9 single numerals |
| \s | single space |
| \t | single tab |
| \p | ()*+,-.:;<=>?[] |
| \W | not \w |
| \D | not \d |
| \S | not \s |
| \. | anything |
| + | match one or more of any of the above (for example, \w+, \d+) |
| * | match zero or more of any of the above (for example, \w*, \d*) |
| ^ | indicates the beginning of a string (^somestring) |
| $ | specify the end of a string (somestring$) |
| \| | indicate an "OR" between multiple strings |

## Conditional Statements

Rule evaluation can be conditional upon other rules having been evaluated as true. The **<if_sid></if_sid>** tag instructs the log inspection engine to only evaluate this subrule if the rule identified in the tag has been evaluated as true. The following example shows three rules: 100123, 100124, and 100125. Rules 100124 and 100125 have been modified to be children of the 100123 rule using the **<if_sid></if_sid>** tag:

```
<group name="syslog,sshd,">
       <rule id="100123" level="2">
               <decoded_as>sshd</decoded_as>
               <description>Logging every decoded sshd message</description>
       </rule>
       <rule id="100124" level="7">
               <if_sid>100123</if_sid>
               <match>^Failed password</match>
```

```
                <group>authentication_failure</group>
                <description>Failed SSHD password attempt</description>
        </rule>
        <rule id="100125" level="3">
                <if_sid>100123</if_sid>
                <match>^Accepted password</match>
                <group>authentication_success</group>
                <description>Successful SSHD password attempt</description>
        </rule>
</group>
```

## Hierarchy of Evaluation

The **<if_sid></if_sid>** tag essentially creates a hierarchical set of rules. That is, by including an **<if_sid></if_sid>** tag in a rule, the rule becomes a child of the rule referenced by the **<if_sid></if_sid>** tag. Before applying any rules to a log, the log inspection engine assesses the **<if_sid></if_sid>** tags and builds a hierarchy of parent and child rules.

**Note:** The hierarchical parent-child structure can be used to improve the efficiency of your rules. If a parent rule does not evaluate as true, the log inspection engine will ignore the children of that parent.

**Note:** Although the **<if_sid></if_sid>** tag can be used to refer to subrules within an entirely different log inspection rule, you should avoid doing this because it makes the rule very difficult to review later on.

The list of available atomic rule conditional options is shown in the following table:

| Tag | Description | Notes |
|---|---|---|
| match | A pattern | Any string to match against the event (log). |
| regex | A regular expression | Any regular expression to match against the event(log). |
| decoded_as | A string | Any prematched string. |
| srcip | A source IP address | Any IP address that is decoded as the source IP address. Use "!" to negate the IP address. |
| dstip | A destination IP address | Any IP address that is decoded as the destination IP address. Use "!" to negate the IP address. |
| srcport | A source port number | Any source port (match format). |
| dstport | A destination port number | Any destination port (match format). |
| user | A username | Any username that is decoded as a username. |
| program_ | A program name | Any program name that is decoded from the syslog process name. |

| Tag | Description | Notes |
|---|---|---|
| name | | |
| hostname | A system hostname | Any hostname that is decoded as a syslog hostname. |
| time | A time range in the format hh:mm - hh:mm or hh:mm am - hh:mm pm | The time range that the event must fall within for the rule to trigger. |
| weekday | A weekday (sunday, monday, tuesday, etc.) | Day of the week that the event must fall on for the rule to trigger. |
| id | An ID | Any ID that is decoded from the event. |
| url | A URL | Any URL that is decoded from the event. |

Use the **<if_sid>100125</if_sid>** tag to make this rule depend on the 100125 rule. This rule will be checked only for sshd messages that already matched the successful login rule.

```
<rule id="100127" level="10">
       <if_sid>100125</if_sid>
       <time>6 pm - 8:30 am</time>
       <description>Login outside business hours.</description>
       <group>policy_violation</group>
</rule>
```

## Restrictions on the Size of the Log Entry

The following example takes the previous example and adds the **maxsize** attribute which tells the log inspection engine to only evaluate rules that are less than the maxsize number of characters:

```
<rule id="100127" level="10" maxsize="2000">
       <if_sid>100125</if_sid>
       <time>6 pm - 8:30 am</time>
       <description>Login outside business hours.</description>
       <group>policy_violation</group>
</rule>
```

The following table lists possible atomic rule tree-based options:

| Tag | Description | Notes |
|---|---|---|
| if_sid | A rule ID | Adds this rule as a child rule of the rules that match the specified signature ID. |
| if_group | A group ID | Adds this rule as a child rule of the rules that match the specified group. |
| if_level | A rule level | Adds this rule as a child rule of the rules that match the specified severity level. |
| description | A string | A description of the rule. |
| info | A string | Extra information about the rule. |

| Tag | Description | Notes |
|---|---|---|
| cve | A CVE number | Any Common Vulnerabilities and Exposures (CVE) number that you would like associated with the rule. |
| options | alert_by_email<br>no_email_alert<br>no_log | Additional rule options to indicate if the Alert should generate an e-mail, alert_by_email, should not generate an email, no_email_alert, or should not log anything at all, no_log. |

## Composite Rules

Atomic rules examine single log entries. To correlate multiple entries, you must use composite rules. Composite rules are supposed to match the current log with those already received. Composite rules require two additional options: the **frequency** option specifies how many times an event or pattern must occur before the rule generates an alert, and the **timeframe** option tells the log inspection engine how far back, in seconds, it should look for previous logs. All composite rules have the following structure:

```
<rule id="100130" level="10" frequency="x" timeframe="y">
</rule>
```

For example, you could create a composite rule that creates a higher severity alert after five failed passwords within a period of 10 minutes. Using the **<if_matched_sid></if_matched_sid>** tag you can indicate which rule needs to be seen within the desired frequency and timeframe for your new rule to create an alert. In the following example, the **frequency** attribute is set to trigger when five instances of the event are seen and the **timeframe** attribute is set to specify the time window as 600 seconds.

The **<if_matched_sid></if_matched_sid>** tag is used to define which other rule the composite rule will watch:

```
<rule id="100130" level="10" frequency="5" timeframe="600">
       <if_matched_sid>100124</if_matched_sid>
       <description>5 Failed passwords within 10 minutes</description>
</rule>
```

There are several additional tags that you can use to create more granular composite rules. These rules, as shown in the following table, allow you to specify that certain parts of the event must be the same. This allows you to tune your composite rules and reduce false positives:

| Tag | Description |
|---|---|
| same_source_ip | Specifies that the source IP address must be the same. |
| same_dest_ip | Specifies that the destination IP address must be the same. |
| same_dst_port | Specifies that the destination port must be the same. |
| same_location | Specifies that the location (hostname or agent name) must be the same. |
| same_user | Specifies that the decoded username must be the same. |
| same_id | Specifies that the decoded id must be the same. |

If you wanted your composite rule to alert on every authentication failure, instead of a specific rule ID, you could replace the **<if_matched_sid></if_matched_sid>** tag with the **<if_matched_ group></if_matched_ group>** tag. This allows you to specify a category, such as **authentication_ failure**, to search for authentication failures across your entire infrastructure.

```
<rule id="100130" level="10" frequency="5" timeframe="600">
       <if_matched_group>authentication_failure</if_matched_group>
       <same_source_ip />
       <description>5 Failed passwords within 10 minutes</description>
</rule>
```

In addition to **<if_matched_sid></if_matched_sid>** and **<if_matched_group></if_matched_ group>** tags, you can also use the **<if_matched_regex></if_matched_regex>** tag to specify a regular expression to search through logs as they are received.

```
<rule id="100130" level="10" frequency="5" timeframe="600">
       <if_matched_regex>^Failed password</if_matched_regex>
       <same_source_ip />
       <description>5 Failed passwords within 10 minutes</description>
</rule>
```

## Real world examples

Deep Security includes many default log inspection rules for dozens of common and popular applications. Through Security Updates, new rules are added regularly. In spite of the growing list of applications supported by log inspection rules, you may find the need to create a custom rule for an unsupported or custom application.

In this section we will walk through the creation of a custom CMS (Content Management System) hosted on the Microsoft Windows Server IIS .Net platform with a Microsoft SQL Database as the data repository.

The first step is to identify the following application logging attributes:

1. Where does the application log to?
2. Which log inspection decoder can be used to decode the log file?
3. What is the general format of a log file message?

For our custom CMS example the answers are as follows:

1. Windows Event Viewer
2. Windows Event Log (eventlog)
3. Windows Event Log Format with the following core attributes:
    - Source: CMS
    - Category: None
    - Event: <Application Event ID>

The second step is to identify the categories of log events by application feature, and then organize the categories into a hierarchy of cascading groups for inspection. Not all inspected groups need to raise events; a match can be used as a conditional statement. For each group, identify the log format attributes which the rule can use as matching criteria. This can also be performed by inspecting all application logs for patterns and logical groupings of log events.

For example, the CMS application supports the following functional features which we will create log inspection rules for:

- CMS Application Log (Source: CMS)
    - Authentication (Event: 100 to 119)
        - User Login successful (Event: 100)
        - User Login unsuccessful (Event: 101)
        - Administrator Login successful (Event: 105)
        - Administrator Login unsuccessful (Event: 106)
    - General Errors (Type: Error)
        - Database error (Event: 200 to 205)
        - Runtime error (Event: 206-249)

- Application Audit (Type: Information)
  - Content
    - New content added (Event: 450 to 459)
    - Existing content modified (Event: 460 to 469)
    - Existing content deleted (Event: 470 to 479)
  - Administration
    - User
      - New User created (Event: 445 to 446)
      - Existing User deleted (Event: 447 to 449)

This structure will provide you with a good basis for rule creation. Now to create a new log inspection rule in Deep Security Manager.

**To create the new CMS Log Inspection Rule:**

1. In the Deep Security Manager, go to **Policies > Common Objects > Rules > Log Inspection Rules** and click **New** to display the **New Log Inspection Rule Properties** window.
2. Give the new rule a name and a description, and then click the **Content** tab.
3. The quickest way to create a new custom rule is to start with a basic rule template. Select the **Basic Rule** radio button.
4. The **Rule ID** field will be automatically populated with an unused ID number of 100,000 or greater, the IDs reserved for custom rules.
5. Set the **Level** setting to **Low (0)**.
6. Give the rule an appropriate Group name. In this case, "cms".

7. Provide a short rule description.

General | Content | Files | Options | Assigned To

**Template**

- (•) Basic Rule
- ( ) Custom (XML)

**General Information**

| | |
|---|---|
| Rule ID: | 100000 |
| Level: | Low (0) |
| Groups (comma separated): | cms |
| Rule Description: | windows events for 'cms' group |

**Pattern Matching**

| | |
|---|---|
| Pattern to Match: | |
| Pattern Type: | String Pattern |

**Dependency**

- (•) None
- ( ) Trigger event on the triggering of another rule:
- ( ) Trigger event on the triggering of any rule belonging to a specific group:

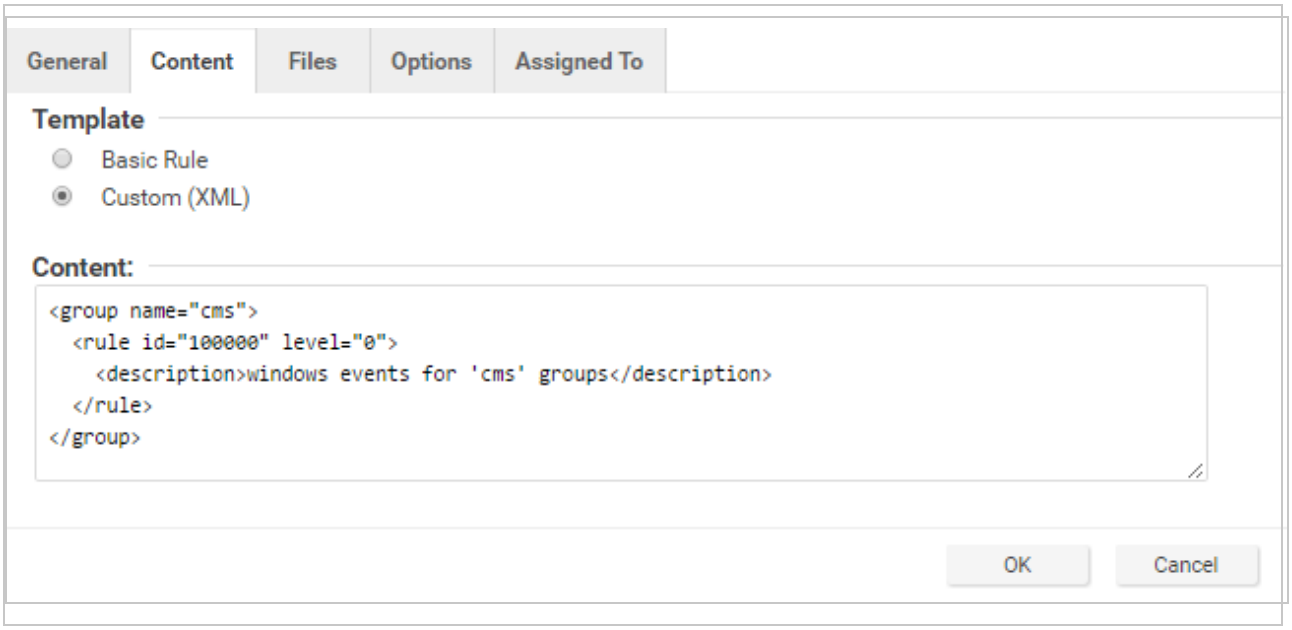
**Composite (optional)**

Only trigger if this rule matches its dependent rule the specified frequency of times in the specified time frame (in seconds).

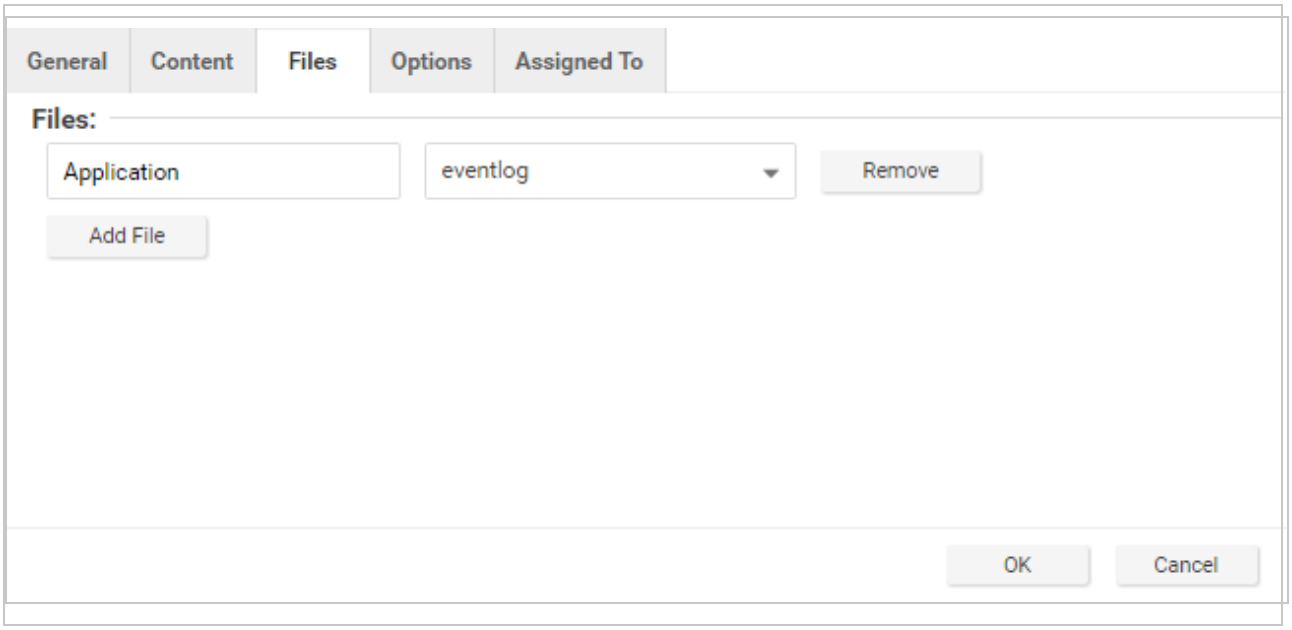
| | |
|---|---|
| Frequency (1 to 128): | |
| Time Frame (1 to 86400): | |

OK | Cancel

8. Now select the **Custom (XML)** option. The options you selected for your "Basic" rule will be converted to XML.




9. Click the **Files** tab and click the **Add File** button to add any application log files and log types which the rule will be applied to. In this case, "Application", and "eventlog" as the file type.




**Note:** **Eventlog** is a unique file type in Deep Security because the location and filename of the log files don't have to be specified. Instead, it is sufficient to type the log name as it

is displayed in the Windows Event Viewer. Other log names for the eventlog file type might be "Security", "System", "Internet Explorer", or any other section listed in the Windows Event Viewer. Other file types will require the log file's location and filename. (*C/C++ strftime()* conversion specifiers are available for matching on filenames. See the table below for a list of some of the more useful ones.)

10. Click **OK** to save the basic rule.
11. Working with the basic rule Custom (XML) created, we can begin adding new rules to the group based on the log groupings identified previously. We will set the base rule criteria to the initial rule. In the following example, the CMS base rule has identified Windows Event Logs with a Source attribute of "CMS":

```
<group name="cms">
       <rule id="100000" level="0">
               <category>windows</category>
               <extra_data>^CMS</extra_data>
               <description>Windows events from source 'CMS' group messages.</descriptio
       </rule>
```

12. Now we build up subsequent rules from the identified log groups. The following example identifies the authentication and login success and failure and logs by Event IDs.

```
<rule id="100001" level="0">
       <if_sid>100000</if_sid>
       <id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id>
       <group>authentication</group>
       <description>CMS Authentication event.</description>
</rule>

<rule id="100002" level="0">
       <if_group>authentication</if_group>
       <id>100</id>
       <description>CMS User Login success event.</description>
</rule>
<rule id="100003" level="4">
       <if_group>authentication</if_group>
       <id>101</id>
       <group>authentication_failure</group>
       <description>CMS User Login failure event.</description>
```

```
</rule>
<rule id="100004" level="0">
       <if_group>authentication</if_group>
       <id>105</id>
       <description>CMS Administrator Login success event.</description>
</rule>
<rule id="100005" level="4">
       <if_group>authentication</if_group>
       <id>106</id>
       <group>authentication_failure</group>
       <description>CMS Administrator Login failure event.</description>
</rule>
```

13. Now we add any composite or correlation rules using the established rules. The follow example shows a high severity composite rule that is applied to instances where the repeated login failures have occurred 5 times within a 10 second time period:

```
<rule id="100006" level="10" frequency="5" timeframe="10">
       <if_matched_group>authentication_failure</if_matched_group>
       <description>CMS Repeated Authentication Login failure event.</description>
</rule>
```

14. Review all rules for appropriate severity levels. For example, error logs should have a severity of level 5 or higher. Informational rules would have a lower severity.
15. Finally, open the newly created rule, click the **Configuration** tab and copy your custom rule XML into the rule field. Click **Apply** or **OK** to save the change.

Once the rule is assigned to a policy or computer, the log inspection engine should begin inspecting the designated log file immediately.

**The complete Custom CMS Log Inspection Rule:**

```
<group name="cms">
        <rule id="100000" level="0">
               <category>windows</category>
               <extra_data>^CMS</extra_data>
               <description>Windows events from source 'CMS' group messages.</description>
       </rule>
        <rule id="100001" level="0">
               <if_sid>100000</if_sid>
               <id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id>
```

```
        <group>authentication</group>
        <description>CMS Authentication event.</description>
</rule>

<rule id="100002" level="0">
        <if_group>authentication</if_group>
        <id>100</id>
        <description>CMS User Login success event.</description>
</rule>

<rule id="100003" level="4">
        <if_group>authentication</if_group>
        <id>101</id>
        <group>authentication_failure</group>
        <description>CMS User Login failure event.</description>
</rule>

<rule id="100004" level="0">
        <if_group>authentication</if_group>
        <id>105</id>
        <description>CMS Administrator Login success event.</description>
</rule>

<rule id="100005" level="4">
        <if_group>authentication</if_group>
        <id>106</id>
        <group>authentication_failure</group>
        <description>CMS Administrator Login failure event.</description>
</rule>

<rule id="100006" level="10" frequency="5" timeframe="10">
        <if_matched_group>authentication_failure</if_matched_group>
        <description>CMS Repeated Authentication Login failure event.</description>
</rule>

<rule id="100007" level="5">
        <if_sid>100000</if_sid>
        <status>^ERROR</status>
        <description>CMS General error event.</description>
        <group>cms_error</group>
```

```
        </rule>

        <rule id="100008" level="10">
                <if_group>cms_error</if_group>
                <id>^200|^201|^202|^203|^204|^205</id>
                <description>CMS Database error event.</description>
        </rule>

        <rule id="100009" level="10">
                <if_group>cms_error</if_group>
                <id>^206|^207|^208|^209|^230|^231|^232|^233|^234|^235|^236|^237|^238|
                        ^239^|240|^241|^242|^243|^244|^245|^246|^247|^248|^249</id>
                <description>CMS Runtime error event.</description>
        </rule>

        <rule id="100010" level="0">
                <if_sid>100000</if_sid>
                <status>^INFORMATION</status>
                <description>CMS General informational event.</description>
                <group>cms_information</group>
        </rule>

        <rule id="100011" level="5">
                <if_group>cms_information</if_group>
                <id>^450|^451|^452|^453|^454|^455|^456|^457|^458|^459</id>
                <description>CMS New Content added event.</description>
        </rule>

        <rule id="100012" level="5">
                <if_group>cms_information</if_group>
                <id>^460|^461|^462|^463|^464|^465|^466|^467|^468|^469</id>
                <description>CMS Existing Content modified event.</description>
        </rule>

        <rule id="100013" level="5">
                <if_group>cms_information</if_group>
                <id>^470|^471|^472|^473|^474|^475|^476|^477|^478|^479</id>
                <description>CMS Existing Content deleted event.</description>
        </rule>
```

```
        <rule id="100014" level="5">
                <if_group>cms_information</if_group>
                <id>^445|^446</id>
                <description>CMS User created event.</description>
        </rule>

        <rule id="100015" level="5">
                <if_group>cms_information</if_group>
                <id>^447|449</id>
                <description>CMS User deleted event.</description>
        </rule>

</group>
```

## Log inspection rule severity levels and their recommended use

| Level | Description | Notes |
|---|---|---|
| Level 0 | Ignored, no action taken | Primarily used to avoid false positives. These rules are scanned before all the others and include events with no security relevance. |
| Level 1 | no predefined use | |
| Level 2 | System low priority notification | System notification or status messages that have no security relevance. |
| Level 3 | Successful or authorized events | Successful login attempts, firewall allow events, etc. |
| Level 4 | System low priority errors | Errors related to bad configurations or unused devices or applications. They have no security relevance and are usually caused by default installations or software testing. |
| Level 5 | User-generated errors | Missed passwords, denied actions, etc. These messages typically have no security relevance. |
| Level 6 | Low relevance attacks | Indicate a worm or a virus that provide no threat to the system such as a Windows worm attacking a Linux server. They also include frequently triggered IDS events and common error events. |
| Level 7 | no predefined use | |
| Level 8 | no predefined use | |
| Level 9 | Error from invalid source | Include attempts to login as an unknown user or from an invalid source. The message might have security relevance especially if repeated. They also include errors regarding the **admin** or **root** account. |
| Level 10 | Multiple user generated errors | Include multiple bad passwords, multiple failed logins, etc. They might indicate an attack, or it might be just that a user forgot his or her credentials. |

| Level | Description | Notes |
|---|---|---|
| Level 11 | no predefined use | |
| Level 12 | High-importance event | Include error or warning messages from the system, kernel, etc. They might indicate an attack against a specific application. |
| Level 13 | Unusual error (high importance) | Common attack patterns such as a buffer overflow attempt, a larger than normal syslog message, or a larger than normal URL string. |
| Level 14 | High importance security event | Typically the result of the correlation of multiple attack rules and indicative of an attack. |
| Level 15 | Attack Successful | Very small chance of false positive. Immediate attention is necessary. |

## *strftime()* conversion specifiers

| Specifier | Description |
|---|---|
| %a | Abbreviated weekday name (e.g., Thu) |
| %A | Full weekday name (e.g., Thursday) |
| %b | Abbreviated month name (e.g., Aug) |
| %B | Full month name (e.g., August) |
| %c | Date and time representation (e.g., Thu Sep 22 12:23:45 2007) |
| %d | Day of the month (01 - 31) (e.g., 20) |
| %H | Hour in 24 h format (00 - 23) (e.g., 13) |
| %I | Hour in 12 h format (01 - 12) (e.g., 02) |
| %j | Day of the year (001 - 366) (e.g., 235) |
| %m | Month as a decimal number (01 - 12) (e.g., 02) |
| %M | Minute (00 - 59) (e.g., 12) |
| %p | AM or PM designation (e.g., AM) |
| %S | Second (00 - 61) (e.g., 55) |
| %U | Week number with the first Sunday as the first day of week one (00 - 53) (e.g., 52) |
| %w | Weekday as a decimal number with Sunday as 0 (0 - 6) (e.g., 2) |
| %W | Week number with the first Monday as the first day of week one (00 - 53) (e.g., 21) |
| %x | Date representation (e.g., 02/24/79) |
| %X | Time representation (e.g., 04:12:51) |
| %y | Year, last two digits (00 - 99) (e.g., 76) |
| %Y | Year (e.g., 2008) |
| %Z | Time zone name or abbreviation (e.g., EST) |
| %% | A % sign (e.g., %) |

More information can be found at the following websites:

https://secure.php.net/manual/en/function.strftime.php

www.cplusplus.com/reference/clibrary/ctime/strftime.html

## Examine a log inspection rule

Log inspection rules are found in the Deep Security Manager at **Policies > Common Objects > Rules > Log Inspection Rules**.

### Log inspection rule structure and the event matching process

This screen shot displays the contents of the **Configuration** tab of the Properties window of the "Microsoft Exchange" log inspection rule:

General | Configuration | Options | Assigned To

Configuration Options

Log Files to monitor:

Add

C:\Windows\system32\LogFiles\SMTPSVC1\ex%y%m%d.l

Remove

Type of Log File(s): syslog

This rule matches events decoded as: msexchange

3800 - Grouping of Exchange rules — Default - Ignore

3801 - E-mail RCPT is not valid (invalid account) — Default - Medium (5)

3851 - Multiple e-mail attempts to an invalid account — Default - High (10)

Frequency (1 to 128): 10

Time Frame (1 to 86400): 120 secs

Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400): 120 secs

3802 - E-mail 500 error code — Default - Medium (4)

3852 - Multiple e-mail 500 error code (spam) — Default - High (9)

Frequency (1 to 128): 12

Time Frame (1 to 86400): 120 secs

Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400): 240 secs

View Rules...

OK | Cancel | Apply

Here is the structure of the rule:

- 3800 - Grouping of Exchange Rules - Ignore
  - 3801 - Email rcpt is not valid (invalid account) - Medium (4)
    - 3851 - Multiple email attempts to an invalid account - High (9)
      - Frequency - 10
      - Time Frame - 120
      - Ignore - 120
  - 3802 - Email 500 error code - Medium (4)
    - 3852 - Email 500 error code (spam) - High (9)
      - Frequency - 12
      - Time Frame - 120
      - Ignore - 240

The log inspection engine will apply log events to this structure and see if a match occurs. For example, if an Exchange event occurs, and this event is an email receipt to an invalid account, the event will match line 3800 (because it is an Exchange event). The event will then be applied to line 3800's sub-rules: 3801 and 3802.

If there is no further match, this "cascade" of matches will stop at 3800. Because 3800 has a severity level of "Ignore", no log inspection event would be recorded.

However, an email receipt to an invalid account does match one of 3800's sub-rules: sub-rule 3801. Sub-rule 3801 has a severity level of "Medium(4)". If the matching stopped here, a log inspection event with a severity level of "Medium(4)" would be recorded.

But there is still another sub-rule to be applied to the event: sub-rule 3851. Sub-rule 3851 with its three attributes will match if the same event has occurred 10 times within the last 120 seconds. If so, a log inspection event with a severity "High(9)" is recorded. (The "Ignore" attribute tells sub-rule 3851 to ignore individual events that match sub-rule 3801 for the next 120 seconds. This is useful for reducing "noise".)

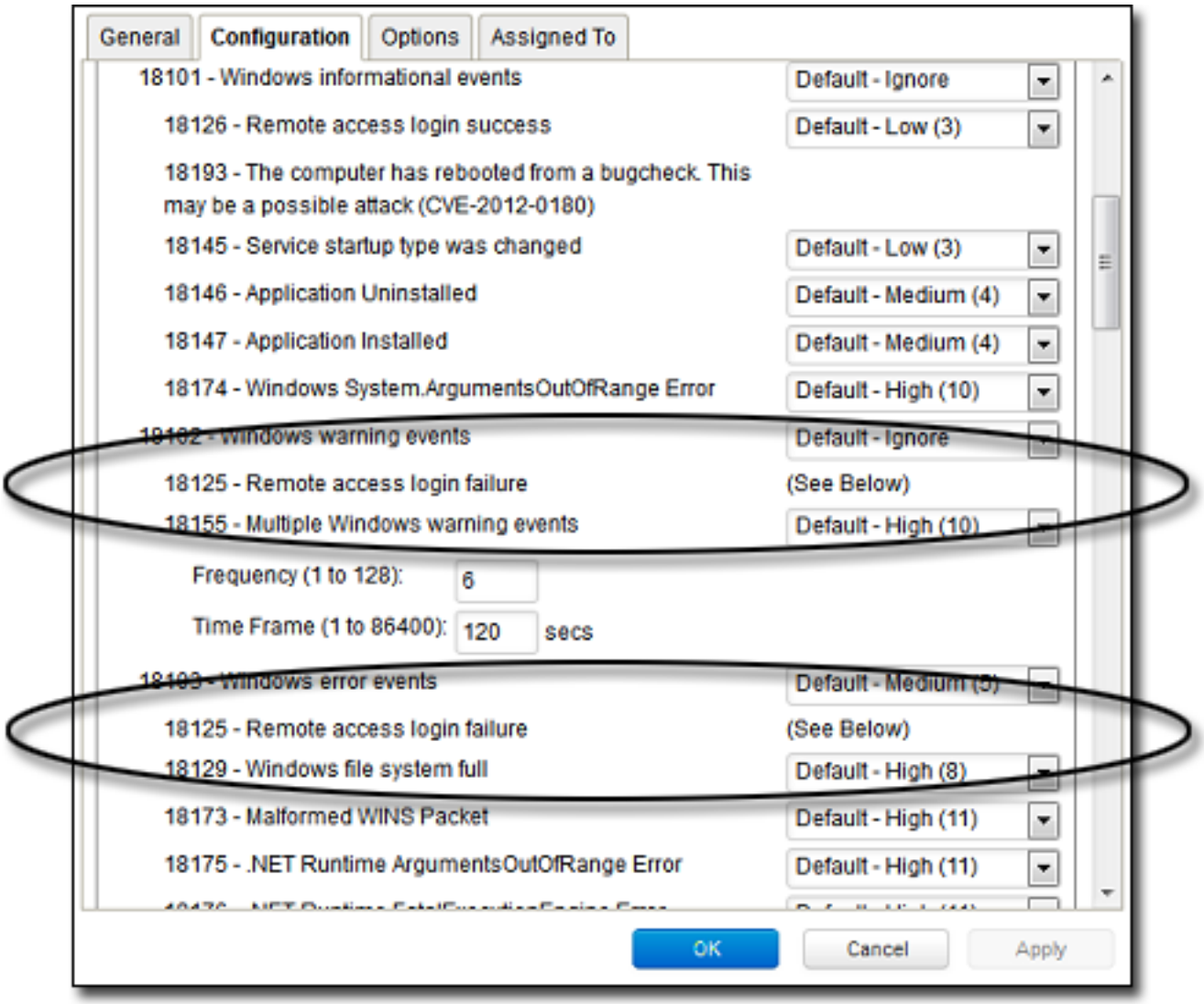
Assuming the parameters of sub-rule 3851 have been matched, a log inspection event with Severity "High(9)" is now recorded.

Looking at the Options tab of the Microsoft Exchange Rule, we see that Deep Security Manager will raise an alert if any sub-rules with a severity level of "Medium(4)" have been matched. Since this is the case in our example, the alert will be raised (if "Alert when this rule logs an event" is selected).

## Duplicate Sub-rules

Some log inspection rules have duplicate sub-rules. To see an example, open the "Microsoft Windows Events" rule and click on the **Configuration** tab. Note that sub-rule 18125 (Remote access login failure) appears under sub-rules 18102 and 18103. Also note that in both cases sub-rule 18125 does not have a severity value, it only says "See Below".

Instead of being listed twice, Rule 18125 is listed once at the bottom of the **Configuration** page:




## Create a list of directories for use in policies

Create lists of directory paths so that you can use them in multiple policies. A single list is easier to manage than several identical lists that are each created in a different policy.

**Tip:** To create a directory list that is similar to an existing one, duplicate the list and then edit it.

The following table describes the syntax for defining directory list items. The use of forward slashes "/" and backslashes "\" are supported for both Windows and Linux conventions:

| Directory | Format | Description | Examples |
|---|---|---|---|
| Directory | DIRECTORY | Includes all files in the specified directory and all files in all subdirectories. | ***C:\Program Files*** Includes all files in the "Program Files" directory and all subdirectories. |
| Network Resource | \\NETWORK RESOURCE | Includes files on a computer included as a network resource on a targeted computer. | ***\\12.34.56.78*** ***\\some-comp-name*** Includes all files on a network resource identified using an IP or a hostname.<br><br>***\\12.34.56.78\somefolder*** ***\\some-comp-name\somefolder*** Includes all files in the folder "somefolder" on a network resource identified using an IP or a hostname. |
| Directory with wildcard (*) | DIRECTORY*\ | Includes any subdirectories with any subdirectory name, but does not include the files in the specified directory. | ***C:\abc**** Includes all files in all subdirectories of "abc" but does not include the files in the "abc" directory.<br><br>***C:\abc\wx*z***<br>*Matches:*<br>C:\abc\wxz\<br>C:\abc\wx123z\<br>*Does not match:*<br>C:\abc\wxz<br>C:\abc\wx123z<br><br>***C:\abc*wx***<br>*Matches:*<br>C:\abc\wx\<br>C:\abc\123wx\<br>*Does not match:*<br>C:\abc\wx<br>C:\abc\123wx |
| Directory with wildcard (*) | DIRECTORY* | Includes any subdirectories with a matching name, but does not include the files in that directory and any subdirectories. | ***C:\abc****<br>*Matches:*<br>C:\abc\<br>C:\abc\1<br>C:\abc\123<br>*Does not match:*<br>C:\abc<br>C:\abc\123\ |

| Directory | Format | Description | Examples |
|---|---|---|---|
| | | | C:\abc\123\456<br>C:\abx\<br>C:\xyz\<br><br>***C:\abc*wx***<br>*Matches:*<br>C:\abc\wx<br>C:\abc\123wx<br>*Does not match:*<br>C:\abc\wx\<br>C:\abc\123wx\<br><br>***C:\abc\wx*z***<br>*Matches:*<br>C:\abc\wxz<br>C:\abc\wx123z<br>*Does not match:*<br>C:\abc\wxz\<br>C:\abc\wx123z\<br><br>***C:\abc\wx****<br>*Matches:*<br>C:\abc\wx<br>C:\abc\wx\<br>C:\abc\wx12<br>C:\abc\wx12\345\<br>C:\abc\wxz\<br>*Does not match:*<br>C:\abc\wx123z\ |
| Environment variable | ${ENV VAR} | Includes all files and subdirectories defined by an environment variable with the format ${ENV VAR}. For a Virtual Appliance, the value pairs for the environment variable must be defined in **Policy or Computer Editor > Settings > General > Environment Variable Overrides.** | ***${windir}***<br>If the variable resolves to "c:\windows", Includes all the files in "c:\windows" and all its subdirectories. |
| Comments | DIRECTORY #Comment | Allows you to add comments to your inclusion definitions. | ***c:\abc #Include the abc directory*** |

1. Click **Policies > Common Objects > Lists > Directory Lists**.
2. Click **New > New Directory List**.
3. Type a name and, optionally, a description.
4. In the **Directory(s)** list, add the directory paths, one per line.
5. Click **OK**.

### Import and export directory lists

You can export one or more directory lists to an XML or CSV file, and import lists from an XML file.

1. Click **Policies > Common Objects > Lists > Directory Lists**.
2. To export one or more lists, select them and click **Export > Export Selected to CSV** or **Export > Export Selected to XML**.
3. To export all lists, click **Export > Export to CSV** or **Export > Export to XML**.
4. To import lists, click **New > Import From File** and follow the instructions on the wizard.

### See which policies use a directory list

It is useful to see which policies use a directory list to be aware of which policies are affected by any changes you make. For example, you can ensure no policies use a directory list before deleting it.

1. Click **Policies > Common Objects > Lists > Directory Lists**.
2. Select the directory list and click **Properties**.
3. Click the **Assigned To** tab.

## Create a list of file extensions for use in policies

Create lists of file extensions so that you can use them in multiple malware scan configurations. A single list is easier to manage than several identical lists that are each created in a different rule. For example, one list of file extensions can be used by multiple malware scan configurations as files to include in a scan. Another list of file extensions can be used by multiple malware scan configurations as files to exclude from a scan.

> **Tip:** To create a file extension list that is similar to an existing one, duplicate the list and then edit it.

You can insert comments into your list by preceding the text with a pound sign ("#").

1. Click **Policies > Common Objects > Lists > File Extension Lists**.
2. Click **New > New File Extension List**.
3. Type a name and, optionally, a description.

4. In the **File Extension(s)** list, add the extensions, one per line.
5. Click **OK**.

### Import and export file extension lists

You can export one or more file extension lists to an XML or CSV file, and import lists from an XML file.

1. Click **Policies > Common Objects > Lists > File Extension Lists**.
2. To export one or more lists, select them and click **Export > Export Selected to CSV** or **Export > Export Selected to XML**.
3. To export all lists, click **Export > Export to CSV** or **Export > Export to XML**.
4. To import lists, click **New > Import From File** and follow the instructions on the wizard.

### See which malware scan configurations use a file extension list

It is useful to see which malware scan configurations use a file extension list to be aware of which rules are affected by any changes you make. For example, you can ensure no scan configurations use a file extension list before deleting it.

1. Click **Policies > Common Objects > Lists > File Extension Lists**.
2. Select the list and click **Properties**.
3. Click the **Assigned To** tab.

## Create a list of files for use in policies

Create lists of file paths so that you can use them in multiple policies. A single list is easier to manage than several identical lists that are each created in a different policy.

**Tip:** To create a file list that is similar to an existing one, duplicate the list and then edit it.

The following table describes the syntax for defining file list items. The use of forward slashes "/" and backslashes "\" are supported for both Windows and Linux conventions:

| Inclusion | Format | Description | Example |
|---|---|---|---|
| File | FILE | Includes all files with the specified file name regardless of its location or directory. | ***abc.doc***<br>Includes all files named "abc.doc" in all directories. Does not include "abc.exe". |

| Inclusion | Format | Description | Example |
|---|---|---|---|
| File path | FILEPATH | Includes the specific file specified by the file path. | ***C:\Documents\abc.doc***<br>Includes only the file named "abc.doc" in the "Documents" directory. |
| **File with wildcard (*)** | FILE* | Includes all files with a matching pattern in the file name. | ***abc*.exe***<br>Includes any file that has prefix of "abc" and extension of ".exe".<br><br>***.db***<br>*Matches:*<br>123.db<br>abc.db<br>*Does not match:*<br>123db<br>123.abd<br>cbc.dba<br><br>***db***<br>*Matches:*<br>123.db<br>123db<br>ac.db<br>acdb<br>db<br>*Does not match:*<br>db123<br><br>***wxy*.db***<br>*Matches:*<br>wxy.db<br>wxy123.db<br>*Does not match:*<br>wxydb |
| File with wildcard (*) | FILE.EXT* | Includes all files with a matching pattern in the file extension. | ***abc.v****<br>Includes any file that has file name of "abc" and extension beginning with ".v".<br><br>***abc.*pp***<br>*Matches:*<br>abc.pp<br>abc.app<br>*Does not match:*<br>wxy.app |

| Inclusion | Format | Description | Example |
|---|---|---|---|
| | | | ***abc.a*p***<br>*Matches:*<br>abc.ap<br>abc.a123p<br>*Does not match:*<br>abc.pp<br><br>***abc.****<br>*Matches:*<br>abc.123<br>abc.xyz<br>*Does not match:*<br>wxy.123 |
| File with wildcard (*) | FILE*.EXT* | Includes all files with a matching pattern in the file name and in the extension. | ***a*c.a*p***<br>*Matches:*<br>ac.ap<br>a123c.ap<br>ac.a456p<br>a123c.a456p<br>*Does not match:*<br>ad.aa |
| Environment variable | ${ENV VAR} | Includes files specified by an environment variable with the format ${ENV VAR}. These can be defined or overridden using **Policy or Computer Editor > Settings > General > Environment Variable Overrides.** | ***${myDBFile}***<br>Includes the file "myDBFile". |
| Comments | FILEPATH #Comment | Allows you to add comments to your inclusion definitions. | ***C:\Documents\abc.doc #This a comment*** |

1. Click **Policies > Common Objects > Lists > File Lists**.
2. Click **New > New File List**.
3. Type a name and, optionally, a description.
4. In the **File(s)** list, add the file paths, one per line.
5. Click **OK**.

## Import and export file lists

You can export one or more file lists to an XML or CSV file, and import lists from an XML file.

1. Click **Policies > Common Objects > Lists > File Lists**.
2. To export one or more lists, select them and click **Export > Export Selected to CSV** or **Export > Export Selected to XML**.
3. To export all lists, click **Export > Export to CSV** or **Export > Export to XML**.
4. To import lists, click **New > Import From File** and follow the instructions on the wizard.

### See which policies use a file list

It is useful to see which policies use a file list to be aware of which policies are affected by any changes you make. For example, you can ensure no policies use a file list before deleting it.

1. Click **Policies > Common Objects > Lists > File Lists**.
2. Select the file list and click **Properties**.
3. Click the **Assigned To** tab.

## Create a list of IP addresses for use in policies

Create lists of IP addresses so that you can use them in multiple firewall rules. A single list is easier to manage than several identical lists that are each defined in a different rule.

> **Tip:** To create an IP list that is similar to an existing one, duplicate the list and then edit it.

You can enter an individual IP address, or you can enter IP ranges and masked IPs. You can also insert comments into your IP list by preceding the text with a hash sign ("#").

Masked IP examples are 192.168.0/24, 192.168.2.0/255.255.255.0, and for IPV6 2001:0DB8::CD30:0:0:0:0/60. IP range examples are 192.168.0.2 - 192.168.0.125 and, for IPV6, FF01::101 - FF01::102

1. Click **Policies > Common Objects > Lists > IP Lists**.
2. Click **New > New IP List**.
3. Type a name and, optionally, a description.
4. In the **IP(s)** list, add the IP addresses, masked IP addresses, or IP ranges (one per line).
5. Click **OK**.

### Import and export IP lists

You can export one or more IP lists to an XML or CSV file, and import lists from an XML file.

1. Click **Policies > Common Objects > Lists > IP Lists**.
2. To export one or more lists, select them and click **Export > Export Selected to CSV** or **Export > Export Selected to XML**.
3. To export all lists, click **Export > Export to CSV** or **Export > Export to XML**.
4. To import lists, click **New > Import From File** and follow the instructions on the wizard.

### See which rules use an IP list

It is useful to see which firewall rules use an IP list to be aware of which rules are affected by any changes you make. For example, you can ensure no firewall rules use an IP list before deleting it.

1. Click **Policies > Common Objects > Lists > IP Lists**.
2. Select the IP list and click **Properties**.
3. Click the **Assigned To** tab.

## Create a list of ports for use in policies

Create lists of port numbers so that you can use them in multiple rules. A single list is easier to manage than several identical lists that are each created in a different rule.

**Tip:** To create a port list that is similar to an existing one, duplicate the list and then edit it.

Individual ports and port ranges can be included on the list, for example 80, and 20-21. You can insert comments into your port list by preceding the text with a pound sign ("#").

**Note:** For a listing commonly accepted port number assignments, see the Internet Assigned Numbers Authority (IANA). For a list of port numbers used by Deep Security Manager, Relay, or Agent, see "Port numbers" on page 96.

1. Click **Policies > Common Objects > Lists > Port Lists**.
2. Click **New > New Port List**.
3. Type a name and, optionally, a description.
4. In the **Port(s)** list, add the port numbers, one per line.
5. Click **OK**.

### Import and export port lists

You can export one or more port lists to an XML or CSV file, and import lists from an XML file.

1. Click **Policies > Common Objects > Lists > Port Lists**.
2. To export one or more lists, select them and click **Export > Export Selected to CSV** or **Export > Export Selected to XML**.

3. To export all lists, click **Export > Export to CSV** or **Export > Export to XML**.
4. To import lists, click **New > Import From File** and follow the instructions on the wizard.

### See which rules use a port list

It is useful to see which rules use a port list to be aware of which rules are affected by any changes you make. For example, you can ensure no rules use a port list before deleting it.

1. Click **Policies > Common Objects > Lists > Port Lists**.
2. Select the port list and click **Properties**.
3. Click the **Assigned To** tab.

## Create a list of MAC addresses for use in policies

Create lists of MAC addresses so that you can use them in multiple policies. A single list is easier to manage than several identical lists that are each created in a different policy.

> **Tip:** To create a MAC list that is similar to an existing one, duplicate the list and then edit it.

MAC lists support MAC addresses in both hyphen- and colon-separated formats, for example 0A-0F-FF-F0-A0-AF and 0A:0F:FF:F0:A0:AF. You can insert comments into your MAC list by preceding the text with a pound sign ("#").

1. Click **Policies > Common Objects > Lists > MAC Lists**.
2. Click **New > New MAC List**.
3. Type a name and, optionally, a description.
4. In the **MAC(s)** list, add the MAC addresses, one per line.
5. Click **OK**.

### Import and export MAC lists

You can export one or more MAC lists to an XML or CSV file, and import lists from an XML file.

1. Click **Policies > Common Objects > Lists > MAC Lists**.
2. To export one or more lists, select them and click **Export > Export Selected to CSV** or **Export > Export Selected to XML**.
3. To export all lists, click **Export > Export to CSV** or **Export > Export to XML**.
4. To import lists, click **New > Import From File** and follow the instructions on the wizard.

### See which policies use a MAC list

It is useful to see which policies use a MAC list to be aware of which policies are affected by any changes you make. For example, you can ensure no policies use a MAC list before deleting it.

1. Click **Policies > Common Objects > Lists > MAC Lists**.
2. Select the MAC list and click **Properties**.
3. Click the **Assigned To** tab.

## Define contexts for use in policies

Contexts are a powerful way of implementing different security policies depending on a computer's network environment.

Contexts are designed to be associated with firewall and intrusion prevention rules. If the conditions defined in the context associated with a rule are met, the rule is applied.

### Configure settings used to determine whether a computer has internet connectivity

1. In the Deep Security Manager, go to **Administration > System Settings > Contexts**.
2. In the **URL for testing Internet Connectivity Status** box, enter the URL to which an HTTP request will be sent to test for internet connectivity. (You must include "http://".)
3. In the **Regular Expression for returned content used to confirm Internet Connectivity Status** box, enter a regular expression that will be applied to the returned content to confirm that HTTP communication was successful. (If you are certain of the returned content, you can use a simple string of characters.)
4. In the **Test Interval** list, select the time interval between connectivity tests.

For example, to test Internet connectivity, you could use the URL "**http://www.example.com**", and the string "**This domain is established to be used for illustrative examples in documents**" which is returned by the server at that URL.

### Define a context

1. In the Deep Security Manager, go to **Policies > Common Objects > Other > Contexts** and then click **New > New Context**.

2. In the **General Information** area, enter the name and description of the context rule. This area also displays the earliest version of the Deep Security Agent the rule will be compatible with.
3. In the **Options** area, specify when the context will be applied:
   - **Context applies when connection is:** Specifying an option here will determine whether the Firewall rule is in effect depending on the ability of the computer to connect to its domain controller or its internet connectivity. (Conditions for testing internet connectivity can be configured in **Administration > System Settings > Contexts**.)

     If the domain controller can be contacted directly (via ICMP), the connection is "Local". If it can be contacted via VPN only, then the connection is "Remote".

     The time interval between domain controller connectivity tests is the same as the internet connectivity test interval, which is configurable in **Administration > System Settings > Contexts**. The internet connectivity test is only performed if the computer is unable to connect to its domain controller.

   - **Context Applies to Interface Isolation Restricted Interfaces:** This context will apply to network interfaces on which traffic has been restricted through the use of interface isolation. This is primarily used for "Allow" or "Force Allow" Firewall rules. See "Detect and configure the interfaces available on a computer" on page 369.

After you assign the context to a rule, it is displayed on the **Assigned To** tab for the context. (To link a security rule to a context, go to the **Options** tab in the security rule's **Properties** window and select the context from the "Context" list.)

## Define stateful firewall configurations

Deep Security's stateful firewall configuration mechanism analyzes each packet in the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions. In the case of stateless protocols like UDP and ICMP, a pseudo-stateful mechanism is implemented based on historical traffic analysis. Packets are handled by the stateful mechanism as follows:

1. A packet is passed to the stateful routine if it has been allowed through by the static firewall rule conditions,

2. The packet is examined to determine whether it belongs to an existing connection, and
3. The TCP header is examined for correctness (e.g. sequence numbers, flag combinations, etc.).

To create a new stateful configuration, you need to:

1. "Add a stateful configuration " below.
2. "Enter stateful configuration information" below.
3. "Select packet inspection options" below.

When you're done with your stateful configuration, you can also learn how to

- "See policies and computers a stateful configuration is assigned to" on page 454
- "Export a stateful configuration " on page 453
- "Delete a stateful configuration " on page 454

## Add a stateful configuration

There are three ways to define a stateful configuration on the **Policies > Common Objects > Other > Firewall Stateful Configurations** page:

- Create a new configuration. Click **New** > **New Firewall Stateful Configuration**.
- Import a configuration from an XML file. Click **New** > **Import From File**.
- Copy and then modify an existing configuration. Right-click the configuration in the Firewall Stateful Configurations list and then click **Duplicate**. To edit the new configuration, select it and then click **Properties**.

## Enter stateful configuration information

Enter a **Name** and **Description** for the configuration.

## Select packet inspection options

You can define options for IP, TCP, UDP and ICMP packet inspection, end enable Active or Passive FTP.

### IP packet inspection

Under the **General** tab, select the **Deny all incoming fragmented packets** to drop any fragmented packets. Dropped packets will bypass fragmentation analysis and generate an "IP fragmented packet" log entry. Packets with a total length smaller than the IP header length are dropped silently.

**Warning:** Attackers sometimes create and send fragmented packets in an attempt to bypass Firewall Rules.

**Note:** The Firewall Engine, by default, performs a series of checks on fragmented packets. This is default behavior and cannot be reconfigured. Packets with the following characteristics are dropped:

- **Invalid fragmentation flags/offset:** A packet is dropped when either the **DF** and **MF** flags in the IP header are set to 1, or the header contains the **DF** flag set to 1 and an **Offset** value different than 0.
- **First fragment too small:** A packet is dropped if its **MF** flag is set to 1, its **Offset** value is at 0, and it has total length of less than 120 bytes (the maximum combined header length).
- **IP fragment out of boundary:** A packet is dropped if its **Offset** flag value combined with the total packet length exceeds the maximum datagram length of 65535 bytes.
- **IP fragment offset too small:** A packet is dropped if it has a non-zero **Offset** flag with a value that is smaller than 60 bytes.

### TCP packet inspection

Under the **TCP** tab, select which of the following options you would like to enable:

- **Deny TCP packets containing CWR, ECE flags:** These flags are set when there is network congestion.

  **Note:** RFC 3168 defines two of the six bits from the Reserved field to be used for ECN (Explicit Congestion Notification), as follows:

- Bits 8 to 15: CWR-ECE-URG-ACK-PSH-RST-SYN-FIN
- TCP Header Flags Bit Name Reference:
  - Bit 8: CWR (Congestion Window Reduced) [RFC3168]
  - Bit 9: ECE (ECN-Echo) [RFC3168]

**Warning:** Automated packet transmission (such as that generated by a denial of service attack, among other things) will often produce packets in which these flags are set.

- **Enable TCP stateful inspection:** Enable stateful inspection at the TCP level. If you enable stateful TCP inspection, the following options become available:
  - **Enable TCP stateful logging:** TCP stateful inspection events will be logged.
  - **Limit the number of incoming connections from a single computer to:** Limiting the number of connections from a single computer can lessen the effect of a denial of service attack.
  - **Limit the number of outgoing connections to a single computer to:** Limiting the number of outgoing connections to a single computer can significantly reduce the effects of Nimda-like worms.
  - **Limit the number of half-open connections from a single computer to:** Setting a limit here can protect you from DoS attacks like SYN Flood. Although most servers have timeout settings for closing half-open connections, setting a value here can prevent half-open connections from becoming a significant problem. If the specified limit for SYN-SENT (remote) entries is reached, subsequent TCP packets from that specific computer will be dropped.

    **Note:** When deciding on how many open connections from a single computer to allow, choose your number from somewhere between what you would consider a reasonable number of half-open connections from a single computer for the type of protocol being used, and how many half-open connections from a single computer your system can maintain without getting congested.

- **Enable ACK Storm protection when the number of already acknowledged packets exceeds:** Set this option to log an event that an ACK Storm attack has occurred.
  - **Drop Connection when ACK Storm detected:** Set this option to drop the connection if such an attack is detected.

> **Note:** ACK Storm protection options are only available on Deep Security Agent 8.0 and earlier.

### FTP Options

Under the **FTP Options** tab, you can enable the following options:

> **Note:** The following FTP options are available in Deep Security Agent version 8.0 and earlier.

- **Active FTP**
  - **Allow Incoming:** Allow Active FTP when this computer is acting as a server.
  - **Allow Outgoing:** Allow Active FTP when this computer is acting as client.
- **Passive FTP**
  - **Allow Incoming:** Allow Passive FTP when this computer is acting as a server.
  - **Allow Outgoing:** Allow Passive FTP when this computer is acting as a client.

### UDP packet inspection

Under the **UDP** tab, you can enable the following options:

- **Enable UDP stateful inspection:** Select to enable stateful inspection of UDP traffic.

  > **Note:** The UDP stateful mechanism drops unsolicited incoming UDP packets. For every outgoing UDP packet, the rule will update its UDP "stateful" table and will then only allow a UDP response if it occurs within 60 seconds of the request. If you wish to allow specific incoming UDP traffic, you will have to create a **Force Allow** rule. For example, if you are running a DNS server, you will have to create a **Force Allow** rule to allow incoming UDP packets to destination port 53.

> **Warning:** Without stateful inspection of UDP traffic, an attacker can masquerade as a DNS server and send unsolicited UDP "replies" from source port 53 to computers behind a firewall.

- **Enable UDP stateful logging:** Selecting this option will enable the logging of UDP stateful inspection events.

### ICMP packet inspection

Under the **ICMP** tab, you can enable the following options:

> **Note:** ICMP stateful inspection is available in Deep Security Agent version 8.0 or earlier.

- **Enable ICMP stateful inspection:** Select to enable stateful inspection of ICMP traffic.

  > **Note:** The ICMP (pseudo-)stateful mechanism drops incoming unsolicited ICMP packets. For every outgoing ICMP packet, the rule will create or update its ICMP "stateful" table and will then only allow a ICMP response if it occurs within 60 seconds of the request. (ICMP pair types supported: Type 0 & 8, 13 & 14, 15 & 16, 17 & 18.)

  > **Warning:** With stateful ICMP inspection enabled, you can, for example, only allow an ICMP echo-reply in if an echo-request has been sent out. Unrequested echo-replies could be a sign of several kinds of attack including a Smurf amplification attack, a Tribe Flood Network communication between master and daemon, or a Loki 2 back-door.

  - **Enable ICMP stateful logging:** Selecting this option will enable the logging of ICMP stateful inspection events.

### Export a stateful configuration

You can export all stateful configurations to a .csv or .xml file by clicking **Export** and selecting the corresponding export action from the list. You can also export specific stateful configurations by first selecting them, clicking **Export** and then selecting the corresponding export action from the list.

### Delete a stateful configuration

To delete a stateful configuration, right-click the configuration in the Firewall Stateful Configurations list, click **Delete** and then click **OK**.

> **Note:** Stateful configurations that are assigned to one or more computers or that are part of a policy cannot be deleted.

### See policies and computers a stateful configuration is assigned to

You can see which policies and computers are assigned to a stateful inspection configuration on the **Assigned To** tab. Click on a policy or computer in the list to see their properties.

## Define a schedule that you can apply to rules

Schedules are reusable timetables that you can assign to rules, agent upgrades, and more.

1. In Deep Security Manager, go to **Policies > Common Objects > Other > Schedules**.
2. Click **New > New Schedule.**
3. In the **General Information** area, enter a name and description used to identify the schedule.
4. Click a time block in the grid to select it. To deselect it, click it while pressing Shift. Schedule periods are defined by hour-long time blocks.

After you assign the schedule to a rule, it is displayed on the **Assigned To** tab for the schedule. To link a security rule to a schedule, go to the **Options** tab in the security rule's **Properties** window and select the schedule from the "Schedule" list.

> **Note:** With agent-based protection, schedules use the same time zone as the protected computer's operating system. With agentless protection, schedules use the same time zone as the Deep Security Virtual Appliance.

# Lock down software with application control

> **Note:** You can enable application control for computers running Deep Security Agent 10.0 or higher. For a list of operating systems where application control is supported, see "Supported

features by platform" on page 77.

Application control continuously monitors for software changes on your protected servers. Based on your policy configuration, application control either prevents unauthorized software from running until it is explicitly allowed, or allows unauthorized software until it is explicitly blocked. Which option you choose depends on the level of control you want over your environment.

**Tip:** Application control is intended for use on stable servers that are not updated frequently, and not for workstations or servers that undergo a lot of software changes.

## Key concepts

**Targeted protection state:** One of the main decisions you need to make when setting up application control is deciding your targeted protection state. Do you want to prevent all new or changed software from running, unless you manually specify that it is allowed? Or do you want it to run by default unless you specifically block it? One approach is to initially allow unrecognized software to run when you first enable application control and there's a lot of unrecognized software. As you add application control rules and the volume of unrecognized software decreases, you could switch to block mode.

**Application control rule:** Rules specify whether software is allowed or blocked on a particular computer.

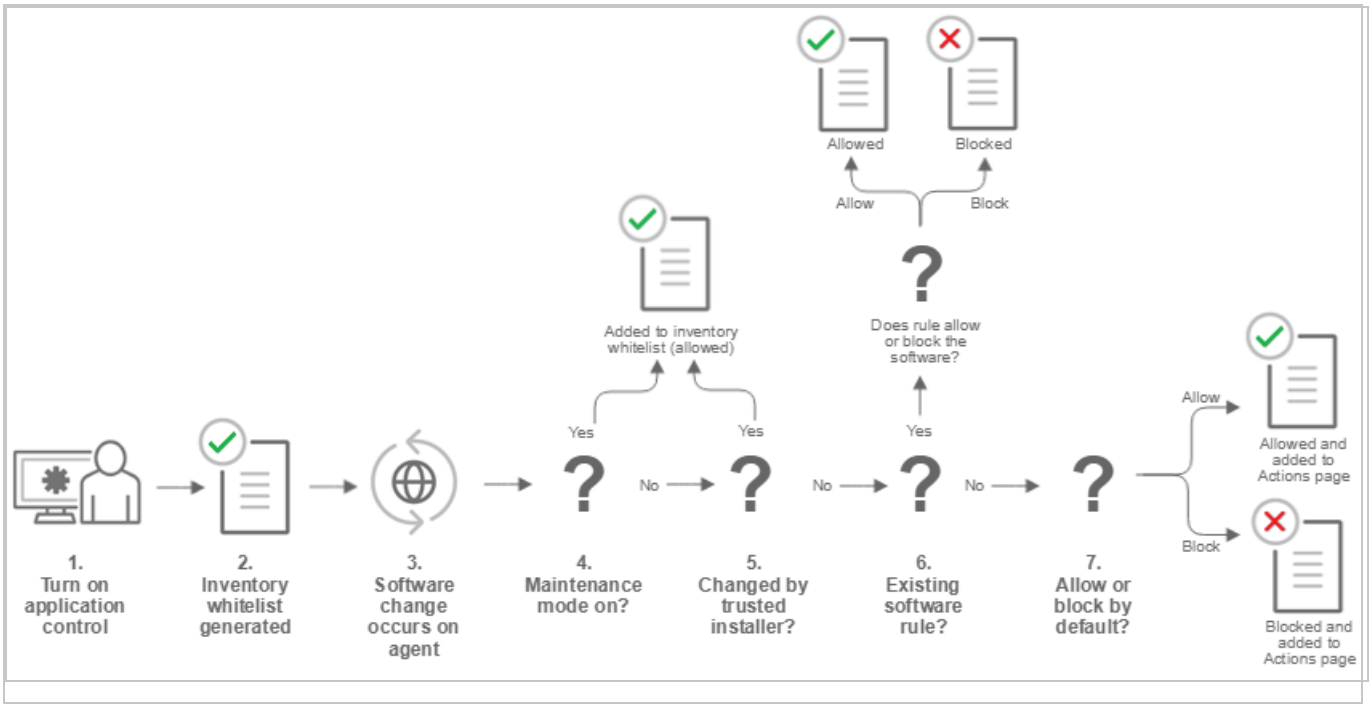
**Inventory:** Initial list of software that is installed on the computer. Make sure only software that you want to allow is installed on the computer. When you enable application control, all currently installed software is added to the computer's inventory and allowed to run. When a computer is in maintenance mode, any software changes made to the computer are added to the computer's inventory and allowed to run. A computer's software inventory is stored on the Deep Security Agent and is not displayed in Deep Security Manager.

**Unrecognized software:** Software that isn't in a computer's inventory and isn't already covered by an application control rule. See "What does application control detect as a software change?" on page 461

**Maintenance mode:** If you are planning to install or update software, we strongly advise that you turn on maintenance mode. While maintenance mode is enabled, application control will

continue to enforce rules that block software, but it will allow new or updated software to run and automatically add it to the computer's inventory. See "Turn on maintenance mode when making planned changes" on page 467.

## How does application control work?




1. You enable application control in a policy and assign the policy to a computer that is protected by a Deep Security Agent (see "Turn on application control" on page 463).
2. When the agent receives the policy, it creates an inventory of all software installed on the computer. All software listed in the inventory is assumed to be safe and is allowed to run on that computer. This inventory is not visible from Deep Security Manager, which means you need to be absolutely certain that only good software is installed on a computer where you intend to enable application control.
3. After the inventory is finished, application control is aware of any software changes on the computer. A software change could be new software that appears on the computer or changes to existing software.
4. If the computer is in maintenance mode, the Deep Security Agent adds the software to its inventory and it is allowed to run. This change is not visible in Deep Security Manager. See "Turn on maintenance mode when making planned changes" on page 467.

5. If the change was made by a trusted installer, the Deep Security Agent adds the software to its inventory and allows it to run. For example, when Microsoft Windows self-initiates a component update, hundreds of new executable files may be installed. Application control auto-authorizes many file changes that are created by well-known Windows processes and does not list these changes in Deep Security Manager. Removing the "noise" associated with expected software changes provides you with clearer visibility into changes that may need your attention.

   **Note:** The trusted installer feature is available with Deep Security Agent 10.2 or later.

6. If the computer's ruleset contains a rule for this exact piece of software, the software is allowed or blocked according to the rule that's in place. See "What does application control detect as a software change?" on page 461
7. If software is not in the computer's inventory and is not covered by an existing rule, it's considered unrecognized software. The policy assigned to the computer specifies how unrecognized software is handled. Depending on the policy configuration, it's either allowed to run or is blocked. If the software is blocked and it is able to produce error messages in the OS, an error message on the protected computer indicates that the software does not have permissions to run or that access is denied.

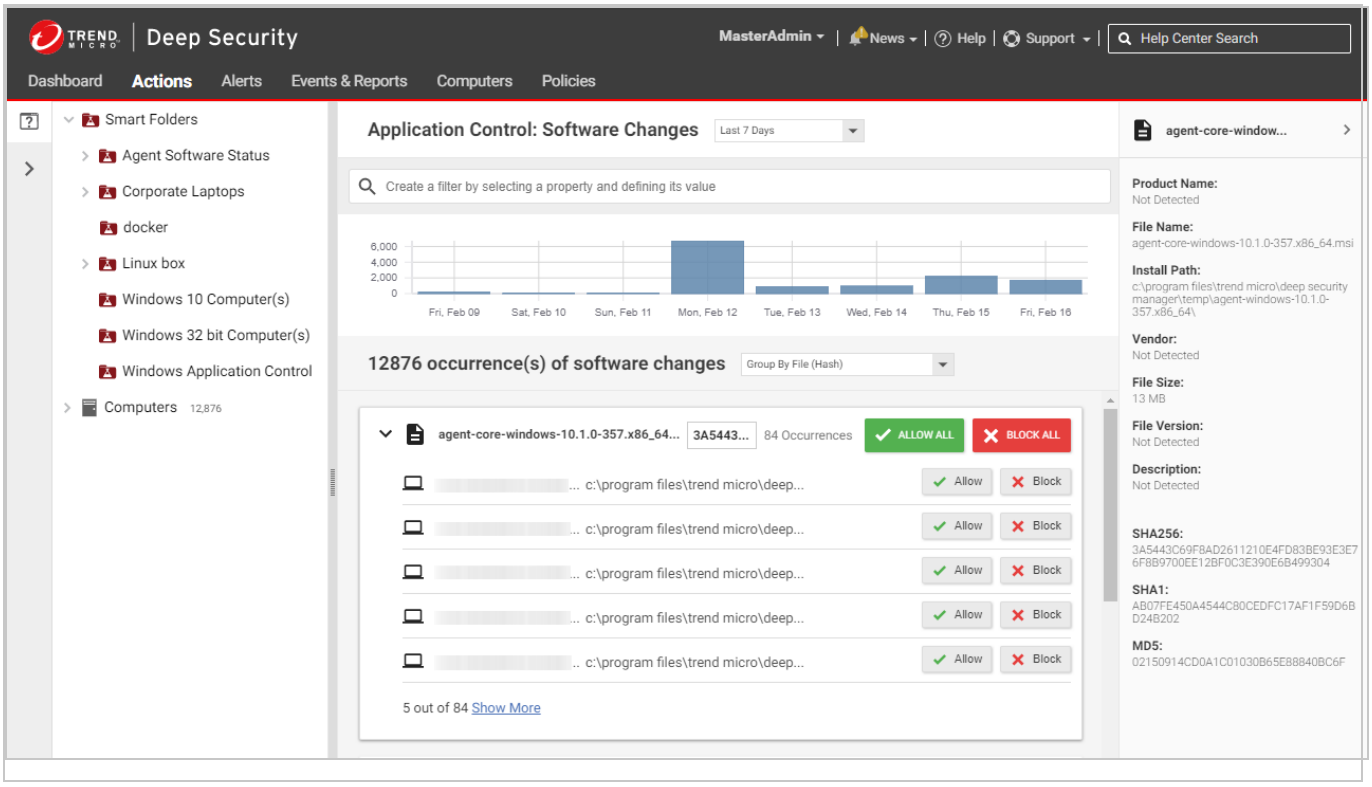
   The unrecognized software appears on the **Application Control - Software Changes** page in Deep Security Manager. On that page, an administrator can click **Allow** or **Block** to create an allow or block rule for that piece of software on a particular computer. An allow or block rule takes precedence over the default action specified in the policy. See "Monitor new and changed software" on page 464.

## A tour of the application control interface

There are a few places in Deep Security Manager where you can see changes related to application control:


- "Application Control: Software Changes (Actions)" on the next page
- "Application Control Rulesets" on page 459
- "Security Events" on page 460
- "Decision Logs" on page 461

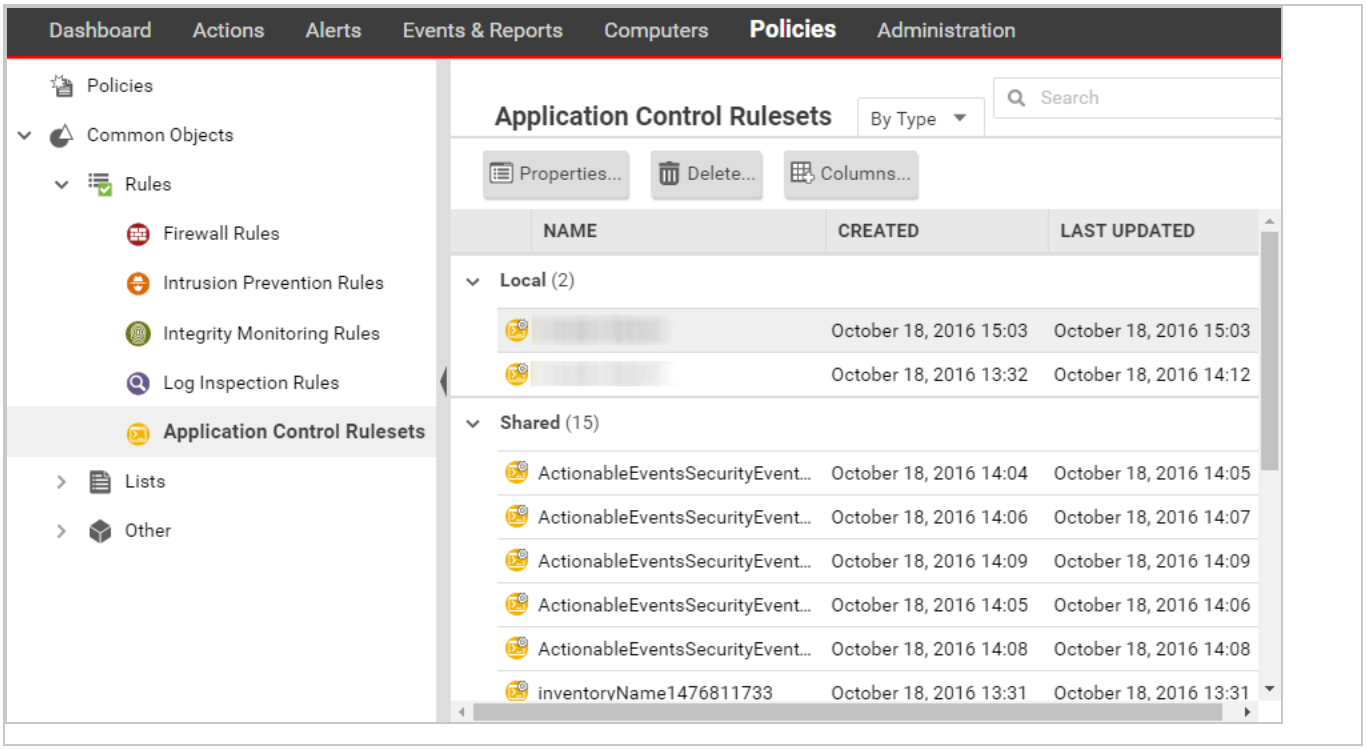
# Application Control: Software Changes (Actions)




The **Application Control: Software Changes** page is displayed when you click **Actions** in Deep Security Manager. It displays all unrecognized software (software that isn't in a computer's inventory and doesn't have a corresponding application control rule). Software changes are allowed or blocked at the computer level, so if a particular piece of software is installed on fifty computers, it will appear on that page fifty times. However, if you know that a certain piece of software should be allowed or blocked everywhere, you can filter the **Actions** page to sort the changes by file hash and then click **Allow All** to allow it on all computers where the software is installed.

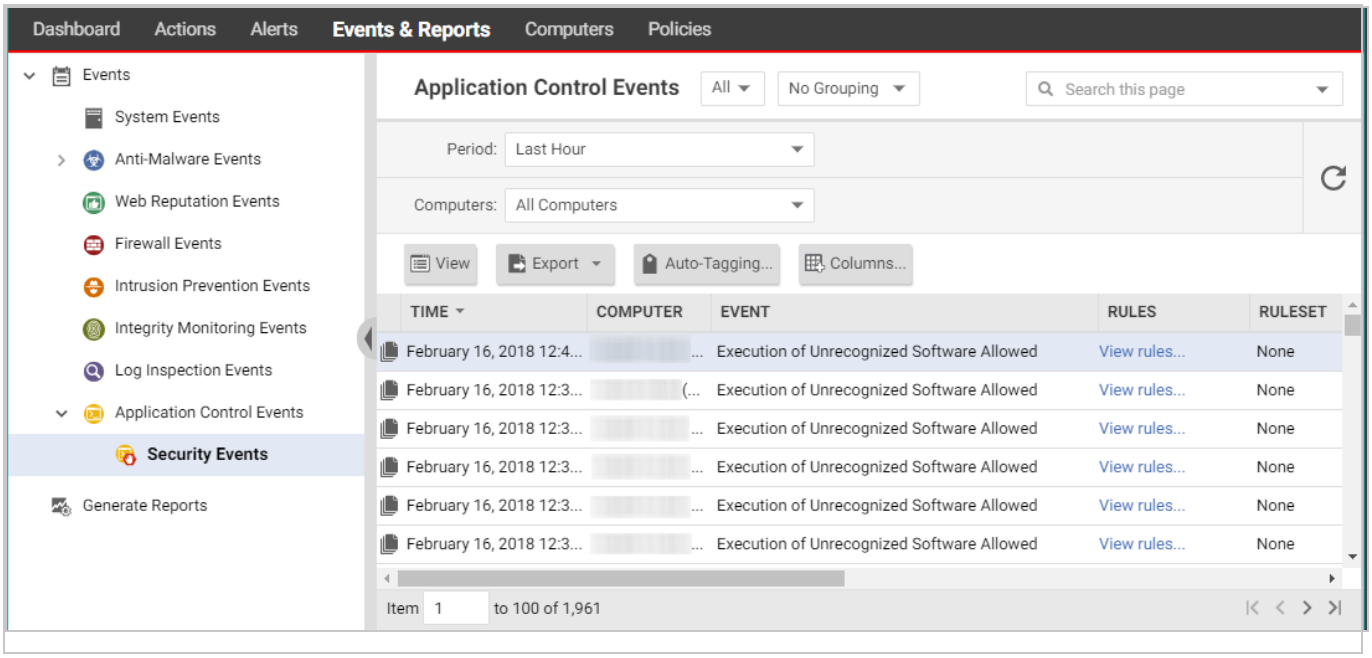
The policy applied to a computer specifies whether it will allow all unrecognized software to run by default, or block all unrecognized software, but no explicit application control rule is created until you click "Allow" or "Block" on the Actions page. When you click Allow or Block, a corresponding rule appears in the ruleset for the computer. The rulesets are displayed on the **Application Control Rulesets** page.

# Application Control Rulesets




To see the ruleset for a computer, go to **Policies > Common Objects > Rules > Application Control Rulesets**. To see which rules are part of a ruleset, double-click the ruleset and go to the **Rules** tab. The Rules tab displays the pieces of software that have rules associated with them and enables you to change allow rules to block, and vice versa.

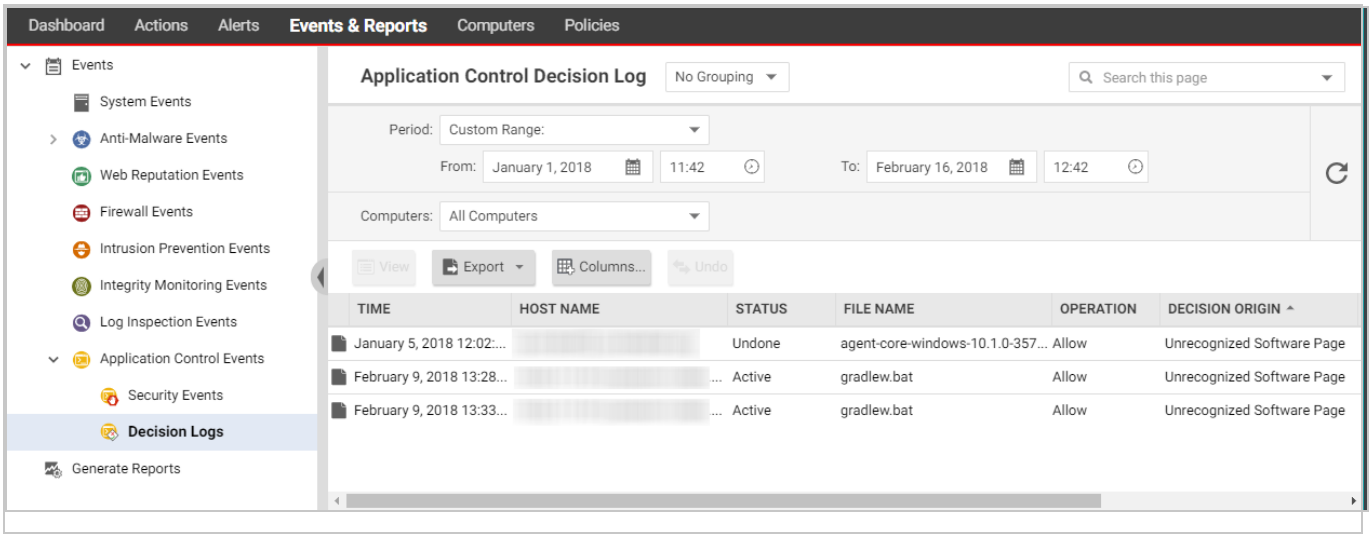
# Security Events




**Events & Reports > Events > Application Control Events > Security Events** displays all unrecognized software that either has been run on a computer or has been prevented from running by a block rule. You can filter this list by time period and other criteria.

For each event (except aggregated events), you can click **View rules** to change the rule from Allow to Block or vice versa. Deep Security Agent 10.2 or later includes event aggregation logic to reduce the volume of logs when the same event occurs repeatedly.

## Decision Logs




**Events & Reports > Events > Application Control Events > Decision Logs** enables administrators to review and undo the allow/block decisions that have been made for software changes. You can also see the decision log for a specific computer from the **computer editor**[1], under **Application Control > Decision Logs**). These three actions result in an event appearing on the Decision Logs page:

- Editing an existing rule in a ruleset from the **Application Control Rulesets** page
- Creating a rule by clicking **Allow** or **Block** on the **Application Control: Software Changes** page
- Editing a rule from the **Application Control Events** page

## What does application control detect as a software change?

Unlike integrity monitoring, which monitors any file, application control looks only for software files when examining the initial installation and monitoring for change.

Software can be:

[1]To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

- Windows applications (.exe, .com, .dll, .sys), Linux libraries (.so) and other compiled binaries and libraries
- Java .jar and .class files, and other compiled byte code
- PHP, Python, and shell scripts, and other web apps and scripts that are interpreted or compiled on the fly
- Windows PowerShell scripts, batch files (.bat), and other Windows-specific scripts (.wsf, .vbs, .js)

For example, WordPress and its plug-ins, Apache, IIS, nginx, Adobe Acrobat, app.war, and /usr/bin/ssh would all be detected as software.

Application control checks a file's extension to determine whether it's a script. Additionally, on Linux, application control treats any file with execute permissions as if it's a script.

**Note:** On Windows computers, application control tracks changes on the local file system, but not on network locations, CD or DVD drives, or USB devices.

Application control is integrated with the kernel (on Linux computers) and file system, so it has permissions to monitor the whole computer, including software installed by root or administrator accounts. The agent watches for disk write activity on software files, and for attempts to execute software.

## Differences in how Deep Security Agent 10.x and 11.x compare files

To determine whether software is new or has changed, Deep Security 10.x agents compare the file with the initially installed software's SHA-256 hash, file size, path, and file name (they have a "file-based" ruleset). Deep Security 11.x agents compare only the file's SHA-256 hash and file size (they have a "hash-based" ruleset). Because the rules created by Deep Security 11.x agents compare only the unique hash and file size, a rule will continue to be applied even if the software file is renamed or moved. As a result, using Deep Security 11.x agents reduces the number of software changes that you need to deal with.

A Deep Security 10.x agent continues to use a file-based ruleset until it is upgraded to Deep Security 11.0 or newer. When you upgrade an agent to version 11.0 or newer, its ruleset is converted to use hash-based rules. If there are multiple file-based rules for the same hash value,

they are consolidated into one hash-based rule. If the rules being consolidated conflict with each other (one rule blocks the file and another allows it), the new hash-based rule will be an "allow" rule.

## Set up application control

For information about how application control works, see "Lock down software with application control" on page 454.

To enable application control and monitor software changes:

1. "Turn on application control" below
2. "Monitor new and changed software" on the next page
3. "Turn on maintenance mode when making planned changes" on page 467

This article also provides "Application control tips and considerations" on page 468 that you should be aware of when working with application control.

Once you've enabled application control, you can also learn how to:

- "View and change application control rulesets" on page 474
- "Reset application control after too much software change" on page 478
- "Monitor application control events" on page 471
- "Use the API to create shared and global rulesets " on page 479

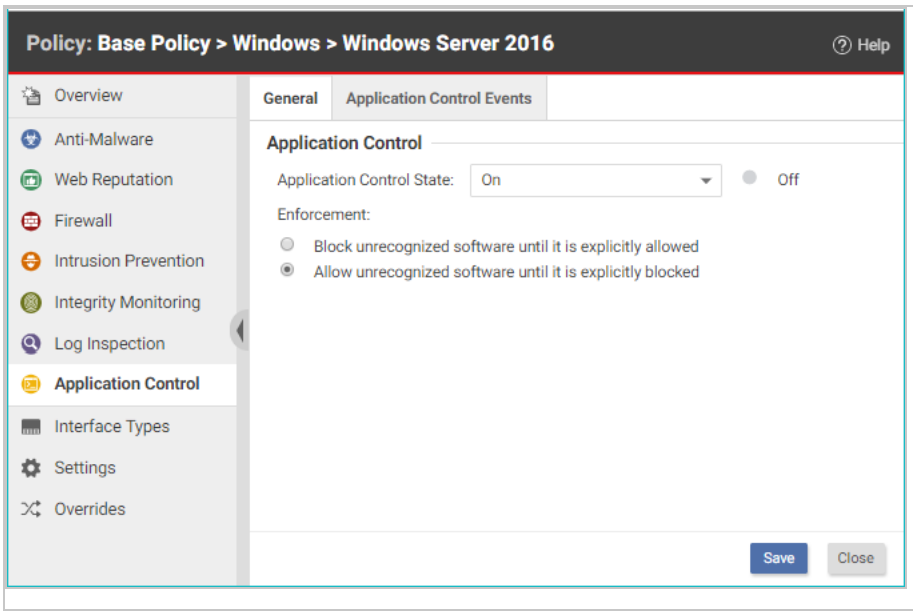
### Turn on application control

You can enable application control in the settings for a computer or in policies:

1. Open the **Computer or Policy editor**[1] and go to **Application Control > General**.
2. Set the **Application Control State** to "On" or "Inherited (On)".

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

3. Under **Enforcement**, select your targeted protection state:
   - **Block unrecognized software until it is explicitly allowed**
   - **Allow unrecognized software until it is explicitly blocked** (we recommend that you choose this option when initially setting up application control)
4. Click **Save**.




The next time that the Deep Security Manager and agent connect, the agent scans and then generates an inventory of all software installed on the computer and creates rules that allow all the software that it finds. This initial inventory can take 15 minutes or longer, depending on your environment.

To check that application control is working as expected, follow the instructions in "Verify that application control is enabled" on page 469.

## Monitor new and changed software

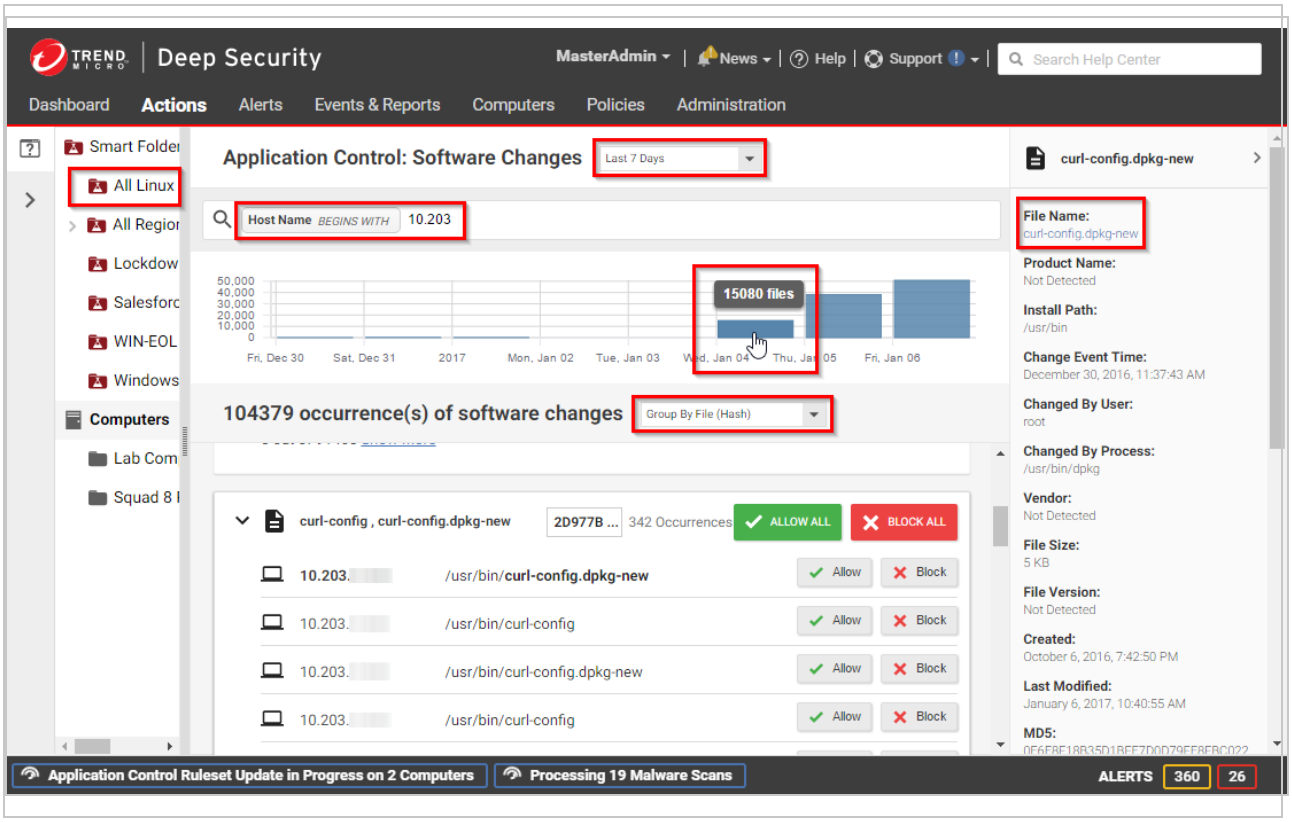
After the inventory has finished on a protected computer, any software executable files that are added or changed are classified as a "software change" and appear on the **Actions** page in Deep Security Manager. When unrecognized software runs, or attempts to run and is blocked, the event is listed under **Events & Reports > Events > Application Control Events > Security Events**.

After you initially enable application control, you will likely see a lot of software changes on the **Actions** page. This can happen when allowed software creates new executables, renames files, or relocates files through the normal course of operation. As you add rules to tune application control, you should see fewer software changes.

To quickly find all software changes on all computers and easily create allow or block rules for them, use the **Actions** tab.

1. In Deep Security Manager, go to **Actions**.
2. There are several ways you can filter to see only specific occurrences of unrecognized software.

> **Tip:** Instead of evaluating each software change on each computer individually, use the filters described below to find software changes that you know are good, and allow them in bulk.




To reduce the number of software changes being displayed:

- From the drop-down list next to **Application Control: Software Changes**, select a time range such as **Last 7 Days**. You can also click a bar in the graph near the top of the page to display the changes for that time period.
- In the pane on the left, click **Computers** and select an individual computer or group, or click **Smart Folders** to display only the computers that are included in a particular smart folder (see "Group computers dynamically with smart folders" on page 1023).

  **Note:** Unlike the **Computers** tab, the **Software Changes** pane usually does not show all computers. It only displays computers where application control has detected software changes that don't already have allow or block rules.

- Enter search terms and operators in the search filter field. You search for these attributes: Change By Process, Change By User, File Name, Host Name, Install Path, MD5, SHA1, and SHA256. For example, you could find all changes made by a particular user that you trust and click **Allow All** to allow all of their changes. Or if a particular software update was installed across your organization (while maintenance mode was not enabled), filter the page according to the hash value of the file and click **Allow All** to allow all occurrences.

  **Tip:** Details about a software change are displayed in the right pane. You can click the file name or computer name in the details to add it to your search filter.

- Select whether to **Group by File (Hash)** or **Group by Computer**.

3. Click either **Allow** or **Block** to add an allow or block rule on that computer, for that software. If you need more information to decide whether to allow or block, click the software name, then use the details panel on the right side.

   The next time that the agent connects with the Deep Security Manager, it receives the new rules.

## Tips for handling changes

- For most environments, we suggest that you select the **Allow unrecognized software until it is explicitly blocked** option to allow software changes by default when you first enable application control and add allow and block rules for changes that you see on the **Actions** page. Eventually, the rate of software changes should decrease. At that point, you could

consider blocking software changes by default and creating allow rules for the software that you know is good. Some organizations prefer to continue to allow changes by default and monitor the **Actions** page for software that should be blocked.

- You may prefer to start by evaluating security events, rather than dealing with unrecognized software first. Security events show you which unrecognized software has run (or attempted to run). For information on security events, see "Monitor application control events" on page 471.
- When an unrecognized file is allowed to execute and you want to continue to allow it, create an Allow rule. In addition to allowing the file's execution, the event is no longer logged for that file, which reduces noise and makes important events easier to find.
- When a known file's execution is blocked, consider cleaning that file from the computer, especially for repeated occurrences.
- Keep in mind that software changes are listed for each computer where they occur. You must allow or block the software for each computer.
- Rules are assigned to computers, not to policies. For example, if `helloworld.py` is detected on three computers, when you click **Allow All** or **Block All**, this would affect only three computers. It won't affect future detections on other computers, because they have their own rulesets.
- If you see changes related to software updates that you can control, use the maintenance mode feature when performing those updates. See "Turn on maintenance mode when making planned changes" below.

## Turn on maintenance mode when making planned changes

When you install patches, upgrade software, or deploy web applications, application control will detect them. Depending on your setting for how to handle unrecognized software, this could block that software until you use the **Actions** tab to create allow rules.

To avoid extra down time and alerts during deployment and maintenance windows, you can put application control into a mode designed for maintenance windows. While maintenance mode is enabled, application control will continue to enforce rules that block software, but it will allow new or updated software to run and automatically add it to the computer's inventory.

1. In Deep Security Manager, go to **Computers**.
2. Select one or more computers, then click **Actions > Turn On Maintenance Mode**.
3. Select the duration of your maintenance window.

   Maintenance mode will automatically disable itself when your maintenance window is scheduled to end. Alternatively, if you'd prefer to manually disable maintenance mode when updates are finished, select **Indefinite**.

   On the **Dashboard**, the **Application Control Maintenance Mode Status** widget indicates whether the command succeeded.

4. Install or upgrade software.
5. If you chose to disable maintenance mode manually, remember to disable maintenance mode in order to start to detect software changes again.

## Application control tips and considerations

- For better performance with application control, use Deep Security anti-malware instead of Windows Defender. See "Disable Windows Defender after installing Deep Security anti-malware on Windows Server 2016" on page 512.
- If you create a block rule for a batch file or PowerShell script, you will not be able to copy, move, or rename the file when using its associated interpreter (powershell.exe for PowerShell scripts or cmd.exe for batch files).
- If you add an allow or block rule, it is normally sent to the agent the next time the agent connects to Deep Security Manager. If you see an error saying that the ruleset upload was not successful, verify that network devices between the agent and the manager or relay allow communications on the heartbeat port number or relay port numbers.
- To verify that a block rule is working, try to run the software that you just blocked. (For details on how Deep Security Agent detects changes, see "What does application control detect as a software change?" on page 461)
- When blocked software remains installed, application control continues to record logs and show alerts when it blocks the software from running. To reduce the permission error logs on the computer and also reduce your attack surface, uninstall the software that application control is blocking. Once that is done, if you want to dismiss related alerts, either go to

**Alerts** or go to **Dashboard**, click the alert, and then click **Dismiss Alert**. Not all alerts can be dismissed. For more information, see "Predefined alerts" on page 903.

- For performance reasons, if the computer has too much software change, application control will continue to enforce existing rules, but stop detecting and displaying software changes. To resolve this, see "Reset application control after too much software change" on page 478.

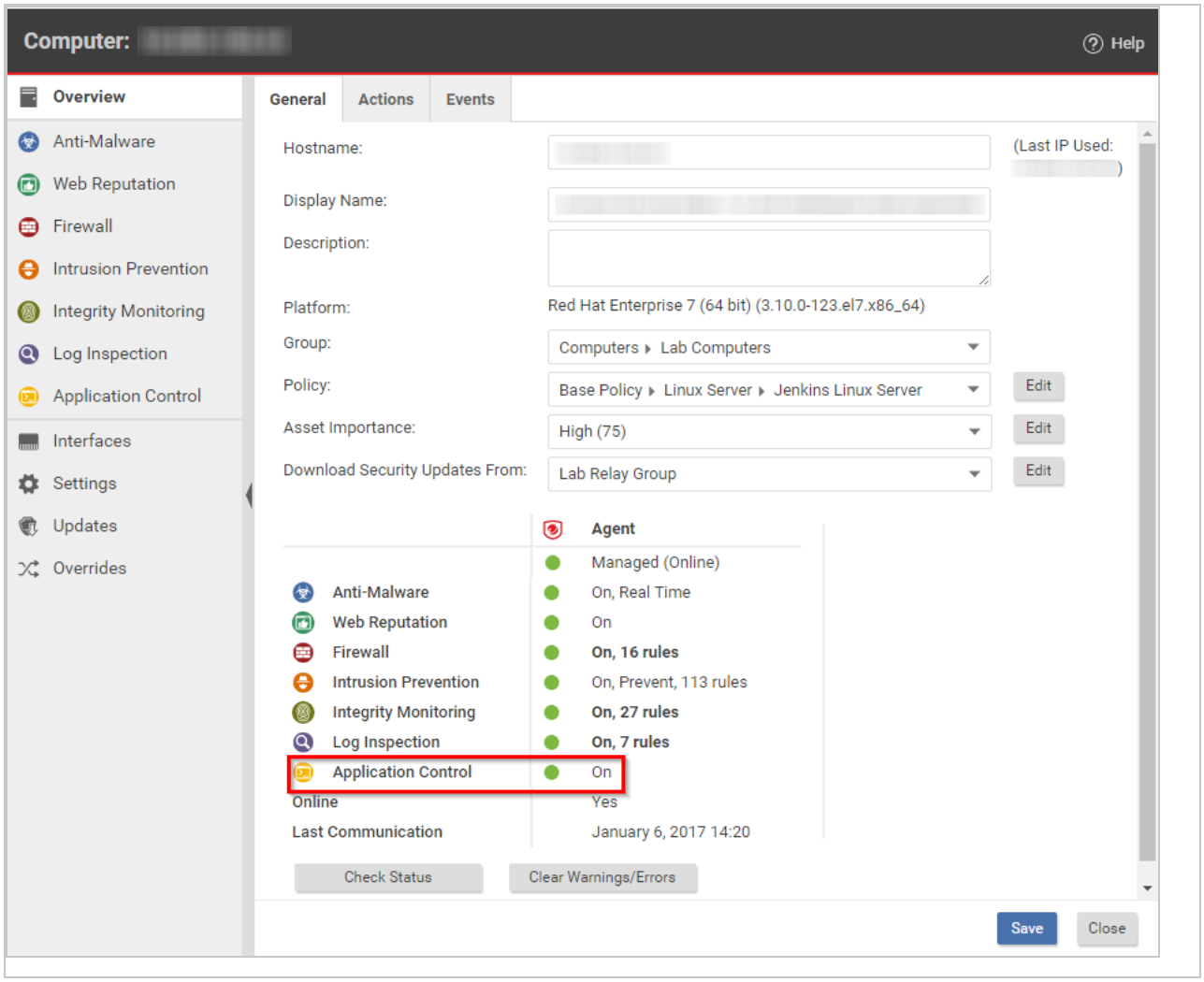
## Verify that application control is enabled

For an overview of application control, see "Lock down software with application control" on page 454. For initial configuration instructions, see "Set up application control" on page 463.

When application control is enabled and has finished its initial software inventory scan:

- The **State** field indicates "On" or "On, Blocking unrecognized software".
- On **Computers**, the **Status** field changes from "Application Control Ruleset Build In Progress" to "Managed (Online)".
- **Events & Reports > Events > System Events** will record "Application Control Ruleset Build Started" and "Application Control Ruleset Build Completed". (If you don’t see any

logs, see "Choose which application control events to log" on the next page.)




To verify that application control is working:

1. Copy an executable to the computer or add execute permissions to a plain text file. Try to run the executable.

   Depending on your enforcement setting for unrecognized software, it should be either blocked or allowed. Once application control has built initial allow rules or downloaded a shared ruleset, if any change is detected, it should appear in the **Actions** tab, which you can use to create allow and block rules (see "Monitor new and changed software" on page 464). Depending on your alert configuration, you will also see an alert if unrecognized software is detected, or if application control blocks software from launching (see "Monitor application control events" on the next page). The event should persist until

the software change no longer exists, or until the oldest data has been removed from the database.

2. Add an allow or block rule for your test software and then try again. This time, application control should apply your allow or block rule.

   Tip: If software is accidentally blocked because you've selected **Block unrecognized software until it is explicitly allowed** and the software isn't being recognized, the **Reason** column in application control event logs can help you to troubleshoot the cause.

## Monitor application control events

For an overview of application control, see "Lock down software with application control" on page 454. For initial configuration instructions, see "Set up application control" on page 463.

By default, when you enable application control it logs events, such as when there are software changes or when it blocks software from executing. Application control events appear on the **Actions** and **Events & Reports** pages. If configured, an alert appears on the **Alerts** page.

You can configure some of which application control event logs are recorded, and which are forwarded to external SIEM systems, or syslog servers.

To monitor for software changes on computers:

1. "Choose which application control events to log" below
2. "View application control event logs" on the next page
3. "Interpret aggregated security events" on the next page
4. "Monitor application control alerts" on page 473

### Choose which application control events to log

1. Go to **Administration > System Settings > System Events**.
2. Scroll down to the application control events such as Event ID 7000 "Application Control Events Exported".
3. If you want to record event logs for that type of event, select **Record**.

When those events occur, they appear on **Events & Reports > Events > System Events**. Logs are kept until they meet maximum log age criteria. For details, see "Event collection in Deep Security" on page 795.

> **Note:** Events that appear on **Computers > Details > Application Control > Events** are not configured here. They are always logged.

4. If you want to forward event logs to a SIEM, or syslog server, select **Forward**.
5. If you use an external SIEM, you may need to load the list of possible application control event logs, and indicate what action to take. For a list of application control events, see "System events" on page 918.

## View application control event logs

Application control generates system events and security events:

- **System event:** An audit event that provides a history of configuration changes or software updates. To see system events click **Events & Reports > Events > System Events**. For a list, see "System events" on page 918.
- **Security event:** An event that occurs on the agent when application control blocks or allows unrecognized software, or blocks software due to a block rule. To see security events, click **Events & Reports > Events > Application Control Events > Security Events**.

## Interpret aggregated security events

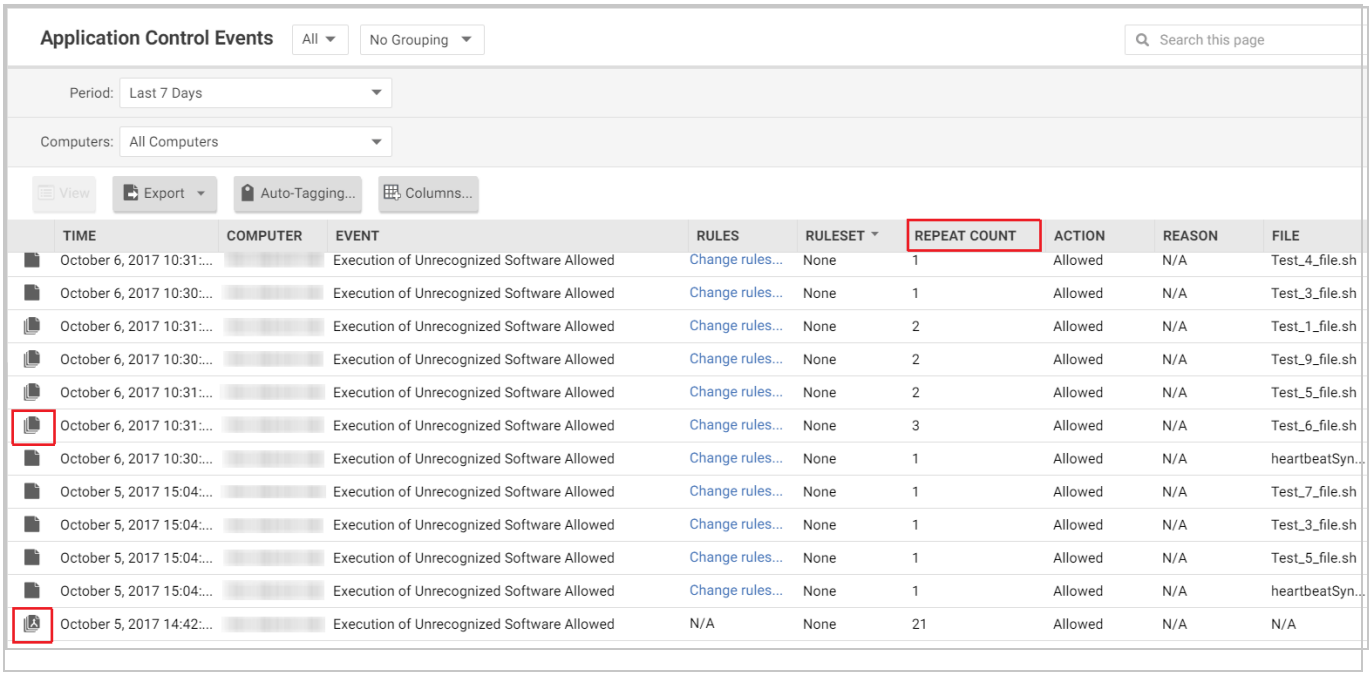
When an agent heartbeat includes several instances of the same security event, Deep Security aggregates the events in the Security Events log. Event aggregation reduces the number of items in the log, making it easier to find important events:

- When the event occurs for the same file, which is usually the case, the log includes the file name with the aggregated event. For example, a heartbeat includes 3 instances of the "Execution of Unrecognized Software Allowed" event for the Test_6_file.sh file, and no other instances of that event. Deep Security aggregates these 3 events for the file Test_6_file.sh.

- When the event occurs for many files, the log omits the file names. For example, a heartbeat includes 21 instances of the "Execution of Unrecognized Software Allowed" event that occurred for several different files. Deep Security aggregates the 21 events in a single event, but does not include a file name.

When aggregated events apply to multiple files, other occurrences of these events have likely been reported in other heartbeats. After you respond to other events where the file name is known, it is likely that no more aggregated events occur.

In the log, aggregated events use special icons, and the **Repeat Count** column indicates the number of events that are aggregated.



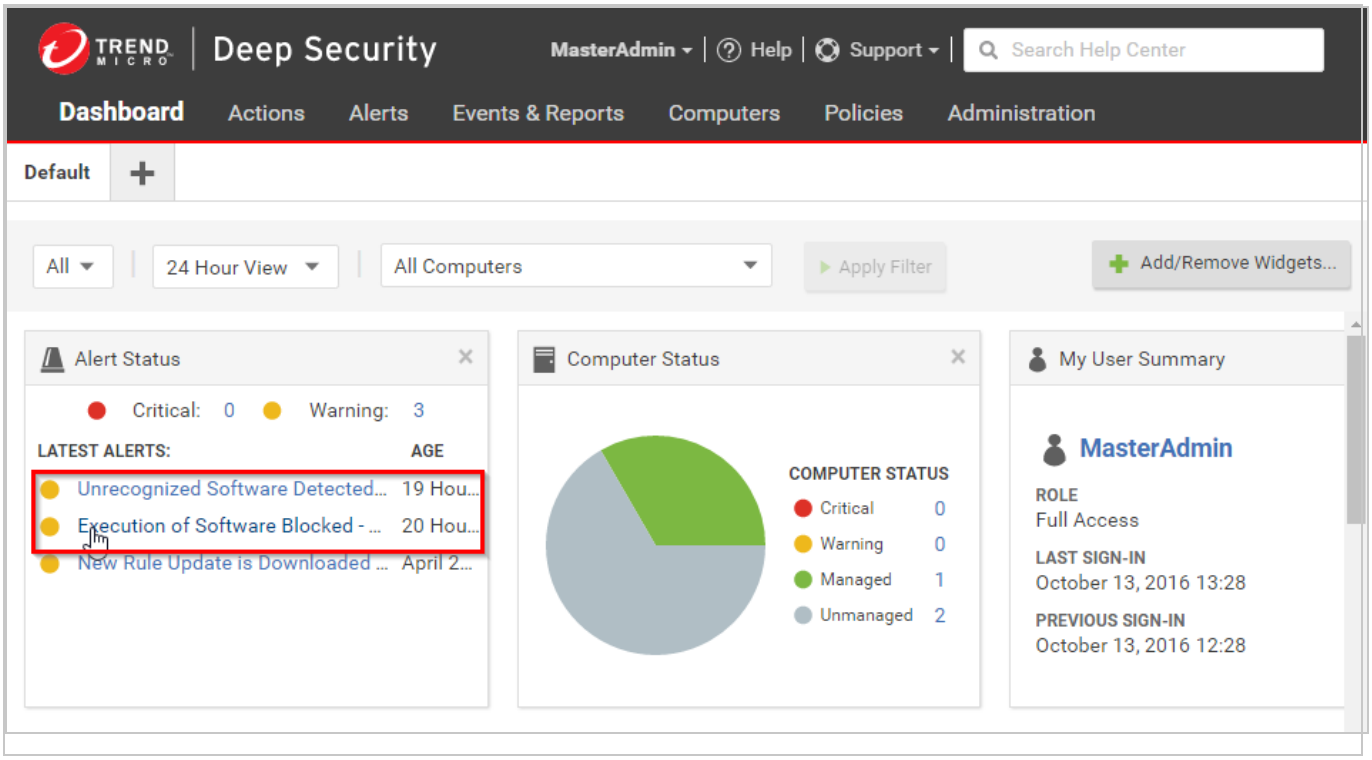

| TIME | COMPUTER | EVENT | RULES | RULESET | REPEAT COUNT | ACTION | REASON | FILE |
|---|---|---|---|---|---|---|---|---|
| October 6, 2017 10:31:... | | Execution of Unrecognized Software Allowed | Change rules... | None | 1 | Allowed | N/A | Test_4_file.sh |
| October 6, 2017 10:30:... | | Execution of Unrecognized Software Allowed | Change rules... | None | 1 | Allowed | N/A | Test_3_file.sh |
| October 6, 2017 10:31:... | | Execution of Unrecognized Software Allowed | Change rules... | None | 2 | Allowed | N/A | Test_1_file.sh |
| October 6, 2017 10:30:... | | Execution of Unrecognized Software Allowed | Change rules... | None | 2 | Allowed | N/A | Test_9_file.sh |
| October 6, 2017 10:31:... | | Execution of Unrecognized Software Allowed | Change rules... | None | 2 | Allowed | N/A | Test_5_file.sh |
| October 6, 2017 10:31:... | | Execution of Unrecognized Software Allowed | Change rules... | None | 3 | Allowed | N/A | Test_6_file.sh |
| October 6, 2017 10:30:... | | Execution of Unrecognized Software Allowed | Change rules... | None | 1 | Allowed | N/A | heartbeatSyn... |
| October 5, 2017 15:04:... | | Execution of Unrecognized Software Allowed | Change rules... | None | 1 | Allowed | N/A | Test_7_file.sh |
| October 5, 2017 15:04:... | | Execution of Unrecognized Software Allowed | Change rules... | None | 1 | Allowed | N/A | Test_3_file.sh |
| October 5, 2017 15:04:... | | Execution of Unrecognized Software Allowed | Change rules... | None | 1 | Allowed | N/A | Test_5_file.sh |
| October 5, 2017 15:04:... | | Execution of Unrecognized Software Allowed | Change rules... | None | 1 | Allowed | N/A | heartbeatSyn... |
| October 5, 2017 14:42:... | | Execution of Unrecognized Software Allowed | N/A | None | 21 | Allowed | N/A | N/A |

## Monitor application control alerts

To configure which application control events or severity levels cause an alert, go to the **Alerts** tab, click the **Configure Alerts** button, and then select an event and double-click **Properties**. For details, see "Configure alerts" on page 781.

When alerts are enabled for application control events, any software change that the application control engine detects and any software that it blocks from executing appear in the **Alerts** tab. If

you have enabled the **Alert Status** widget, application control alerts also appear on the Dashboard.




To monitor which computers are in maintenance mode, you can also click **Add/Remove Widgets** and enable the **Application Control Maintenance Mode** widget, which displays a list of the computers and their scheduled maintenance windows.

## View and change application control rulesets

Each computer has its own application control ruleset. You can:

- "View application control rulesets" on the next page and find out which rules they include.

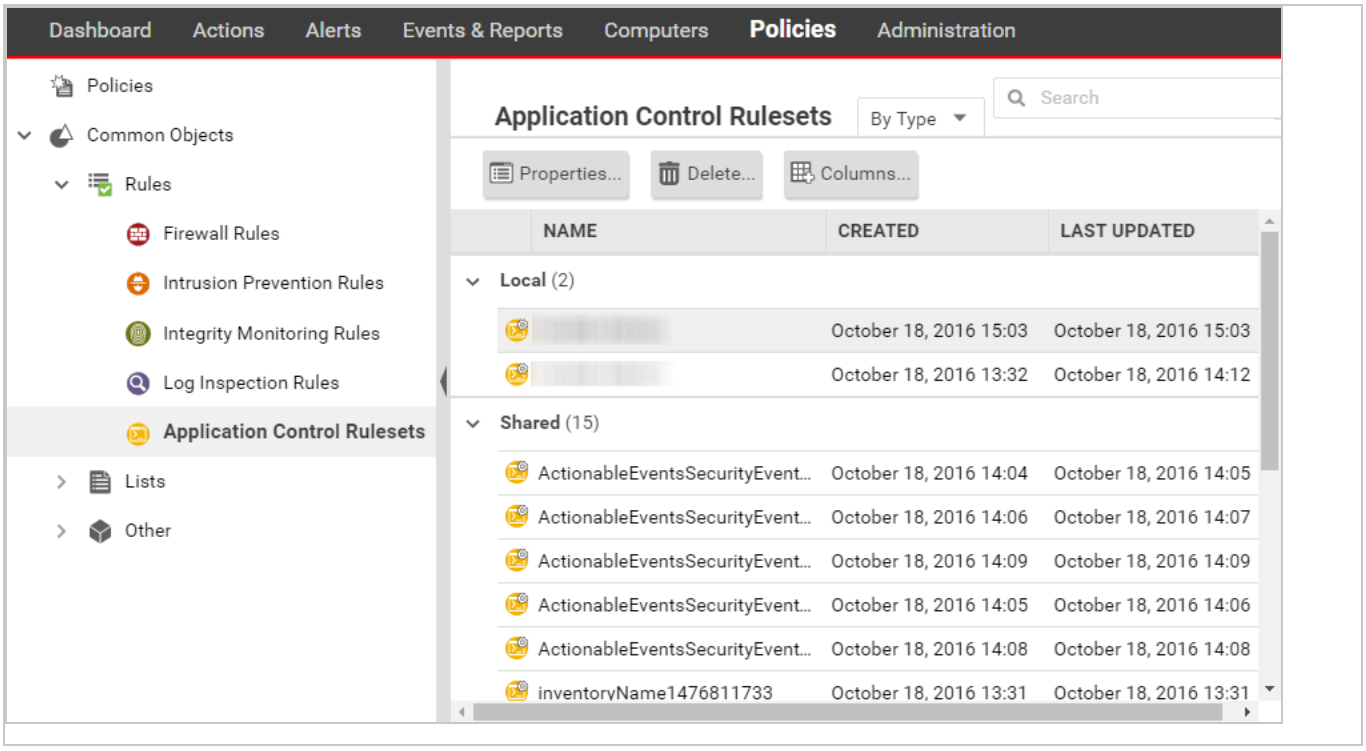
  **Tip:** When you first enable application control for a computer, the software installed on the computer is added to the computer's inventory and allowed to run. However, you cannot see the rules associated with the inventory from Deep Security Manager unless you use the Deep Security API to do so (see "Use the API to create shared and global rulesets " on page 479). In Deep Security Manager, a computer's ruleset appears empty until you create some allow/block rules for the computer.

- "Change the action for an application control rule" on the next page if a software file should no longer be allowed/blocked.
- "Delete an individual application control rule" on page 478 if the software has been removed and isn't likely to return.
- "Delete an application control ruleset" on page 478 if the computer associated with the ruleset has been removed.

**Tip:** If a user reports that application control is blocking software that they need to run on a particular computer, you can undo the block rule on that computer. Go to **Events & Reports > Application Control Events > Security Events**, find the computer, locate the block event, and then click **View Rules**. In the pop-up that appears, you can change the block rule to an allow rule.

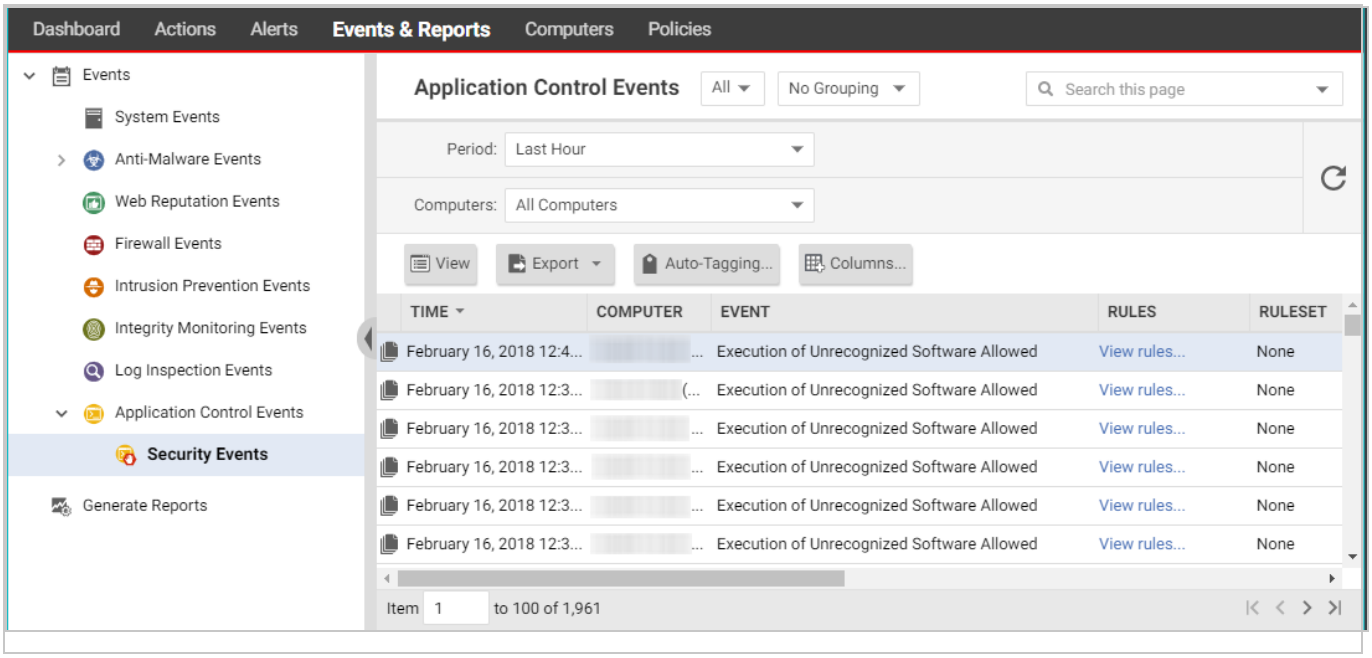
## View application control rulesets

To view the list of application control rulesets, go to **Policies > Common Objects > Rules > Application Control Rulesets**.



To see which rules are part of a ruleset, double-click the ruleset and go to the **Rules** tab. The Rules tab displays the software files that have rules associated with them and enables you to change allow rules to block, and vice versa. (See "Change the action for an application control rule" below.)

### Security Events




**Events & Reports > Events > Application Control Events > Security Events** displays all unrecognized software that either has been run on a computer or has been actively blocked from running. You can filter this list by time period and other criteria.

For each event (except aggregated events), you can click **View rules** to change the rule from Allow to Block or vice versa.

Deep Security Agent 10.2 or later includes event aggregation logic to reduce the volume of logs when the same event occurs repeatedly. (See "Interpret aggregated security events" on page 472.)

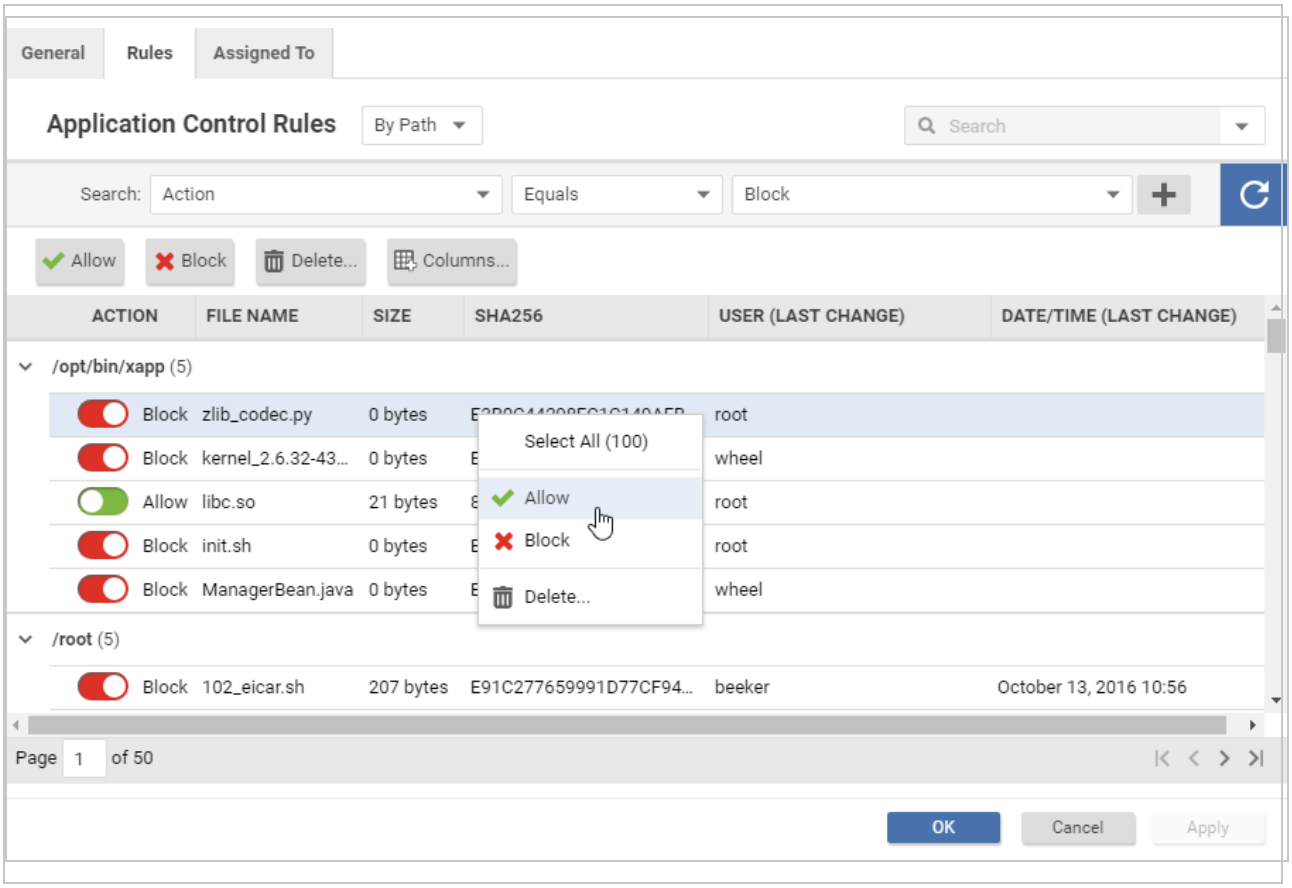
## Change the action for an application control rule

If you want to allow a software that you previously blocked (or the opposite), you can edit the action in the rule. If you need to undo the rule so that the software is not recognized by

application control (in other words, delete the rule, not only change its action), see "Delete an individual application control rule" on the next page instead.

1. Go to **Policies > Common Objects > Rules > Application Control Rulesets**.
2. Double-click to select the ruleset that contains the rule that you want to change.
3. On the pop-up window that appears, go to the **Rules** tab.
4. If you want to focus on software that was blocked (or allowed), then in the menu next to **Application Control Rules**, select **By Action** or **By Path** to group similar rules. Alternatively, you can use the search to filter the list.

   If you want to change the action for a software file, but it has multiple different file names or paths, select **By File Name** or **By Path** to group related rules.




5. Find the row for the specific software that you want to allow or block.
6. In the **Action** column, change the setting to allow or block, then click **OK**.

The next time that the agent connects with Deep Security Manager, the rule will be updated, and the version number will increase.

## Delete an individual application control rule

If you want to undo a rule that you created, go to **Policies > Common Objects > Rules > Application Control Rulesets**, double-click the ruleset that contains the rule, go to the **Rules** tab, select the rule and then click **Delete**.

Some things to keep in mind:

- When the rules are not needed anymore, you can delete them to reduce the size of the ruleset. This improves performance by reducing RAM and CPU usage.
- If you delete a rule, application control will not recognize the software anymore. If the software is installed again, it will appear again on the **Actions** tab.
- If a software update is unstable and you might need to downgrade, keep rules that allow rollback to the previous software version until you have completed testing.
- To find the oldest rules, go to **Policies > Rules > Application Control Rulesets**, then click **Columns**. Select **Date/Time (Last Change)**, click **OK**, and then click that column's header to sort by date.

## Delete an application control ruleset

If an application control ruleset is not being used anymore (for example, if the computer associated with the ruleset no longer exists), you can delete it.

To delete a ruleset, go to **Policies > Rules > Application Control Rulesets**, click a ruleset to select it, and click **Delete**.

# Reset application control after too much software change

For an overview of application control, see "Lock down software with application control" on page 454.

Application control is intended for use on stable servers that are not updated frequently, and not for workstations or servers that undergo a lot of software changes.

Too many changes make large rulesets that consume more RAM, unless you remove old rules. If you don't use maintenance mode during authorized software updates, too many changes can also result in high administrator workload because they must manually create allow rules for each change.

**If unrecognized software changes exceed the maximum, application control will stop detecting and displaying all of the computer's software changes.** This stoppage is designed to prevent out-of-memory and disk space errors that can occur if the ruleset grows too large.

When a stoppage occurs, Deep Security Manager will notify you through an alert ("Unresolved software change limit") and an event log ("Unresolved software change limit reached"). You must resolve the issue to continue detecting software changes.

1. Examine the computer's processes and security events. Verify that the computer has not been compromised. If you are not sure, or do not have enough time, the safest and fastest way is to restore the system from a backup or VM snapshot.

   **Warning:** If you don't remove any unauthorized software (including zero-day malware), application control will ignore it when you reset application control. It won't appear on the Actions tab anymore and if its process has already executed and it is in RAM, application control won't log any events or alerts about it until you reboot the computer.

2. If the computer was running software updates, including auto-updates (for example, browser, Adobe Reader, or yum auto-updates), disable them or schedule them so that they occur only when you have enabled application control's maintenance mode (see "Turn on maintenance mode when making planned changes" on page 467).
3. Reset application control. To do this, disable application control in the **Computer editor**[1]. Once the agent has acknowledged it and cleared the error status, enable application control again. The agent generates a new software inventory allow list.

## Use the API to create shared and global rulesets

For an overview of application control, see "Lock down software with application control" on page 454. For initial configuration instructions, see "Set up application control" on page 463.

---

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

Using the Deep Security Manager interface, you can create a local, individual ruleset for each computer that you are protecting. Using the Deep Security API, you can also create shared rulesets and global rulesets. You can use one type of ruleset, or a combination.

- **Local ruleset:** Rules that are added as part of a computer's software inventory or when in maintenance mode are stored only on the protected computer and are not visible in Deep Security Manager. Allow or block rules that you configure in Deep Security Manager are sent to the agent and stored in both places. Because agents don't transfer their inventory information to the manager, local rulesets offer better performance than shared rulesets.

  To determine whether software is new or has changed, Deep Security 10.x agents compare the file with the initially installed software's SHA-256 hash, file size, path, and file name (they have a "file-based" local ruleset). Deep Security 11.x agents compare only the file's SHA-256 hash and file size (they have a "hash-based" local ruleset). Because the rules created by Deep Security 11.x agents compare only the unique hash and file size, a rule will continue to be applied even if the software file is renamed or moved. As a result, using Deep Security 11.x agents reduces the number of software changes that you need to deal with. A Deep Security 10.x agent continues to use a file-based local ruleset until it is upgraded to Deep Security 11.0 or newer. When you upgrade an agent to version 11.0 or newer, its local ruleset is converted to use hash-based rules.

  **Note:** If there are multiple file-based rules for the same hash value, they are consolidated into one hash-based rule. If the rules being consolidated conflict with each other (one rule blocks the file and another allows it), the new hash-based rule will be an "allow" rule.

- **Shared ruleset:** Syncs all of its rule data onto both agents and manager (and also relays, if enabled). This increases network and disk space usage. However, it may be easier if you need to verify the rules from the initial inventory scan or maintenance mode, or if you manage a server farm with many computers that should be identical. For example, if you have a server pool of identical LAMP web servers, or if they are virtual machines (VMs) that are part of an auto-scaling group, shared rulesets can be useful. It can also reduce administrator workload. To create a shared ruleset, see "Create a shared ruleset" on page 482.

> **Warning:** Don't use a shared ruleset if you enabled **Block unrecognized software until it is explicitly allowed**, and if computers are merely similar (but not identical). It will block all software on other computers that isn't in the first computer's ruleset. If those include critical files, it could break the OS. If that happens, you may be required to reinstall, revert to a backup, or use the OS recovery mode.

When you create a new shared ruleset using Deep Security 11.1 or newer, it can only contain hash-based rules (rules that compare only a file's hash and size). If you created a shared ruleset using Deep Security 11.0 or earlier, it contains file-based rules (rules that compare a file's name, path, size, and hash). Older shared rulesets will continue to use file-based rules until all agents using the shared ruleset are upgraded to Deep Security Agent 11.0 or newer. When all agents are version 11.0 or newer, the shared ruleset will be converted to use hash-based rules.

> **Warning:** Don't create a new shared ruleset unless all agents using the ruleset are version 11.0 or newer. New shared rulesets are hash-based and are not compatible with 10.3 or earlier agents, which support only file-based rulesets.

> **Note:** If there are multiple file-based rules for the same hash value, they are consolidated into one hash-based rule. If the rules being consolidated conflict with each other (one rule blocks the file and another allows it), the new hash-based rule will be an "allow" rule.

- **Global ruleset:** Like shared rulesets, global rulesets are distributed to agents by the manager (and also relays, if enabled). This increases network and disk space usage. However, because they are global, you don't need to spend time selecting them in each policy. Global rules aren't part of the rulesets you can see in Deep Security Manager. To view them, use the API. (See "Use the Deep Security API to automate tasks" on page 261.) Global rulesets can only contain block rules, not allow rules.

  Global rulesets require Deep Security Agent 10.2 or newer. The manager will not send the global ruleset to older agents. Global rulesets take precedence over all other application control rules and are enforced on all computers where application control is enabled. The rules in global rulesets are based on a file's SHA-256 hash. Because a software file's hash

is unique, you can block specific software everywhere - regardless of file path, policy, or computer group, and regardless of whether application control has detected the software before.

**Note:** In a multi-tenant deployment, each tenant has a separate global ruleset. To block software for all tenants, create the same global rules for each tenant.

In this article:


- "Create a shared ruleset" below
- "Change from shared to computer-specific allow and block rules" on the next page
- "Deploy application control shared rulesets via relays" on page 484
- "Considerations when using relays with share rulesets" on page 485


## Create a shared ruleset

You can use the API to create shared allow or block rules and apply the ruleset to other computers. This can be useful if you have many identical computers (such as a load balanced web server farm). **Shared rulesets should be applied only to computers with the exact same inventory.**

1. Use the API to build a computer's shared allow and block rules. For more information, see "Use the Deep Security API to automate tasks" on page 261. If you want to examine the shared ruleset before you deploy it, see "View and change application control rulesets" on page 474.
2. Go to **Computer or Policy editor**[1] > **Application Control**.
3. In the ruleset section, make sure **Inherit settings** is not selected and then select **Use a shared ruleset**. Indicate which shared rules to use.

   **Note:** These settings are hidden until you use the API to create at least one shared

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

ruleset. If you haven't created any shared rulesets, or if you keep the default settings, each computer will keep its own allow and block rules locally. Changes to local rules don't affect other computers.

4. Click **Save**.

   The next time that the Deep Security Agent on the computer connects with Deep Security Manager, the agent applies those rules.

   If you see an error saying that the ruleset upload was not successful, verify that network devices between the agent and the manager or relay allow communications on the heartbeat port number or relay port numbers.

## Change from shared to computer-specific allow and block rules

If the computer is currently using shared allow or block rules created via the API, you can change it to use local rules. Application control will scan the file system for all currently installed software and create an initial ruleset for it, similarly to when you first enabled application control.

**Warning:** Before you start, verify that only good software is currently installed. Rebuilding the ruleset will allow all currently installed software, even if it is insecure or malware. If you are not sure what is installed, the safest approach is to make a clean install and then enable application control.

The steps below configure a computer's agent to use a local ruleset. If you want all computers to use local rules, edit the setting in the **Policies** tab instead.

1. Go to **Computer editor**[1] > **Application Control**.
2. In the ruleset section, deselect **Inherit settings** (if necessary), and then select **Use local ruleset initially based on installed software**.
3. Click **Save**.

   To verify the change, the next time the agent and Deep Security Manager connect, look for event log messages about building the application control ruleset.

---

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

## Deploy application control shared rulesets via relays

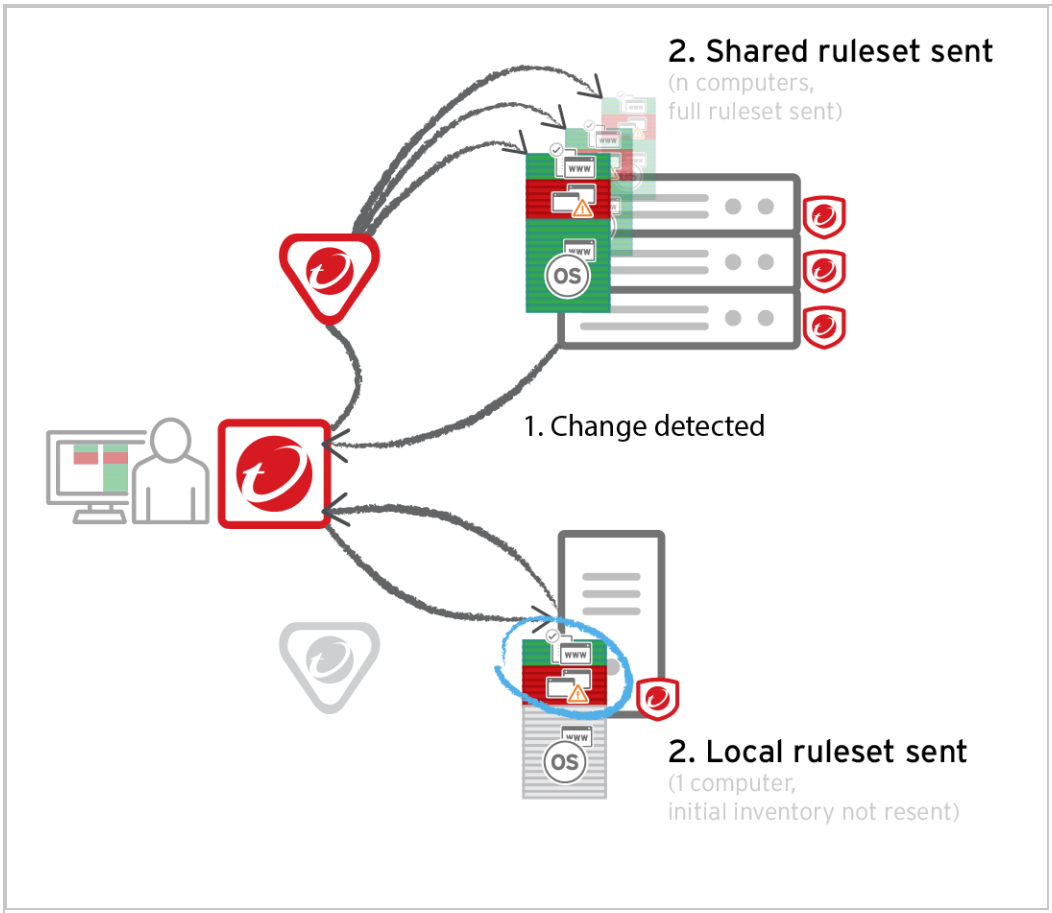
Each time you create an application control ruleset or change it, it must be distributed to all computers that use it. Shared rulesets are bigger than local rulesets. Shared rulesets are also often applied to many servers. If they all downloaded the ruleset directly from the manager at the same time, high load could cause slower performance. Global rulesets have the same considerations.

Using Deep Security Relays can solve this problem. (For information on configuring relays, see "Distribute security and software updates with relays" on page 234.)

Steps vary depending whether or not you have a multi-tenant deployment.

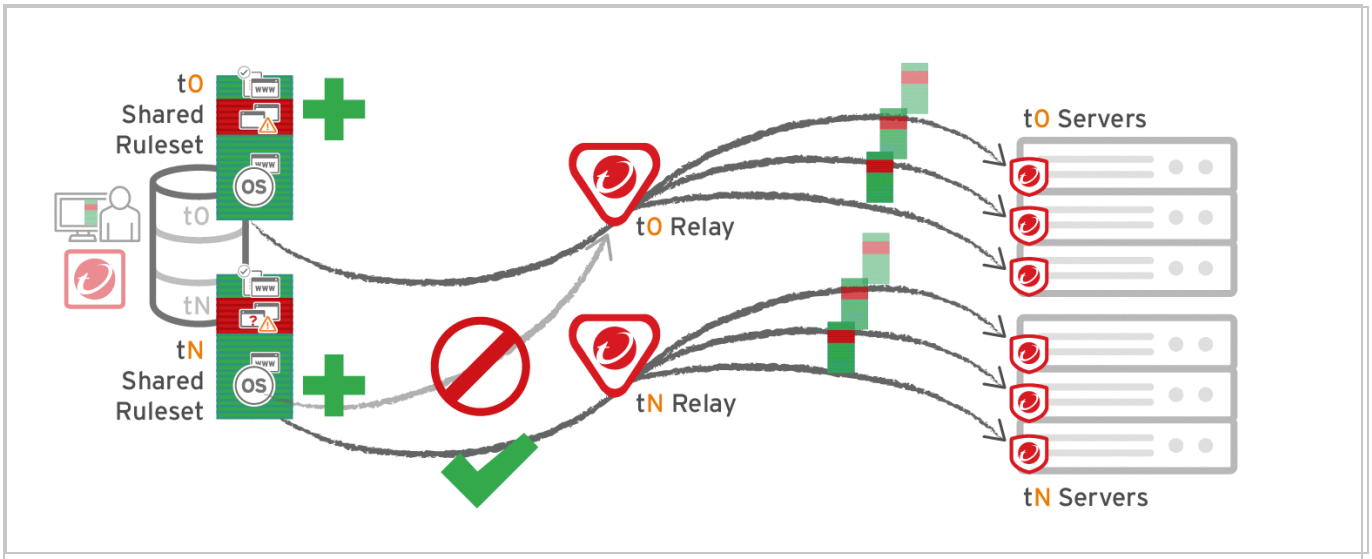
### Single tenant deployments

Go to **Administration > System Settings > Advanced** and then select **Serve application control rulesets from relays**.



### Multi-tenant deployments

The primary tenant (t0) can't access other tenants' (tN) configurations, so t0 relays don't have tN application control rulesets. Other tenants (Tn) must create their own relay group, then select **Serve application control rulesets from relays**.




## Considerations when using relays with share rulesets

Before using relays, verify that they are compatible with your deployment. If the agent doesn't have any previously downloaded ruleset currently in effect, and **if it doesn't receive new application control rules, then the computer won't be protected by application control.** If application control ruleset download fails, a ruleset download failure event will be recorded on the manager and on the agent.

- If you are using a proxy to connect agents to a manager, you must use a relay.

  **Note:** In Deep Security Agent 10.0 GM and earlier, agents didn't have support for connections through a proxy to relays. If a ruleset download fails due to a proxy, and if your agents require a proxy to access the relay or manager (including Deep Security as a Service), then you must either:

  - update agents' software, then configure the proxy
  - bypass the proxy

- add a relay and then select **Serve application control rulesets from relays**

- If you are using shared or global rulesets, a relay can result in faster performance.
- If you are using local rulesets, a relay can cause slower performance,
- Do not use a relay with multi-tenant configurations when non-primary tenants (tN) use the default, primary (t0) relay group.

# Protect against malware

The Deep Security anti-malware module provides agent computers with both real-time and on-demand protection against file-based threats, including malware, viruses, Trojans, and spyware. To identify threats, the anti-malware module checks files on the local hard drive against a comprehensive threat database. The anti-malware module also checks files for certain characteristics, such as compression and known exploit code.

Portions of the threat database are hosted on Trend Micro servers or are stored locally as patterns. Deep Security Agents periodically download anti-malware patterns and updates to ensure protection against the latest threats.

**Note:** A newly installed Deep Security Agent cannot provide anti-malware protection until it has contacted an update server to download anti-malware patterns and updates. Ensure that your Deep Security Agents can communicate with a Deep Security Relay or the Trend Micro Update Server after installation.

The anti-malware module eliminates threats while minimizing the impact on system performance. The anti-malware module can clean, delete, or quarantine malicious files. It can also terminate processes and delete other system objects that are associated with identified threats.

To turn on and configure the anti-malware module, see "Enable and configure anti-malware" on page 494.

- "Types of malware scans" on the next page
- "Malware scan configurations" on page 489

- "Malware events" on page 489
- "SmartScan" on page 490
- "Predictive Machine Learning" on page 490
- "Types of malware scans" below


## Types of malware scans

The anti-malware module performs several types of scans. See also "Select the types of scans to perform" on page 495.

### Real-time scan

Scan immediately each time a file is received, opened, downloaded, copied, or modified, Deep Security scans the file for security risks. If Deep Security detects no security risk, the file remains in its location and users can proceed to access the file. If Deep Security detects a security risk, it displays a notification message that shows the name of the infected file and the specific security risk.

Real-time scans are in effect continuously unless another time period is configured using the Schedule option.

> **Tip:** You can configure real-time scanning to run when it will not have a large impact on performance; for example, when a file server is scheduled to back up files.

This scan can run on all platforms supported by the anti-malware module.

### Manual scan

Runs a full system scan on all processes and files on a computer. The time required to complete a scan depends on the number of files to scan and the computer's hardware resources. A manual scan requires more time than a Quick Scan.

A manual scan executes when **Full Scan for Malware** is clicked.

This scan can be run on all platforms supported by the anti-malware module.

## Scheduled scan

Runs automatically on the configured date and time. Use scheduled scan to automate routine scans and improve scan management efficiency.

A scheduled scan runs according to the date and time you specify when you create a **Scan computers for Malware task** using scheduled tasks (see "Schedule Deep Security to perform tasks" on page 263).

This scan can be run on all platforms supported by the anti-malware module.

## Quick scan

Only scans a computer's critical system areas for currently active threats. A Quick Scan will look for currently active malware but it will not perform deep file scans to look for dormant or stored infected files. It is significantly faster than a Full Scan on larger drives. Quick scan is not configurable.

A Quick Scan runs when you click **Quick Scan for Malware**.

> **Note:** Quick Scan can run only on Windows computers.

## Scan objects and sequence

The following table lists the objects scanned during each type of scan and the sequence in which they are scanned.

| Targets | Full Scan (Manual or Scheduled) | Quick Scan |
|---|---|---|
| Drivers | 1 | 1 |
| Trojan | 2 | 2 |
| Process Image | 3 | 3 |
| Memory | 4 | 4 |
| Boot Sector | 5 | - |

| Targets | Full Scan (Manual or Scheduled) | Quick Scan |
|---|---|---|
| Files | 6 | 5 |
| Spyware | 7 | 6 |

## Malware scan configurations

Malware scan configurations are sets of options that control the behavior of malware scans. When you configure anti-malware using a policy or for a specific computer, you select a malware scan configuration to use. You can create several malware scan configurations and use them with different policies when different groups of computers have different scan requirements.

Real-time, manual, and scheduled scans all use malware scan configurations. Deep Security provides a default malware scan configuration for each type of scan. These scan configurations are used in the default security policies. You can use the default scan configurations as-is, modify them, or create your own.

**Note:** Quick Scans are not configurable, and do not use malware scan configurations.

You can specify which files and directories are included or excluded during a scan and which actions are taken if malware is detected on a computer (for example, clean, quarantine, or delete).

For more information, see "Configure malware scans" on page 497.

## Malware events

When Deep Security detects malware it triggers an event that appears in the event log. From there you can see information about the event, or create an exception for the file in case of false positives. You can also restore quarantined files that are actually benign. (See "Anti-malware events" on page 942 and "Handle malware" on page 525.)

## SmartScan

Smart Scan uses threat signatures that are stored on Trend Micro servers and provides several benefits:

- Provides fast, cloud-based, real-time security status lookups
- Reduces the time required to deliver protection against emerging threats
- Reduces network bandwidth consumed during pattern updates (bulk of pattern definition updates only need to be delivered to the cloud, not to many computers)
- Reduces cost and overhead of corporate-wide pattern deployments
- Lowers kernel memory consumption on computers (consumption increases minimally over time)

When Smart Scan is enabled, Deep Security first scans locally for security risks. If Deep Security cannot assess the risk of the file during the scan, it will try to connect to a local Smart Scan server. If no local Smart Scan Server is detected, Deep Security will attempt to connect to the Trend Micro Global Smart Scan server. For more information on this feature, see "Smart Protection in Deep Security" on page 522.

## Predictive Machine Learning

Deep Security provides enhanced malware protection for unknown threats and zero-day attacks through Predictive Machine Learning. Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging security risks through digital DNA fingerprinting, API mapping, and other file features.

Predictive Machine Learning is effective in protecting against security breaches that result from targeted attacks using techniques such as phishing and spear phishing. In these cases, malware that is designed specifically to target your environment can bypass traditional malware scanning techniques.

During real-time scans, when Deep Security detects an unknown or low-prevalence file, Deep Security scans the file using the Advanced Threat Scan Engine (ATSE) to extract file features. It then sends the report to the Predictive Machine Learning engine which is hosted on the Trend

Micro Smart Protection Network. Through the use of malware modeling, Predictive Machine Learning compares the sample to the malware model, assigns a probability score, and determines the probable malware type that the file contains.

If the file is identified as a threat, Deep Security quarantines the file to prevent the threat from continuing to spread across your network.

For information about using Predictive Machine Learning, see "Detect emerging threats using Predictive Machine Learning" on page 513.

## Malware types

The anti-malware module protects against many file-based threats. See also "Scan for specific types of malware" on page 498 and "Configure how to handle malware" on page 507

### Virus

Viruses infect files by inserting malicious code. Typically, when an infected file is opened the malicious code automatically runs and delivers a payload in addition to infecting other files. Below are some of the more common types of viruses:

- **COM and EXE infectors** infect DOS and Windows executable files, which typically have COM and EXE extensions.
- **Macro viruses** infect Microsoft Office files by inserting malicious macros.
- **Boot sector viruses** infect the section of hard disk drives that contain operating system startup instructions

The anti-malware module uses different technologies to identify and clean infected files. The most traditional method is to detect the actual malicious code that is used to infect files and strip infected files of this code. Other methods include regulating changes to infectable files or backing up such files whenever suspicious modifications are applied to them.

### Trojans

Some malware does not spread by injecting code into other files. Instead, it has other methods or effects:

- **Trojans:** Malware files that execute and infect the system when opened (like the mythological Trojan horse).
- **Backdoors:** Malicious applications that open port numbers to allow unauthorized remote users to access infected systems.
- **Worms:** Malware programs that use the network to propagate from system to system. Worms are known to propagate by taking advantage of social engineering through attractively packaged email messages, instant messages, or shared files. They are also known to copy themselves to accessible network shares and spread to other computers by exploiting vulnerabilities.
- **Network viruses:** Worms that are memory-only or packet-only programs (not file-based). Anti-malware is unable to detect or remove network viruses.
- **Rootkits:** File-based malware that manipulate calls to operating system components. Applications, including monitoring and security software, need to make such calls for very basic functions, such as listing files or identifying running processes. By manipulating these calls, rootkits are able to hide their presence or the presence of other malware.

## Packer

Packers are compressed and encrypted executable programs. To evade detection, malware authors often pack existing malware under several layers of compression and encryption. Anti-malware checks executable files for compression patterns associated with malware.

## Spyware/grayware

Spyware and grayware comprises applications and components that collect information to be transmitted to a separate system or collected by another application. Spyware/grayware detections, although exhibiting potentially malicious behavior, may include applications used for legitimate purposes such as remote monitoring. Spyware/grayware applications that are inherently malicious, including those that are distributed through known malware channels, are typically detected as other Trojans.

Spyware and grayware applications are typically categorized as:

- **Spyware:** software installed on a computer to collect and transmit personal information.
- **Dialers:** malicious dialers are designed to connect through premium-rate numbers causing unexpected charges. Some dialers also transmit personal information and download malicious software.
- **Hacking tools:** programs or sets of programs designed to assist unauthorized access to computer systems.
- **Adware (advertising-supported software):** any software package that automatically plays, displays, or downloads advertising material.
- **Cookies:** text files stored by a Web browser. Cookies contain website-related data such as authentication information and site preferences. Cookies are not executable and cannot be infected; however, they can be used as spyware. Even cookies sent from legitimate websites can be used for malicious purposes.
- **Keyloggers:** software that logs user keystrokes to steal passwords and other private information. Some keyloggers transmit logs to remote systems.

### What is grayware?

Although they exhibit what can be intrusive behavior, some spyware-like applications are considered legitimate. For example, some commercially available remote control and monitoring applications can track and collect system events and then send information about these events to another system. System administrators and other users may find themselves installing these legitimate applications. These applications are called "grayware".

To provide protection against the illegitimate use of grayware, the anti-malware module detects grayware but provides an option to "approve" detected applications and allow them to run.

## Cookie

Cookies are text files stored by a web browser, transmitted back to the web server with each HTTP request. Cookies can contain authentication information, preferences, and (in the case of stored attacks from an infected server) SQL injection and XSS exploits.

### Other threats

Other threats includes malware not categorized under any of the malware types. This category includes joke programs, which display false notifications or manipulate screen behavior but are generally harmless.

### Possible malware

Possible malware is a file that appears suspicious but cannot be classified as a specific malware variant. When possible malware is detected, Trend Micro recommends that you contact your support provider for assistance in further analysis of the file. By default, these detections are logged and files are anonymously sent back to Trend Micro for analysis.

## Enable and configure anti-malware

To use anti-malware, perform these basic steps:

1. "Turn on the anti-malware module" on the next page.
2. "Select the types of scans to perform" on the next page.
3. "Configure scan exclusions" on the next page
4. "Ensure that Deep Security can keep up to date on the latest threats" on page 496.

When you have completed these steps, review "Configure malware scans" on page 497 and refine the anti-malware scan behavior.

**Tip:** For most anti-malware settings, you can either configure them for each individual computer or in a policy that applies to multiple computers (for example, to all Windows 2008 Servers). To make management easier, configure the settings in the policy (not individual computers) wherever possible. For more information, see "Policies, inheritance, and overrides" on page 354.

**Tip:** CPU usage and RAM usage varies by your anti-malware configuration. To optimize anti-malware performance on Deep Security Agent, see "Performance tips for anti-malware" on page 510.

For an overview of the anti-malware feature, see "Protect against malware" on page 486.

## Turn on the anti-malware module

1. Go to **Policies**.
2. Double-click the policy for which you want to enable anti-malware.
3. Go to **Anti-Malware > General**.
4. From **Anti-Malware State**, select **On**.
5. Click **Save**.

## Select the types of scans to perform

When anti-malware is turned on, Deep Security needs to know what type of scans it should perform (see "Types of malware scans" on page 487).

1. Go to **Policies**.
2. Double-click the policy to configure.
3. Click **Anti-Malware > General**.
4. Enable or disable each type of scan:
   a. To perform the scan using default settings, select **Default**.
   b. To perform the scan using a malware scan configuration that you can customize, select a malware scan configuration.
   c. To disable the scan, for the malware scan configuration select **No Configuration**.
5. Click **Save**.

**Tip:** Trend Micro recommends that you configure Deep Security to perform weekly scheduled scans on all protected servers. You can do this using Scheduled Tasks. (See "Schedule Deep Security to perform tasks" on page 263.)

## Configure scan exclusions

To reduce scanning time and minimize the use of computing resources, you can configure Deep Security malware scans to exclude specific folders, files, and file types from all types of scans. You can also exclude process image files from real-time malware scans that are run on Windows servers.

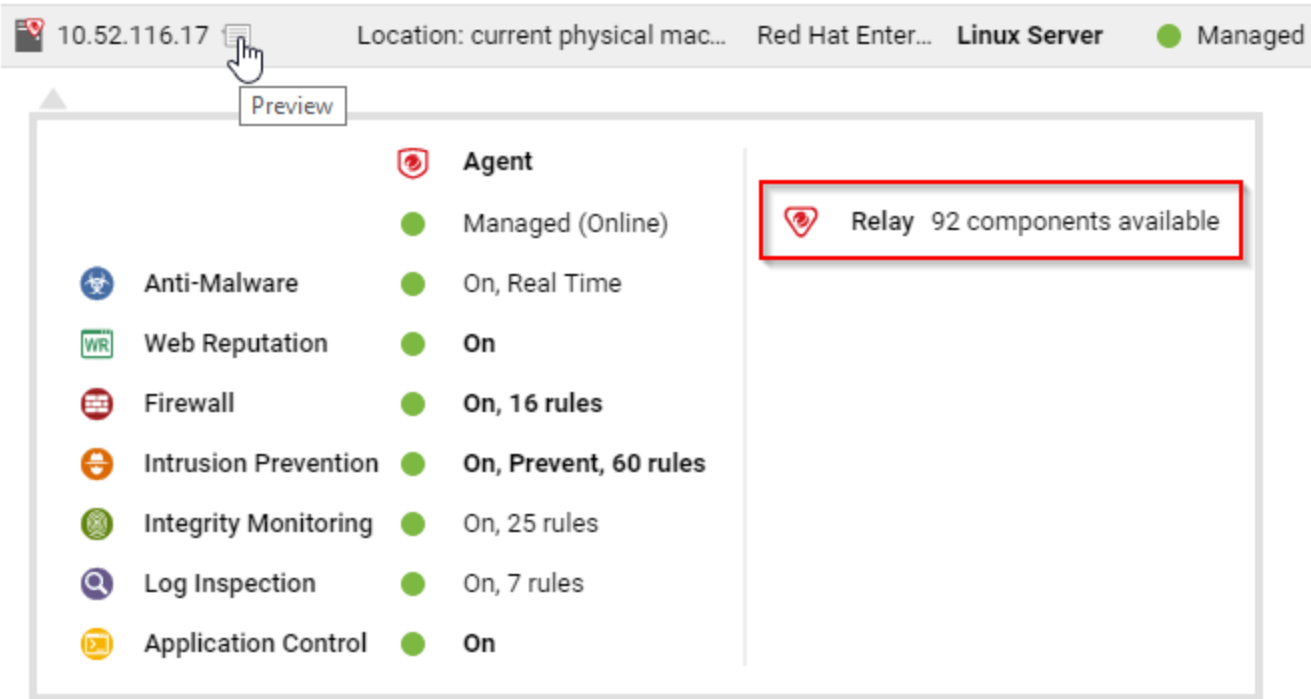
All of these exclusions are specified by selecting exclusion lists on the **Exclusions** tab of the Malware Scan Configuration editor. See "Specify the files to scan" on page 501.

**Tip:** If any performance-related issues are experienced when Deep Security anti-malware protection is enabled, you can use exclusions to help troubleshoot these issues by excluding specific folders or files from scanning.

## Ensure that Deep Security can keep up to date on the latest threats

To remain effective against new viruses and exploits, Deep Security Agents need to be able to download the latest software and security update packages from Trend Micro or indirectly, from your own Relay. These packages contain threat definitions and patterns. Relay-enabled agents, organized into relay groups (also managed and configured by the Deep Security Manager) retrieve security updates from Trend Micro, and then distribute them to other agents and appliances.

1. Go to **Administration > System Settings > Updates.**
2. Configure Deep Security's ability to retrieve security updates from Trend Micro. Make sure you have at least one relay-enabled agent, and it is assigned to the appropriate agents and appliances.
   To determine if a Deep Security Agent is a relay, next to a computer, click **Preview**.



3. Go to **Administration > Scheduled Tasks**.
4. Verify that there is a scheduled task to regularly download available updates for both security and software updates.

## Configure malware scans

Malware scan configurations are reusable saved settings that you can apply when configuring anti-malware in a policy or for a computer. A malware scan configuration specifies what types of malware scanning Deep Security performs and which files it scans. Some policy properties also affect the behavior of malware scans.

- "Create or edit a malware scan configuration" below
- "Scan for specific types of malware" on the next page
- "Specify the files to scan" on page 501
- "Specify when real-time scans occur" on page 506
- "Configure how to handle malware" on page 507
- "Identify malware files by file hash digest" on page 509
- "Configure notifications on the computer" on page 509

The Deep Security Best Practice Guide also provides several recommendations for configuration malware scans.

**Tip:** CPU usage and RAM usage varies by your anti-malware configuration. To optimize anti-malware performance on the Deep Security Agent, see "Performance tips for anti-malware" on page 510.

### Create or edit a malware scan configuration

Create or edit a malware scan configuration to control the behavior of a real-time, manual, or scheduled scan. (For more information, see "Malware scan configurations" on page 489.) You can create multiple malware scan configurations as required.

- After you create a malware scan configuration, you can then associate it with a scan in a policy or computer (see "Select the types of scans to perform" on page 495)

- When you edit a malware scan configuration that a policy or computer is using, the changes affect the scans that are associated with the configuration.

**Tip:** To create a malware scan configuration that is similar to an existing one, duplicate the existing configuration and then edit it.

You can create two types of malware scan configurations according to the type of scan it controls (see "Types of malware scans" on page 487):

- **Real-time scan configuration:** Controls real-time scans. Some actions such as **Deny Access** are only available to real-time scan configurations
- **Manual/scheduled scan configuration:** Controls either manual or scheduled scans. Some options such as **CPU Usage** are only available to manual/scheduled scan configurations

Deep Security provides a default malware scan configuration for each type of scan.

1. Go to **Policies > Common Objects > Other > Malware Scan Configurations**.
2. To create a scan configuration, click **New** and then click **New Real-Time Scan Configuration** or **New Manual/Scheduled Scan Configuration**.
   a. Type a name to identify the scan configuration. You see the name in a list when configuring malware scans in a policy.
   b. (Optional) Type a description that explains the use case for the configuration.
3. To view and edit an existing scan configuration, select it and click **Properties**.
4. To duplicate a scan configuration, select it and click **Duplicate**.

**Tip:** To see the policies and computers that are using a malware scan configuration, see the AssignedTo tab of the properties.

## Scan for specific types of malware

- "Scan for spyware and grayware" on the next page
- "Scan for compressed executable files (real-time scans only)" on the next page
- "Scan process memory (real-time scans only)" on the next page
- "Scan compressed files" on page 500
- "Scan embedded Microsoft Office objects" on page 500

See also:

- "Enhanced anti-malware and ransomware scanning with behavior monitoring" on page 514

### Scan for spyware and grayware

When spyware and grayware protection is enabled, the spyware scan engine quarantines suspicious files when they are detected.

1. Open the properties of the malware scan configuration.
2. On the **General** tab, select **Enable spyware/grayware protection**.
3. Click **OK**.

To identify a specific file that the spyware scan engine should ignore, see "Create anti-malware exceptions" on page 533.

### Scan for compressed executable files (real-time scans only)

Viruses often use real-time compression algorithms to attempt to circumvent virus filtering. The IntelliTrap feature blocks real-time compressed executable files and pairing them with other malware characteristics.

**Note:** Because IntelliTrap identifies such files as security risks and may incorrectly block safe files, consider quarantining (not deleting or cleaning) files when you enable IntelliTrap. (See "Configure how to handle malware" on page 507.) If users regularly exchange real-time compressed executable files, disable IntelliTrap. IntelliTrap uses the virus scan engine, IntelliTrap Pattern, and IntelliTrap Exception Pattern.

1. Open the properties of the malware scan configuration.
2. On the **General** tab, select **Enable IntelliTrap**.
3. Click **OK**.

### Scan process memory (real-time scans only)

Monitor process memory in real time and perform additional checks with the Trend Micro Smart Protection network to determine whether a suspicious process is known to be malicious. If the

process is malicious, Deep Security terminates the process. For more information, see "Smart Protection in Deep Security" on page 522

1. Open the properties of the malware scan configuration.
2. On the **General** tab, select **Scan process memory for malware**.
3. Click **OK**.

### Scan compressed files

Extract compressed files and scan the contents for malware. When you enable the scan, you specify the maximum size and number of files to extract (large files can affect performance). You also specify the levels of compression to inspect so that you can scan compressed files that reside inside compressed files. Level 1 compression is a single compressed file. Compressed files inside that file are level two. You can scan a maximum of 6 compression levels, however higher levels can affect performance.

1. Open the properties of the malware scan configuration.
2. On the **Advanced** tab, select **Scan compressed files**.
3. Specify the maximum size of content files to extract, in MB, the levels of compression to scan, and the maximum number of files to extract.
4. Click **OK**.

### Scan embedded Microsoft Office objects

Certain versions of Microsoft Office use Object Linking and Embedding (OLE) to insert files and other objects into Office files. These embedded objects can contain malicious code.

Specify the number of OLE layers to scan to detect objects that are embedded in other objects. To reduce the impact on performance, you can scan only a few layers of embedded objects within each file.

1. Open the properties of the malware scan configuration.
2. On the **Advanced** tab, select **Scan Embedded Microsoft Office Objects**.
3. Specify the number of OLE layers to scan.
4. Click **OK**.

## Specify the files to scan

To specify the files to scan for malware, identify files and directories to include in the scan and then of those files and directories, identify exclusions. You can also scan network directories:

- "Inclusions" below
- "Exclusions" on the next page
- "Scan a network directory (real-time scan only)" on page 506

### Inclusions

Specify the directories to scan as well as the files inside the directories to scan.

To identify directories to scan, you can specify all directories or a list of directories. The directory list uses patterns with a specific syntax to identify the directories to scan. (See "Syntax for directory lists" on the next page.)

To identify the files to scan, use one of the following options:

- All files
- File types that are identified by IntelliScan. IntelliScan only scans file types that are vulnerable to infection, such as .zip or .exe. IntelliScan does not rely on file extensions to determine file type but instead reads the header and content of a file to determine whether it should be scanned. Compared to scanning all files, Intelliscan reduces the number of files to scan and improves performance.
- Files that have a file name extension that is included in a specified list: The file extension list uses patterns with a specific syntax. (See "Syntax of file extension lists" on page 506.)

1. Open the properties of the malware scan configuration.
2. Click the **Inclusions** tab.
3. To specify the directories to scan, select **All directories** or **Directory List**.
4. If you selected Directory List, from the drop-down menu either select an existing list or select **New** to create one.
5. To specify the files to scan, select either **All files**, **File types scanned by IntelliScan**, or **File Extension List**.

6. If you selected File Extension List, from the drop-down menu either select an existing list or select **New** to create one.
7. Click **OK**.

### Exclusions

Exclude specific directories, files, and file extensions from being scanned. For real-time scans (except when performed by Deep Security Virtual Appliance), you can also exclude specific process image files from being scanned. For example, if you are creating a malware scan configuration for a Microsoft Exchange server, you should exclude the SMEX quarantine folder to avoid re-scanning files that have already been confirmed to be malware.

**Note:** If you choose to run malware scans on database servers used by Deep Security Manager, exclude the data directory. The Deep Security Manager captures and stores intrusion prevention data that might include viruses, which can trigger a quarantine by the Deep Security Agent, leading to database corruption.

To exclude directories, files, and process image files, you create a list that uses patterns to identify the item to exclude.

1. Open the properties of the malware scan configuration.
2. Click the **Exclusions** tab.
3. Specify the directories to exclude:
   a. Select **Directory List**.
   b. Select a directory list or select New to create one. (See "Syntax for directory lists" below.)
   c. If you created a directory list, select it in the directory list.
4. Similarly, specify the file list, file extension list, and process image file list to exclude. (See "Syntax of file lists" on page 504, "Syntax of file extension lists" on page 506, and "Syntax of process image file lists (real-time scans only):" on page 506.)
5. Click **OK**.

### Syntax for directory lists

**Note:** Directory list items accept either forward slash "/" or backslash "\" to support both Windows and Linux conventions.

| Exclusion | Format | Description | Examples |
|---|---|---|---|
| Directory | DIRECTORY\ | Excludes all files in the specified directory and all files in all subdirectories. | ***C:\Program Files***<br>Excludes all files in the "Program Files" directory and all subdirectories. |
| Directory with wildcard (*) | DIRECTORY*\ | Excludes all subdirectories except for the specified subdirectory and the files that it contains. | ***C:\abc****<br>Excludes all files in all subdirectories of "abc" but does not exclude the files in the "abc" directory.<br><br>***C:\abc\wx*z***<br>*Matches:*<br>C:\abc\wxz\<br>C:\abc\wx123z\<br>*Does not match:*<br>C:\abc\wxz<br>C:\abc\wx123z<br><br>***C:\abc*wx***<br>*Matches:*<br>C:\abc\wx\<br>C:\abc\123wx\<br>*Does not match:*<br>C:\abc\wx<br>C:\abc\123wx |
| Directory with wildcard (*) | DIRECTORY* | Excludes any subdirectories with a matching name, but does not exclude the files in that directory and any subdirectories. | ***C:\abc****<br>*Matches:*<br>C:\abc\<br>C:\abc\1<br>C:\abc\123<br>*Does not match:*<br>C:\abc<br>C:\abc\123\<br>C:\abc\123\456<br>C:\abx\<br>C:\xyz\<br><br>***C:\abc*wx***<br>*Matches:*<br>C:\abc\wx<br>C:\abc\123wx<br>*Does not match:*<br>C:\abc\wx\<br>C:\abc\123wx\<br><br>***C:\abc\wx*z*** |

| Exclusion | Format | Description | Examples |
|---|---|---|---|
| | | | *Matches:*<br>C:\abc\wxz<br>C:\abc\wx123z<br>*Does not match:*<br>C:\abc\wxz\<br>C:\abc\wx123z\<br><br>***C:\abc\wx****<br>*Matches:*<br>C:\abc\wx<br>C:\abc\wx\<br>C:\abc\wx12<br>C:\abc\wx12\345\<br>C:\abc\wxz\<br>*Does not match:*<br>C:\abc\wx123z\ |
| Environment variable | ${ENV VAR} | Excludes all files and subdirectories defined by an environment variable. For a Virtual Appliance, the value pairs for the environment variable must be defined in **Policy or Computer Editor > Settings > General > Environment Variable Overrides.** | ***${windir}***<br>If the variable resolves to "c:\windows", excludes all the files in "c:\windows" and all its subdirectories. |
| Comments | DIRECTORY #Comment | Adds a comment to your exclusion definitions. | `c:\abc #Exclude the abc directory` |

## Syntax of file lists

| Exclusion | Format | Description | Example |
|---|---|---|---|
| File | FILE | Excludes all files with the specified file name regardless of its location or directory. | ***abc.doc***<br>Excludes all files named "abc.doc" in all directories. Does not exclude "abc.exe". |
| File path | FILEPATH | Excludes the specific file specified by the file path. | ***C:\Documents\abc.doc***<br>Excludes only the file named "abc.doc" in the "Documents" directory. |
| File path with wildcard (*) | FILEPATH | Excludes all the specific files specified by the file path. | `C:\Documents\abc.co*` (For Windows Agent platforms only) Excludes any file that has file name of "abc" and extension beginning with ".co" in the "Documents" directory. |
| File with wildcard (*) | FILE* | Excludes all files with a matching pattern in the file name. | ***abc*.exe***<br>Excludes any file that has prefix of "abc" and extension of ".exe".<br><br>***.db***<br>*Matches:*<br>123.db |

| Exclusion | Format | Description | Example |
|---|---|---|---|
| | | | abc.db<br>*Does not match:*<br>123db<br>123.abd<br>cbc.dba<br><br>***db***<br>*Matches:*<br>123.db<br>123db<br>ac.db<br>acdb<br>db<br>*Does not match:*<br>db123<br><br>***wxy*.db***<br>*Matches:*<br>wxy.db<br>wxy123.db<br>*Does not match:*<br>wxydb |
| File with wildcard (*) | FILE.EXT* | Excludes all files with a matching pattern in the file extension. | ***abc.v****<br>Excludes any file that has file name of "abc" and extension beginning with ".v".<br><br>***abc.*pp***<br>*Matches:*<br>abc.pp<br>abc.app<br>*Does not match:*<br>wxy.app<br><br>***abc.a*p***<br>*Matches:*<br>abc.ap<br>abc.a123p<br>*Does not match:*<br>abc.pp<br><br>***abc.****<br>*Matches:*<br>abc.123<br>abc.xyz<br>*Does not match:*<br>wxy.123 |
| File with wildcard (*) | FILE*.EXT* | Excludes all files with a matching pattern in the file name and in the extension. | ***a*c.a*p*** |

| Exclusion | Format | Description | Example |
|---|---|---|---|
| | | | *Matches:*<br>ac.ap<br>a123c.ap<br>ac.a456p<br>a123c.a456p<br>*Does not match:*<br>ad.aa |
| Environment variable | ${ENV VAR} | Excludes files specified by an environment variable with the format ${ENV VAR}. These can be defined or overridden using **Policy or Computer Editor > Settings > General > Environment Variable Overrides.** | ***${myDBFile}***<br>Excludes the file "myDBFile". |
| Comments | FILEPATH #Comment | Adds a comment to your exclusion definitions. | `C:\Documents\abc.doc #This is a comment` |

### Syntax of file extension lists

| Exclusion | Format | Description | Example |
|---|---|---|---|
| File Extension | EXT | Matches all files with a matching file extension. | ***doc***<br>Matches all files with a ".doc" extension in all directories. |
| Comments | EXT #Comment | Adds a comment to your exclusion definitions. | `doc #This a comment` |

### Syntax of process image file lists (real-time scans only):

| Exclusion | Format | Description | Example |
|---|---|---|---|
| File path | FILEPATH | Excludes the specific Process Image file specified by the file path. | ***C:\abc\file.exe***<br>Excludes only the file named "file.exe" in the "abc" directory. |

## Scan a network directory (real-time scan only)

If you want to scan files and folders in network shares and mapped network drives that reside in a Network File System (NFS), Server Message Block (SMB) or Common Internet File System (CIFS), select **Enable Network Directory Scan**. This option is available only for real-time scans.

> **Note:** Resources accessed in "**~/.gvfs**" via GVFS, a virtual file system available for the GNOME desktop, will be treated as local resources, not network drives.

## Specify when real-time scans occur

Choose between scanning files when they are opened for reading, when they are written to, or both.

1. Open the properties of the malware scan configuration.
2. On the **Advanced** tab, select one of the options for the **Real-Time Scan** property.
3. Click **OK**.

## Configure how to handle malware

Configure how Deep Security behaves when malware is detected:

- "Customize malware remedial actions" below
- "Generate alerts for malware detection" on the next page

### Customize malware remedial actions

When Deep Security detects malware, it performs a remedial action to handle the file. There are five possible actions that Deep Security can take when it encounters malware:

- **Pass:** Allows full access to the infected file without doing anything to the file. (An Anti-Malware Event will still be recorded.)
- **Clean:** Cleans a cleanable file before allowing full access to the file. (Not available for Possible Malware.)
- **Delete:** Deletes the infected file.
- **Deny Access:** This scan action can only be performed during Real-time scans. When Deep Security detects an attempt to open or execute an infected file, it immediately blocks the operation. If a malware scan configuration with the "Deny Access" option selected is applied during a Manual/Scheduled scan, a "Pass" action will be applied and an Anti-Malware Event will be recorded.
- **Quarantine:** Moves the file to the quarantine directory on the computer or Virtual Appliance. (Once quarantined, you can download the file to a location of your choice. See "View and restore identified malware" on page 526 for more information.)

The default remediation actions in the malware scan configurations are appropriate for most circumstances. However, you can customize the actions to take when Deep Security detects malware. You can either use the action that ActiveAction determines, or specify the action for each type of vulnerability.

ActiveAction is a predefined group of cleanup actions that are optimized for each malware category. Trend Micro continually adjusts the actions in ActiveAction to ensure that individual detections are handled properly. (See "ActiveAction actions" below.)

1. Open the properties of the malware scan configuration.
2. On the **Advanced** tab, for **Remediation Actions** select Custom.
3. Specify the action to take:
   a. To let ActiveAction decide which action to take, select **Use action recommended by ActiveAction**.
   b. To specify an action for each type of vulnerability, select **Use custom actions**, and then select the actions to use.
4. Specify the action to take for Possible Malware.
5. Click **OK**.

## ActiveAction actions

The following table lists the actions that ActiveAction takes:

| Malware Type | Action |
|---|---|
| "Virus" on page 491 | Clean |
| "Trojans" on page 491 | Quarantine |
| "Packer" on page 492 | Quarantine |
| "Spyware/grayware" on page 492 | Quarantine |
| "Cookie" on page 493 | Delete<br>(Does not apply to real-time scans) |
| "Other threats" on page 494 | Clean |
| "Possible malware" on page 494 | ActiveAction |

**Note:** When the agent downloads virus pattern updates from an ActiveUpdate server or relay, it may change its ActiveAction scan actions.

## Generate alerts for malware detection

When Deep Security detects malware, you can generate an alert.

1. Open the properties of the malware scan configuration.
2. On the **General** tab, for **Alert** select **Alert when this Malware Scan Configuration logs an event**.
3. Click **OK**.

## Identify malware files by file hash digest

Deep Security can calculate the hash value of a malware file and display it on the **Events & Reports > Events > Anti-Malware Events** page. Because a particular piece of malware can go by several different names, the hash value is useful because it uniquely identifies the malware. You can use the hash value when looking up information about the malware from other sources.

1. Open the policy or computer editor that you want to configure.
2. Click **Anti-Malware > Advanced**.
3. Under **File Hash Calculation**, clear the **Default** or **Inherited** check box. (**Default** is displayed for a root policy and **Inherited** is displayed for child policies).

   **Note:** When **Inherited** is selected, the file hash settings are inherited from the current policy's parent policy.

   **Note:** When **Default** is selected, Deep Security does not calculate any hash values.

4. Select the **Calculate hash values of all anti-malware events**.
5. By default, Deep Security will use produce SHA-1 hash values. If you want to produce additional hash values, you can select one or both of **MD5** and **SHA256**.
6. You can also change the maximum size of malware files that will have hash values calculated. The default is to skip files that are larger than 128MB, but you can change the value to anything between 64 and 512 MB.

## Configure notifications on the computer

On Windows-based agents, you might occasionally see onscreen notification messages alerting you of Deep Security actions you must take that are related to the anti-malware and web reputation modules. For example, you might see the message, `A reboot is required for Anti-Malware cleanup task`. You must click OK on the dialog box to dismiss it.

If you don't want these notifications to appear:

1. Go to the **Computer or Policy editor**[1].
2. Click **Settings** on the left.
3. Under the **General** tab, scroll to the **Notifications** section.
4. Set **Suppress all pop-up notifications on host** to **Yes**. The messages still appear as alerts or events in Deep Security Manager. For more information about the notifier, see "Deep Security Notifier" on page 345.

## Performance tips for anti-malware

To improve system resources utilization on Deep Security Agent, you can optimize these performance-related settings according to best practices.

See also:

- "Create anti-malware exceptions" on page 533
- "Identify malware files by file hash digest" on the previous page

### Minimize disk usage

Reserve an appropriate amount of disk space for storing identified malware files. The space that you reserve applies globally to all computers: physical machines, virtual machines, and Deep Security Virtual Appliances. The setting can be overridden at the policy level and at the computer level.

**Tip:** Alerts are raised when there is not enough disk space to store an identified file.

1. Open the policy or computer editor that you want to configure.
2. Click **Anti-Malware > Advanced**.
3. Under **Identified Files**, clear **Default**.
4. Specify the disk space to use in the **Maximum disk space used to store identified files** box.
5. Click **Save**.

---

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

## Optimize CPU usage

- Exclude files from real-time scans if they are normally safe but have high I/O, such as databases, Microsoft Exchange quarantines, and network shares (on Windows, you can use procmon to find files with high I/O). See "Exclusions" on page 502.
- Do not scan network directories. See "Scan a network directory (real-time scan only)" on page 506
- Do not use Smart Scan if the computer doesn't have reliable network connectivity to the Trend Micro Smart Protection Network or your Smart Protection Server. See "Smart Protection in Deep Security" on page 522.
- Reduce the CPU impact of malware scans by setting CPU Usage to **Medium** (Recommended; pauses when overall CPU usage exceeds 50%,) or **Low** (Pauses when overall CPU usage exceeds 20%).
  a. Open the properties of the malware scan configuration.
  b. On the **Advanced** tab, select the **CPU Usage** during which scans run.
  c. Click **OK**.
- Create a scheduled task to run scans at a time when CPU resources are more readily available. See "Schedule Deep Security to perform tasks" on page 263.
- Reduce or keep small default values for the maximum file size to scan, maximum levels of compression from which to extract files, maximum size of individual extracted files, maximum number of files to extract, and OLE Layers to scan. See "Scan for specific types of malware" on page 498.

  **Warning:** Most malware is small, and nested compression indicates malware. But if you don't scan large files, there is a small risk that anti-malware won't detect some malware. You can mitigate this risk with other features such as integrity monitoring. See
- Use multi-threaded processing for manual and scheduled scans (real-time scans use multi-threaded processing by default). Multi-threaded processing is effective only on systems that support this capability. To apply the setting, after you have enabled it, restart the computer.

**Note:** Do not enable multi-threaded processing under the following circumstances:

- Resources are limited (for example, CPU-bound tasks)
- Resources should be held by only one operator at a time (for example, IO-bound tasks)

a. Click **Policies**.

b. Double-click to open the policy where you want to enable multi-threaded processing.

c. Click **Anti-Malware > Advanced**.

d. In the Resource Allocation for Malware Scans section, select **Yes**.

e. Restart the computers on which you enabled multi-threaded processing for the setting to take effect.

**Note:** Multi-threaded processing may reduce the number of CPU cores available at a given time to the computer's other processes.

### Optimize RAM usage

- Reduce or keep small default values for the maximum file size to scan, maximum levels of compression from which to extract files, maximum size of individual extracted files, maximum number of files to extract, and OLE Layers to scan. See "Scan for specific types of malware" on page 498.

  **Warning:** Most malware is small, and nested compression indicates malware. But if you don't scan large files, there is a small risk that anti-malware won't detect some malware. You can mitigate this risk with other features such as integrity monitoring. See "Set up integrity monitoring" on page 632

## Disable Windows Defender after installing Deep Security anti-malware on Windows Server 2016

When you install the Anti-Malware module for a Deep Security 10.0 Agent on Windows Server 2016, the agent will automatically disable Windows Defender, but not all of the Windows processes related to the Windows Defender service. To do so, you need to reboot Windows

Server 2016 after the Deep Security Anti-Malware module installation finishes. The Deep Security Agent will open a Windows message to let you know when to reboot.

**Note:** The agent will report a computer warning event ("Computer reboot is required for Anti-Malware protection") to the Deep Security Manager. This event will remain indefinitely, and will need to be manually dismissed by an administrator.

### Installing the Anti-Malware module when Windows Defender is already disabled

If you disable Windows Defender before installing the Deep Security Anti-Malware module, the Deep Security Agent will not open a Windows reboot message. However, you still need to reboot Windows Server 2016 to ensure that Deep Security Anti-malware functions correctly.

## Detect emerging threats using Predictive Machine Learning

Use Predictive Machine Learning to detect unknown or low-prevalence malware. (For more information, see "Predictive Machine Learning" on page 490.)

Predictive Machine Learning uses the Advanced Threat Scan Engine (ATSE) to extract file features and sends the report to the Predictive Machine Learning engine, hosted on the Trend Micro Smart Protection Network. To enable Predictive Machine Learning, perform the following:

1. "Ensure Internet connectivity" below
2. "Enable Predictive Machine Learning" on the next page

As with all detected malware, Predictive Machine Learning logs an event when it detects malware. (See "Event collection in Deep Security" on page 795.) You can also create an exception for any false positives. (See "Create anti-malware exceptions" on page 533.)

### Ensure Internet connectivity

Predictive Machine Learning requires access to the Global Census Service, Good File Reputation Service, and Predictive Machine Learning Service. These services are hosted in the cloud, in the Trend Micro Smart Protection Network. If your Deep Security Agents or Virtual Appliance cannot access the Internet directly, see "Configure agents that have no Internet access" on page 207 for workarounds.

## Enable Predictive Machine Learning

Predictive Machine Learning is configured as part of a real-time scan configuration that is applied to a policy or individual computer. (See "Configure malware scans" on page 497.) After you configure the scan configuration, apply it to a policy or computer.

**Note:** Predictive Machine Learning protects only the files and directories that real-time scan is configured to scan. See "Specify the files to scan" on page 501.

These settings can only be applied to the real-time scan configuration for Windows computers.

1. Go to **Policies > Common Objects > Other > Malware Scan Configurations**.
2. Select the real-time scan configuration to configure and click **Details**.

   You can also create a new real-time scan configuration if desired.

3. On the **General** tab, under **Predictive Machine Learning**, select **Enable Predictive Machine Learning.**
4. Click **OK**.
5. Open the policy or computer editor to which you want to apply the scan configuration and go to **Anti-Malware > General**.
6. Ensure that **Anti-Malware State** is **On** or **Inherited (On)**.
7. In the **Real-Time Scan** section, select the malware scan configuration.
8. Click **Save**.

# Enhanced anti-malware and ransomware scanning with behavior monitoring

Deep Security provides security settings that you can apply to Windows machines that are protected by a Deep Security Agent to enhance your malware and ransomware detection and clean rate. These settings enable you to go beyond malware pattern matching and identify suspicious files that could potentially contain emerging malware that hasn't yet been added to the anti-malware patterns (known as a zero-day attack).

In this article:

- "How does enhanced scanning protect you?" below
- "How to enable enhanced scanning" on the next page
- "What happens when enhanced scanning finds a problem?" on page 517
- "What if my agents can't connect to the Internet directly?" on page 522


For an overview of the anti-malware module, see "Protect against malware" on page 486.

## How does enhanced scanning protect you?

**Threat detection:** To avoid detection, some types of malware attempt to modify system files or files related to known installed software. These types of changes often go unnoticed because the malware takes the place of legitimate files. Deep Security can monitor system files and installed software for unauthorized changes to detect and prevent these changes from occurring.

**Anti-exploit:** Malware writers can use malicious code to hook in to user mode processes in order to gain privileged access to trusted processes and to hide the malicious activity. Malware writers inject code into user processes through DLL injection, which calls an API with escalated privilege. They can also trigger an attack on a software exploit by feeding a malicious payload to trigger code execution in memory. In Deep Security, the anti-exploit functionality monitors for processes that may be performing actions that are not typically performed by a given process. Using a number of mechanisms, including Data Execution Prevention (DEP), Structured Exception Handling Overwrite Protection (SEHOP), and heap spray prevention, Deep Security can determine whether a process has been compromised and then terminate the process to prevent further infection.

**Extended ransomware protection:** Recently, ransomware has become more sophisticated and targeted. Most organizations have a security policy that includes anti-malware protection on their endpoints, which offers a level of protection against known ransomware variants; however, it may not be sufficient to detect and prevent an outbreak for new variants. The ransomware protection offered by Deep Security can protect documents against unauthorized encryption or modification. Deep Security has also incorporated a data recovery engine that can optionally create copies of files being encrypted to offer users an added chance of recovering files that may have been encrypted by a ransomware process.

## How to enable enhanced scanning

Enhanced scanning is configured as part of the anti-malware settings that are applied to a policy or individual computer. For general information on configuring anti-malware protection, see "Enable and configure anti-malware" on page 494.

**Note:** These settings can only be applied to Windows machines that are protected by a Deep Security Agent.

The first step is to enable enhanced scanning in a real-time malware scan configuration:

1. In Deep Security Manager, go to **Policies > Common Objects > Other > Malware Scan Configurations**.
2. Double-click an existing real-time scan configuration to edit it (for details on malware scan configurations, see "Configure malware scans" on page 497).
3. On the **General** tab, select these options:
   - **Detect suspicious activity and unauthorized changes (incl. ransomware):** Enables the threat detection, anti-exploit, and ransomware detection features that are described above.
   - **Back up and restore ransomware-encrypted files:** When this option is selected, Deep Security will create backup copies of files that are being encrypted, in case they are being encrypted by a ransomware process.
4. Click **OK**.

**Note:** By default, real-time scans are set to scan all directories. If you change the scan settings to scan a directory list, the enhanced scanning may not work as expected. For example, if you set **Directories to scan** to scan "Folder1" and ransomware occurs in Folder1, it may not be detected if the encryption associated with the ransomware happens to files outside of Folder1.

Next, apply the malware scan configuration to a policy or an individual computer:

1. In the **Computer or Policy editor**[1], go to **Anti-Malware > General**.
2. Ensure that the **Anti-Malware State** is **On** or **Inherited (On)**.
3. The General tab contains sections for **Real-Time Scan**, **Manual Scan**, and **Scheduled Scan**. In the appropriate sections, use the **Malware Scan Configuration** list to select the scan configuration that you created above.
4. Click **Save**.

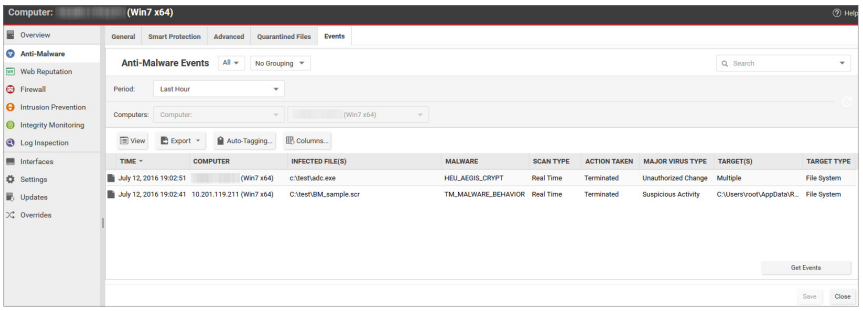
## What happens when enhanced scanning finds a problem?

When Deep Security discovers activity or files that match the enhanced scan settings you have enabled, it will log an event (go to **Events & Reports > Events > Anti-Malware Events** to see a list of events). The event will be identified as "Suspicious activity" or "Unauthorized change" in the **Major Virus Type** column and details will be displayed in the **Target(s)** and **TargetType** columns.

Deep Security performs many types of checks related to the enhanced scan settings, and the actions that it takes depend on the type of check that finds an issue. Deep Security may "Deny Access", "Terminate", or "Clean" a suspicious object. These actions are determined by Deep Security and are not configurable, with the exception of the "Clean" action:

- **Deny Access:** When Deep Security detects an attempt to open or execute a suspicious file, it immediately blocks the operation and records an anti-malware event.
- **Terminate:** Deep Security terminates the process that performed the suspicious operation and records an anti-malware event.
- **Clean:** Deep Security checks the Malware Scan Configuration and performs the action specified for Trojans on the Actions tab. One or more additional events will be generated relating to the action performed on the Trojan files.

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).




Double-click an event to see details:

General | Tags

**General Information**

| | |
|---|---|
| Computer: | (Win7 x64) |
| Origin: | Agent |

**Malware Information**

| | |
|---|---|
| Detection Time: | July 12, 2016 19:02:41 |
| Malware: | TM_MALWARE_BEHAVIOR |
| Infected File(s): | C:\test\BM_sample.scr |
| Scan Type: | Real Time |
| Action Taken: | Terminated |
| Reason: | Default Real-Time Scan Configuration |
| Major Virus Type: | Suspicious Activity |

**Behavior Monitoring Information**

| | |
|---|---|
| Target: | C:\Users\root\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\StartupFile.exe |
| TargetType: | File System |

< Back | Next > | Close

Events related to ransomware have an additional **Targeted Files** tab:

General | Targeted Files | Tags

**General Information**

| | |
|---|---|
| Computer: | (Win7 x64) |
| Origin: | Agent |

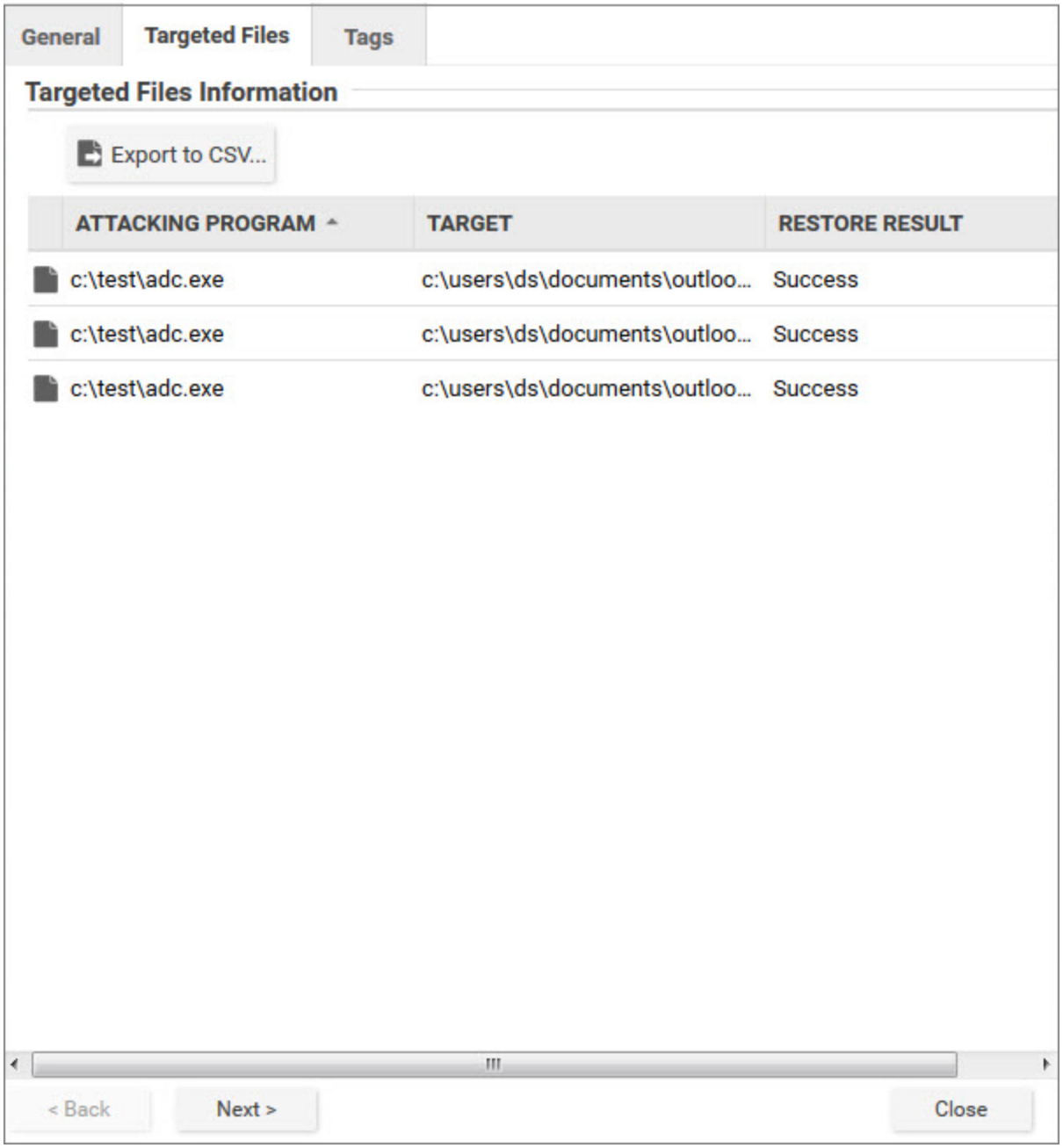
**Malware Information**

| | |
|---|---|
| Detection Time: | July 12, 2016 19:02:51 |
| Malware: | HEU_AEGIS_CRYPT |
| Infected File(s): | c:\test\adc.exe |
| Scan Type: | Real Time |
| Action Taken: | Terminated |
| Reason: | Default Real-Time Scan Configuration |
| Major Virus Type: | Unauthorized Change |

**Behavior Monitoring Information**

| | |
|---|---|
| Target: | Multiple |
| TargetType: | File System |

< Back | Next > | Close




If you investigate and find that an identified file is not harmful, you can right-click the event and click **Allow** to add the file to a scan exclusion list for the computer or policy. You can check the scan exclusion list in the policy or computer editor, under **Anti-Malware > Advanced > Behavior Monitoring Protection Exceptions**.

### What if my agents can't connect to the Internet directly?

The enhanced scanning features described in this article require Internet access to check files against the Global Census Server and Good File Reputation Service. If your Deep Security Agents cannot access the Internet directly, see "Configure agents that have no Internet access" on page 207 for workarounds.

## Smart Protection in Deep Security

Smart Protection Network integration is available for your computers and workloads through anti-malware and web reputation modules. Smart Feedback, which is set at the system level, allows you to provide continuous feedback to the Smart Protection Network.

For more about Trend Micro's Smart Protection Network, see Smart Protection Network.

In this topic:


- "Anti-malware and Smart Protection" below
- "Web Reputation and Smart Protection" on page 524
- "Smart Feedback" on page 525


See also "Deploy a Smart Protection Server in AWS" on page 228 for AWS deployment instructions, and the Smart Protection Server documentation for instructions on manually deploying the server.

### Anti-malware and Smart Protection


- "Enable Smart Scan" below
- "Smart Protection Server for File Reputation Service" on the next page


#### Enable Smart Scan

Smart Scan is available in the anti-malware module. It leverages Trend Micro's Smart Protection Network to allow local pattern files to be small and reduces the size and number of updates required by agents and Appliances. When Smart Scan is enabled, the agent downloads a small version of the much larger full malware pattern from a Smart Protection Server. This smaller

pattern can quickly identify files as either "confirmed safe", or "possibly dangerous". "Possibly dangerous" files are compared against the larger complete pattern files stored on Trend Micro Smart Protection Servers to determine with certainty whether they pose a danger or not.

Without Smart Scan enabled, your relay agents must download the full malware pattern from a Smart Protection Server to be used locally on the agent. The pattern will only be updated as scheduled security updates are processed. The pattern is typically updated once per day for your agents to download and is around 120 MB.

**Note:** Verify that the computer can reliably connect to the global Trend Micro Smart Protection Network URLs (see "Port numbers" on page 96 for a list of URLs). If connectivity is blocked by a firewall, proxy, or AWS security group or if the connection is unreliable, it will reduce anti-malware performance.

1. Go to **Policies**.
2. Double-click a policy.
3. Go to **Anti-Malware** > **Smart Protection**.
4. In the **Smart Scan** section, either:
   - select **Inherited** (if the parent policy has Smart Scan enabled)
   - deselect **Inherited**, and then select either **On** or **On for Deep Security Agent, Off for Virtual Appliance**.
5. Click **Save**.

**Note:** A computer that is configured to use Smart Scan will not download full anti-malware patterns locally. Therefore if your anti-malware license expires while a computer is configured to use Smart Scan, switching Smart Scan off will not result in local patterns being used to scan for malware since no anti-malware patterns will be present locally.

## Smart Protection Server for File Reputation Service

Smart Protection Server for File Reputation Service is available in the anti-malware module. It supplies file reputation information required by Smart Scan.

To edit Smart Protection Server for File Reputation Service:

1. Go to **Computers** or **Policies > Anti-Malware > Smart Protection**.
2. You can select to connect directly to Trend Micro's Smart Protection Server or to connect to one or more locally installed Smart Protection Servers.
3. If you want to use a proxy for communication between agents and the Smart Protection Network, we recommend that you create a proxy server specifically for the Smart Protection Network. You can view and edit the list of available proxies on the **Proxies** tab on the **Administration > System Settings** page. For information on proxy protocols, see "Proxy protocols supported by Deep Security" on page 214.

   **Note:** After you select a proxy, you will need to restart any agents that will be using it.

4. Select the **When off domain, connect to global Smart Protection Service (Windows only)** option to use the global Smart Protection Service if the computer is off domain. The computer is considered to be off domain if it cannot connect to its domain controller. (This option is for Windows agents only.)

   **Note:** If you have a locally installed Smart Protection Server, this option should be set to **Yes** on at least one computer so that you are notified if there is a problem with the Smart Protection Server itself.

5. Set the **Smart Protection Server Connection Warning** to generate error events and alerts when a computer loses its connection to the Smart Protection Server.

## Web Reputation and Smart Protection

Smart Protection Server for Web Reputation supplies web reputation information required by the web reputation module.

To edit Smart Protection Server for Web Reputation Service:

1. Go to **Computers** or **Policies > Web Reputation > Smart Protection**.
2. You can select to connect directly to Trend Micro's Smart Protection Server or to connect to one or more locally installed Smart Protection Servers.
3. If you want to use a proxy for communication between agents and the Smart Protection Network, we recommend that you create a proxy server specifically for the Smart Protection Network. You can view and edit the list of available proxies on the **Proxies** tab on the **Administration > System Settings** page. For information on proxy protocols, see "Proxy protocols supported by Deep Security" on page 214.

> **Note:** After you select a proxy, you will need to restart any agents that will be using it.

4. Select the **When off domain, connect to global Smart Protection Service (Windows only)** option to use the global Smart Protection Service if the computer is off domain. The computer is considered to be off domain if it cannot connect to its domain controller. (This option is for Windows agents only.)

   > **Note:** If you have a locally installed Smart Protection Server, this option should be set to **Yes** on at least one computer so that you are notified if there is a problem with the Smart Protection Server itself.

5. Set the **Smart Protection Server Connection Warning** to generate error events and alerts when a computer loses its connection to the Smart Protection Server.

## Smart Feedback

Trend Micro Smart Feedback provides continuous communication between Trend Micro products and the company's 24/7 threat research centers and technologies. With Smart Feedback, products become an active part of the Trend Micro Smart Protection Network, where large amounts of threat data is shared and analyzed in real time. This interconnection enables never before possible rates of analysis, identification, and prevention of new threats-a level of responsiveness that addresses the thousands of new threats and threat variants released daily.

Trend Micro Smart Feedback is a system setting in the Deep Security Manager. When enabled, Smart Feedback shares anonymous threat information with the Smart Protection Network, allowing Trend Micro to rapidly identify and address new threats. By default, Smart Feedback is enabled. You can disable it or adjust its settings by going to **Administration > System Settings > Smart Feedback**.

> **Note:** Smart Feedback will use the agents, appliances, and relays (security updates) proxy selected in the Proxy Server Use section on the **Administration > System Settings > Proxies** tab.

# Handle malware

You can perform the following tasks to handle malware that the anti-malware module detects:

- "View and restore identified malware" below
- "Create anti-malware exceptions" on page 533
- "Increase debug logging for anti-malware in protected Linux instances" on page 536


See also "Generate alerts for malware detection" on page 508.

For an overview of the anti-malware module, see "Protect against malware" on page 486.

## View and restore identified malware

An identified file is a file that has been found to be or to contain malware and has therefore been encrypted and moved to a special folder. (See the "Quarantine" action in "Customize malware remedial actions" on page 507.) Whether or not an infected file is quarantined depends on the anti-malware configuration that was in effect when the file was scanned.


- "See a list of identified files" below
- "Working with identified files" on the next page
- "Search for an identified file" on page 528
- "Restore quarantined files" on page 530
- "Manually restore quarantined files" on page 533


For information about events that are generated when malware is encountered, see "Anti-malware events" on page 942.

### See a list of identified files

The Events and Reports page provides a list of identified files. From there you can see the details for any of those files.

1. Click **Events & Reports** > **Events** > **Anti-Malware Events** > **Identified Files**.
2. To see the details of a file, select the file and click **View**.

The list of identified files includes the following columns of information:

- **Infected File:** Shows the name of the infected file and the specific security risk.
- **Malware:** Names the malware infection.

- **Computer:** Indicates the name of the computer with the suspected infection.

The Details window provides the following information:

- **Detection Time:** The date and time on the infected computer that the infection was detected.
- **Infected File(s):** The name of the infected file.
- **File SHA-1:** The SHA-1 hash of the file.
- **Malware:** The name of the malware that was found.
- **Scan Type:** Indicates whether the malware was detected by a Real-time, Scheduled, or Manual scan.
- **Action Taken:** The result of the action taken by Deep Security when the malware was detected.
- **Computer:** The computer on which this file was found. (If the computer has been removed, this entry will read "Unknown Computer".)
- **Container Name:** Name of the Docker container where the malware was found.
- **Container ID:** ID of the Docker container where the malware was found.
- **Container Image Name:** Image name of the Docker container where the malware was found.

## Working with identified files

The **Identified Files** page allows you to manage tasks related to identified files. Using the menu bar or the right-click context menu, you can:

- **Restore** only quarantined files back to their original location and condition.
- **Download** identified files from the computer or Virtual Appliance to a location of your choice.
- **Analyze** identified files from the computer or Virtual Appliance to a location of your choice.

- **Delete** one or more identified files from the computer or Virtual Appliance.
- **Export** information about the identified file(s) (not the file itself) to a CSV file.
- **View** the details of an identified file.
- **Computer Details** displays the screen of the computer on which the malware was detected.
- **View Anti-Malware Event** displays the anti-malware event associated with this identified file.
- **Add or Remove Columns** by clicking **Add/Remove.**
- **Search** for a particular identified file.

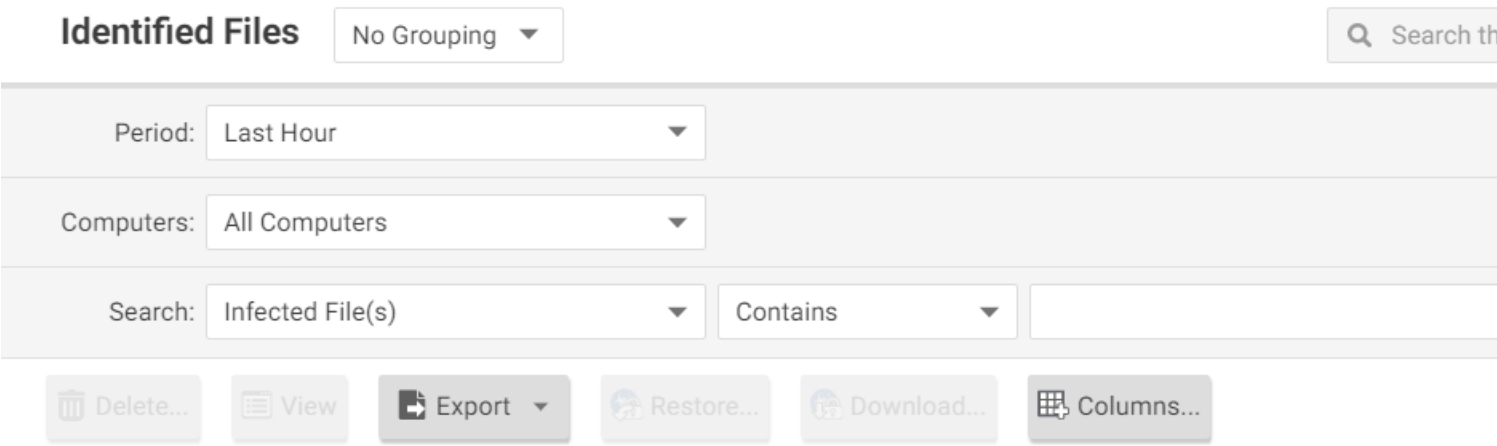
Note: Identified files are automatically deleted from a Virtual Appliance under the following circumstances:

- When a VM is moved to another ESXi host by vMotion, identified files associated with that VM will be deleted from the Virtual Appliance.
- When a VM is deactivated from the Deep Security Manager, identified files associated with that VM will be deleted from the Virtual Appliance.
- When a Virtual Appliance is deactivated from the Deep Security Manager, all the identified files stored on that Virtual Appliance will be deleted.
- When a Virtual Appliance is deleted from the vCenter, all the identified files stored on that Virtual Appliance will also be deleted.

## Search for an identified file

- Use the **Period** drop down menu to see only the files that were identified within a specific time frame.
- Use the **Computers** drop-down menu to organize files by Computer Groups or Computer Policies.

- Click **Search this page > Open Advanced Search** to toggle the display of the advanced search options:




Advanced searches include one or more search criteria for filtering identified files. Each criterion is a logical statement comprised of the following items:

- The characteristic of the identified file to filter on, such as the type of file (infected file or malware) or the computer that was affected.
- An operator:
  - **Contains:** The entry in the selected column contains the search string.
  - **Does Not Contain:** The entry in the selected column does not contain the search string.
  - **Equals:** The entry in the selected column exactly matches the search string.
  - **Does Not Equal:** The entry in the selected column does not exactly match the search string.
  - **In:** The entry in the selected column exactly matches one of the comma-separated search string entries.
  - **Not In:** The entry in the selected column does not exactly match any of the comma-separated search string entries.
- A value.

To add a criterion, click the "plus" button (+) to the right of the topmost criterion.To search, click the Search button (the circular arrow).

**Note:** Searches are not case-sensitive.

## Restore quarantined files

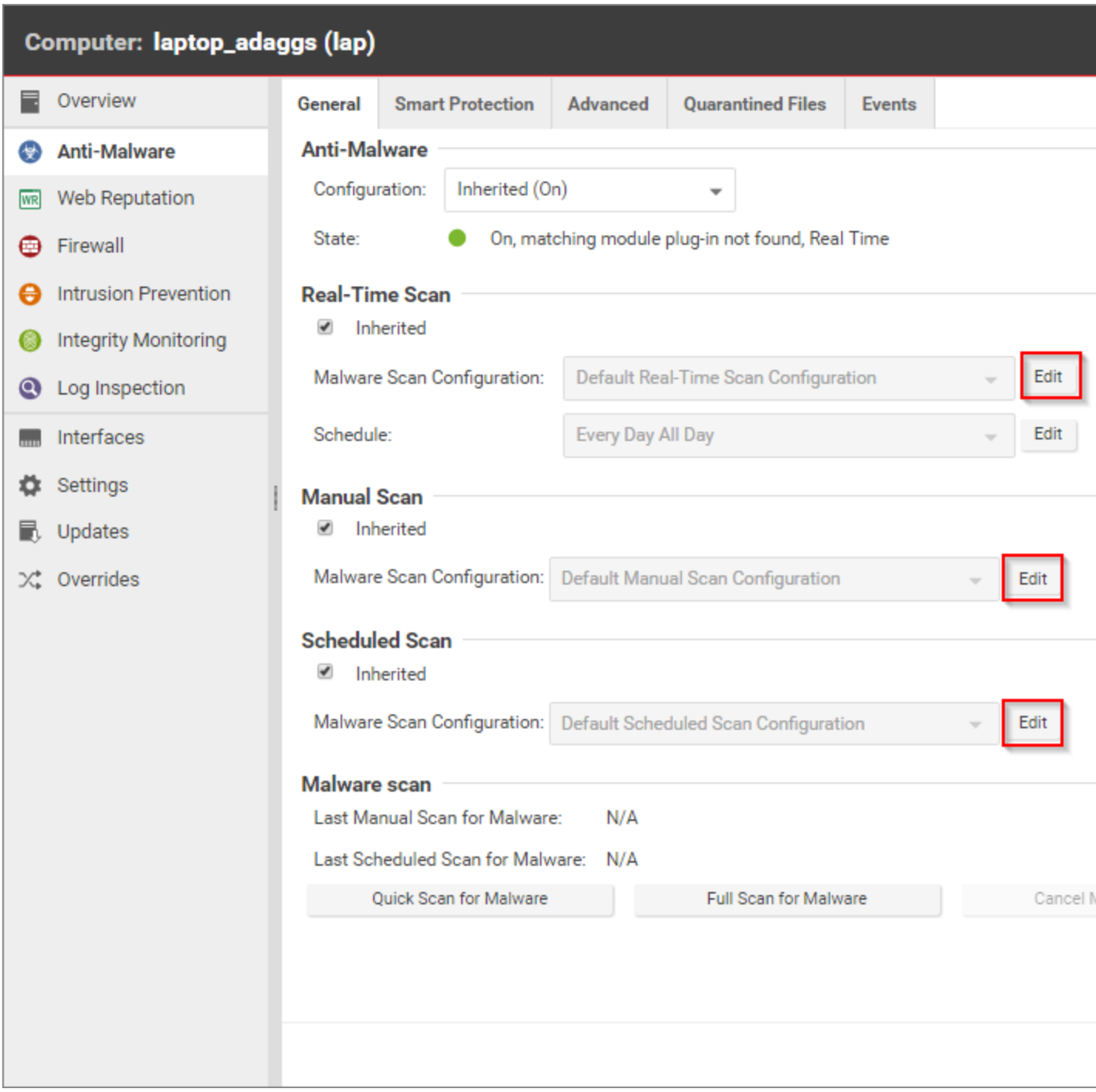
### Create a scan exclusion for the file

Before you can restore the file to its original location you have to create a scan exclusion so that Deep Security doesn't immediately re-quarantine the file when it reappears on the computer.

**Note:** The following instructions describe how to create an exclusion for the file on an individual computer but you can make the same configuration changes at the policy level.

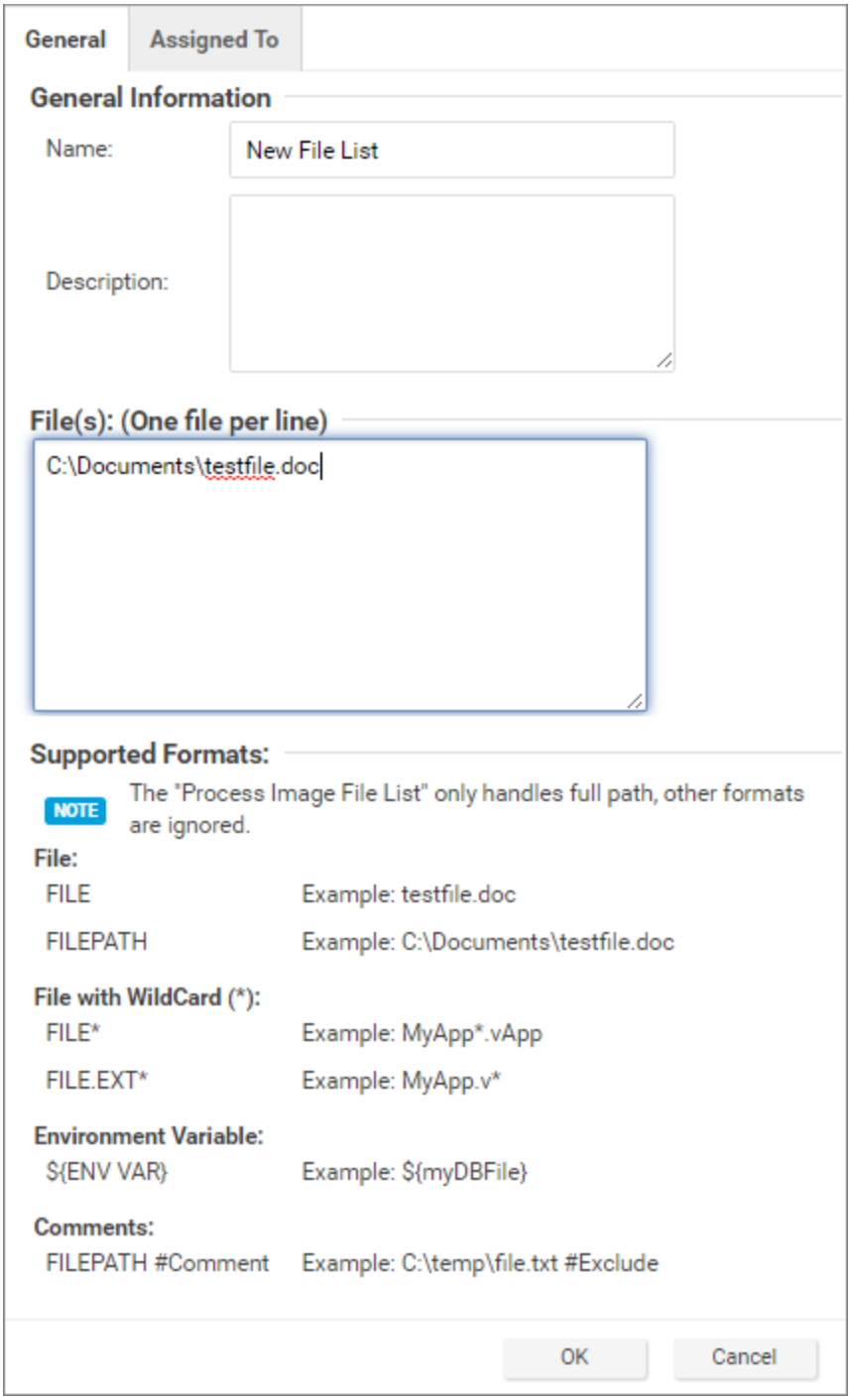
1. Open the Computers page and go to **Anti-Malware > Identified Files** and double click the quarantined file to view its properties.
2. Note the file's exact name and original location.
3. Still in the Computers page, go to **Anti-Malware > General** and click the Edit button next to each Malware Scan that's in effect to open the Malware Scan Configuration properties

window.




4. In the **Malware Scan Configuration** properties window, click on the **Exclusions** tab.
5. In the **Scan Exclusions** area, select **File List** and then either press edit if a file list is already selected, or select **New** from the menu to create a new File List.

6. In the **File List** properties window, enter the file path and name of the file to be restored. Click **OK** to close the File List properties window.




7. Close the **Malware Scan Configuration** properties window by clicking **OK**.

8. When you've edited all the **Malware Scan Configurations**, click **Save** in the Computers page to save your changes. You're now ready to restore your file.

### Restore the file

1. Still in the Computers page, go to the **Anti-Malware > Identified Files** tab.
2. Right-click the quarantined file and select **Actions > Restore** and follow the steps in the wizard.

Your file will be restored to its original location.

### Manually restore quarantined files

To manually restore a quarantined file, download the file to your computer. The **Identified File** wizard will display a link to an **Administration Utility** which you can use to decrypt, examine, or restore the file. Use the quarantined file decryption utility to decrypt the file and then move it back to its original location.

The decryption utility is in a zip file, **QFAdminUtil_win32.zip**, located in the "util" folder under the Deep Security Manager root directory. The zipped file contains two utilities which perform the same function: **QDecrypt.exe** and **QDecrypt.com**. Running **QDecrypt.exe** invokes an open file dialog that lets you select the file for decryption. **QDecrypt.com** is a command-line utility with the following options:

- **/h, --help**: show this help message
- **--verbose**: generate verbose log messages
- **/i, --in=<str>**: quarantined file to be decrypted, where **<str>** is the name of the quarantined file
- **/o, --out=<str>**: decrypted file output, where **<str>** is the name given to the resulting decrypted file

**Note:** This utility is supported only on Windows 32-bit systems.

## Create anti-malware exceptions

Files that are not malicious can be falsely identified as malware if they share certain characteristics with malware. If a file is known to be benign and is identified as malware, you can

create an exception for that file. When an exception is created, the file does not trigger an event when Deep Security scans the file.

For an overview of the anti-malware module, see "Protect against malware" on page 486.

**Note:** You can also exclude files from real-time, manual, and scheduled scans. See "Specify the files to scan" on page 501.

Exceptions can be created for the following types of malware and malware scans:

- Predictive Machine Learning scans (for information, see "Detect emerging threats using Predictive Machine Learning" on page 513.)
- Scans for spyware and grayware (for information, see "Scan for spyware and grayware" on page 499)
- Behavior monitoring protection (for information, see "Enhanced anti-malware and ransomware scanning with behavior monitoring" on page 514)

Deep Security maintains a list of exceptions for each type of malware scan in policy and computer properties.

1. To see the lists of exceptions, open the policy or computer editor.
2. Click **Anti-Malware > Advanced**.
   The exceptions are listed in the **Allowed Spyware/Grayware**, **Document Exploit Protection Rule Exceptions**, **Predictive Machine Learning Detection Exceptions**, and **Behavior Monitoring Protection Exceptions** sections.

See also "Scan exclusion recommendations" on page 536.

## Create an exception from an anti-malware event

When a file is identified as malware, Deep Security generates an anti-malware event. If you know that the file is benign, you can create an exception for the file from the event report.

1. Click **Events & Reports > Events > Anti-Malware Events** and locate the malware detection event.
2. Right-click the event.
3. Select **Allow**.

## Manually create an anti-malware exception

You can manually create anti-malware exceptions for spyware or grayware, document exploit protection rules, predictive machine learning, and behavior monitoring exceptions. To add the exception, you need specific information from the anti-malware event that the scan generated. The type of malware or scan determines the information that you need:

- **Spyware or grayware:** The value in the "MALWARE" field, for example `SPY_CCFR_CPP_TEST.A`
- **Document exploit protection rules:** The value in the "MALWARE" field, for example `HEUR_OLEP.EXE`
- **Predictive machine learning:** The SHA1 digest of the file from the "FILE SHA-1" field, for example `3395856CE81F2B7382DEE72602F798B642F14140`
- **Behavior monitoring:** The process image path, for example `C:\test.exe`

1. Click **Events & Reports > Events > Anti-Malware Events** and copy the field value that is required to identify the malware.
2. Open the policy or computer editor where you want to create the exception.
3. Click **Anti-Malware > Advanced**.
4. In the **Allowed Spyware/Grayware**, **Document Exploit Protection Rule Exceptions**, **Predictive Machine Learning Detection Exceptions**, or **Behavior Monitoring Protection Exceptions** section, enter the information from the event in the text box.
5. Click **Add**.

## Exception strategies for spyware and grayware

When spyware is detected the malware can be immediately quarantined, depending on the malware scan configuration that controls the scan. After you create the exception for a spyware or grayware event, you might have to restore the quarantined file. (See "Restore quarantined files" on page 530.)

Alternatively, you can temporarily scan for spyware and grayware with the action set to "Pass" so that all spyware and grayware detections are recorded on the Anti-Malware Events page but neither quarantined nor deleted. You can then create exceptions for the detected spyware and grayware. When your exception list is robust, you can set the action to "Quarantine" or "Delete" modes.

For information about setting the action, see "Configure how to handle malware" on page 507.

### Scan exclusion recommendations

The best and most comprehensive source for scan exclusions is from the software vendor. The following are some high-level scan exclusion recommendations:

- Quarantine folders (such as `SMEX` on Microsoft Windows Exchange Server) should be excluded to avoid rescanning files that have already been confirmed to be malware.
- Large databases and database files (for example, dsm.mdf and dsm.ldf) should be excluded because scanning could impact database performance. If it is necessary to scan database files, you can create a scheduled task to scan the database during off-peak hours. Since Microsoft SQL Server databases are dynamic, exclude the directory and backup folders from the scan list:

  ${ProgramFiles}\Microsoft SQL Server\MSSQL\Data\
  ${Windir}\WINNT\Cluster\ # if using SQL Clustering
  Q:\ # if using SQL Clustering

For a list of recommended scan exclusions, see the Trend Micro recommended scan exclusion list. Microsoft also maintains an Anti-Virus Exclusion List that you can use as a reference for excluding files from scanning on Windows servers.

## Increase debug logging for anti-malware in protected Linux instances

You can increase or decrease verbosity of the anti-malware (AM) debug logging used to diagnose any issue related to AM when running on a Linux operating system.

Anti-malware debug logs are automatically included when you create a diagnostic package for technical support.

For information on creating a diagnostic package, see "Create a diagnostic package and logs" on page 1105.

**To increase the anti-malware debug log level:**

- Enter the following command in a shell on the Linux instance as root:

```
killall -USR1 ds_am
```

This command will increase the level one unit. By default the level is 6 and the maximum is 8.

**To decrease the anti-malware debug log level:**

- Enter the following command in a shell on the Linux instance as root:

```
killall -USR2 ds_am
```

This command decreases the level by one unit. The minimum level is 0.

# Block exploit attempts using intrusion prevention

The intrusion prevention module protects your computers from known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities.

When patches are not available for known vulnerabilities in applications or operating systems, intrusion prevention rules can intercept traffic that is trying to exploit the vulnerability. It identifies malicious software that is accessing the network and it increases visibility into, or control over, applications that are accessing the network. Therefore your computers are protected until patches that fix the vulnerability are released, tested, and deployed.

Protection is available for file sharing and messaging software such as Skype, but also web applications with vulnerabilities such as SQL injection and cross-site scripting (XSS). In this way, intrusion prevention can also be used as a lightweight web application firewall (WAF).

To enable and configure intrusion prevention, see "Set up intrusion prevention" on page 541.

## Intrusion prevention rules

Intrusion prevention rules define a set of conditions that are compared to the payload session and application layers of network packets (such as DNS, HTTP, SSL, and SMTP), as well as the sequence of those packets according to those higher-layer protocols.

**Tip:** Firewall rules examine the network and transport layers of a packet (IP, TCP, and UDP, for example).

When Deep Security Agents scan network traffic and the traffic meets a rule's match conditions, the agent handles it as a possible or confirmed attack and performs one of the following actions, depending on the rule:

- Replace specifically defined or suspicious byte sequences
- Completely drop packets
- Reset the connection

Intrusion prevention rules are assigned to policies and computers. Therefore you can enforce sets of rules on groups of computers based on the policy that they use, and override policies as required. (See "Policies, inheritance, and overrides" on page 354.)

For information about how you can affect the functionality of rules, see "Configure intrusion prevention rules" on page 549.

## Application types

Application types organize rules by the application that they are associated with. Application types can also store property values that rules can reference as required, such as protocols used for communications, and port numbers. Some application types have configurable properties. For example, the Database Microsoft SQL application type contains rules that are associated with Microsoft SQL Server. You can configure this application type to specify the ports used to connect to the database.

For more information, see "Application types" on page 571.

## Rule updates

Trend Micro creates intrusion prevention rules for application vulnerabilities as they are discovered. Security updates can include new or updated rules and application types. When a rule is already assigned to a policy, and an update includes rules upon which the assigned rule depends, you can choose to automatically assign the updated rules.

**Tip:** Intrusion prevention rules from Trend Micro include information about the vulnerability against which it protects.

Intrusion prevention rules from Trend Micro are not directly editable through Deep Security Manager. However some rules are configurable, and some rules require configuration. (See "Setting configuration options (Trend Micro rules only)" on page 555.)

### Recommendation scans

You can use recommendation scans discover the intrusion prevention rules that you should assign to your policies and computers. (See "Manage and run recommendation scans" on page 359.)

## Use behavior modes to test rules

Intrusion protection works in either Detect or Prevent mode:

- **Detect**: Intrusion prevention uses rules to detect matching traffic and generate events, but does not block traffic. Detect mode is useful to test that intrusion prevention rules do not interfere with legitimate traffic.
- **Prevent**: Intrusion detention uses rules to detect matching traffic, generate events, and block traffic to prevent attacks.

When you first apply new intrusion prevention rules, use Detect mode to verify that they don't accidentally block normal traffic (false positives). When you are satisfied that no false positives occur, you can use Prevent mode to enforce the rules and block attacks. (See "Enable intrusion prevention in Detect mode" on page 542 and "Switch to prevent mode" on page 547.)

**Tip:** Similar to using intrusion prevention in Detect mode, the Deep Security network engine can run in tap mode for testing purposes. In tap mode, intrusion prevention detects rule-matching traffic and generates events, but doesn't block traffic. However, tap mode uses a copy of the packet stream, not the actual stream. Also, tap mode affects the firewall and web reputation modules. You can use Detect mode to test intrusion prevention rules separately. You use tap mode with intrusion prevention in the same way that tap mode is used for testing firewall rules. See "Test firewall rules before deploying them" on page 585.

## Override the behavior mode for rules

You can configure a rule's behavior mode to override the mode that is set for intrusion prevention at the policy or computer level. Overriding is useful for testing new rules that are applied to a policy or computer. For example, when a policy is configured such that intrusion prevention works in Protect mode , you can configure a rule to use Detect mode. For that rule only, intrusion prevention merely logs the traffic, and enforces other rules that do not override the policy's behavior mode. (See "Override the behavior mode for a rule" on page 557.)

Some rules issued by Trend Micro use Detect mode by default. For example, mail client rules generally use Detect mode because in Protect mode they block the downloading of all mail. Some rules trigger an alert only when a condition occurs a large number times, or a certain number of times within a certain period of time. These types of rules apply to traffic that constitutes suspicious behavior only when a condition recurs, and a single occurrence of the condition is considered normal.

**Warning:**
To prevent blocking legitimate traffic and interrupting network services, when a rule requires configuration, keep it in Detect mode until you've configured the rule. Switch a rule to Prevent mode only after configuration and testing.

# Intrusion prevention events

By default, the Deep Security Manager collects firewall and intrusion prevention event logs from the Deep Security **agents and appliances**[1] at every heartbeat. Once collected by the Deep Security Manager, event logs are kept for a period of time which can be configured. The default setting is one week. (See "Log and event storage best practices" on page 799.) You can configure event logging for individual rules as required. (See "Configure event logging for rules" on page 554.)

Event tagging can help you to sort events. You can manually apply tags to events or automatically tag them. You can also use the auto-tagging feature to group and label multiple

[1]The Deep Securty Agent and Deep Security Virtual Appliance are the components that enforce the Deep Security policies that you have defined. Agents are deployed directly on a computer. Appliances are used in VMware vSphere environments to provide agentless protection. They are not available with Deep Security as a Service.

events. For more information on event tagging, see "Apply tags to identify and group events" on page 804.

## Support for secure connections

The intrusion prevention module supports inspecting packets over secure connections. See "Inspect SSL or TLS traffic" on page 573.

## Contexts

Contexts are a powerful way of implementing different security policies depending on the computer's network environment. You typically use contexts to create policies that apply different firewall and intrusion prevention rules to computers (usually mobile laptops) depending on whether that computer is in the office or away.

To determine a computer's location, contexts examine the nature of the computer's connection to its domain controller. For more information, see "Define contexts for use in policies" on page 447.

## Interface tagging

You can use interface types when you need to assign firewall or intrusion prevention rules to a specific interface when a machine has multiple network interfaces. By default, firewall and intrusion prevention rules are assigned to all interfaces on a computer. For example, to apply special rules only to the wireless network interface, use interface types to accomplish this. For more information, see "Configure a policy for multiple interfaces" on page 369.

## Set up intrusion prevention

Enable the intrusion prevention module and monitor network traffic for exploits using Detect mode. When you are satisfied with how your intrusion prevention rules are assigned, switch to Protect mode.

1. "Enable intrusion prevention in Detect mode" on the next page
2. "Test intrusion prevention" on page 544

3. "Apply recommended rules" on page 545
4. "Monitor your system" on page 547
5. "Enable 'fail open' for packet or system failures" on page 547
6. "Switch to prevent mode" on page 547
7. "Implement best practices for specific rules" on page 548

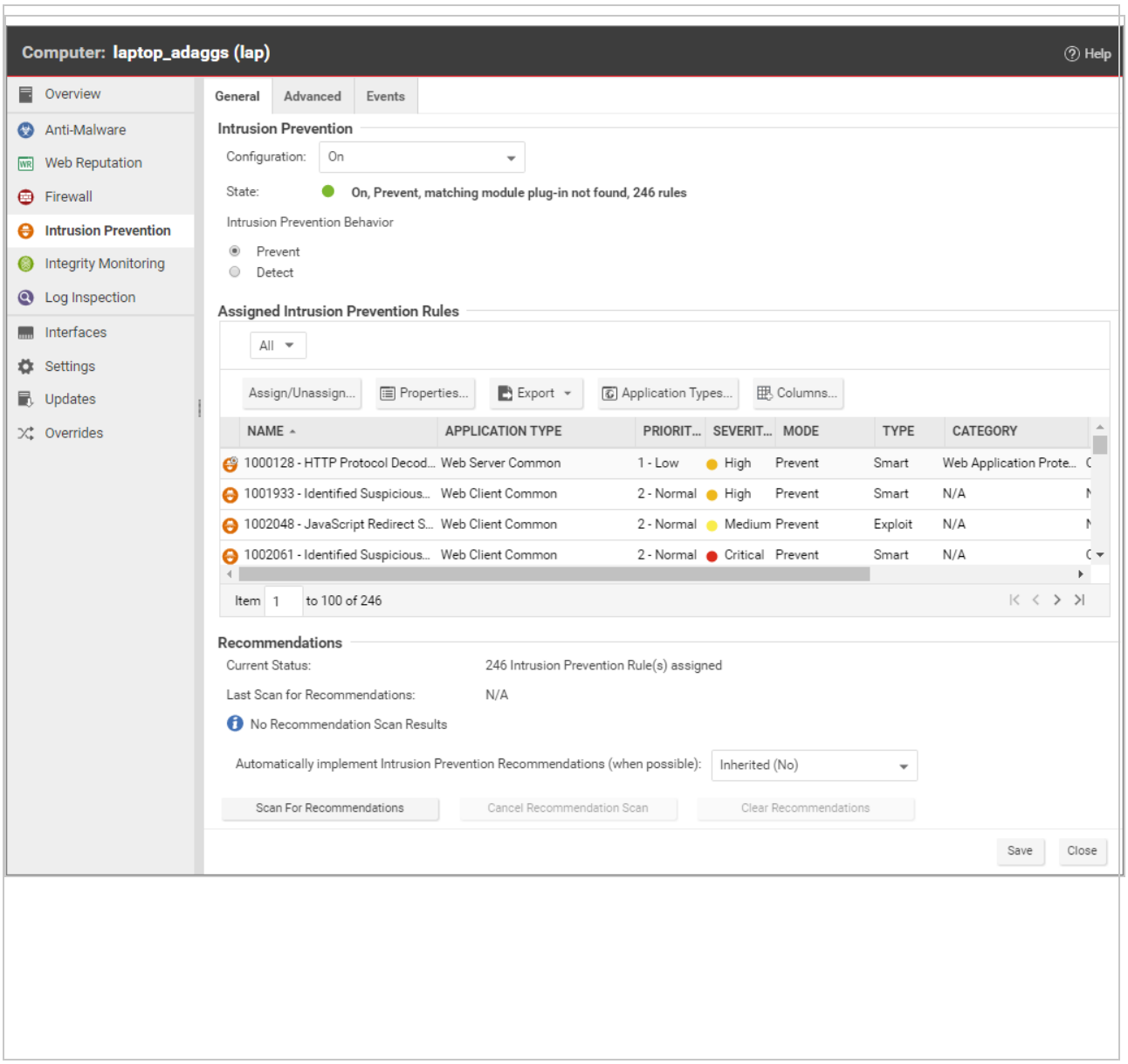
**Note:** CPU usage and RAM usage varies by your IPS configuration. To optimize IPS performance on Deep Security Agent, see "Performance tips for intrusion prevention" on page 581.

For an overview of the intrusion prevention module, see "Block exploit attempts using intrusion prevention" on page 537.

## Enable intrusion prevention in Detect mode

Enable intrusion prevention and use Detect mode for monitoring. Configure intrusion prevention using the appropriate policies to affect the targeted computers. You can also configure individual computers.

1. Go to **Computer or Policy editor**[1] > **Intrusion Prevention** > **General**.
2. For **Configuration**, select either **On** or **Inherited (On)**.




3. For **Intrusion Prevention Behavior**, select **Detect**.
4. Click **Save**.

---

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

**Tip:** If the behavior settings are not available, **Network Engine Mode** may be set to **Tap**. (See "Test firewall rules before deploying them" on page 585.)

For more fine-grained control, when you assign intrusion prevention rules, you can override the global behavior mode and configure specific rules to either prevent or detect. (See "Override the behavior mode for a rule" on page 557.)

## Test intrusion prevention

You should test that the intrusion prevention module is working properly before continuing with further steps.

1. If you have an agent-based deployment, make sure you have a computer that has an agent running. For an agentless deployment, make sure your Deep Security Virtual Appliance is running normally.
2. Turn off the web reputation module. In Deep Security Manager, click **Computers**, then double-click the computer where you'll test intrusion prevention. In the computer's dialog box, click **Web Reputation**, and select **Off**. Web reputation is now disabled and won't interfere with the intrusion prevention functionality.
3. Make sure bad traffic is blocked. Still in the computer's dialog box, click **Intrusion Prevention**, and under the **General** tab, select **Prevent**. (If it is shaded, set the **Configuration** drop-down list to **Inherited**.)
4. Assign the EICAR test policy. Still in the computer's dialog box, click **Intrusion Prevention**. Click **Assign/Unassign**. Search for `1005924`. The **1005924 - Restrict Download of EICAR Test File Over HTTP** policy appears. Select its check box and click **OK**. The policy is now assigned to the computer.
5. Try to download the EICAR file (you can't, if intrusion prevention is running properly). On Windows, go to this link: http://www.eicar.org/download/eicar.com.txt. On Linux, enter this command: `curl -O http://www.eicar.org/download/eicar.com`
6. Check the intrusion prevention events for the computer. Still in the computer's dialog box, click **Intrusion Prevention > Intrusion Prevention Events**. Click **Get Events** to see events that have occurred since the last heartbeat. An event appears with a **Reason** of **1005924 - Restrict Download of EICAR Test File Over HTTP**. The presence of this event indicates that intrusion prevention is working.

7. Revert your changes to return your system to its previous state. Turn on the Web Reputation module (if you turned it off), reset the **Prevent** or **Detect** option, and remove the EICAR policy from the computer.

## Apply recommended rules

To maximize performance, minimize the number of intrusion prevention rules that are assigned to your policies and computers. Therefore, you should assign only the rules that are required. Use a recommendation scan to obtain a list of rules that are appropriate.

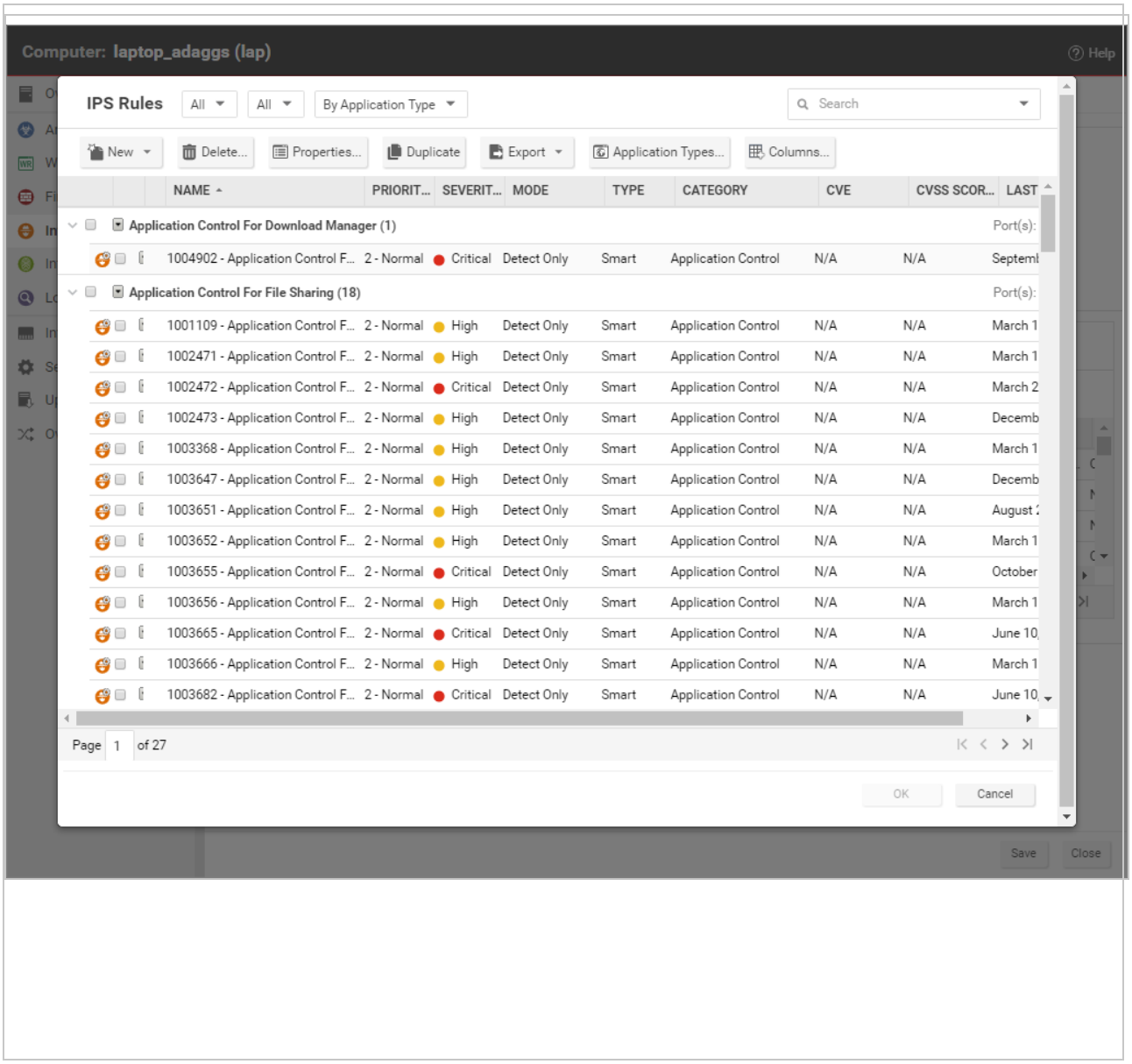
Although recommendation scans are performed for a specific computer, you can assign the recommendations to a policy that the computer uses.

For more information, see "Manage and run recommendation scans" on page 359.

1. Open the properties for the computer to scan. Run the recommendation scan as described in "Manually run a recommendation scan" on page 363.

   **Note:** Do not automatically assign the recommended rules.

2. Open the policy to which you want to assign the rules, and complete the rule assignments as described in "Check scan results and manually assign rules" on page 365.




**Tip:** To automatically and periodically fine tune your assigned intrusion prevention rules, you can schedule recommendation scans. See "Schedule Deep Security to perform tasks" on page 263.

## Monitor your system

After you apply intrusion prevention rules, monitor system performance and intrusion prevention event logs.

### Monitor system performance

Monitor CPU, RAM, and network usage to verify that system performance is still acceptable. If not, you can modify some settings and deployment aspects to improve performance. (See "Performance tips for intrusion prevention" on page 581.)

### Check intrusion prevention events

Monitor intrusion prevention events to ensure that rules are not matching legitimate network traffic. If a rule is causing false positives you can unassign the rule. (See "Assign and unassign rules" on page 553.)

To see intrusion prevention events, click **Events & Reports** > **Intrusion Prevention Events**.

## Enable 'fail open' for packet or system failures

The intrusion prevention module includes a network engine that might block packets before intrusion prevention rules can be applied. This might lead to downtime or performance issues with your services and applications. You can change this behavior so that packets are allowed through when system or internal packet failures occur. For details, see "Enable 'fail open' behavior" on page 587.

## Switch to prevent mode

When you are satisfied that intrusion prevention is not finding false positives, configure your policy to use intrusion prevention in Prevent mode so that rules are enforced and related events are logged.

1. Go to **Computer or Policy editor**[1] > **Intrusion Prevention** > **General**.
2. For **Intrusion Prevention Behavior**, select **Detect**.
3. Click **Save**.

## Implement best practices for specific rules

### HTTP Protocol Decoding rule

The HTTP Protocol Decoding rule is the most important rule in the "Web Server Common" Application Type. This rule decodes the HTTP traffic before the other rules inspect it. This rule also allows you to control various components of the decoding process.

This rule is required when you use any of the Web Application Common or Web Server Common rules that require it. The Deep Security Manager automatically assigns this rule when it is required by other rules. As each web application is different, the policy that uses this rule should run in Detect mode for a period of time before switching to Prevent mode to determine if any configuration changes are required.

Quite often, changes are required to the list of illegal characters.

Refer to the following Knowledge Base articles for more details on this rule and how to tune it:

- https://success.trendmicro.com/solution/1098016
- https://success.trendmicro.com/solution/1054481
- https://success.trendmicro.com/solution/1096566

### Cross-site scripting and generic SQL injection rules

Two of the most common application-layer attacks are SQL injection and cross-site scripting (XSS). Cross-site scripting and SQL injection rules intercept the majority of attacks by default, but you may need to adjust the drop score for specific resources if they cause false positives.

---

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

Both rules are smart filters that need custom configuration for web servers. If you have output from a Web Application Vulnerability Scanner, you should leverage that information when applying protection. For example, if the user name field on the login.asp page is vulnerable to SQL injection, ensure that the SQL injection rule is configured to monitor that parameter with a low threshold to drop on.

For more information, see https://success.trendmicro.com/solution/1098159

## Configure intrusion prevention rules

Perform the following tasks to configure and work with intrusion prevention rules:


- "See the list of intrusion prevention rules" on the next page
- "See information about an intrusion prevention rule" on the next page
- "See information about the associated vulnerability (Trend Micro rules only)" on page 552
- "Assign and unassign rules" on page 553
- "Automatically assign updated required rules" on page 553
- "Configure event logging for rules" on page 554
- "Generate alerts" on page 555
- "Setting configuration options (Trend Micro rules only)" on page 555
- "Schedule active times" on page 556
- "Exclude from recommendations" on page 556
- "Set the context for a rule" on page 557
- "Override the behavior mode for a rule" on page 557
- "Override rule and application type configurations" on page 558
- "Export and import rules" on page 559
- "Configure an SQL injection prevention rule" on page 559


For an overview of the intrusion prevention module, see "Block exploit attempts using intrusion prevention" on page 537.

## See the list of intrusion prevention rules

The Policies page provides a list of intrusion prevention rules. You can search for intrusion prevention rules, and open and edit rule properties. In the list, rules are grouped by application type, and some rule properties appear in different columns.

> **Tip:** The "TippingPoint" column contains the equivalent Trend Micro TippingPoint rule ID. In the Advanced Search for intrusion prevention, you can search on the TippingPoint rule ID. You can also see the TippingPoint rule ID in the list of assigned intrusion prevention rules in the policy and computer editor.

To see the list, click **Policies**, and then below **Common Objects/Rules** click **Intrusion Prevention Rules**.

## See information about an intrusion prevention rule

The properties of intrusion prevention rules include information about the rule and the exploit against which it protects.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.

### General Information

- **Name:** The name of the intrusion prevention rule.
- **Description:** The description of the intrusion prevention rule.
- **Minimum Agent/Appliance Version:** The minimum version of the Deep Security **Agent or Appliance**[1] required to support this intrusion prevention rule.

[1]The Deep Securty Agent and Deep Security Virtual Appliance are the components that enforce the Deep Security policies that you have defined. Agents are deployed directly on a computer. Appliances are used in VMware vSphere environments to provide agentless protection. They are not available with Deep Security as a Service.

### Details

Clicking **New** ( ) or **Properties** ( ) displays the **Intrusion Prevention Rule Properties** window.

> **Note:** Note the **Configuration** tab. Intrusion Prevention Rules from Trend Micro are not directly editable through Deep Security Manager. Instead, if the Intrusion Prevention Rule requires (or allows) configuration, those configuration options will be available on the **Configuration** tab. Custom Intrusion Prevention Rules that you write yourself will be editable, in which case the **Rules** tab will be visible.

## See the list of intrusion prevention rules

The Policies page provides a list of intrusion prevention rules. You can search for intrusion prevention rules, and open and edit rule properties. In the list, rules are grouped by application type, and some rule properties appear in different columns.

> **Tip:** The "TippingPoint" column contains the equivalent Trend Micro TippingPoint rule ID. In the Advanced Search for intrusion prevention, you can search on the TippingPoint rule ID. You can also see the TippingPoint rule ID in the list of assigned intrusion prevention rules in the policy and computer editor.

To see the list, click **Policies**, and then below **Common Objects/Rules** click **Intrusion Prevention Rules**.

## General Information

- **Application Type:** The application type under which this intrusion prevention rule is grouped.

  > **Tip:** You can edit application types from this panel. When you edit an application type from here, the changes are applied to all security elements that use it.

- **Priority:** The priority level of the rule. Higher priority rules are applied before lower priority rules.

- **Severity:** Setting the severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as sorting criteria when viewing a list of intrusion prevention rules. More importantly, each severity level is associated with a severity value; this value is multiplied by a computer's Asset Value to determine the Ranking of an Event. (See **Administration > System Settings > Ranking**.)
- **CVSS Score:** A measure of the severity of the vulnerability according the National Vulnerability Database.

### Identification (Trend Micro rules only)

- **Type:** Can be either Smart (one or more known and unknown (zero day) vulnerabilities), Exploit (a specific exploit, usually signature based), or Vulnerability (a specific vulnerability for which one or more exploits may exist).
- **Issued:** The date the rule was released. This does not indicate when the rule was downloaded.
- **Last Updated:** The last time the rule was modified either locally or during Security Update download.
- **Identifier:** The rule's unique identification tag.

## See information about the associated vulnerability (Trend Micro rules only)

Rules that Trend Micro provides can include information about the vulnerability against which the rule protects. When applicable, the Common Vulnerability Scoring System (CVSS) is displayed. (For information on this scoring system, see the CVSS page at the National Vulnerability Database.)

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Vulnerabilities** tab.

## Assign and unassign rules

To apply intrusion prevention rules during agent scans, you assign them to the appropriate policies and computers. When the rule is no longer necessary because the vulnerability has been patched you can unassign the rule.

If you cannot unassign intrusion prevention rules from a **Computer editor**[1], it is likely because the rules are currently assigned in a policy. Rules assigned at the policy level must be removed using the **Policy editor**[2] and cannot be removed at the computer level.

When you make a change to a policy, it affects all computers using the policy. For example, when you unassign a rule from a policy you remove the rule from all computers that are protected by that policy. To continue to apply the rule to other computers, create a new policy for that group of computers. (See "Policies, inheritance, and overrides" on page 354.)

**Tip:** To see the policies and computers to which a rule is assigned, see the Assigned To tab of the rule properties.

1. Go to the **Policies** page, right-click the policy to configure and click **Details**.
2. Click **Intrusion Prevention > General**.
   The list of rules that are assigned to the policy appear in the **Assigned Intrusion Prevention Rules** list.
3. Under **Assigned Intrusion Prevention Rules**, click **Assign/Unassign**.
4. To assign a rule, select the check box next to the rule.
5. To unassign a rule, deselect the check box next to the rule.
6. Click **OK**.

## Automatically assign updated required rules

Security updates can include new or updated application types and intrusion prevention rules which require the assignment of secondary intrusion prevention rules. Deep Security can

---

[1]To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2]To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

automatically assign these rules if they are required. You enable these automatic assignments in the the policy or computer properties.

1. Go to the **Policies** page, right-click the policy to configure and click **Details**.
2. Click **Intrusion Prevention > Advanced**.
3. To enable the automatic assignments, in the **Rule Updates** area, select **Yes**.
4. Click **OK**.

## Configure event logging for rules

Configure whether events are logged for a rule, and whether to include packet data in the log.

**Note:** Deep Security can display X-Forwarded-For headers in intrusion prevention events when they are available in the packet data. This information can be useful when the Deep Security Agent is behind a load balancer or proxy. The X-Forwarded-For header data appears in the event's Properties window. To include the header data, include packet data in the log. In addition, rule 1006540 " Enable X-Forwarded-For HTTP Header Logging" must be assigned.

Because it would be impractical to record all packet data every time a rule triggers an event, Deep Security records the data only the first time the event occurs within a specified period of time. The default time is five minutes, however you can change the time period using the "Period for Log only one packet within period" property of a policy's Advanced Network Engine settings. (See Advanced Network Engine Options.)

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on page 558.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. On the General tab, go to the Events area and select the desired options:
   - To disable logging for the rule, select **Disable Event Logging**.
   - To log an event when a packet is dropped or blocked, select **Generate Event on Packet Drop**.
   - To include the packet data in the log entry, select **Always Include Packet Data**.

- To log several packets that precede and follow the packet that the rule detected, select **Enable Debug Mode**.Use debug mode only when your support provider instructs you to do so.

Additionally, to include packet data in the log, the policy to which the rule is assigned must allow rules to capture packet data:

1. On the Policies page, open the policy that is assigned the rule.
2. Click **Intrusion Prevention > Advanced**.
3. In the **Event Data** area, select **Yes**.

## Generate alerts

Generate an alert when an intrusion prevention rule triggers an event.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on page 558.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the Options tab, and in the **Alert** area select **On**.
4. Click **OK**.

## Setting configuration options (Trend Micro rules only)

Some intrusion prevention rules that Trend Micro provides have one or more configuration options such as header length, allowed extensions for HTTP, or cookie length. Some options require you to configure them. If you assign a rule without setting a required option, an alert is generated that informs you about the required option. (This also applies to any rules that are downloaded and automatically applied by way of a Security Update.)

Intrusion prevention rules that have configuration options appear in the Intrusion Prevention Rules list with a small gear over their icon .

**Note:** Custom intrusion prevention rules that you write yourself include a **Rules** tab where you can edit the rules.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on page 558.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Configuration** tab.
4. Configure the properties and then click **OK**.

## Schedule active times

Schedule a time during which an intrusion prevention rule is active. Intrusion prevention rules that are active only at scheduled times appear in the Intrusion Prevention Rules page with a small clock over their icon .

> **Note:** With Agent-based protection, schedules use the same time zone as the endpoint operating system. With Agentless protection, schedules use the same time zone as the Deep Security Virtual Appliance. Agentless protection is not available with Deep Security as a Service.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on page 558.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Options** tab.
4. In the **Schedule** area, select **New** or select a frequency.
5. Edit the schedule as required.
6. Click **OK**.

## Exclude from recommendations

Exclude intrusion prevention rules from rule recommendations of recommendation scans.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on the next page.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Options**tab.
4. In the **Recommendations Options** area, select **Exclude from Recommendations**.
5. Click **OK**.

## Set the context for a rule

Set the context in which the rule is applied.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on the next page.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Options** tab.
4. In the **Context** area, select **New** or select a context.
5. Edit the context as required.
6. Click **OK**.

## Override the behavior mode for a rule

Set the behavior mode of an intrusion prevention rule to Detect when testing new rules. In Detect mode, the rule creates a log entry prefaced with the words "detect only:" and does not interfere with traffic. Some intrusion prevention rules are designed to operate only in Detect mode. For these rules, you cannot change the behavior mode.

> **Note:** If you disable logging for the rule, the rule activity is not logged regardless of the behavior mode.

For more information about behavior modes, see "Use behavior modes to test rules" on page 539.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" below.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Select **Detect Only**.

## Override rule and application type configurations

From a **Computer or Policy editor**[1] , you can edit an intrusion prevention rule so that your changes apply only in the context of the policy or computer. You can also edit the rule so that the changes apply globally so that the changes affect other policies and computers that are assigned the rule. Similarly, you can configure application types for a single policy or computer, or globally.

1. Go to the **Policies** page, right-click the policy to configure and click **Details**.
2. Click **Intrusion Prevention**.
3. To edit a rule, right-click the rule and select one of the following commands:
   - **Properties**: Edit the rule only for the policy.
   - **Properties (Global)**: Edit the rule globally, for all policies and computers.
4. To edit the application type of a rule, right-click the rule and select one of the following commands:
   - **Application Type Properties**: Edit the application type only for the policy.
   - **Application Type Properties (Global)**: Edit the application type globally, for all policies and computers.
5. Click **OK**.

**Tip:** When you select the rule and click Properties, you are editing the rule only for the policy that you are editing.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

**Note:** You cannot assign one port to more than eight application types. If they are, the rules will not function on that port.

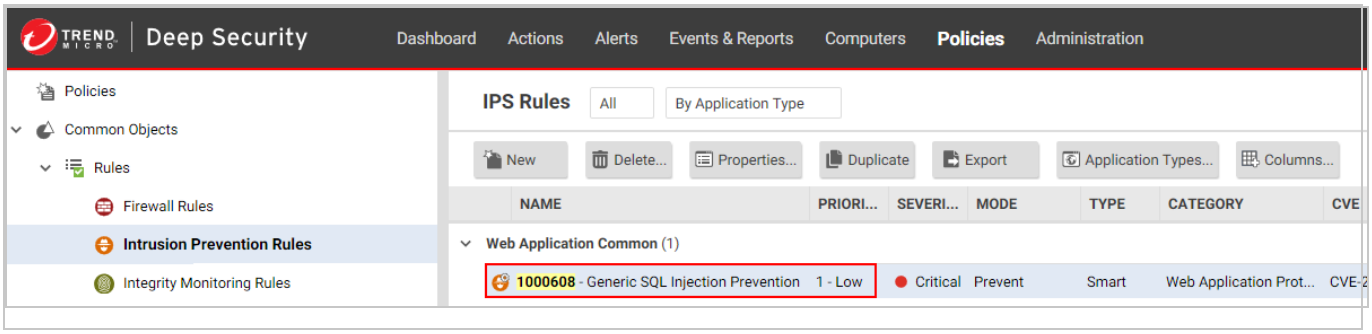
## Export and import rules

You can export one or more intrusion prevention rules to an XML or CSV file, and import rules from an XML file.

1. Click **Policies > Intrusion Prevention Rules**.
2. To export one or more rules, select them and click **Export > Export Selected to CSV** or **Export > Export Selected to XML**.
3. To export all rules, click **Export > Export to CSV** or **Export > Export to XML**.
4. To import rules, click **New > Import From File** and follow the instructions on the wizard.

# Configure an SQL injection prevention rule

Deep Security's intrusion prevention module includes a built-in rule that detects SQL injection attacks and drops the connection or logs it depending on its characteristics. The rule is called **1000608 - Generic SQL Injection Prevention** and can be configured to suit your organization's needs. For example, you can change the sensitivity of the rule by modifying the drop threshold.




Topics in this article:


- "What is an SQL injection attack?" on the next page
- "What are common characters and strings used in SQL injection attacks?" on the next page
- "How does the Generic SQL Injection Prevention rule work?" on page 562

- "Examples of the rule and scoring system in action" on page 564
- "Configure the Generic SQL Injection Prevention rule" on page 566
- "Character encoding guidelines" on page 569


## What is an SQL injection attack?

An SQL injection attack, or SQL phishing attack, is a method of attacking data-driven applications wherein an attacker includes portions of SQL statements in an entry field. The newly-formed rogue SQL command is passed by the website to your database where it is executed. The command can result in the attacker being able to read, add, delete, or change information in the database.

## What are common characters and strings used in SQL injection attacks?

Here are some commonly used characters and strings. The list is not exhaustive.

- ('
- %27
- \x22
- %22
- char
- ;
- ascii
- %3B
- %2B
- --
- %2D%2D
- /*
- %2F%2A
- */

- %2A%2F
- substring
- drop table
- drop+table
- insert into
- insert+into
- version(
- values
- group by
- group+by
- create table
- create+table
- delete
- update
- bulk insert
- bulk+insert
- load_file
- shutdown
- union
- having
- select
- declare
- exec
- and
- or
- like
- @@hostname

- @@tmpdir
- is null
- is+null
- is not null
- is+not+null
- %3D
- CONCAT
- %40%40basedir
- version%28,user(
- user%28,system_user(
- (,%28,)
- %29
- @
- %40
- cast

## How does the Generic SQL Injection Prevention rule work?

To detect SQL injection attacks, the Generic SQL Injection Prevention rule uses a scoring system. It works like this:

1. Packets from your application arrive at the Deep Security Agent for analysis.
2. The Generic SQL Injection Prevention rule looks at the packets and determines whether any of the strings shown in the table below are present. Notice that the strings are separated by commas and divided into ten groups.
3. If strings are found, a score is calculated as follows:
    - If a single string is found, then the score associated with its group constitutes the total score.
    - If multiple strings are found in *different* groups, then the scores of those groups are added together.

- If multiple strings are found in the *same* group, then the score of that group is counted only once.
  See "Examples of the rule and scoring system in action" on the next page for clarification.

4. Using the total score, Deep Security determines whether to drop the connection or log it. If the total score exceeds the **Drop Threshold** score, then the connection is dropped, and if it exceeds the **Log Threshold** score, then it is logged.

**Note:** Trend Micro frequently updates its rules, so the strings in the table below might not match exactly the ones in Deep Security Manager.

**Note:** The use of '`\W`' in the lines below means 'followed by a non-alphanumeric character'.

| Group | Score |
|---|---|
| drop table,drop+table,insert into,insert+into,values\W,create table,create+table,delete\W,update\W,bulk insert,bulk+insert,shutdown\W,from\W | 2 |
| declare\W,select\W | 2 |
| cast\W,exec\W,load_file | 2 |
| union\W,group by,group+by,order by,order+by,having\W | 2 |
| and\W,or\W,like\W,is null,is+null,is not null,is+not+null,where\W | 1 |
| --,%2D%2D,/*,%2F%2A,*/,%2A%2F | 1 |
| ',%27,\x22,%22,char\W | 1 |
| ;,%3B | 1 |
| %2B,CONCAT\W | 1 |
| %3D | 1 |
| (,%28,),%29,@,%40 | 1 |
| ascii,substring | 1 |

| Group | Score |
|---|---|
| version(,version%28,user(,user%28,system_user(,system_user%28,database (,database%28,@@hostname,%40%40hostname,@@basedir,%40%40basedir,@@tmpdir,%40%40tmpdir, @@datadir,%40%40datadir | 2 |

## Examples of the rule and scoring system in action

Below are some examples of how the scores are tallied and what actions are undertaken in each scenario.

### Example 1: Logged and dropped traffic

Let's assume you are using this rule configuration (where the score for the group comes after the colon (":")):

```
drop table,drop+table,insert into,insert+into,values\W,create
table,create+table,delete\W,update\W,bulk insert,bulk+insert,shutdown\W,from\W:2
declare\W,select\W:2
cast\W,exec\W,load_file:2
union\W,group by,group+by,order by,order+by,having\W:2
and\W,or\W,like\W,is null,is+null,is not null,is+not+null,where\W:1
--,%2D%2D,/*,%2F%2A,*/,%2A%2F:1
',%27,\x22,%22,char\W:1
;,%3B:1
%2B,CONCAT\W:1
%3D:1
(,%28,),%29,@,%40:1
ascii,substring:1
version(,version%28,user(,user%28,system_user(,system_user%28,databas
(,database%28,@@hostname,%40%40hostname,@@basedir,%40%40basedir,@@tmpdir,%40%40tmpd
ir,@@datadir,
%40%40datadir:2

Log Threshold: 3
Drop Threshold: 4
```

And this attack string is encountered:

```
productID=BB10735166+UNION/**/+SELECT+FROM+user
```

Then the total score is 5 (2+1+0+2) because:

- The string `UNION/` matches the fourth group for a score of 2.
- The string `/*` matches the sixth group for a score of 1.
- The string `*/` matches the sixth group for a score of 0 (because the score of the sixth group has already been counted).
- The string `SELECT+` matches the second group for a score of 2.

With a total score of 5, a log is generated and the traffic is dropped.

## Example 2: No logged or dropped traffic

Let's assume you are using this rule configuration (where the `select\W` string has been moved to the same line as `union\W`):

```
drop table,drop+table,insert into,insert+into,values\W,create
table,create+table,delete\W,update\W,bulk insert,bulk+insert,shutdown\W,from\W:2
declare\W:2
cast\W,exec\W,load_file:2
union\W,select\W,group by,group+by,order by,order+by,having\W:2
and\W,or\W,like\W,is null,is+null,is not null,is+not+null,where\W:1
--,%2D%2D,/*,%2F%2A,*/,%2A%2F:1
',%27,\x22,%22,char\W:1
;,%3B:1
%2B,CONCAT\W:1
%3D:1
(,%28,),%29,@,%40:1
ascii,substring:1
version(,version%28,user(,user%28,system_user(,system_user%28,databas
(,database%28,@@hostname,%40%40hostname,@@basedir,%40%40basedir,@@tmpdir,
%40%40tmpdir,@@datadir,%40%40datadir:2

Log Threshold: 3
Drop Threshold: 4
```

And this attack string is encountered:

```
productID=BB10735166+UNION/**/+SELECT+FROM+user
```

Then the total score is 3 (2+1+0+0) because:

- The string `UNION/` matches the fourth group for a score of 2.
- The string `/*` matches the sixth group for a score of 1.
- The string `*/` matches the sixth group for a score of 0 (because the score of the sixth group has already been counted).
- The string `SELECT+` matches the fourth group for a score of 0 (because the score of the fourth group has already been counted).

With a total score of 3, no log is generated and no traffic is dropped. The score must *exceed* the thresholds for them to take effect.

## Configure the Generic SQL Injection Prevention rule

You can configure the Generic SQL Injection Prevention rule to suit your organization's needs. The configurable options are shown in the image below.

Generic SQL Injection Prevention Properties - Microsoft Edge

app.deepsecurity.trendmicro.com/com.trendmicro.ds.network--PayloadFilter2Pro

General | Vulnerability | Details | Configuration | Options | Assigned To

**Configuration Options**

SQL Injection Patterns. One group per line separated by ','. The score for the group is at the end of the line after ':'. For ',' use \x2c and for '"' use \x22. The Maximum number of groups is 32.
eg. script, object, embed:2

```
drop table,drop+table,insert
into,insert+into,values\W,create
table,create+table,delete\W,update\W,bulk
insert,bulk+insert,shutdown\W,from\W:2
declare\W,select\W:2
```

Drop Threshold (if the score exceeds this value, the connection will be dropped): 4

Log Threshold (if the score exceeds this value, a log will be generated): 4

Max distance between matches (if this many characters go by without seeing a pattern in any group, the score is reset to 0 ): 35

Note: If Log Threshold is greater or equal to Drop Threshold then only Drop events will be generated. In the default configuration both are equal.

Pages (resource) with a non-default score to drop on. The score for each resource is at the end of the line after ':' eg. /index.html:5 : (One per line)

```
/example/questionnaire.html:8
```

Form parameters with a non-default score to drop on. Each line begins with the resource name followed by the resource parameters separated by a ':'. The score for each parameter is set at the end of the parameter after '='. eg. /index.html:userid=5,passwd=7 (One per line).

```
/example/login.html:username=10
```

View Rules...

OK | Cancel | Apply

To configure the rule:

1. Log in to Deep Security Manager.
2. At the top, click **Policies**.
3. In the search box on the right, enter `1000608` which is the Generic SQL Injection Prevention rule's numeric identifier. Press Enter. The rule appears in the main pane.
4. Double-click the rule.
5. Click the **Configuration** tab. You see the SQL injection pattern in the text box at the top.
6. Update the SQL injection pattern with the latest version, if you haven't customized it yet. To update to the latest pattern, go to the **Details** tab, copy the text under the **Default SQL Pattern** heading and paste it into the **SQL Injection Patterns** text box on the **Configuration** tab. You are now working with the most up-to-date pattern from Trend Micro.
7. Edit the fields as follows:
   - **SQL Injection Patterns**: This is where you to specify the list of characters and strings used in SQL injection attacks. Characters and strings are grouped and assigned a score. If you want to add or change the strings, make sure to use the proper encoding. See "Character encoding guidelines" on the next page below for details.
   - **Drop Threshold**: This is where you specify the drop score. The connection is dropped when the score exceeds this threshold. (If the score equals the drop threshold, the connection is maintained.) The default is `4`.
   - **Log Threshold**: This is where you specify the log score. The connection is logged when the score exceeds this threshold. (If the score equals the log threshold, nothing is logged.) The default is `4`.
   - **Max distance between matches**: This is where you specify the number of bytes that can pass without a match to reset the score to `0`. The default is `35`.
   - **Note:** Consider using the next two options to create overrides for pages and fields that might cause the normal thresholds to be exceeded.
   - **Pages (resource) with a non-default score to drop on**: This is where you can override the **Drop Threshold** for specific resources. For example, if your **Drop Threshold** is `4`, but you want a drop score of `8` for a questionnaire page, specify `/example/questionnaire.html:8`. With this configuration, `/example/questionnaire.html` needs to have a score *higher than* `8` in order for the

connection to be dropped, while all other resources only need a score higher than `4`. Specify each resource on a separate line.

- **Form parameters with a non-default score to drop on**: This is where you can override the thresholds defined in **Drop Threshold** or the **Pages (resources)with a non-default score to drop on** fields for specific form fields. For example, if your **Drop Threshold** score is `4`, but you want a higher drop score of `10` for a username field, specify `/example/login.html:username=10`, where `/example/login.html` is replaced with the path and name of the page where the username field appears, and `username` is replaced with the username field used by your application. With this configuration, the username field needs to have a score *higher than* `10` for the connection to be dropped, while the page itself only needs a score higher than `4`. Specify each form field on a separate line.

  > **Note:** The **Log Threshold** does not take effect when connections are dropped due to a match on the **Pages (resources) with a non-default score to drop on** or **Form parameters with a non-default score to drop on** fields. For example, if you set the form parameter field to `/example/login.html:username=10`, and the username field scores `11`, the connection is dropped but there is no log of this event.

8. Click **OK**.

You have now configured the Generic SQL Injection Prevention rule.

## Character encoding guidelines

If you want to change or add strings to the Generic SQL Injection Prevention rule, you must encode them properly. For example, if you want to use the quote character `'` in your pattern, you must enter `\x22`.

The table below shows characters and their encoded equivalents, as well as character classes that you can use to denote extended patterns.

| Enter this string... | To denote... |
|---|---|
| \a | alphabetic characters, a-z A-Z |

| Enter this string... | To denote... |
| --- | --- |
| \A | non-alphabetic characters<br><br>example: `delete\a` means "the word 'delete' followed by alphabetical characters" |
| \w<br><br>\W | alphanumeric characters, a-z A-Z 0-9<br><br>non-alphanumeric characters<br><br>example: `delete\W` means "the word 'delete' followed by non-alphnumeric characters" |
| \d<br><br>\D | digits 0-9<br><br>non-digit characters<br><br>example: `delete\d` means "the word 'delete' followed by digits between zero and nine" |
| \s<br><br>\S | whitespace<br><br>not whitespace [\r,\n,\t,0x32]<br><br>example: `delete\S` means "the word 'delete' followed by non-whitespace" |
| \p<br><br>\P | punctuation character, printable ascii other than above<br><br>non-punctuation character<br><br>example: `delete\p` means "the word 'delete' followed by a punctuation character or printable ascii" |
| \c<br><br>\C | control character, below 32, or greater than or equal to 127, not including whitespace<br><br>non-control character |

| Enter this string... | To denote... |
|---|---|
| | You can find details on control characters here. |
| \. | any |
| \xDD | hex byte 0xDD |
| \x2c | comma character (,) |
| \x22 | double-quotes character (") |
| \\ | escaped backslash (\) |
| \\| | escaped pipe (\|) |
| \|xx xx xx...\| | hex pipe (byte sequence) |

## Application types

The applications defined by Application Types are identified by the direction of traffic, the protocol being used, and the port number through which the traffic passes. Application Types are useful for grouping intrusion prevention rules.that have a common purpose. Rule groups simplify the process of selecting a set of intrusion prevention rules to assign to a computer. For example, consider the set of rules required to protect HTTP traffic to an Oracle Report Server. Simply select the rules in the "Web Server Common" and "Web Server Oracle Report Server" application types and then exclude unneeded rules, such as the rules that are specific to IIS servers.

### See a list of application types

Open the list of application types where you can see the properties of existing application types, as well as configure, export, and duplicate them. You can export to XML or CSV files. You can import XML files. You can also create and delete application types.

1. Click **Policies > Intrusion Prevention Rules**.
2. Click **Application Types**.
3. To apply a command to an application type, select the type and click the appropriate button.

**Tip:** Application types that have configurable properties have an icon with a gear.

See also "Override rule and application type configurations" on page 558.

## General Information

The name and description of the Application Type. "Minimum Agent/Appliance Version" tells you what version of the Deep Security **agent or appliance**[1] is required to support this Application Type.

## Connection

- **Direction:** The direction of the initiating communication. That is, the direction of the first packet that establishes a connection between two computers. For example, if you wanted to define an Application Type for Web browsers, you would select "Outgoing" because it is the Web browser that sends the first packet to a server to establish a connection (even though you may only want to examine traffic traveling from the server to the browser). The Intrusion Prevention Rules associated with a particular Application Type can be written to examine individual packets traveling in either direction.
- **Protocol:** The protocol this Application Type applies to.
- **Port:** The port(s) this Application Type monitors. (*Not* the port(s) over which traffic is exclusively allowed.)

[1]The Deep Securty Agent and Deep Security Virtual Appliance are the components that enforce the Deep Security policies that you have defined. Agents are deployed directly on a computer. Appliances are used in VMware vSphere environments to provide agentless protection. They are not available with Deep Security as a Service.

### Configuration

The **Configuration** tab displays options that control how Intrusion Prevention Rules associated with this Application Type behave. For example, the "Web Server Common" Application Type has an option to "Monitor responses from Web Server". If this option is deselected, Intrusion Prevention Rules associated with this Application Type will not inspect response traffic.

### Options

Items in the **Options** tab control how the Deep Security Manager uses and applies the Application Type. For example, most Application Types have an option to exclude them from Recommendation Scans. This means that if the "Exclude from Recommendations" options is selected, a Recommendation Scan will not recommend this Application Type and its associated Intrusion Prevention Rules for a computer even if the application in question is detected.

### Assigned To

The **Assigned To** tab lists the Intrusion Prevention Rules associated with this Application Type.

## Inspect SSL or TLS traffic

For the intrusion prevention module, you can configure SSL inspection for a given credential-port pair on one or more interfaces of your protected computer.

> **Note:** Compressed traffic does not support SSL inspection.

Credentials can be imported in PKCS#12 or PEM format. The credential file must include the private key. Windows computers can use CryptoAPI directly.

For an overview of the intrusion prevention module, see "Block exploit attempts using intrusion prevention" on page 537.

In this topic:


- "Configure SSL inspection" on the next page
- "Change port settings" on page 575

- "Use Intrusion Prevention when traffic is encrypted with Perfect Forward Secrecy (PFS)" on the next page
- "Supported ciphers" on page 577
- "Supported protocols" on page 578


## Configure SSL inspection

1. In Deep Security Manager, select the computer to configure and click **Details** to open the computer editor.
2. In the left pane of the computer editor, click **Intrusion Prevention > Advanced > View SSL Configurations,** and click **View SSL Configurations** to open the SSL computer Configurations window.
3. Click **New** to open the SSL Configuration wizard.
4. Specify the interface to which to apply the configuration on this computer:
   - To apply to all interfaces on this computer, select **All Interface(s)**.
   - To apply to specific interfaces, select **Specific Interface(s)**.
5. Select **Port(s)** or **Ports List** and select a list, then click **Next**.
6. On the IP Selection screen, select **All IPs** or provide a **Specific IP** on which to perform SSL inspection, then click **Next**.
7. On the Credentials screen, select how to provide the credentials:
   - **I will upload credentials now**
   - **The credentials are on the computer**

     > **Note:** The credential file must include the private key.

8. If you chose the option to upload credentials now, enter their type, location, and pass phrase (if required).

   If the credentials are on the computer, provide Credential Details.

   - If you are using PEM or PKCS#12 credential formats stored on the computer, identify the location of the credential file and the file's pass phrase (if required).
   - If you are using Windows CryptoAPI credentials, choose the credentials from the list of credentials found on the computer.

9. Provide a name and description for this configuration.
10. Review the summary and close the SSL Configuration Wizard. Read the summary of the configuration operation and click **Finish** to close the wizard.

## Change port settings

Change the port settings for the computer to ensure that the agent is performing the appropriate intrusion prevention filtering on the SSL-enabled ports. The changes you make are applied to a specific application type, such as Web Server Common, on the agent computer. The changes do not affect the application type on other computers.

1. Go to **Intrusion Prevention Rules** in the computer's Details window to see the list of intrusion prevention rules being applied on this computer.
2. Sort the rules by **Application Type** and locate the "Web Server Common" application type. (You can perform these changes to similar application types as well.)
3. Right-click a rule in the application type and click **Application Type Properties**.
4. Override the inherited "HTTP" Port List so that you include the port you defined during the SSL Configuration setup as well as port 80. Enter the ports as comma-separated values. For example, if you use port 9090 in the SSL configuration, enter 9090, 80.
5. To improve performance, on the **Configuration** tab, deselect **Inherited and Monitor responses from Web Server**.
6. Click **OK** to close the dialog.

## Use Intrusion Prevention when traffic is encrypted with Perfect Forward Secrecy (PFS)

Perfect Forward Secrecy (PFS) can be used to create a communication channel that cannot be decrypted if, at a later time, the server's private key is compromised. It relies on the Diffie-Hellman key exchange algorithm which uses ephemeral keys to establish a TLS session. You can identify a server that uses Diffie-Hellman Exchange if its cipher suite contains the string `DHE` (for example, `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`) or `EDH` in some OpenSSL configurations.

Since the intent of Perfect Forward Secrecy is to prevent decryption after the session is over, it also prevents SSL inspection through the Deep Security intrusion prevention module.

To work around this issue, we recommend you do the following:

1. Use Perfect Forward Secrecy for TLS traffic between the Internet and your load balancer (or reverse proxy).
2. Terminate the Perfect Forward Secrecy session at your load balancer (or reverse proxy).
3. Use a non-PFS cipher suite (see "Supported ciphers" on the next page below) for traffic between the load balancer (or reverse proxy) and the web server or application server, so that the intrusion prevention module on the server can decrypt the TLS sessions and inspect them.
4. Restrict traffic to the web server for application server ports that do not use Perfect Forward Secrecy.

## Special considerations for Diffie-Hellman ciphers

On some web servers, Diffie-Hellman ciphers might be the default, so it is important to check the server's configuration file and disable it for TLS traffic between the web server and load balancer (or reverse proxy). For example, to disable Diffie-Hellman on an Apache server:

1. Open the server's configuration file. The file name and location of web server configuration files vary by operating system (OS) and distribution. For example, the path could be:
   - **Default installation on RHEL4:** `/etc/httpd/conf.d/ssl.conf`
   - **Apache 2.2.2 on Red Hat Linux:** `/apache2/conf/extra/httpd-ssl.conf`
2. In the configuration file, find the " `SSLCipherSuite` " variable.
3. Add `!DH:!EDH:!ADH:` to these fields, if this string does not already appear. (The " `!` " tells Apache to "not" use this cipher.)
4. For example, you might edit the Apache configuration file's cipher suite to look like this:

```
SSLCipherSuite !DH:!EDH:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
```

For more information, see the Apache Documentation for `SSLCipherSuite` : http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite.

## Supported ciphers

| Hex Value | OpenSSL Name | IANA Name | NSS Name |
|---|---|---|---|
| 0x00,0x04 | RC4-MD5 | TLS_RSA_WITH_RC4_128_MD5 | SSL_RSA_WITH_RC4_128_MD5 |
| 0x00,0x05 | RC4-SHA | TLS_RSA_WITH_RC4_128_SHA | SSL_RSA_WITH_RC4_128_SHA |
| 0x00,0x09 | DES-CBC-SHA | TLS_RSA_WITH_DES_CBC_SHA | SSL_RSA_WITH_DES_CBC_SHA |
| 0x00,0x0A | DES-CBC3-SHA | TLS_RSA_WITH_3DES_EDE_CBC_SHA | SSL_RSA_WITH_3DES_EDE_CBC_SHA |
| 0x00,0x2F | AES128-SHA | TLS_RSA_WITH_AES_128_CBC_SHA | TLS_RSA_WITH_AES_128_CBC_SHA |
| 0x00,0x35 | AES256-SHA | TLS_RSA_WITH_AES_256_CBC_SHA | TLS_RSA_WITH_AES_256_CBC_SHA |
| 0x00,0x3C | AES128-SHA256 | TLS_RSA_WITH_AES_128_CBC_SHA256 | TLS_RSA_WITH_AES_128_CBC_SHA256 |
| 0x00,0x3D | AES256-SHA256 | TLS_RSA_WITH_AES_256_CBC_SHA256 | TLS_RSA_WITH_AES_256_CBC_SHA256 |
| 0x00,0x41 | CAMELLIA128-SHA | TLS_RSA_WITH_CAMELLIA_128_CBC_SHA | TLS_RSA_WITH_CAMELLIA_128_CBC_SHA |
| 0x00,0x84 | CAMELLIA256-SHA | TLS_RSA_WITH_CAMELLIA_256_CBC_SHA | TLS_RSA_WITH_CAMELLIA_256_CBC_SHA |

| Hex Value | OpenSSL Name | IANA Name | NSS Name |
|---|---|---|---|
| 0x00,0xBA | CAMELLIA128-SHA256 | TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 | TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 |
| 0x00,0xC0 | not implemented | TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 | TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 |

### Supported protocols

The following protocols are supported:

- SSL 3.0
- TLS 1.0
- TLS 1.1
- TLS 1.2

## Configure anti-evasion settings

Anti-evasion settings control the network engine handling of abnormal packets that may be attempting to evade analysis. Anti evasion settings are configured in a policy or an individual computer. The Security Posture setting controls how rigorous intrusion prevention analyzes packets, and can be set to one of the following values:

- **Normal:** Prevents the evasion of intrusion prevention rules without false positives. This is the default value.
- **Strict:** Performs more stringent checking than Normal mode but can produce some false-positive results. Strict mode is useful for penetration testing but should not be enabled under normal circumstances.
- **Custom:** If you select **Custom**, additional settings are available that enable you to specify how Deep Security will handle issues with packets. For these settings (with the exception

of **TCP Timestamp PAWS Window**), the options are **Allow** (Deep Security sends the packet through to the system), **Log Only** (same behavior as Allow, but an event is logged), **Deny** (Deep Security drops the packet and logs an event), or **Deny Silent** (same behavior as Deny, but no event is logged):

**Note:** If you changed the posture to "Custom" in Deep Security 10.1 or earlier, all default values for the anti-evasion settings were set to "Deny". This led to a dramatic increase in block events. The default custom values have changed in Deep Security 10.2, as indicated in the table below.

| Setting | Description | Normal value | Strict value | Default custom value (pre-10.2) | Default custom value (10.2 or later) |
|---|---|---|---|---|---|
| Invalid TCP Timestamps | Action to take when a TCP timestamp is too old | Ignore and Log (same function as Log Only) | Deny | Deny | Ignore and Log (same function as Log Only) |
| TCP Timestamp PAWS Window | Packets can have timestamps. When a timestamp has an earlier timestamp than the one that came before it, it can be suspicious. The tolerance for the difference in timestamps depends on the operating system. For Windows systems, select 0 (the system will only accept packets with a timestamp that is equal to or newer than the previous packet). For Linux systems, select 1 (the system will accept packets with a timestamp that is a maximum of one second earlier than the previous packet). | 1 for Linux agents, otherwise 0 | 1 for Linux agents, otherwise 0 | 0 | 1 for Linux agents, otherwise 0 |
| Timestamp PAWS Zero Allowed | Action to take when a TCP timestamp is zero | Deny for Linux agents or NDIS5, otherwise Allow | Deny for Linux agents or NDIS5, otherwise Allow | Deny | Deny for Linux agents or NDIS5, otherwise Allow |

| Setting | Description | Normal value | Strict value | Default custom value (pre-10.2) | Default custom value (10.2 or later) |
|---|---|---|---|---|---|
| Fragmented Packets | Action to take when a packet is fragmented | Allow | Allow | Deny | Allow |
| TCP Zero Flags | Action to take when a packet has zero flags set | Deny | Deny | Deny | Deny |
| TCP Congestion Flags | Action to take when a packet has congestion flags set | Allow | Allow | Deny | Allow |
| TCP Urgent Flags | Action to take when a packet has urgent flags set | Allow | Deny | Deny | Allow |
| TCP Syn Fin Flags | Action to take when a packet has both SYN and FIN flags set | Deny | Deny | Deny | Deny |
| TCP Syn Rst Flags | Action to take when a packet has both SYN and RST flags set | Deny | Deny | Deny | Deny |
| TCP Rst Fin Flags | Action to take when a packet has both RST and FIN flags set | Deny | Deny | Deny | Deny |
| TCP Syn with Data | Action to take when a packet has a SYN flag set and also contains data | Deny | Deny | Deny | Deny |
| TCP Split Handshake | Action to take when a SYN is received instead of SYNACK, as a reply to a SYN. | Deny | Deny | Deny | Deny |
| RST Packet Out of Connection | Action to take for a RST packet without a known connection | Allow | Deny | Deny | Allow |
| FIN Packet Out of Connection | Action to take for a FIN packet without a known connection | Allow | Deny | Deny | Allow |
| OUT Packet Out of Connection | Action to take for an outgoing packet without a known connection | Allow | Deny | Deny | Allow |

| Setting | Description | Normal value | Strict value | Default custom value (pre-10.2) | Default custom value (10.2 or later) |
|---|---|---|---|---|---|
| Evasive Retransmit | Action to take for a packet with duplicated or overlapping data | Allow | Deny | Deny | Allow |
| TCP Checksum | Action to take for a packet with an invalid checksum | Allow | Deny | Deny | Allow |

## Performance tips for intrusion prevention

To improve system resources utilization on Deep Security Agent, optimize certain performance-related settings.

For an overview of the intrusion prevention module, see "Block exploit attempts using intrusion prevention" on page 537.

| System resource | Settings that impact performance |
|---|---|
| CPU usage | • Log an event when a packet is dropped or blocked. Logging packet modifications may result in a lot of log entries. (See "Configure event logging for rules" on page 554)<br>• Include packet data in the event log only during troubleshooting. (See "Configure event logging for rules" on page 554)<br>• Assign only intrusion prevention rules that apply to the computer's OS and applications. See "Manage and run recommendation scans" on page 359 for information about using recommendation scans to discover applicable vulnerabilities and rules.<br>• Don't assign more than 300 rules. |
| Network usage or throughput | • Log an event when a packet is dropped or blocked. Logging packet modifications may result in a lot of log entries. (See "Configure event |

| System resource | Settings that impact performance |
|---|---|
| | logging for rules" on page 554)<br>• Include packet data in the event log only during troubleshooting. (See "Configure event logging for rules" on page 554)<br>• Do not monitor HTTP responses from the web server, especially if the policy has many signatures applied:<br>a. Click **Policies > Intrusion Prevention Rules**.<br>b. Right-click a rule in the Web Server Common application type and click **Application Type Properties**.<br>c. On the **Configuration** tab, deselect **Inherited and Monitor responses from Web Server**. |
| Disk usage | • Include packet data in the event log only during troubleshooting. (See "Configure event logging for rules" on page 554) |

## Maximum size for configuration packages

When an agent is assigned a large number of intrusion prevention rules, the size of the configuration package can exceed the maximum allowed size. When the allowed size is exceeded, the status of the agent changes to "Agent configuration package too large" and the event message "Configuration package too large" appears.

**Note:** There is a configuration limit of 20 MB in Windows 32-bit platform because it has smaller kernel memory available. For other platforms, the limit is 32 MB.

For performance reasons, you should have less than 350 intrusion prevention rules assigned to a computer. To minimize the number of required rules, ensure all available patches are applied to the computer operation system and any third-party software that is installed.

1. Apply available patches to the computer operating system.
2. Apply available patches to any third-party software that is installed.

3. Apply only the intrusion prevention rules that a recommendation scan recommends. Remove any rules from the computer or the assigned policy that are recommended for unassignment. (See "Manage and run recommendation scans" on page 359.)
4. If you are managing intrusion prevention at the policy level and the configuration package is still too large, configure intrusion prevention in one of the following ways:
   - Make the policy more granular, so that all servers in that policy have the same operating system and applications.
   - Manage intrusion prevention at the server level so that rules are added and removed automatically for the computer.

Use the following procedure to manage intrusion prevention at the server level.

1. Open the editor for the policy that is assigned to the computer.
2. Click **Intrusion Prevention > General**.
3. In the **Recommendations** section, set **Automatically implement Intrusion Prevention Recommendations (when possible)** to **Yes**.
4. Remove any intrusion prevention rules from the policy.
5. Run a recommendation scan on the computer.

# Control endpoint traffic using the firewall

The firewall module provides bidirectional stateful inspection of incoming and outgoing traffic. Firewall rules define what actions to take on individual packets in that traffic. Packets can be filtered by IP and MAC address, port and packet flag across all IP-based protocols and frame types. The firewall module can also help prevent denial of service attacks and detect and prevent reconnaissance scans.

To enable and configure the firewall, see "Set up the Deep Security firewall" on the next page.

## Firewall rules

Firewall rules can process traffic using one of the following actions, listed in order of precedence:

- Bypass
- Log Only
- Force Allow
- Deny
- Allow

Rules also have a priority level between 4 (highest priority) to 0 (lowest priority). Within a specific priority level rules are processed in order based on the precedence of the action type of the rule as listed above. This means that unlike what you may have experienced when configuring other firewalls, the Deep Security firewall processes rules independently of their assignment order.

For more information on how rule priorities and actions determine processing order, see "Firewall rule actions and priorities" on page 605.

For more detailed information on how to create firewall rules, see "Create a firewall rule" on page 597.

**Note:** When creating your rules, make sure to test them using the Tap and Inline modes of the firewall module before deploying them. For information on how to do so, see the "Test firewall rules before deploying them" section of "Set up the Deep Security firewall" below.

## Set up the Deep Security firewall

The Deep Security firewall is a highly flexible firewall that you can configure to be restrictive or permissive. Like the intrusion prevention and web reputation modules, the firewall module can also be run in two modes: inline or tap. It is recommended that you test your firewall rules in tap mode and then switch to inline mode when everything is working correctly.

The configuration and administration of your firewall must be performed carefully and there is no one set of rules that fits all environments. Make sure you understand the firewall rule actions and rule priorities before creating your rules and proceed with extra caution when creating Allow rules because they implicitly deny everything else not defined.

In this article:

- "Test firewall rules before deploying them" below
- "Enable 'fail open' behavior" on page 587
- "Turn on firewall " on page 588
- "Default firewall rules" on page 589
- "Restrictive or permissive firewall design" on page 590
- "Firewall rule actions" on page 591
- "Firewall rule priorities" on page 592
- "Recommended firewall policy rules" on page 593
- "Reconnaissance scans" on page 593
- "Stateful inspection" on page 595
- "Example" on page 595
- "Important things to remember" on page 596


## Test firewall rules before deploying them

The firewall module (as well as the intrusion prevention and web reputation modules) includes a Deep Security network engine that decides whether to block or allow packets. For the firewall and intrusion prevention modules, the network engine performs a packet sanity check and also makes sure each packet passes the firewall and intrusion prevention rules. The network engine operates in one of two modes:

- **Tap mode**: Packet streams are not modified. The traffic is still processed by the firewall and/or intrusion prevention modules, if they are enabled. However any issues detected do not result in packet or connection drops. When in Tap mode, Deep Security offers no protection beyond providing a record of events.
- **Inline mode**: Packet streams pass directly through the Deep Security network engine. All rules are applied to the network traffic before they proceed up the protocol stack.

It’s important to test your firewall rules in either Tap mode or Inline mode with the action for the rules set to Log Only before deploying them. This allows you to preview the effect of the rules on traffic, without any action being taken. If rules aren’t properly tested before deployment, all traffic could become blocked and your computer could become inaccessible.

## Test in Tap mode

Tap mode allows you to test your firewall rules, without disturbing the flow of traffic.

1. Go to **Computers** or **Policies** in the Deep Security Manager.
2. Right-click a computer (or policy) and select **Details** to open the **Computer or Policy editor**[1].
3. Go to **Settings > Advanced > Network Engine Mode**.
4. Select **Tap** from the list and click **Save**.
5. Create your rules and click **OK**. To check your rules, go to **Events & Reports > Events > Firewall Events.**

**Note:** It is not necessary to set the action of the rule to Log Only in Tap mode.

Once you are satisfied with your firewall rules, go back to the **Computer or Policy editor**[2], select **Inline** from the drop-down list, and click **Save**.

## Test in Inline mode

In most situations, Tap mode is a good way to test your firewall rules without disturbing traffic. However, you can also test your rules in Inline mode, if the action of the rule is set to Log Only. This way, the real world process of analyzing the traffic takes place without having to perform any action, such as blocking or denying packets.

---

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

1. Go to **Computers** or **Policies** in the Deep Security Manager.
2. Right-click a computer (or policy) and select **Details** to open the **Computer or Policy editor**[1].
3. Go to **Settings > Advanced > Network Engine Mode**.
4. Select **Inline** from the drop down menu and click **Save**.
5. While you're creating your rule, ensure the action is set to **Log Only.**
6. To check your rules, go to **Events & Reports > Events > Firewall Events**.

Once you are satisfied with your firewall rules, change the action from Log Only to your desired action and click **OK**.

## Enable 'fail open' behavior

In some cases, the network engine blocks packets before the firewall rules (or intrusion prevention rules) can be applied. By default, the network engine blocks packets if:

- the agent or virtual appliance host has a system problem, for example, it's out of memory
- the packet sanity check fails

This 'fail closed' behavior offers a high level of security: it ensures that cyber attacks cannot penetrate your network when an agent or virtual appliance is not functioning properly, and safeguards against potentially malicious packets. The drawback to 'fail closed' is that your services and applications might become unavailable because of problems on the agent or virtual appliance. You might also experience performance issues if a large number of packets are being dropped unnecessarily as a result of the packet sanity check (too many false-positives).

If you have concerns about service availability, consider changing the default behavior to allow packets through (or 'fail open') for system and packet check failures, as explained below.

---

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

1. Go to **Computers** or **Policies** in the Deep Security Manager.
2. Right-click a computer (or policy) and select **Details** to open the **Computer or Policy editor**[1].
3. Click **Settings** on the left.
4. Click the **Advanced** tab.
5. Under **Network Engine Settings**, set the **Failure Response** settings as follows:
6. Set **Network Engine System Failure** to **Fail open** to allow packets through if the network engine host experiences problems, such as out of memory failures, allocated memory failures, and network engine (DPI) decoding failures. Consider using fail open here if your agent or virtual appliance frequently encounters network exceptions because of heavy loads or a lack of resources. With fail open, the network engine allows the packet through, does not perform rules checking, and logs an event. Your services and applications remain available despite the problems on the agent or virtual appliance.
7. Set **Network Packet Sanity Check Failure** to **Fail open** to allow packets through that fail the network engine's packet sanity checks. Examples of packet sanity checks: firewall sanity checks, network layer 2, 3, or 4 attribute checks, and TCP state checks. Consider using fail open here if you want do rules checking only on 'good' packets that pass the sanity check. With fail open, the network engine allows the failed packet through, does not perform rules checking on it, and logs an event.
8. Click **Save**.

You have now enabled fail open behavior for system or packet check failures.

## Turn on firewall

To enable firewall functionality on a computer:

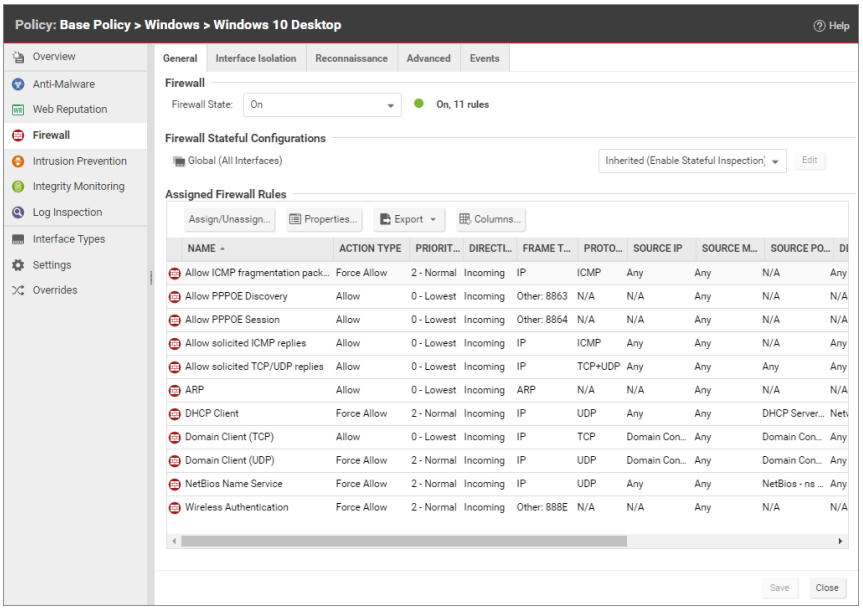
[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

1. In the **Computer or Policy editor**[1], go to **Firewall** > **General**.
2. Select **On** and then click **Save**.

## Default firewall rules

No outbound rules are assigned to the policies that come with Deep Security by default but several recommended inbound rules are. You can view the default inbound rules assigned to each policy by going to the **Firewall** tab in the relevant operating system policy. The example below shows the default assigned firewall rules for the Windows 10 Desktop policy. You can configure these firewall rules to meet the needs of your environment, but we have provided several default rules for you to get you started.

**Tip:** To minimize the impact on system performance, try not to assign more than 300 firewall rules. It is also good practice to document all firewall rule changes in the "Description" field of the firewall rule. Make a note of when and why rules were created or deleted for easier firewall maintenance.




[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

### Default Bypass rule for Deep Security Manager Traffic

The Deep Security Manager automatically implements a **Priority 4 Bypass Rule** that opens the listening port number of the agent for heartbeats on computers running Deep Security Agent. A priority of 4 ensures that this rule is applied before any Deny rule, and Bypass guarantees that the traffic is never impaired. The Bypass rule is not explicitly shown in the firewall rule list because the rule is created internally.

This rule, however, accepts traffic from any IP address and any MAC address. To harden the Deep Security Agent's listening ports, you can create an alternative, more restrictive, Bypass rule for this port. The agent will override the default Deep Security Manager traffic rule with the new custom rule if it has these settings:

- **Priority:** 4 - Highest
- **Packet direction:** Incoming
- **Frame type:** IP
- **Protocol:** TCP
- **Packet Destination Port:** Agent's listening port for heartbeats from the Manager

The custom rule must use the above parameters to replace the default rule. Ideally, the IP address or MAC address of the actual Deep Security Manager should be used as the packet source for the rule.

## Restrictive or permissive firewall design

Typically, firewall policies are based on one of two design strategies. Either they permit any service unless it is expressly denied or they deny all services unless expressly allowed. It is best practice to decide what type of firewall you would like to implement. This helps reduce administrative overhead in terms of creating and maintaining the rules.

### Restrictive firewall

A restrictive firewall is the recommended best practice from a security perspective. All traffic is stopped by default and only traffic that has been explicitly allowed is permitted. If the primary goal of your planned firewall is to block unauthorized access, the emphasis needs to be on restricting rather than enabling connectivity. A restrictive firewall is easier to maintain and more

secured. Allow rules are used only to permit certain traffic across the firewall and deny everything else.

**Note:** As soon as you assign a single outgoing Allow rule, the outgoing firewall will operate in restrictive mode. This is also true for the inbound firewall: as soon as you assign a single incoming Allow rule, the inbound firewall will operate in restrictive mode.

### Permissive firewall

A permissive firewall permits all traffic by default and only blocks traffic believed to be malicious based on signatures or other information. A permissive firewall is easy to implement but it provides minimal security and requires complex rules. Deny rules are used to explicitly block traffic.

## Firewall rule actions

You can configure the firewall to take the following actions:

**Warning:** If you assign only incoming rules, all outgoing traffic will be allowed. If you assign a single outgoing Allow rule, the outgoing firewall will operate in restrictive mode. There is one exception to this: ICMPv6 traffic is always permitted unless it is specifically blocked by a Deny rule.

| | |
|---|---|
| Allow | Explicitly allows traffic that matches the rule to pass and then implicitly denies everything else.<br><br>**Note:** You should use an Allow action with caution because it implicitly denies everything else not defined. Be careful when creating Allow rules without defining the related rules correctly because doing so can cause all traffic to be blocked except for the traffic that the Allow rule is created for. Traffic that is not explicitly allowed by an Allow rule is dropped and gets recorded as a 'Out of "allowed" Policy' firewall event. |
| Bypass | Allows traffic to bypass both firewall and intrusion prevention analysis. Bypass rules should always be created in pairs (for both incoming and outgoing traffic). A Bypass rule can be based on IP, port, traffic direction, and protocol.<br><br>The Bypass rule is designed for media-intensive protocols or traffic originating from trusted sources. |

| | |
|---|---|
| Deny | Explicitly blocks traffic that matches the rule. |
| Force Allow | If a packet matches a force allow rule, it is passed but still filtered by intrusion prevention. No events are logged.<br><br>This type of firewall rule action must be used for UDP and ICMP traffic. |
| Log only | Traffic will only be logged. No other action will be taken. |

For more information on how to create a firewall rule, see "Create a firewall rule" on page 597.

## Firewall rule priorities

Rule priority determines the order in which filters are applied. This means that high priority rules get applied before low priority rules. When actions share the same priority, the orders of precedence for rules are: Bypass, Force Allow, and then Deny. However, a Deny action with a higher priority will take precedence over a Bypass action with a lower priority. For more information on how rule priorities and actions determine processing order, see "Firewall rule actions and priorities" on page 605.

To simplify the administration of firewall rules, consider reserving certain priority levels for specific actions. For example, apply a default of priority 3 to rules that use Bypass, priority 2 for Force Allow rules, and priority 1 for Deny rules. This reduces the potential for rule conflicts.

### Allow rules

Allow rules can only have a priority of 0. This is to ensure it is processed after all Force Allow and Deny rules at higher priorities. Keep this in mind when using Allow rules to implicitly deny traffic (any traffic not matching the Allow rules are denied). This means that when a Deny rule is assigned, it will take precedence over all of the existing assigned Allow rules.

### Force Allow rules

Force Allow rules are recommended for traffic that must always be allowed, such as Address Resolution Protocol (ARP). The Force Allow action only acts as a trump card to a deny rule at the same or higher priority. For example, if you have a Deny rule at priority 3 that prevents access to an allowed port number from the 10.0.0.0/8 subnet, and you want to allow host

10.102.12.56 to access that, you must create a Force Allow rule at priority 3 or 4 to trump the Deny rule at priority 3. Once a packet triggers this rule, it is immediately allowed and the lower priority rules will not process it anymore.

### Bypass rules

The Bypass rule is a special type of rule that allows a packet to bypass both the firewall and Deep Packet Inspection (DPI) engines. This rule must be priority 4 and created in pairs, one rule for each traffic direction.

## Recommended firewall policy rules

We recommend that you make the following rules mandatory for all of your firewall policies:

- **ARP**: This rule allows incoming ARP requests for the host to reply to queries for its MAC address. If you do not assign this rule, no devices on the network can query the host for its MAC address and it will be inaccessible from the network.
- **Allow solicited TCP/UDP replies**: Ensures that the computer is able to receive replies to its own TCP and UDP messages. This works in conjunction with TCP and UDP stateful configuration.
- **Allow solicited ICMP replies**: Ensures that the host computer is able to receive replies to its own ICMP messages. This works in conjunction with ICMP stateful configuration.
- **DNS Server**: Ensures that the DNS servers can receive inbound DNS requests.
- **Remote Access RDP**: Ensures that the computer can accept Remote Desktop connections.
- **Remote Access SSH**: Ensures that the computer can accept SSH connections.

## Reconnaissance scans

You can configure the firewall to detect possible reconnaissance scans and help prevent attacks by blocking traffic from the source IPs for a period of time. Once an attack has been detected, you can instruct agents and appliances to block traffic from the source IPs for a period of time. Use the Block Traffic lists on the on the **Policy or Computer Editor** > **Firewall** > **Reconnaissance** tab to set the number of minutes.

- **Computer OS Fingerprint Probe:** The agent or appliance detects an attempt to discover the computers OS.
- **Network or Port Scan:** The agent or appliance reports a network or port scan if it detects that a remote IP is visiting an abnormal ratio of IPs to ports. Normally, an agent or appliance computer will only see traffic destined for itself, so a port scan is the most common type of probe that will be detected. The statistical analysis method used in computer or port scan detection is derived from the "TAPS" algorithm proposed in the paper "Connectionless Port Scan Detection on the Backbone" presented at IPCCC in 2006.
- **TCP Null Scan:** The agent or appliance detects packages with no flags set.
- **TCP SYNFIN Scan:** The agent or appliance detects packets with only the SYN and FIN flags set.
- **TCP Xmas Scan:** The agent or appliance detects packets with only the FIN, URG, and PSH flags set or a value of 0xFF (every possible flag set).

For each type of attack, the agent or appliance can be instructed to send the information to the Deep Security Manager where an alert will be triggered by selecting the option **Notify DSM Immediately**. For this option to work, the agents and appliances must be configured for agent or appliance-initiated or bidirectional communication in **Policy / Computer Editor** > **Settings** > **Computer**.) If enabled, the agent or appliance will initiate a heartbeat to the Deep Security Manager immediately upon detecting the attack or probe.

**Note:** If you want to enable reconnaissance protection, you must also enable the firewall and stateful inspection on the **Policy or Computer Editor** > **Firewall** > **General** tab. You should also go to the **Policy or Computer Editor** > **Firewall** > **Advanced** tab and enable the **Generate Firewall Events** for packets that are 'Out of Allowed Policy' setting. This will generate firewall events that are required for reconnaissance.

**Note:** The reconnaissance scans detection requires there to be at least one active firewall rule assigned to the policy of the agent.

For information on how to handle reconnaissance warnings, see "Warning: Reconnaissance Detected" on page 986.

## Stateful inspection

Deep Security firewall stateful configuration mechanism should be enabled when the firewall is on. This mechanism analyzes each packet in the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions. In the case of stateless protocols like UDP and ICMP, a pseudo-stateful mechanism is implemented based on historical traffic analysis.

Packets are handled by the stateful mechanism as follows:

1. A packet is passed to the stateful routine if it has been allowed through by the static firewall rule conditions.
2. The packet is examined to determine whether it belongs to an existing connection.
3. The TCP header is examined for correctness (for example, sequence numbers, flag combinations, and so on).

The Deep Security firewall stateful configuration enables protection against attacks such as denial of service, provided that a default configuration with stateful TCP, ICMP, or UDP protocol is enabled and only solicited replies are allowed. If the UDP stateful option is enabled, Force Allow must be used when running UDP servers (for example, DHCP). If there is no DNS or WINS server configured for the Deep Security Agents, a Force Allow Incoming UDP Ports 137 rule might be required for NetBIOS.

Stateful logging should be disabled unless required for ICMP or UDP protocols.

## Example

This is an example of how a simple firewall policy can be created for a web server:

1. Enable stateful inspection for TCP, UDP, and ICMP using a global firewall stateful configuration with these options enabled.
2. Add a firewall rule to allow TCP and UDP replies to requests originated on the workstation. To do this create an incoming Allow rule with the protocol set to **TCP + UDP** and select **Not** and **Syn** under **Specific Flags**. At this point the policy only allows TCP and UDP packets that are replies to requests initiated by a user on the workstation. For example, in conjunction with the stateful analysis options enabled in step 1, this rule allows a user on this computer to perform DNS lookups (via UDP) and to browse the Web via HTTP (TCP).

3. Add a firewall rule to allow ICMP replies to requests originated on the workstation. To do this, create an incoming Allow rule with the protocol set to **ICMP** and select the **Any Flags** check box. This means that a user on this computer can ping other workstations and receive a reply but other users will not be able to ping this computer.

4. Add a firewall rule to allow incoming TCP traffic to port 80 and 443 with the **Syn** check box checked in the **Specific Flags** section. This means that external users can access a Web server on this computer.

   At this point we have a basic firewall policy that allows solicited TCP, UDP and ICMP replies and external access to the Web server on this computer all other incoming traffic is denied.

   For an example of how Deny and Force Allow rule actions can be used to further refine this policy consider how we may want to restrict traffic from other computers in the network. For example, we may want to allow access to the Web server on this computer to internal users but deny access from any computers that are in the DMZ. This can be done by adding a Deny rule to prohibit access from servers in the DMZ IP range.

5. Add a Deny rule for incoming TCP traffic with source IP 10.0.0.0/24 which is the IP range assigned to computers in the DMZ. This rule denies any traffic from computers in the DMZ to this computer.

   We may, however, want to refine this policy further to allow incoming traffic from the mail server which resides in the DMZ.

6. Use a Force Allow for incoming TCP traffic from source IP 10.0.0.100. This Force Allow overrides the Deny rule we created in the previous step to permit traffic from this one computer in the DMZ.

## Important things to remember

- All traffic is first checked against firewall rules before being analyzed by the stateful inspection engine. If the traffic clears the firewall rules, the traffic is then analyzed by the stateful inspection engine (provided stateful inspection is enabled in the Firewall Stateful Configuration).

- Allow rules are prohibitive. Anything not specified in the Allow rules is automatically dropped. This includes traffic of other frame types so you need to remember to include rules to allow other types of required traffic. For example, don't forget to include a rule to allow ARP traffic if static ARP tables are not in use.
- If UDP stateful inspection is enabled a Force Allow rule must be used to allow unsolicited UDP traffic. For example, if UDP stateful inspection is enabled on a DNS server then a Force Allow for port 53 is required to allow the server to accept incoming DNS requests.
- If ICMP stateful inspection is enabled a Force Allow rule must be used to allow unsolicited ICMP traffic. For example, if you wish to allow outside ping requests a Force Allow rule for ICMP type 3 (Echo Request) is required.
- A Force Allow acts as a trump card only within the same priority context.
- If you do not have a DNS or WINS server configured (which is common in test environments) a "Force Allow incoming UDP port 137" rule may be required for NetBIOS (Windows shares).

**Note:** When troubleshooting a new firewall policy the first thing you should do is check the firewall rule logs on the **agent or appliance**[1]. The firewall rule logs contain all the information you need to determine what traffic is being denied so that you can further refine your policy as required.

## Create a firewall rule

Firewall rules examine the control information in individual packets, and either block or allow them according to the criteria that you define. Firewall rules can be assigned to a policy or directly to a computer.

**Note:** This article specifically covers how to create a firewall rule. For information on how to configure the firewall module, see "Set up the Deep Security firewall" on page 584.

To create a new firewall rule, you need to:

---

[1]The Deep Securty Agent and Deep Security Virtual Appliance are the components that enforce the Deep Security policies that you have defined. Agents are deployed directly on a computer. Appliances are used in VMware vSphere environments to provide agentless protection. They are not available with Deep Security as a Service.

1. "Add a new rule" below.
2. "Select the behavior and protocol of the rule" below.
3. "Select a Packet Source and Packet Destination" on page 601.

When you're done with your firewall rule, you can also learn how to:

- "Configure rule events and alerts" on page 602
- "Set a schedule for the rule" on page 602
- "See policies and computers a rule is assigned to" on page 603
- "Assign a context to the rule " on page 603

## Add a new rule

There are three ways to add a new firewall rule on the **Policies** > **Common Objects** > **Rules** > **Firewall Rules** page. You can:

- Create a new rule. Click **New** > **New Firewall Rule**.
- Import a rule from an XML file. Click **New** > **Import From File**.
- Copy and then modify an existing rule. Right-click the rule in the Firewall Rules list and then click **Duplicate**. To edit the new rule, select it and then click **Properties**.

## Select the behavior and protocol of the rule

1. Enter a **Name** and **Description** for the rule.

   **Tip:** It is good practice to document all firewall rule changes in the Description field of the firewall rule. Make a note of when and why rules were created or deleted for easier firewall maintenance.

2. Select the **Action** that the rule should perform on packets. You can select from one of the following five actions:

   **Note:** Only one rule action is applied to a packet, and rules (of the same priority) are applied in the order of precedence listed below.

- The rule can allow traffic to **bypass** the firewall. A bypass rule allows traffic to pass through the firewall and intrusion prevention engine at the fastest possible rate. Bypass rules are meant for traffic using media intensive protocols where filtering may not be desired or for traffic originating from trusted sources.

  **Tip:** For an example of how to create and use a bypass rule for trusted sources in a policy, see "Allow trusted traffic to bypass the firewall" on page 603.

  **Note:** Bypass rules are unidirectional. Explicit rules are required for each direction of traffic.

  **Tip:** You can achieve maximum throughput performance on a bypass rule with the following settings:
  - **Priority:** Highest
  - **Frame Type:** IP
  - **Protocol:** TCP, UDP, or other IP protocol. (Do not use the "Any" option.)
  - **Source and Destination IP and MAC:** all "Any"
  - If the protocol is TCP or UDP and the traffic direction is "incoming", the destination ports must be one or more specified ports (not "Any"), and the source ports must be "Any".
  - If the protocol is TCP or UDP and the traffic direction is "outgoing", the source ports must be one or more specified ports (Not "Any"), and the destination ports must be "Any".
  - **Schedule:** None.

- The rule can **log only**. This action will make entries in the logs but will not process traffic.
- The rule can **force allow** defined traffic (it will allow traffic defined by this rule without excluding any other traffic.)
- The rule can **deny** traffic (it will deny traffic defined by this rule.)
- The rule can **allow** traffic (it will exclusively allow traffic defined by this rule.)

> **Note:** If you have no allow rules in effect on a computer, all traffic is permitted unless it is specifically blocked by a deny rule. Once you create a single allow rule, all other traffic is blocked unless it meets the requirements of the allow rule. There is one exception to this: ICMPv6 traffic is always permitted unless it is specifically blocked by a deny rule.

3. Select the **Priority** of the rule. The priority determines the order in which rules are applied. If you have selected "force allow", "deny", or "bypass" as your rule action, you can set a priority of 0 (low) to 4 (highest). Setting a priority allows you to combine the actions of rules to achieve a cascading rule effect.

   > **Note:** **Log only** rules can only have a priority of **4**, and **Allow** rules can only have a priority of **0**.

   > **Note:** High priority rules get applied before low priority rules. For example, a port 80 incoming deny rule with a priority of 3 will drop a packet before a port 80 incoming force allow rule with a priority of 2 gets applied to it.

   For detailed information on how actions and priority work together, see "Firewall rule actions and priorities" on page 605.

4. Select a **Packet Direction**. Select whether this rule will be applied to **incoming** (from the network to the host) or **outgoing**(from the host to the network) traffic.

   > **Note:** An individual firewall rule only apply to a single direction of traffic. You may need to create incoming and outgoing firewall rules in pairs for specific types of traffic.

5. Select an Ethernet **Frame Type**. The term "frame" refers to Ethernet frames, and the available protocols specify the data that the frame carries. If you select "Other" as the frame type, you need to specify a frame number.

6. > **Note:** **IP** covers both IPv4 and IPv6. You can also select **IPv4** or **IPv6** individually

   > **Note:** Linux Agents will only examine packets with IP or ARP frame types. Packets with other frame types will be allowed through. Note that the Virtual Appliance does not have

these restrictions and can examine all frame types, regardless of the operating system of the virtual machine it is protecting.

If you select the Internet Protocol (IP) frame type, you need to select the transport **Protocol**. If you select "Other" as the protocol, you also need to enter a protocol number.

## Select a Packet Source and Packet Destination

Select a combination of **IP** and **MAC** addresses, and if available for the frame type, **Port** and **Specific Flags** for the Packet Source and Packet Destination.

**Tip:** You can use a previously created IP, MAC or port list.

Support for IP-based frame types is as follows:

| | IP | MAC | Port | Flags |
|---|---|---|---|---|
| Any | ✔ | ✔ | | |
| ICMP | ✔ | ✔ | | ✔ |
| ICMPV6 | ✔ | ✔ | | ✔ |
| IGMP | ✔ | ✔ | | |
| GGP | ✔ | ✔ | | |
| TCP | ✔ | ✔ | ✔ | ✔ |
| PUP | ✔ | ✔ | | |
| UDP | ✔ | ✔ | ✔ | |
| IDP | ✔ | ✔ | | |
| ND | ✔ | ✔ | | |
| RAW | ✔ | ✔ | | |
| TCP+UDP | ✔ | ✔ | ✔ | ✔ |

**Note:** ARP and REVARP frame types only support using MAC addresses as packet sources and destinations.

You can select **Any Flags** or individually select the following flags:

- URG
- ACK
- PSH
- RST
- SYN
- FIN

## Configure rule events and alerts

When a firewall rule is triggered, it logs an event in the Deep Security Manager and records the packet data.

**Note:** Note that rules using the "Allow", "Force Allow" and "Bypass" actions will not log any events.

### Alerts

You can configure rules to also trigger an alert if they log an event. To do so, open the properties for a rule, click on **Options**, and then select **Alert when this rule logs an event**.

**Note:** Only firewall rules with an action set to "Deny" or "Log Only" can be configured to trigger an alert.

## Set a schedule for the rule

Select whether the firewall rule should only be active during a scheduled time.

For more information on how to do so, see "Define a schedule that you can apply to rules" on page 454.

## Assign a context to the rule

Rule contexts allow you to set firewall rules uniquely for different network environments. Contexts are commonly used to allow for different rules to be in effect for laptops when they are on and off-site.

For more information on how to create a context, see "Define contexts for use in policies" on page 447.

> **Tip:** For an example of a policy that implements firewall rules using contexts, look at the properties of the "Windows Mobile Laptop" Policy.

## See policies and computers a rule is assigned to

You can see which policies and computers are assigned to a firewall rule on the **Assigned To** tab. Click on a policy or computer in the list to see their properties.

## Export a rule

You can export all firewall rules to a .csv or .xml file by clicking **Export** and selecting the corresponding export action from the list. You can also export specific rules by first selecting them, clicking **Export** and then selecting the corresponding export action from the list.

## Delete a rule

To delete a rule, right-click the rule in the Firewall Rules list, click **Delete** and then click **OK**.

> **Note:** Firewall Rules that are assigned to one or more computers or that are part of a policy cannot be deleted.

# Allow trusted traffic to bypass the firewall

You can set up Deep Security to allow trusted traffic to bypass the firewall.

To configure this, the basic steps are as follows:

1. "Create a new IP list of trusted traffic sources" below
2. "Create incoming and outbound firewall rules for trusted traffic using the IP list" below
3. "Assign the firewall rules to a policy used by computers that trusted traffic flows through" on the next page

After the firewall rules have been assigned to a policy, Deep Security will allow traffic from trusted sources in the IP list and will not scan the traffic for stateful issues or vulnerabilities.

## Create a new IP list of trusted traffic sources

1. Click **Policies**.
2. In the left pane, click **Lists > IP Lists**.
3. Click **New > New IP List**.
4. Enter a name for the IP list.
5. Paste the IP addresses for your trusted sources into the **IP(s)** box, one per line.
6. Click **OK**.

## Create incoming and outbound firewall rules for trusted traffic using the IP list

1. Click **Policies**.
2. In the left pane, click **Rules**.
3. Click **Firewall Rules > New > New Firewall Rule**.
4. Create a firewall rule for incoming trusted traffic using the values in the below:

| | |
|---|---|
| Name: | *source name* Traffic - Incoming |
| Action: | Bypass |
| Protocol: | Any |
| Packet Source: | IP List (select the IP list created above) |

5. Create a firewall rule for outgoing trusted traffic using the values in the below:

| | |
|---|---|
| Name: | *source name* Traffic - Outgoing |
| Action: | Bypass |
| Protocol: | Any |
| Packet Destination: | IP List (select the IP list created above) |

## Assign the firewall rules to a policy used by computers that trusted traffic flows through

1. Click **Policies**.
2. In the left pane, click **Policies**.
3. Double-click a policy to open its properties window.
4. In the left pane of the policy's properties window, click **Firewall**.
5. Click **Assign/Unassign**.
6. Ensure your view at the top left shows **All** firewall rules.
7. Use the search window to find the rules you created and select them.
8. Click **OK**.
9. Repeat the steps above for each computer that trusted traffic flows through.

# Firewall rule actions and priorities

In this article:


- "Firewall rule actions" below
- "Firewall rule sequence" on page 608
- "How firewall rules work together" on page 610
- "Rule priority" on page 611
- "Putting rule action and priority together" on page 612


## Firewall rule actions

Firewall rules can take the following actions:

- **Allow:** Explicitly allows traffic that matches the rule to pass, and then implicitly denies everything else.
- **Bypass:** Allows traffic to bypass both firewall and intrusion prevention analysis. Use this setting for media-intensive protocols or for traffic originating from trusted sources. A bypass rule can be based on IP, port, traffic direction, and protocol.

- **Deny:** Explicitly blocks traffic that matches the rule.
- **Force Allow:** Forcibly allows traffic that would otherwise be denied by other rules.

  **Note:** Traffic permitted by a Force Allow rule will still be subject to analysis by the intrusion prevention module.

- **Log only:** Traffic will only be logged. No other action will be taken.

## More about Allow rules

Allow rules have two functions:

1. Permit traffic that is explicitly allowed.
2. Implicitly deny all other traffic.

**Note:** Traffic that is not explicitly allowed by an Allow rule is dropped, and gets recorded as an 'Out of "Allowed" Policy' firewall event.

Commonly applied Allow rules include:

- **ARP**: Permits incoming Address Resolution Protocol (ARP) traffic .
- **Allow solicited TCP/UDP replies**: Ensures that the host computer is able to receive replies to its own TCP and UDP messages. This works in conjunction with TCP and UDP stateful configuration.
- **Allow solicited ICMP replies**: Ensures that the host computer is able to receive replies to its own ICMP messages. This works in conjunction with ICMP stateful configuration.

## More about Bypass rules

The Bypass rule is designed for media-intensive protocols or for traffic originating from trusted sources where filtering by the firewall or intrusion prevention modules is neither required nor desired.

A packet that matches the conditions of a Bypass rule:

- Is not subject to conditions of stateful configuration settings.
- Bypasses both firewall and Intrusion prevention analysis.

Since stateful inspection is not applied to bypassed traffic, bypassing traffic in one direction does not automatically bypass the response in the other direction. Bypass rules should always be created and applied in pairs, one rule for incoming traffic and another for outgoing.

**Note:** Bypass rule events are not recorded. This is not a configurable behavior.

**Tip:** If the Deep Security Manager uses a remote database that is protected by a Deep Security Agent, intrusion prevention-related false alarms may occur when the Deep Security Manager saves intrusion prevention rules to the database. The contents of the rules themselves could be misidentified as an attack. One of the workarounds for this is to create a bypass rule for traffic from the Deep Security Manager to the database host.

### Default Bypass rule for Deep Security Manager traffic

The Deep Security Manager automatically implements a priority 4 Bypass rule that opens incoming TCP traffic on the agent's listening port for heartbeats (see "Configure the heartbeat" on page 196) on computers running Deep Security Agent. Priority 4 ensures that this rule is applied before any Deny rules, and Bypass guarantees that the traffic is never impaired. The Bypass rule is not explicitly shown in the firewall rule list because the rule is created internally.

This rule, however, accepts traffic from any IP address and any MAC address. To harden the agent's security on this port, you can create an alternative, more restrictive bypass rule for this port. The agent will actually disable the default Deep Security Manager traffic rule in favor of the new custom rule provided it has these characteristics:

- **Priority:** 4 - Highest
- **Packet direction:** Incoming
- **Frame type:** IP
- **Protocol:** TCP
- **Packet Destination Port:** agent's listening port number for heartbeats from the Manager

The custom rule must use the above parameters to replace the default rule. Ideally, the IP address or MAC address of the actual Deep Security Manager should be used as the packet source for the rule.

### More about Force Allow rules

The Force Allow option excludes a sub-set of traffic that could otherwise have been covered by a Deny action. Its relationship to other actions is illustrated below. Force Allow has the same effect as a Bypass rule. However, unlike Bypass, traffic that passes the firewall because of this action is still subject to inspection by the intrusion prevention module. The Force Allow action is particularly useful for making sure that essential network services are able to communicate with the DSA computer. Generally, Force Allow rules should only be used in conjunction with Allow and rules to Allow a subset of traffic that has been prohibited by the Allow and Deny rules. Force Allow rules are also required to Allow unsolicited ICMP and UDP traffic when ICMP and UDP stateful are enabled.

**Note:** When using multiple Deep Security Managers in a multi-node arrangement, it may be useful to define an IP list for these servers, and then create a custom Deep Security Manager traffic rule with that list.

## Firewall rule sequence

Packets arriving at a computer get processed first by firewall rules, then the firewall stateful configuration conditions, and finally by the intrusion prevention rules.

This is the order in which firewall rules are applied (incoming and outgoing):

1. Firewall rules with priority **4 (highest)**
   a. **Bypass**
   b. **Log Only** (Log Only rules can only be assigned a priority of **4 (highest)**)
   c. **Force Allow**
   d. **Deny**
2. Firewall rules with priority **3 (high)**
   a. **Bypass**
   b. **Force Allow**
   c. **Deny**
3. Firewall rules with priority **2 (normal)**
   a. **Bypass**
   b. **Force Allow**
   c. **Deny**

4. Firewall rules with priority **1 (low)**
    a. **Bypass**
    b. **Force Allow**
    c. **Deny**
5. Firewall rules with priority **0 (lowest)**
    a. **Bypass**
    b. **Force Allow**
    c. **Deny**
    d. **Allow**(Note that an Allow rule can only be assigned a priority of **0 (lowest)**)

**Note:** If you have no Allow rules in effect on a computer, all traffic is permitted unless it is specifically blocked by a Deny rule. Once you create a single Allow rule, all other traffic is blocked unless it meets the conditions of the Allow rule. There is one exception to this: ICMPv6 traffic is always permitted unless it is specifically blocked by a Deny rule.

Within the same priority context, a Deny rule will override an Allow rule, and a Force Allow rule will override a Deny rule. By using the rule priorities system, a higher priority Deny rule can be made to override a lower priority Force Allow rule.

Consider the example of a DNS server policy that makes use of a Force Allow rule to Allow all incoming DNS queries. Creating a Deny rule with a higher priority than the Force Allow rule lets you specify a particular range of IP addresses that must be prohibited from accessing the same public server.

Priority-based rule sets allow you set the order in which the rules are applied. If a Deny rule is set with the highest priority, and there are no Force Allow rules with the same priority, then any packet matching the Deny rule is automatically dropped and the remaining rules are ignored. Conversely, if a Force Allow rule with the highest priority flag set exists, any incoming packets matching the Force Allow rule will be automatically allowed through without being checked against any other rules.

## A note on logging

Bypass rules will never generate an event. This is not configurable.

Log Only rules will only generate an event if the packet in question is not subsequently stopped by either:

- a Deny rule, or
- an Allow rule that excludes it.

If the packet is stopped by one of those two rules, those rules will generate the Event and not the Log Only rule. If no subsequent rules stop the packet, the Log Only rule will generate an event.

## How firewall rules work together

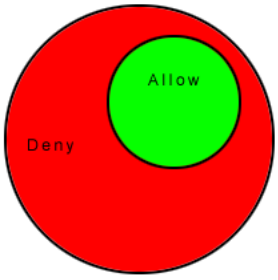
Deep Security firewall rules have both a rule action and a rule priority. Used in conjunction, these two properties allow you to create very flexible and powerful rule-sets. Unlike rule-sets used by other firewalls, which may require that the rules be defined in the order in which they should be run, Deep Security Firewall rules are run in a deterministic order based on the rule action and the rule priority, which is independent of the order in which they are defined or assigned.

### Rule Action

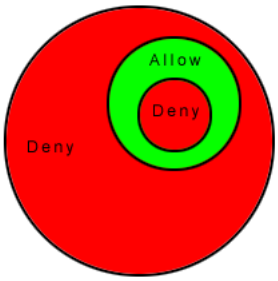
Each rule can have one of four actions.

1. **Bypass:** if a packet matches a Bypass rule, it is passed through both the firewall *and the Intrusion Prevention Engine* regardless of any other rule (at the same priority level).
2. **Log Only:** if a packet matches a Log Only rule it is passed and the event is logged.
3. **Force Allow:** if a packet matches a Force Allow rule it is passed regardless of any other rules (at the same priority level).
4. **Deny:** if a packet matches a Deny rule it is dropped.
5. **Allow:** if a packet matches an Allow rule, it is passed. Any traffic not matching one of the Allow rules is denied.

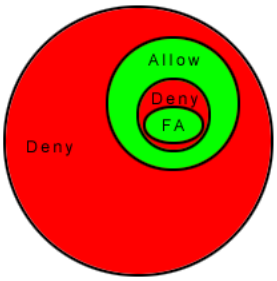
Implementing an Allow rule will cause all other traffic not specifically covered by the Allow rule to be denied:




A Deny rule can be implemented over an Allow to block specific types of traffic:




A Force Allow rule can be placed over the denied traffic to Allow certain exceptions to pass through:




## Rule priority

Rule actions of type Deny and Force Allow can be defined at any one of 5 priorities to allow further refinement of the permitted traffic defined by the set of Allow rules. Rules are run in priority order from highest (Priority 4) to lowest (Priority 0). Within a specific priority level the rules are processed in order based on the rule action (Force Allow, Deny, Allow, log only).

The priority context Allows a User to successively refine traffic controls using Deny and Force Allow rule combinations. Within the same priority context, an Allow rule can be negated with a Deny rule, and a Deny rule can be negated by a Force Allow rule.

**Note:** Rule actions of type Allow run only at priority 0 while rule actions of type Log Only run only at priority 4.

### Putting rule action and priority together

Rules are run in priority order from highest (Priority 4) to lowest (Priority 0). Within a specific priority level the rules are processed in order based on the rule action. The order in which rules of equal priority are processed is as follows:

- Bypass
- Log Only
- Force Allow
- Deny
- Allow

**Note:** Remember that rule actions of type Allow run only at priority 0 while rule actions of type Log Only run only at priority 4.

**Note:** It is important to remember that if you have a Force Allow rule and a Deny rule at the same priority the Force Allow rule takes precedence over the Deny rule and therefore traffic matching the Force Allow rule will be permitted.

## Firewall settings

The **Firewall** module provides bidirectional stateful firewall protection. It prevents denial of service attacks and provides coverage for all IP-based protocols and frame types as well as filtering for ports and IP and MAC addresses.

The Firewall section of the **Computer or Policy editor**[1] has the following tabbed sections:


- "General" below
- "Interface Isolation" on page 615
- "Reconnaissance" on page 615
- "Advanced" on page 618
- "Events" on page 618


**Note:** This article includes references to the Deep Security Virtual Appliance, which is not available with Deep Security as a Service.

## General

### Firewall

You can configure this policy or computer to inherit its firewall On/Off state from its parent policy or you can lock the setting locally.

### Firewall Stateful Configurations

Select which firewall stateful configuration to apply to this policy. If you have defined multiple Interfaces for this policy (above), you can specify independent configurations for each interface. For more information on creating a stateful configuration see "Define stateful firewall configurations" on page 625.

### Port Scan (Computer Editor only)

**Last Port Scan:** The last time that the Deep Security manager ran a port scan on this computer.

**Scanned Ports:** The ports that were scanned during the most recent port scan.

---

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

**Open Ports:** Listed beneath the IP address of the local computer will be a list of ports that were found to be open.

The **Scan For Open Ports** and the **Cancel Port Scan** buttons let you initiate or cancel a port scan on this computer. Deep Security Manager will scan the range of ports defined in **Computer or Policy editor**[1] **> Settings > General > Open Ports > Ports to Scan**.

> **Note:** Regardless of the ports configured to be scanned, Deep Security Manager will always scan the agent or appliance's listening port number for heartbeat connections from the Manager.

## Assigned Firewall Rules

Displays the firewall rules that are in effect for this policy or computer. To add or remove firewall rules, click **Assign/Unassign** This will display a window showing all available firewall rules from which you can select or deselect rules.

From a **Computer or Policy editor**[2] window, you can edit a firewall rule so that your changes apply only locally in the context of your editor, or you can edit the rule so that the changes apply globally to all other policies and computers that are using the rule.

**To edit the Rule locally,** right-click the rule and click **Properties**.

**To edit the Rule globally,** right-click the rule and click **Properties (Global)**.

For more information on creating firewall rules, see "Create a firewall rule" on page 597.

---

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

# Interface Isolation

## Interface Isolation

You can configure this policy or computer to inherit its Interface Isolation enabled or disabled state from its parent policy or you can lock the setting locally.

**Warning:** Before you enable Interface Isolation make sure that you have configured the interface patterns in the proper order and that you have removed or added all necessary string patterns. Only interfaces matching the highest priority pattern will be permitted to transmit traffic. Other interfaces (which match any of the remaining patterns on the list) will be "restricted". Restricted Interfaces will block all traffic unless an Allow Firewall Rule is used to allow specific traffic to pass through.

## Interface Patterns

When Interface Isolation is enabled, the firewall will try to match the regular expression patterns to interface names on the local computer.

**Note:** Deep Security uses POSIX basic regular expressions to match interface names. For information on basic POSIX regular expressions, see http://pubs.opengroup.org/onlinepubs/009695399/basedefs/xbd_chap09.html#tag_09_03

Only interfaces matching the highest priority pattern will be permitted to transmit traffic. Other interfaces (which match any of the remaining patterns on the list) will be "restricted". Restricted Interfaces will block all traffic unless an **Allow** firewall rule is used to allow specific traffic to pass through.

Selecting **Limit to one active interface** will restrict traffic to only a single interface (even if more than one interface matches the highest priority pattern).

# Reconnaissance

## Reconnaissance Scans

The **Reconnaissance** page allows you to enable and configure traffic analysis settings on your computers. This feature can detect possible reconnaissance scans that attackers often use to

discover weaknesses before beginning a targeted attack.

- **Reconnaissance Scan Detection Enabled:** Turn the ability to detect reconnaissance scans on or off.
- **Computers/Networks on which to perform detection:** Choose from the list the IPs to protect. Choose from existing IP Lists. (You can use the **Policies > Common Objects > Lists > IP Lists** page to create an IP List specifically for this purpose.)
- **Do not perform detection on traffic coming from:** Select from a set of IP Lists which computers and networks to ignore. (As above, you can use the **Policies > Common Objects > Lists > IP Lists** page to create an IP List specifically for this purpose.)

**Note:** If you want to enable reconnaissance protection, you must also enable the Firewall and Stateful Inspection on the **Computer or Policy editor**[1] **> Firewall > General** tab. You should also go to the **Computer or Policy editor**[2] **> Firewall > Advanced** tab and enable the **Generate Firewall Events for packets that are 'Out of Allowed Policy'** setting. This will generate firewall events that are required for reconnaissance.

For each type of attack, the **agent or appliance**[3] can be instructed to send the information to the Deep Security Manager where an alert will be triggered. You can configure the Deep Security Manager to send an email notification when the alerts are triggered. (See **Administration > System Settings > Alerts**. The alerts are: "Network or Port Scan Detected", "Computer OS Fingerprint Probe Detected", "TCP Null Scan Detected", "TCP FIN Scan Detected", and "TCP Xmas Scan Detected.") Select **Notify DSM Immediately** for this option.

---

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[3]The Deep Securty Agent and Deep Security Virtual Appliance are the components that enforce the Deep Security policies that you have defined. Agents are deployed directly on a computer. Appliances are used in VMware vSphere environments to provide agentless protection. They are not available with Deep Security as a Service.

**Note:** For the "Notify DSM Immediately" option to work, the agents and appliances must be configured for **agent or appliance-initiated** or **bidirectional** communication in **Computer or Policy editor**[1] **> Settings > General.**) If enabled, the agent or appliance will initiate a heartbeat to the Deep Security Manager immediately upon detecting the attack or probe.

Once an attack has been detected, you can instruct the agents and appliances to block traffic from the source IPs for a period of time. Use the **Block Traffic** lists to set the number of minutes.

- **Computer OS Fingerprint Probe:** The agent or appliance detects an attempt to discover the computers OS.
- **Network or Port Scan:** The agent or appliance reports a network or port scan if it detects that a remote IP is visiting an abnormal ratio of IPs to ports. Normally, an agent or appliance computer will only see traffic destined for itself, so a port scan is the most common type of probe that will be detected. The statistical analysis method used in computer or port scan detection is derived from the "TAPS" algorithm proposed in the paper "Connectionless Port Scan Detection on the Backbone" presented at IPCCC in 2006.
- **TCP Null Scan:** The agent or appliance detects packages with no flags set.
- **TCP SYNFIN Scan:** The agent or appliance detects packets with only the SYN and FIN flags set.
- **TCP Xmas Scan:** The agent or appliance detects packets with only the FIN, URG, and PSH flags set or a value of 0xFF (every possible flag set).

**Note:** "Network or Port Scans" differs from the other types of reconnaissance in that it cannot be recognized by a single packet and requires Deep Security to watch traffic for a period of time.
The agent or appliance reports a computer or port scan if it detects that a remote IP is visiting an abnormal ratio of IPs to ports. Normally an agent or apppliance computer will only see traffic destined for itself, so a port scan is by far the most common type of probe that will be detected.

---

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

However, if a computer is acting as a router or bridge it could see traffic destined for a number of other computers, making it possible for the agent or appliance to detect a computer scan (ex. scanning a whole subnet for computers with port 80 open).
Detecting these scans can take several seconds since the agent or appliance needs to be able to track failed connections and decide that there are an abnormal number of failed connections coming from a single computer in a relatively short period of time.

**Note:** Deep Security Agents running on Windows computers with browser applications may occasionally report false-positive reconnaissance scans due to residual traffic arriving from closed connections.

For information on how to handle reconnaissance warnings, see "Warning: Reconnaissance Detected" on page 986.

## Advanced

### Events

Set whether to generate events for packets that are "Out of Allowed Policy". These are packets that have been blocked because they have not been specifically allowed by an **Allow** firewall rule. Setting this option to **Yes** may generate a large number of events depending on the firewall rules you have in effect.

## Events

Firewall events are displayed the same way as they are in the main Deep Security Manager window except that only events relating to this policy or specific computer are displayed.

# Firewall settings with Oracle RAC

Deep Security supports:

- SUSE Linux Enterprise Server 11 SP3 with Oracle RAC 12c Release 1 (v12.1.0.2.0)
- Red Hat Linux Enterprise Server 6.6 with Oracle RAC 12c Release 1 (v12.1.0.2.0)
- Red Hat Linux Enterprise Server 7.0 with Oracle RAC 12c Release 1 (v12.1.0.2)

The default Linux Server Deep Security policy is compatible with the Oracle RAC environment, with the exception of firewall settings. Because there are complex communication channels between RAC nodes, the RAC nodes will fail to create a virtual NIC and scan the NIC, due to firewall interference. As a result, Oracle Clusterware would fail to start on some nodes. You can disable the firewall or customize the firewall settings.

## Add a rule to allow communication between nodes

1. In the Deep Security Manager, go to the **Policies** tab.
2. Right-click the **Linux Server** policy and click **Duplicate**.
3. Click the new **Linux Server_2** policy and click **Details**.
4. Give the policy a new name, for example, "Oracle RAC" and click **Save**.
5. Click **Firewall**.
6. Click **Assign/Unassign**.
7. Click **New > New Firewall Rule**.
8. Under **General Information**, set the **Name** to something descriptive, like "Allow communication with Oracle nodes". Set **Action** to "Force Allow" and set **Protocol** to "Any".
9. Under **Packet Source**, set **MAC** to "MAC List". In the **Select MAC List** that appears, select "New". A "New MAC List Properties" dialog box appears.
10. Give the MAC list a name, like "Oracle RAC MAC list". Under **MAC(s): (One MAC per line)**, add all of the MAC addresses used by all Oracle nodes (including MACs from both private and public NICs). Click **OK** when finished.
11. Under **Packet Destination**, set **MAC** to "MAC List". In the **Select MAC List** that appears, select the MAC list you created in step 10 and then click **OK**.
12. In the Firewall Rules list for the policy, ensure that this new rule is selected and click **OK** and then click **Save**.

## Add a rule to allow UDP port 42424

Follow the steps described in the procedure above to add a new rule that allows UDP port 42424. This port number is used by the Cluster Synchronization Service daemon (CSSD), Oracle Grid Interprocess Communication (GIPCD) and Oracle HA Services daemon (OHASD).

**Note:** Please note that the MAC list that you created above may not be able to cover this rule. This rule is essential for Oracle RAC.

General | Options | Assigned To

**General Information**

Name: New Firewall Rule

Description:

Action: Force Allow

Priority: 0 - Lowest

Packet direction: Incoming

Frame Type: IP — Not

Protocol: UDP — Not

**Packet Source**

IP: Any — Not

MAC: Any — Not

Port: Any — Not

**Packet Destination**

IP: Any — Not

MAC: Any — Not

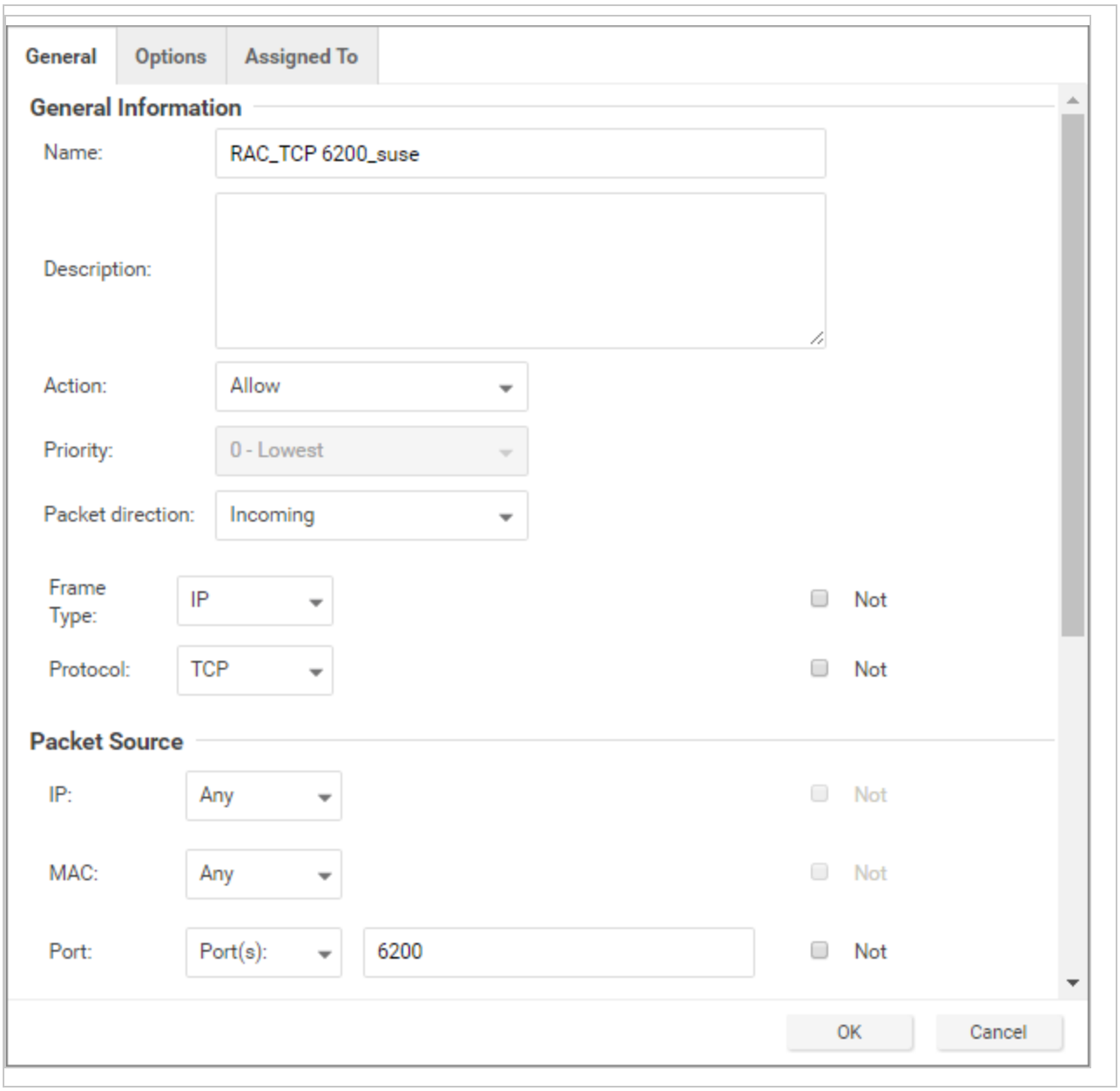
Port: Port(s): 42424 — Not

OK | Cancel

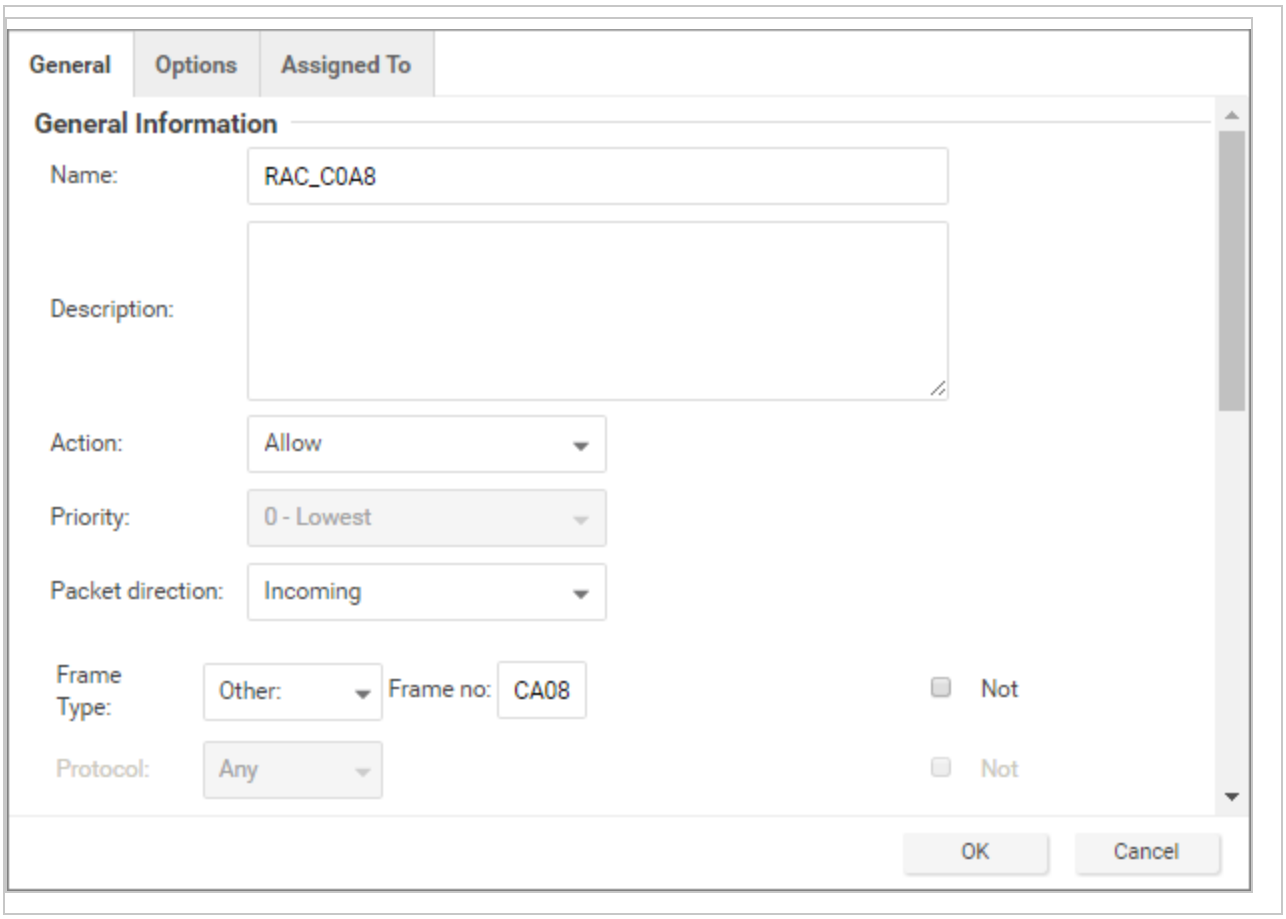
## Allow other RAC-related packets

Oracle RAC will send a very large number of packets with Frame Type C08A and 0ACB. Blocking them may cause some unpredictable behavior.

- **Allow TCP post 6200:** Add the public IP addresses of the RAC nodes in the **IP** fields under **Packet Source** and **Packet Destination** and set destination port to 6200. This port number is used by Oracle Notification Services (ONS). This port is configurable, so check the value on your system set the correct port number if it is something other than 6200.

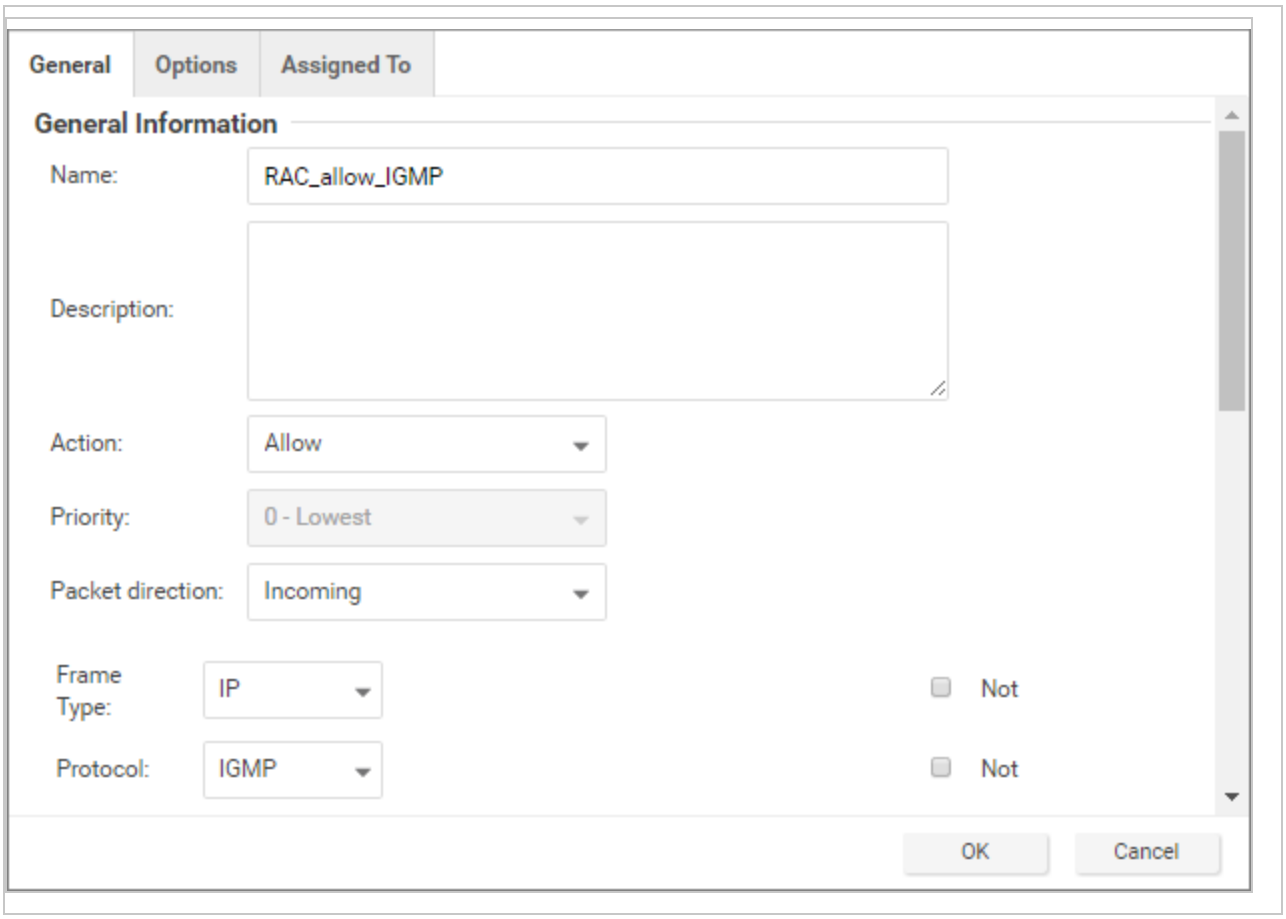



- **Allow Frame Type C0A8:** Add a rule with the **Frame Type** set to "Other" and the **Frame no** set to "C0A8".




- **Allow Frame Type 0ACB:** Add a rule with the **Frame Type** set to "Other" and the **Frame no** set to "0ACB".
- **Allow Frame Type 0AC9:** Add a rule with the **Frame Type** set to "Other" and the **Frame no** set to "0AC9".

- **Allow IGMP protocol:** Add a rule with the **Protocol** set to "IGMP".




Please refer to the following link to check whether there are additional RAC-related components in your system that need extra firewall rules to allow certain ports:

https://docs.oracle.com/database/121/RILIN/ports.htm#RILIN1178

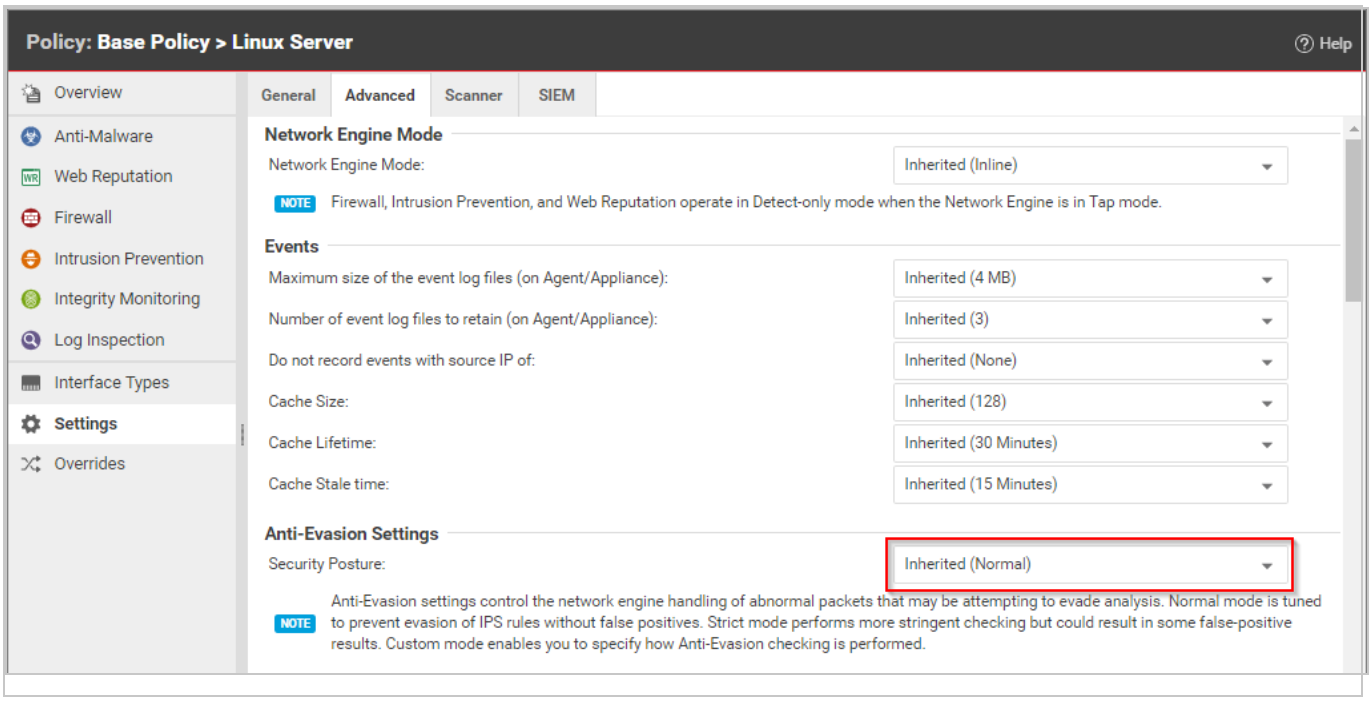
## Ensure that the Oracle SQL Server rule is assigned

Check that the "Oracle SQL Server" Firewall rule is assigned to the Linux Server policy. This is a pre-defined Deep Security Firewall rule that allows port 1521.

## Ensure that anti-evasion settings are set to "Normal"

In the properties for the Linux Server policy, **Settings > Network Engine > Anti-Evasion Settings** are set to "Normal" by default. If this setting is set to "Strict", the RAC database response will be

extremely slow.




## Define stateful firewall configurations

Deep Security's stateful firewall configuration mechanism analyzes each packet in the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions. In the case of stateless protocols like UDP and ICMP, a pseudo-stateful mechanism is implemented based on historical traffic analysis. Packets are handled by the stateful mechanism as follows:

1. A packet is passed to the stateful routine if it has been allowed through by the static firewall rule conditions,
2. The packet is examined to determine whether it belongs to an existing connection, and
3. The TCP header is examined for correctness (e.g. sequence numbers, flag combinations, etc.).

To create a new stateful configuration, you need to:

1. "Add a stateful configuration " on the next page.
2. "Enter stateful configuration information" on the next page.
3. "Select packet inspection options" on the next page.

When you're done with your stateful configuration, you can also learn how to


- "See policies and computers a stateful configuration is assigned to" on page 630
- "Export a stateful configuration " on page 630
- "Delete a stateful configuration " on page 630


## Add a stateful configuration

There are three ways to define a stateful configuration on the **Policies > Common Objects > Other > Firewall Stateful Configurations** page:

- Create a new configuration. Click **New** > **New Firewall Stateful Configuration**.
- Import a configuration from an XML file. Click **New** > **Import From File**.
- Copy and then modify an existing configuration. Right-click the configuration in the Firewall Stateful Configurations list and then click **Duplicate**. To edit the new configuration, select it and then click **Properties**.

## Enter stateful configuration information

Enter a **Name** and **Description** for the configuration.

## Select packet inspection options

You can define options for IP, TCP, UDP and ICMP packet inspection, end enable Active or Passive FTP.

### IP packet inspection

Under the **General** tab, select the **Deny all incoming fragmented packets** to drop any fragmented packets. Dropped packets will bypass fragmentation analysis and generate an "IP fragmented packet" log entry. Packets with a total length smaller than the IP header length are dropped silently.

**Warning:** Attackers sometimes create and send fragmented packets in an attempt to bypass Firewall Rules.

**Note:** The Firewall Engine, by default, performs a series of checks on fragmented packets. This is default behavior and cannot be reconfigured. Packets with the following characteristics are dropped:

- **Invalid fragmentation flags/offset:** A packet is dropped when either the **DF** and **MF** flags in the IP header are set to 1, or the header contains the **DF** flag set to 1 and an **Offset** value different than 0.
- **First fragment too small:** A packet is dropped if its **MF** flag is set to 1, its **Offset** value is at 0, and it has total length of less than 120 bytes (the maximum combined header length).
- **IP fragment out of boundary:** A packet is dropped if its **Offset** flag value combined with the total packet length exceeds the maximum datagram length of 65535 bytes.
- **IP fragment offset too small:** A packet is dropped if it has a non-zero **Offset** flag with a value that is smaller than 60 bytes.

## TCP packet inspection

Under the **TCP** tab, select which of the following options you would like to enable:

- **Deny TCP packets containing CWR, ECE flags:** These flags are set when there is network congestion.

  **Note:** RFC 3168 defines two of the six bits from the Reserved field to be used for ECN (Explicit Congestion Notification), as follows:

  - Bits 8 to 15: CWR-ECE-URG-ACK-PSH-RST-SYN-FIN
  - TCP Header Flags Bit Name Reference:
    - Bit 8: CWR (Congestion Window Reduced) [RFC3168]
    - Bit 9: ECE (ECN-Echo) [RFC3168]

  **Warning:** Automated packet transmission (such as that generated by a denial of service attack, among other things) will often produce packets in which these flags are set.

- **Enable TCP stateful inspection:** Enable stateful inspection at the TCP level. If you enable stateful TCP inspection, the following options become available:
  - **Enable TCP stateful logging:** TCP stateful inspection events will be logged.
  - **Limit the number of incoming connections from a single computer to:** Limiting the number of connections from a single computer can lessen the effect of a denial of service attack.
  - **Limit the number of outgoing connections to a single computer to:** Limiting the number of outgoing connections to a single computer can significantly reduce the effects of Nimda-like worms.
  - **Limit the number of half-open connections from a single computer to:** Setting a limit here can protect you from DoS attacks like SYN Flood. Although most servers have timeout settings for closing half-open connections, setting a value here can prevent half-open connections from becoming a significant problem. If the specified limit for SYN-SENT (remote) entries is reached, subsequent TCP packets from that specific computer will be dropped.

    Note: When deciding on how many open connections from a single computer to allow, choose your number from somewhere between what you would consider a reasonable number of half-open connections from a single computer for the type of protocol being used, and how many half-open connections from a single computer your system can maintain without getting congested.

  - **Enable ACK Storm protection when the number of already acknowledged packets exceeds:** Set this option to log an event that an ACK Storm attack has occurred.
    - **Drop Connection when ACK Storm detected:** Set this option to drop the connection if such an attack is detected.

    Note: ACK Storm protection options are only available on Deep Security Agent 8.0 and earlier.

## FTP Options

Under the **FTP Options** tab, you can enable the following options:

Note: The following FTP options are available in Deep Security Agent version 8.0 and earlier.

- Active FTP
  - **Allow Incoming:** Allow Active FTP when this computer is acting as a server.
  - **Allow Outgoing:** Allow Active FTP when this computer is acting as client.
- Passive FTP
  - **Allow Incoming:** Allow Passive FTP when this computer is acting as a server.
  - **Allow Outgoing:** Allow Passive FTP when this computer is acting as a client.

## UDP packet inspection

Under the **UDP** tab, you can enable the following options:

- **Enable UDP stateful inspection:** Select to enable stateful inspection of UDP traffic.

  Note: The UDP stateful mechanism drops unsolicited incoming UDP packets. For every outgoing UDP packet, the rule will update its UDP "stateful" table and will then only allow a UDP response if it occurs within 60 seconds of the request. If you wish to allow specific incoming UDP traffic, you will have to create a **Force Allow** rule. For example, if you are running a DNS server, you will have to create a **Force Allow** rule to allow incoming UDP packets to destination port 53.

  Warning: Without stateful inspection of UDP traffic, an attacker can masquerade as a DNS server and send unsolicited UDP "replies" from source port 53 to computers behind a firewall.

  - **Enable UDP stateful logging:** Selecting this option will enable the logging of UDP stateful inspection events.

## ICMP packet inspection

Under the **ICMP** tab, you can enable the following options:

Note: ICMP stateful inspection is available in Deep Security Agent version 8.0 or earlier.

- **Enable ICMP stateful inspection:** Select to enable stateful inspection of ICMP traffic.

  **Note:** The ICMP (pseudo-)stateful mechanism drops incoming unsolicited ICMP packets. For every outgoing ICMP packet, the rule will create or update its ICMP "stateful" table and will then only allow a ICMP response if it occurs within 60 seconds of the request. (ICMP pair types supported: Type 0 & 8, 13 & 14, 15 & 16, 17 & 18.)

  **Warning:** With stateful ICMP inspection enabled, you can, for example, only allow an ICMP echo-reply in if an echo-request has been sent out. Unrequested echo-replies could be a sign of several kinds of attack including a Smurf amplification attack, a Tribe Flood Network communication between master and daemon, or a Loki 2 back-door.

  - **Enable ICMP stateful logging:** Selecting this option will enable the logging of ICMP stateful inspection events.

## Export a stateful configuration

You can export all stateful configurations to a .csv or .xml file by clicking **Export** and selecting the corresponding export action from the list. You can also export specific stateful configurations by first selecting them, clicking **Export** and then selecting the corresponding export action from the list.

## Delete a stateful configuration

To delete a stateful configuration, right-click the configuration in the Firewall Stateful Configurations list, click **Delete** and then click **OK**.

**Note:** Stateful configurations that are assigned to one or more computers or that are part of a policy cannot be deleted.

## See policies and computers a stateful configuration is assigned to

You can see which policies and computers are assigned to a stateful inspection configuration on the **Assigned To** tab. Click on a policy or computer in the list to see their properties.

# Scan for open ports

The Deep Security Manager can be instructed to scan a computer for open ports by right-clicking the computer and selecting **Actions > Scan for Open ports**, or by clicking the **Scan for Open Ports** button in the **Firewall** page of the **Computer editor**[1] window (where the results of the latest scan are displayed).

(Port scans can also be initiated by right-clicking an existing computer on the Manager's **Computers** page and choosing "Scan for Open Ports". Another way to initiate port scans is to create a **Scheduled Task** to regularly carry out port scans on a list of computers.)

By default, the range of ports that are scanned is the range known as the "Common Ports", 1-1024, but you can define a different set of ports to scan.

**Note:** The agent's port number for incoming heartbeat connections from the Manager is always scanned regardless of port range settings. It is the port on the computer to which communications initiated by the Manager are sent. If communication direction is set to "Agent/Appliance Initiated" for a computer (**Computer or Policy editor**[2] **> Settings > General**), however, that port number will be closed.

1. Go to **Policies > Common Objects > Lists > Port Lists** and click **New** in the menu bar. The **New Port List** window will appear.
2. Type a name and description for the new port list and then define the ports in the **Port(s)** text box using the accepted formats. (For example, to scan ports 100, 105, and 110 through 120, you would type "100" on the first line "105" on the second, and "110-120" on the third.) Click **OK**.

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

3. Go to **Computer or Policy editor**[1] > **Settings** > **General** and click the "Ports to Scan" menu. Your newly defined Port List will be one of the choices.

# Monitor for system changes with integrity monitoring

The integrity monitoring module scans for unexpected changes to registry values, registry keys, services, processes, installed software, ports and files on Deep Security Agents. Using a baseline secure state as a reference, the integrity monitoring module performs scans on the above and logs an event (and an optional alert) if it detects any unexpected changes.

To enable and configure integrity monitoring, see "Set up integrity monitoring" below.

To more information on creating integrity monitoring rules, see "Create an integrity monitoring rule" on page 640. You can create a rule from a file or registry monitoring template, or by using the Deep Security XML-based "Integrity monitoring rules language" on page 645.

## Set up integrity monitoring

The Integrity Monitoring protection module detects changes to files and critical system areas like the Windows registry that could indicate suspicious activity. It does this by comparing current conditions to a baseline reading it has previously recorded. Deep Security ships with predefined Integrity Monitoring rules and new Integrity Monitoring rules are provided in security updates.

**Note:** Integrity Monitoring detects changes made to the system, but will not prevent or undo the change.

### How to enable Integrity Monitoring

You can enable Integrity Monitoring in policies or at the computer level. To do so, you will need to:

---

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

1. "Turn on Integrity Monitoring" below.
2. "Run a Recommendation scan" on the next page.
3. "Apply the Integrity Monitoring rules" on page 635.
4. "Build a baseline for the computer" on page 637.
5. "Periodically scan for changes" on page 637.

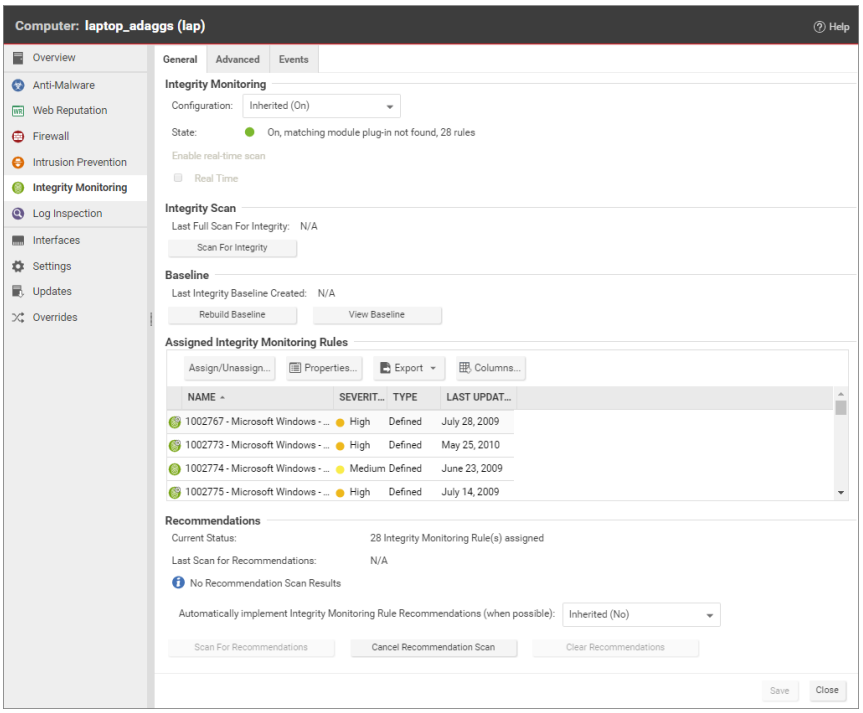
Once you've enabled integrity monitoring, you can also learn more about

- "When Integrity Monitoring scans are performed" on page 637
- "Integrity Monitoring scan performance settings" on page 638
- "Integrity Monitoring event tagging" on page 639

Following is a typical procedure for enabling Integrity Monitoring:

## Turn on Integrity Monitoring

You can enable Integrity Monitoring in the settings for a computer or in policies. To do this, open the Policy or Computer editor and go to **Integrity Monitoring** > **General**. Set the Configuration to "On" or "Inherited (On)" and then click **Save**.




## Run a Recommendation scan

Run a Recommendation scan on the computer to get recommendations about which rules would be appropriate. To do this, open the Computer editor and go to **Integrity Monitoring** > **General**. In the Recommendations section, click **Scan for Recommendations**. You can optionally specify that Deep Security should implement the rule recommendations that it finds.

Recommended Integrity Monitoring rules may result in too many monitored entities and attributes. The best practice is to decide what is critical and should be monitored, then create custom rules or tune the predefined rules. Pay extra attention to rules that monitor frequently-

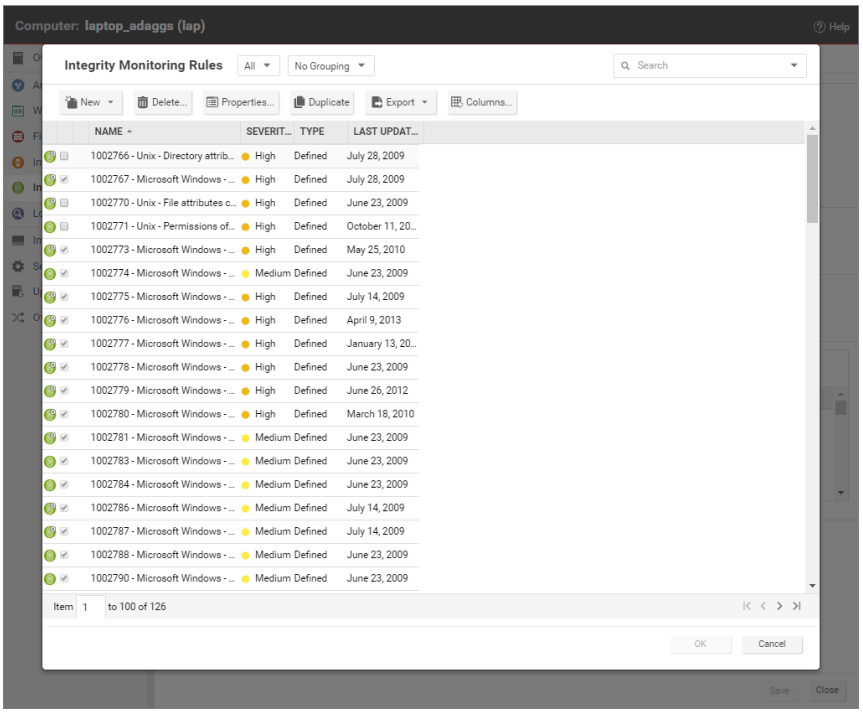
changed properties such as process IDs and source port numbers because they can be noisy and may need some tuning.

If you have enabled real-time integrity monitoring scans and find that some recommended rules produce too many events because they are monitoring directories that change frequently, you can disable real-time scanning for those rules. Go to **Policies > Common Objects > Rules > Integrity Monitoring Rules** and double-click the rule. On the **Options** tab, clear the **Allow Real Time Monitoring** checkbox.

## Apply the Integrity Monitoring rules

As described above, when you run a Recommendation scan, you can have Deep Security implement the recommended rules automatically. You can also manually assign rules.

In the Computer or Policy editor, go to **Integrity Monitoring** > **General**. The "Assigned Integrity Monitoring Rules" section displays the rules that are in effect for this policy or computer. To add or remove Integrity Monitoring Rules, click **Assign/Unassign**. This will display a window showing all available Integrity Monitoring Rules, from which you can select or deselect rules.




Some Integrity Monitoring rules written by Trend Micro require local configuration to function properly. If you assign one of these rules to your computers or one of these rules gets assigned automatically, an alert will be raised to notify you that configuration is required.

You can edit an Integrity Monitoring rule locally so that the changes apply only to the computer or policy being edited, or globally so that the changes apply to all other policies or computers that are using the rule. To edit a rule locally, right-click it and click **Properties**. To edit a rule globally, right-click it and click **Properties (Global)**.

You can also create custom rules to monitor for specific changes that concern your organization, such as a new user being added or new software being installed. For information on how to create a custom rule, see "Integrity monitoring rules language" on page 645.

**Tip:** Integrity Monitoring rules should be as specific as possible to improve performance and to avoid conflicts and false positives. For example, do not create a rule that monitors the entire hard drive.

### Build a baseline for the computer

The baseline is the original secure state that an Integrity Scan's results will be compared against. To create a new baseline for Integrity Scans on a computer, open the Computer editor, go to **Integrity Monitoring** > **General** and click **Rebuild Baseline**.

To view the current baseline data, click **View Baseline**.

**Tip:** It's a best practice to run a new baseline scan after applying patches.

### Periodically scan for changes

Periodically scan for changes. To perform an on-demand scan, open the Computer editor, go to **Integrity Monitoring** > **General** and click **Scan for Integrity**. You can also create a scheduled task that performs scans on a regular basis.

## When Integrity Monitoring scans are performed

There are three options for performing Integrity Monitoring scans:

- **On-demand scans:** You can initiate an on-demand integrity monitoring scan as needed by opening the **Computer editor**[1], and going to **Integrity Monitoring > General**. In the Integrity Scan section, click **Scan for Integrity**.
- **Scheduled scans:** You can schedule integrity monitoring scans just like other Deep Security operations. Deep Security checks the entities that are being monitored and identifies and records an event for any changes since the last time it performed a scan.

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

Multiple changes to monitored entities between scans will not be tracked; only the last change will be detected. To detect and report multiple changes to an entity's state, consider increasing the frequency of scheduled scans (for example, daily instead of weekly) or enable real-time scanning for entities that change frequently. To enable scheduled integrity monitoring scans, go to **Administration > Scheduled Tasks > New**. In the New Scheduled Task Wizard, select **Scan Computers for Integrity Changes** and the frequency for the scheduled scan. Fill in the information requested by the New Scheduled Task Wizard with your desired specifications. For more information on scheduled tasks, see "Schedule Deep Security to perform tasks" on page 263.

- **Real-time scans:** You can enable real-time scanning. When this option is selected, Deep Security monitors entities for changes in real time and raises integrity monitoring events when it detects changes. Events are forwarded in real time via syslog to the SIEM or when the next heartbeat communication to the Deep Security Manager occurs. To enable real-time scans, go to the **Computer or Policy Editor**[1] **> Integrity Monitoring > General** and select **Real Time**. With Deep Security Agent 11.0 or higher on 64-bit Linux platforms, the real-time scan results indicate the user and process that changed the file. For details about which platforms support this feature, see "Supported features by platform" on page 77.

## Integrity Monitoring scan performance settings

Changing the following settings may help to improve the performance of Integrity Monitoring scans:

### Limit CPU usage

Integrity Monitoring uses local CPU resources during the system scan that leads to the creation of the initial baseline and during the system scan that compares a later state of the system to the previously created baseline. If you are finding that Integrity Monitoring is consuming more resources than you want it to, you can restrict the CPU usage to the following levels:

---

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

- **High:** Unlimited CPU usage
- **Medium:** The Integrity Monitoring process will not consume more than 50% of CPU resources
- **Low:** The Integrity Monitoring process will not consume more than 25% of CPU resources

To change the **Integrity Monitoring CPU Usage Level** setting, open the **Computer or Policy editor**[1] and go to **Integrity Monitoring** > **Advanced**.

### Change the content hash algorithm

You can select the hash algorithm(s) that will be used by the Integrity Monitoring module to store baseline information. You can select more than one algorithm, but this is not recommended because of the detrimental effect on performance.

You can change the content hash algorithm

### Enable a VM Scan Cache configuration

Using scan caching for Integrity Monitoring improves the efficiency of scans by eliminating the unnecessary scanning of identical content across multiple VMs in large VMware deployments. To select which scan cache configuration is used by a virtual machine, open the **Computer or Policy editor**[2] and go to **Integrity Monitoring > Advanced > VM Scan Cache**.

## Integrity Monitoring event tagging

The events generated by the Integrity Monitoring module are displayed in Deep Security Manager, under **Events & Reports** > **Integrity Monitoring Events**. Event tagging can help you to

---

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

sort events and determine which ones are legitimate and which ones need to be investigated further.

You can manually apply tags to events by right-clicking the event and then clicking **Add Tag(s)**. You can choose to apply the tag to only the selected event or to any similar Integrity Monitoring events.

You can also use the auto-tagging feature to group and label multiple events. To configure this feature in the Deep Security Manager, go to **Events and Reports** > **Integrity Monitoring Events** > **Auto-Tagging** > **New Trusted Source**. There are three sources that you can use to perform the tagging:

- A Local Trusted Computer.
- The Trend Micro Certified Safe Software Service.
- A Trusted Common Baseline, which is a set of file states collected from a group of computers.

For more information on event tagging, see "Apply tags to identify and group events" on page 804.

## Create an integrity monitoring rule

Integrity monitoring rules describe how Deep Security Agents should scan for and detect changes to a computer's files, directories, and registry keys and values, as well as changes in installed software, processes, listening ports, and running services. Integrity monitoring rules can be assigned directly to computers or can be made part of a policy.

**Note:** This article specifically covers how to create an integrity monitoring rule. For information on how to configure the Integrity Monitoring module, see "Set up integrity monitoring" on page 632.

There are two types of integrity monitoring rules: those that you have created, and those that are issued by Trend Micro. For more information on how to configure rules issued by Trend Micro, see the "Configure Trend Micro integrity monitoring rules" on page 643 section.

To create a new integrity monitoring rule, you need to:

1. "Add a new rule" below.
2. "Enter integrity monitoring rule information " below.
3. "Select a rule template and define rule attributes" on the next page.

When you're done with your rule, you can also learn how to

- "Configure rule events and alerts" on page 644
- "See policies and computers a rule is assigned to" on page 644
- "Export a rule" on page 644
- "Delete a rule" on page 644

## Add a new rule

There are three ways to add an integrity monitoring rule on the **Policies** > **Common Objects** > **Rules** > **Integrity Monitoring Rules** page. You can:

- Create a new rule. Click **New** > **New Integrity Monitoring Rule**.
- Import a rule from an XML file. Click **New** > **Import From File**.
- Copy and then modify an existing rule. Right-click the rule in the Integrity Monitoring Rules list and then click **Duplicate**. To edit the new rule, select it and then click **Properties**.

## Enter integrity monitoring rule information

1. Enter a **Name** and **Description** for the rule.

   **Tip:** It is good practice to document all integrity monitoring rule changes in the Description field of the firewall rule. Make a note of when and why rules were created or deleted for easier maintenance.

2. Set the **Severity** of the rule.

   **Note:** Setting the severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as sorting criteria when viewing a list of integrity monitoring rules. More importantly, each severity level is associated with a severity

value; this value is multiplied by a computer's Asset Value to determine the ranking of an event. (See **Administration > System Settings > Ranking**.)

## Select a rule template and define rule attributes

Go to the **Content** tab and select from one of the following three templates:

### Registry Value template

Create an integrity monitoring rule to specifically monitor changes to registry values.

**Note:** The Registry Value template is only for Windows-based computers .

1. Select the **Base Key** to monitor and whether or not to monitor contents of sub keys.
2. List **Value Names** to be included or excluded. You can use "?" and "*" as wildcard characters.
3. Enter **Attributes** to monitor. Entering "STANDARD" will monitor changes in registry size, content and type. For more information on Registry Value template attributes see the "RegistryValueSet" on page 678 documentation.

### File template

Create an integrity monitoring rule to specifically monitor changes to files.

1. Enter a **Base Directory** for the rule (for example, `C:\Program Files\MySQL`.) Select **Include Sub Directories** to include the contents of all subdirectories relative to the base directory.

2. Use the **File Names** fields to include or exclude specific files. You can use wildcards (" `?` " for a single character and " `*` " for zero or more characters.

   **Note:** Leaving the **File Names** fields blank will cause the rule to monitor all files in the base directory. This can use significant system resources if the base directory contains numerous or large files.

3. Enter **Attributes** to monitor. Entering "STANDARD" will monitor changes in file creation date, last modified date, permissions, owner, group, size, content, flags (Windows), and

SymLinkPath (Linux). For more information on File template attributes see the "FileSet" on page 662 documentation.

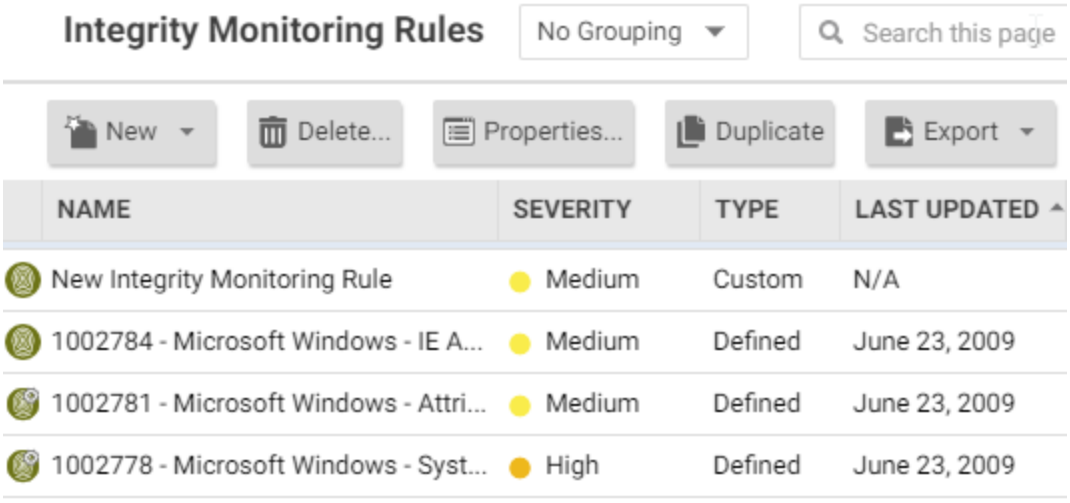
### Custom (XML) template

Create a custom integrity monitoring rule template to monitor directories, registry values, registry keys, services, processes, installed software, ports and files using the Deep Security XML-based "Integrity monitoring rules language" on page 645.

> **Tip:** You can create your rule in your preferred text editor and paste it to the **Content** field when you are done.

## Configure Trend Micro integrity monitoring rules

Integrity monitoring rules issued by Trend Micro cannot be edited in the same way as the custom rules you create. Some Trend Micro rules cannot be modified at all, while other rules may offer limited configuration options. Both of these rule types will show as "Defined" under the "Type" column, but rules that can be configured will display a gear in the Integrity Monitoring icon ( ).




You can access the configuration options for a rule by opening the properties for the rule and clicking on the **Configuration** tab.

Rules issued by Trend Micro also show the following additional information under the **General** tab:

- When the rule was first issued and last updated, as well as a unique identifier for the rule.
- The minimum versions of the Agent and the Deep Security Manager that are required for the rule to function.

Although you cannot edit rules issued by Trend Micro directly, you can duplicate them and then edit the copy.

## Configure rule events and alerts

Any changes detected by an integrity monitoring rule is logged as an event in the Deep Security Manager.

### Real-time event monitoring

By default, events are logged at the time they occur. If you only want events to be logged when you manually perform a scan for changes, deselect **Allow Real Time Monitoring**.

### Alerts

You can also configure the rules to trigger an alert when they log an event. To do so, open the properties for a rule, click on **Options**, and then select **Alert when this rule logs an event**.

## See policies and computers a rule is assigned to

You can see which policies and computers are assigned to an integrity monitoring rule on the **Assigned To** tab. Click on a policy or computer in the list to see their properties.

## Export a rule

You can export all integrity monitoring rules to a .csv or .xml file by clicking **Export** and selecting the corresponding export action from the list. You can also export specific rules by first selecting them, clicking **Export** and then selecting the corresponding export action from the list.

## Delete a rule

To delete a rule, right-click the rule in the Integrity Monitoring Rules list, click **Delete** and then click **OK**.

**Note:** Integrity monitoring rules that are assigned to one or more computers or that are part of a policy cannot be deleted.

## Integrity monitoring rules language

The integrity monitoring rules language is a declarative XML-based language that describes the system components and associated attributes that should be monitored by Deep Security. It also provides a means to specify what components within a larger set of components should be excluded from monitoring.

**Tip:** If you only need to monitor for unauthorized changes to files or the Windows registry, you can use File and Registry rule templates instead of creating a custom one. For more information on using these templates, see "Create an integrity monitoring rule" on page 640.

To create a new custom integrity monitoring rule, start with the procedure in "Create an integrity monitoring rule" on page 640 (selecting **Custom (XML)** as the template type), then create your custom rule according to the integrity monitoring rules language, as covered in the following sections:


- "Entity Sets" on the next page
- "Hierarchies and wildcards" on page 647
- "Syntax and concepts" on page 648
- "Include tag" on page 649
- "Exclude tag" on page 650
- "Case sensitivity" on page 650
- "Entity features" on page 651
- "ANDs and ORs" on page 653
- "Order of evaluation" on page 654
- "Entity attributes" on page 654
- "Shorthand attributes" on page 655

- "onChange attribute" on page 656
- "Environment variables" on page 656
- "Registry values" on page 657
- "Use of ".."" on page 658
- "Best practices" on page 658


## Entity Sets

System components included in an integrity monitoring rule are referred to as "Entities". Each type of component is a class of Entity. For example, files, registry keys, and processes are each a class of Entity. The Integrity Monitoring Rules language provides a tag for describing a set of Entities (an Entity Set) for each class of Entity. The following **Entity Set** types are available to be used in a rule:

- **DirectorySet**: rules will scan the integrity of directories
- **FileSet**: rules will scan the integrity of files
- **GroupSet:** rules will scan the integrity of groups
- **InstalledSoftwareSet**: rules will scan the integrity of installed software
- **PortSet:** rules will scan the integrity of listening ports
- **ProcessSet**: rules will scan the integrity of processes
- **RegistryKeySet**: rules will scan registry keys
- **RegistryValueSet**: rules will scan registry values
- **ServiceSet**: rules will scan the integrity of services
- **UserSet:** rules will scan the integrity of users
- **WQLSet:** rules will monitor the integrity of the results of a Windows Management Instrumentation WQL query statement

A single Integrity Rule can contain multiple Entity Sets. This allows you to, for example, secure an application with a single rule that monitors multiple files and registry entries.

## Hierarchies and wildcards

For Entity Sets that represent a hierarchical data type such as FileSet and RegistryKeySet, section-based pattern matching is supported:

- `/` **(forward slash)** : demarcates sections of the pattern to be applied to levels of the hierarchy
- `**` **(two stars)** : matches zero or more sections

The following wildcards are supported:

- `?` **(question mark)** : matches one character
- `*` **(one star)** : matches zero or more characters

"Escaping" characters is also supported:

- `\` **(back slash)** : escapes the next character

The pattern is divided into sections using the " `/` " character, with each section of the pattern being applied to successive levels of the hierarchy as long as it continues to match. For example, if the pattern:

```
/a?c/123/*.java
```

is applied to the path:

```
/abc/123/test.java
```

Then:

- `"a?c` " matches "abc"
- `"123` " matches "123"
- `"*.java` " matches "test.java"

When the pattern is applied to the path:

```
/abc/123456/test.java
```

Then:

- `"a?c` " matches "abc"
- " `123` " does *not* match "123456", and so no more matching is performed

The " `**` " notation pattern matches zero or more sections, and so:

```
/abc/**/*.java
```

matches both "abc/123/test.java" and "abc/123456/test.java". It would also match "abc/test.java" and "abc/123/456/test.java".

## Syntax and concepts

This section will present some example integrity monitoring rules. The examples will use the **FileSet** Entity Set but the topics and components described are common to all Entity Sets. A minimal integrity monitoring rule could look like this:

```
<FileSet base="C:\Program Files\MySQL">
 </FileSet>
```

The "base" attribute specifies the base directory for the FileSet. Everything else about the rule will be relative to this directory. If nothing further is added to the rule, everything (including subdirectories) below the "base" will be monitored for changes.

**Note:** The " `*` " and " `?` " wildcards can be used in a "base" attribute string, but only in the last path component of the base. So this is valid:

```
base="C:\program files\CompanyName * Web Server"
```

but this is not:

```
base="C:\* files\Microsoft Office"
```

Within an Entity Set, "include" and "exclude" tags can be used to control pattern matching. These tags have a "key" attribute that specifies the pattern to match against. The source of the key varies by Entity Set. For example, for Files and Directories it is their path, while for Ports it is the unique protocol/IP/portNumber tuple.

**Note:** If a path supplied in an include or exclude rule is syntactically invalid, the Agent will generate an "Integrity Monitoring Rule Compile Issue" Agent Event and supply the rule ID and the path (after expansion) as parameters. An example of an invalid path would be `C:\test1\D:\test2` since a file name may not contain two volume identifiers.

## Include tag

The include tag is essentially an allow list. Using it means that only those Entities matched by it (or other include tags) will be included. By adding an include tag, the following rule now only monitors changes to files with the name "*.exe" in the "C:\Program Files\MySQL" folder and sub folders:

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**/*.exe"/>
 </FileSet>
```

"Includes" can be combined. The following rule will monitor changes to files with the names "*.exe" and "*.dll" in the "C:\Program Files\MySQL" folder and sub folders:

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**/*.exe"/>
 <include key="**/*.dll"/>
 </FileSet>
```

It is also possible to combine multiple criteria in a single include block, in which case **all** criteria must be true for a given Entity to be included. The following "include" tag requires that an Entity both end in ".exe" and start with "sample" to be included. Although this requirement could be represented more succinctly, the usefulness of this becomes more apparent as key patterns are combined with other features of the Entity, as described in the "Features" section below.

```
<include>
 <key pattern="**/*.exe"/>
 <key pattern="**/sample*"/>
 </include>
```

The following is another way to express the same requirements:

```
<include key="**/*.exe">
 <key pattern="**/sample*"/>
 </include>
```

## Exclude tag

The exclude tag functions as a block list, removing files from the set that would otherwise be returned. The following (unlikely) example would place everything but temp files under watch.

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**"/>
 <exclude key="**/*.tmp"/>
 </FileSet>
```

The following rule excludes the "MySQLInstanceConfig.exe" from the set of EXEs and DLLs:

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**/*.exe"/>
 <include key="**/*.dll" />
 <exclude key="**/MySQLInstanceConfig.exe"/>
 </FileSet>
```

Like the "include" tag, the "exclude" tag can be written to require multiple criteria. The following example shows a multi-criteria "exclude" tag.

```
<exclude>
 <key pattern="**/MySQLInstanceConfig*" />
 <key pattern="**/*.exe" />
 </exclude>
```

## Case sensitivity

The case sensitivity of pattern matching for an include or exclude tag may be controlled by the "casesensitive" attribute. The attribute has three allowed values:

- **true**
- **false**
- **platform**

The default value for this attribute is "platform", which means that the case sensitivity of the pattern will match the platform on which it is running. In the following example, both "Sample.txt" and "sample.txt" would be returned on a Windows system, but only "Sample.txt" would be returned on a Unix system:

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**/*Sample*"/>
 </FileSet>
```

In this example, only "Sample.txt" would be returned on Windows and Unix:

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**/*Sample*" casesensitive="true"/>
 </FileSet>
```

**Note:** A case sensitive setting of "true" is of limited use on a platform such as Windows which is case insensitive when it comes to most object names.

## Entity features

The inclusion and exclusion of Entities based on features other than their "key" is also supported for some Entity types. The set of features differs by Entity type. The following example will include all executable files. It does not depend on the file extension as previous examples using file extensions did, but instead will check the first few hundred bytes of the file to determine if it is executable on the given OS.

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**" executable="true"/>
 </FileSet>
```

Feature attributes must appear in an "include" or "exclude" tag. To use them as part of a multi-criteria include or exclude, they must be specified as attributes of the enclosing include or exclude tag. The following example includes all files that contain the string "MySQL" in their name and are also executable:

```
<include executable="true">
 <key pattern="**/*MySQL*"/>
 </include>
```

The previous example can be more succinctly expressed as:

```
<include key="**/*MySQL*" executable="true"/>
```

Some feature attributes are simply matches against the value of one of the Entity's attributes. In such cases, wildcard matches using " `*` " and " `?` " are sometimes supported. The help pages for the individual Entity Sets indicate which attributes can be used in include or exclude rules in this way, and whether they support wildcard matching or simple string matching.

**Note:** Where wildcard matches *are* supported, it is important to note that the match is against the string value of the attribute and that no normalization takes place. Constructs available for Entity key matches such as `"**` " and the use of " `/` " to separate hierarchical components don't apply. Matching a path name on Windows requires the use of " `\` " since that is the character which appears in the value of the attribute being tested, whereas Unix systems will use " `/` " in path values so matches against Unix paths need to use " `/` ".

The following is an example of a feature match using the "state" attribute:

```
<ServiceSet>
 <include state="running"/>
 </ServiceSet>
```

**Note:** Wildcards are not supported in state matches.

The following example matches any processes where the path of the binary ends in "\notepad.exe":

```
<ProcessSet>
 <include path="*\notepad.exe"/>
 </ProcessSet>
```

The following example matches any processes where the command-line begins with "/sbin/":

```
<ProcessSet>
 <include commandLine="/sbin/*"/>
 </ProcessSet>
```

**Note:** Be careful when using wildcards. A wildcard expression like " `**` " will look at every file in every sub directory beneath "base". Creating a baseline for such an expression can take a lot of time and resources.

## ANDs and ORs

It is possible to express logical ANDs and ORs through the use of multi-criteria includes and excludes and multiple includes and excludes.

There are several ways that a multi criteria include or exclude can be used to express an AND. The most straightforward is to include multiple criteria within a single enclosing tag. The following example shows a simple multi-criteria AND-ing:

```
<include>
 <key pattern="**/*MySQL*" />
 <key pattern="**/*.exe"/>
 </include>
```

As well, any criteria expressed as an attribute of the including tag will be grouped with the enclosed criteria as part of the multi-criteria requirement. The following example shows the previous multi-criteria "include" re-written in this way:

```
<include key="**/*.exe">
 <key pattern="**/*MySQL*" />
 </include>
```

Finally, if multiple criteria are expressed as attributes of an include or exclude they are treated as an AND:

```
<include executable="true" key="**/*MySQL*" />
```

ORs are expressed simply by the inclusion of multiple include or exclude tags. The following code includes files if their extensions are ".exe" OR ".dll":

```
<include key="**/*.dll" />
 <include key="**/*.exe" />
```

## Order of evaluation

All "includes" are processed first, regardless of order of appearance in the rule. If an object name matches at least one "include" tag, it is then tested against the "exclude" tags. It is removed from the set of monitored objects if it matches at least one "exclude" tag.

## Entity attributes

A given Entity has a set of attributes that can be monitored. If no attributes are specified for an Entity Set (i.e. the attributes wrapper tag is not present) then the STANDARD set of attributes for that Entity is assumed. (See the *Shorthand Attributes* sections for the individual Entity Sets.)

However, for a given Entity Set only certain attributes of the Entity may be of interest for Integrity Monitoring. For example, changes to the contents of a log file are most likely expected and allowed. However changes to the permissions or ownership should be reported.

The "attributes" tag of the Entity Sets allows this to be expressed. The "attributes" tag contains a set of tags enumerating the attributes of interest. The set of allowed "attribute" tags varies depending on the Entity Set for which they are being supplied.

**Note:** If the "attributes" tag is present, but contains no entries, then the Entities defined by the rule are monitored for existence only.

The following example monitors executable files in "C:\Program Files\MySQL" whose name includes "SQL" for changes to their "last modified", "permissions", and "owner" attributes:

```
<FileSet base="C:\Program Files\MySQL" >
 <include key="**/*SQL*" executable="true"/>
 <attributes>
 <lastModified/>
 <permissions/>
 <owner/>
 </attributes>
 </FileSet>
```

The following example monitors the "permissions", and "owner" attributes of log files in "C:\Program Files\MySQL":

```
<FileSet base="C:\Program Files\MySQL" >
 <attributes>
 <permissions/>
 <owner/>
 </attributes>
 <include key="**/*.log" />
 </FileSet>
```

In the following example, the STANDARD set of attributes will be monitored. (See Shorthand Attributes, below)

```
<FileSet base="C:\Program Files\MySQL" >
 <include key="**/*.log" />
 </FileSet>
```

In the following example, no attributes will be monitored. Only the existence of the Entities will be tracked for change.

```
<FileSet base="C:\Program Files\MySQL" >
 <attributes/>
 <include key="**/*.log" />
 </FileSet>
```

## Shorthand attributes

Shorthand attributes provide a way to specify a group of attributes using a single higher level attribute. Like regular attributes the set of allowed values differs based on the Entity Set for which they are being supplied.

Shorthand Attributes are useful in cases where a set of attributes naturally group together, in cases where exhaustively listing the set of attributes would be tedious, and in cases where the set of attributes represented by the high level attribute may change with time or system configuration. An example of each case follows:

| Attribute | Description |
|---|---|
| STANDARD | The set of attributes to monitor for the Entity Set. This is different than "every possible attribute" for the Entity Set. For example, it would not include every possible hash algorithm, just the ones deemed sufficient. For the list of "standard" attributes for each Entity Set, see sections for the individual Entity Sets. |
| CONTENTS | This is Shorthand for the hash, or set of hashes, of the contents of the file. Defaults to SHA-1. |

## onChange attribute

An EntitySet may be set to monitor changes in real time. If the onChange attribute of an EntitySet is set to true (the default value) then the entities returned by the EntitySet will be monitored for changes in real time. When a change is detected the Entity is immediately compared against its baseline for variation. If the onChange attribute of an EntitySet is set to false, it will be run only when a baseline is built or when it is triggered via a scheduled task or on demand by the Deep Security Manager.

The following sample monitors the MySQL binaries in real time:

```
<FileSet base="C:\Program Files\MySQL" onChange="true">
 <include key="**/*.exe"/>
 <include key="**/*.dll" />
 </FileSet>
```

## Environment variables

Environment variables can be included in the base value used in Entity Sets. They are enclosed in "${}". The variable name itself is prefaced with "env.".

The following example sets the base directory of the FileSet to the path stored in the PROGRAMFILES environment variable:

```
<FileSet base="${env.PROGRAMFILES}"/>
```

**Note:** The values of referenced environment variables are read and stored by the Deep Security Agent on Agent startup. If the value of an environment variable changes, the Agent must be restarted to register the change.

If a referenced environment variable is not found, the Entity Sets referencing it are not scanned or monitored, but the rest of the configuration is used. An alert is triggered indicating that the variable is not present. The Agent reports an invalid environment variable using Agent event "Integrity Monitoring Rule Compile Issue". The ID of the integrity monitoring rule and the environment variable name are supplied as parameters to the event.

The following are the default environment variables that integrity monitoring uses:

| Name | Value |
|---|---|
| ALLUSERSPROFILE | C:\ProgramData |
| COMMONPROGRAMFILES | C:\Program Files\Common Files |
| PROGRAMFILES | C:\Program Files |
| SYSTEMDRIVE | C: |
| SYSTEMROOT | C:\Windows |
| WINDIR | C:\Windows |

### Environment variable overrides

Override environment variables when non-standard locations are used in the Windows operating system. For example, the **Microsoft Windows - 'Hosts' file modified** integrity monitoring rule, which monitors changes to the Windows **hosts** file, looks for that file in the **C:\WINDOWS\system32\drivers\etc** folder. However not all Windows installations use the **C:\WINDOWS** directory, so the integrity monitoring rule uses the **WINDIR** environment variable and represents the directory as **%WINDIR%\system32\drivers\etc**.

**Note:** Environment variables are used primarily by the virtual appliance when performing agentless integrity monitoring on a virtual machine. This is because the virtual appliance has no way of knowing if the operating system on a particular virtual machine is using standard directory locations.

1. Open the **Computer or Policy editor**[1] where you want to override an environment variable.
2. Click **Settings > Advanced**.
3. In the **Environment Variable Overrides** section, click the **View Environment Variables** button to display the **Environment Variable Overrides** page.
4. Click **New** in the menu bar and enter a new name-value pair (for example, WINDIR and D:\Windows) and click **OK**.

## Registry values

Registry values can be included in the base value used in Entity Sets. They are enclosed in ${}. The path to the registry value itself is prefaced with "reg.". The following example sets the base

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

directory of the FileSet to the path stored in the *"HKLM\Software\Trend Micro\Deep Security Agent\InstallationFolder*" registry value:

```
<FileSet base="${reg.HKLM\Software\Trend Micro\Deep Security
Agent\InstallationFolder}"/>
```

The values of referenced registry values are read when a new or changed rule is received by the Agent. The Agent also checks all rules at startup time and will rebuild the baseline for affected Rules if any referenced registry values change.

If a referenced registry value is not found, the EntitySets referencing it are not scanned or monitored, but the rest of the configuration is used. An alert notifying that the variable is not present is raised. The Agent reports an invalid environment variable expansion using Agent Event 8012. The ID of the integrity monitoring rule and the registry value path are supplied as parameters to the event.

**Note:** A wildcard is allowed only in the last hierarchical component of a base name. For example, base="HKLM\Software\ATI*" is valid and will find both "HKLM\Software\ATI" and "HKLM\Software\ATI Technologies"; however, "base="HKLM*\Software\ATI*" is invalid.

## Use of ".."

The ".." convention for referencing a parent directory is supported in all current versions of the Agent. The Agent will attempt to normalize base directory names for FileSet and DirectorySet elements by resolving ".." references and converting Windows short names to long names. For example, on some newer versions of WIndows the following FileSet would have a base directory of "C:\Users". On earlier versions of Windows it would be "C:\Documents and Settings".

```
<FileSet base="${env.USERPROFILE}\..">
 <include key="*/Start Menu/Programs/Startup/*"/>
 </FileSet>
```

## Best practices

Rules should be written to only include objects and attributes that are of significance. This will ensure that no events are reported if other attributes of the object change. For example, your change monitoring policy may place restrictions on permission and ownership of files in " `/bin`

". Your integrity monitoring rule should monitor owner, group, and permissions, but not other attributes like lastModified or hash values.

When using integrity monitoring rules to detect malware and suspicious activity, monitor services, watch for use of NTFS data streams, and watch for executable files in unusual places such as " `/tmp` " or " `${env.windir}\temp` ".

Always be as specific as possible when specifying what objects to include in a rule. The fewer objects you include, the less time it will take to create your baseline and the less time it will take to scan for changes. Exclude objects which are expected to change and only monitor the attributes you are concerned about.

When creating a rule, do not:

- Use " `**/...` " from a top-level of the hierarchy such as " `/` ", "C:\", or " `HKLM\Software` " .
- Use more than one content hash type unless absolutely necessary.
- Reference user-specific locations such as `HKEY_CURRENT_USER` , `${env.USERPROFILE}` , or `${env.HOME}` .

Any of these statements in your integrity monitoring rules will cause performance issues as the Deep Security Agent searches through many items in order to match the specified patterns.

## DirectorySet

The DirectorySet tag describes a set of Directories.

### Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| base | Sets the base directory of the DirectorySet. Everything else in the tag | Yes | N/A | String values resolving to syntactically valid path (Path is not required to exist) **Note**: UNC paths are allowed by Windows Agents, but require that the remote system allow access by the "LocalSystem" account of the Agent computer. The Agent is a Windows service and runs as LocalSystem, aka NT |

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| | is relative to this directory | | | AUTHORITY\SYSTEM. When accessing a network resource, the LocalSystem uses the computer's credentials, which is an account named *DOMAIN\MACHINE*$. The access token presented to the remote computer also contains the "Administrators" group for the computer, so remote shares must grant read privileges to either the Agent computer's account, the Agent computer's Administrators group, or "Everyone".<br><br>If the base value is not syntactically valid, the FileSet will not be processed. The rest of the config will be evaluated. |
| onChange | Whether the directories returned should be monitored in real time. | No | false | true, false |
| followLinks | Will this DirectorySet follow symbolic links. | No | false | true, false |

## Entity Set Attributes

These are the attributes of the Entity that may be monitored by Integrity Monitoring Rules.

- **Created:** Timestamp when the directory was created
- **LastModified:** Timestamp when the directory was last modified
- **LastAccessed:** Timestamp when the directory was last accessed. On Windows this value does not get updated immediately, and recording of the last accessed timestamp can be disabled as a performance enhancement. See File Times for details. The other problem with this attribute is that the act of scanning a directory requires that the Agent open the directory, which will change its last accessed timestamp.
- **Permissions:** The directory's security descriptor (in SDDL format) on Windows or Posix-style ACLs on Unix systems that support ACLs, otherwise the Unix style rwxrwxrwx file permissions in numeric (octal) format.
- **Owner:** User ID of the directory owner (commonly referred to as the "UID" on Unix)
- **Group:** Group ID of the directory owner (commonly referred to as the "GID" on Unix)

- **Flags:** Windows-only. Flags returned by the GetFileAttributes() Win32 API. Windows Explorer calls these the "Attributes" of the file: Read-only, Archived, Compressed, etc.
- **SymLinkPath:** If the directory is a symbolic link, the path of the link is stored here. On Windows, use the SysInternals "junction" utility to create the Windows equivalent of symbolic links.
- **InodeNumber** (Unix and Linux only): Inode number of the disk on which the inode associated with the file is stored
- **DeviceNumber** (Unix and Linux only): Device number of the disk on which the inode associated with the directory is stored

## Short Hand Attributes

The following are the Short Hand Attributes, and the attributes to which they map.

- **STANDARD:**
  - Created
  - LastModified
  - Permissions
  - Owner
  - Group
  - Flags (Windows only)
  - SymLinkPath

## Meaning of "Key"

Key is a pattern to match against the path of the directory relative to the directory specified by "dir". This is a hierarchical pattern, with sections of the pattern separated by "/" matched against sections of the path separated by the file separator of the given OS.

## Sub Elements

- **Include**
- **Exclude**

See "Integrity monitoring rules language" on page 645 for a general description of Include and Exclude for their allowed attributes and sub elements. Only information specific to includes and excludes relating to this EntitySet class are included here.

## FileSet

The FileSet tag describes a set of Files.

### Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| base | Sets the base directory of the FileSet. Everything else in the tag is relative to this directory. | Yes | N/A | String values resolving to syntactically valid path (Path is not required to exist). **Note**: UNC paths are allowed by Windows Agents, but require that the remote system allow access by the "LocalSystem" account of the Agent computer. The Agent is a Windows service and runs as LocalSystem, aka NT AUTHORITY\SYSTEM. When accessing a network resource, the LocalSystem uses the computer's credentials, which is an account named *DOMAIN\MACHINE*$. The access token presented to the remote computer also contains the "Administrators" group for the computer, so remote shares must grant read privileges to either the Agent computer's account, the Agent computer's Administrators group, or "Everyone".<br><br>If the base value is not syntactically valid, the FileSet will not be processed. The rest of the config will be evaluated. |
| onChange | Whether the files returned should be monitored in real time. | No | false | true, false |
| followLinks | Will this FileSet follow symbolic links. | No | false | true, false |

### Entity Set Attributes

These are the attributes of the FileSet that can be monitored by Integrity Monitoring Rules.

- **Created:** Timestamp when the file was created
- **LastModified:** Timestamp when the file was last modified
- **LastAccessed:** Timestamp when the file was last accessed. On Windows this value does not get updated immediately, and recording of the last accessed timestamp can be disabled as a performance enhancement. See File Times for details. The other problem with this attribute is that the act of scanning a file requires that the Agent open the file, which will change its last accessed timestamp. On Unix, the Agent will use the O_NOATIME flag if it is available when opening the file, which prevents the OS from updating the last accessed timestamp and speeds up scanning.
- **Permissions:** The file's security descriptor (in SDDL format) on Windows or Posix-style ACLs on Unix systems that support ACLs, otherwise the Unix style rwxrwxrwx file permissions in numeric (octal) format.
- **Owner:** User ID of the file owner (commonly referred to as the "UID" on Unix)
- **Group:** Group ID of the file owner (commonly referred to as the "GID" on Unix)
- **Size:** size of the file
- **Sha1:** SHA-1 hash
- **Sha256:**SHA-256 hash
- **Md5:** MD5 hash (deprecated)
- **Flags:** Windows-only. Flags returned by the GetFileAttributes() Win32 API. Windows Explorer calls these the "Attributes" of the file: Read-only, Archived, Compressed, etc.
- **SymLinkPath** (Unix and Linux only): If the file is a symbolic link, the path of the link is stored here. Windows NTFS supports Unix-like symlinks, but only for directories, not files. Windows shortcut objects are not true symlinks since they are not handled by the OS; the Windows Explorer handles shortcut files (*.lnk) but other applications that open a *.lnk file will see the contents of the lnk file.
- **InodeNumber** (Unix and Linux only): Inode number of the disk on which the inode associated with the file is stored
- **DeviceNumber** (Unix and Linux only): Device number of the disk on which the inode associated with the file is stored
- **BlocksAllocated** (Linux and Unix only): The number of blocks allocated to store the file.

- **Growing:** (DSA 7.5+) contains the value "true" if the size of the file stays the same or increases between scans, otherwise "false". This is mainly useful for log files that have data appended to them. Note that rolling over a log file will trigger a change in this attribute.
- **Shrinking:** (DSA 7.5+) contains the value "true" if the size of the file stays the same or decreases between scans, otherwise "false".

### Short Hand Attributes

The following are the Short Hand Attributes, and the attributes to which they map.

- **CONTENTS:** Resolves to the content hash algorithm set in **Computer or Policy editor**[1] **> Integrity Monitoring > Advanced**.
- **STANDARD:** Created, LastModified, Permissions, Owner, Group, Size, Contents, Flags (Windows only), SymLinkPath (Unix only)

### Drives Mounted as Directories

Drives mounted as directories are treated as any other directory, unless they are a network drive in which case they are ignored.

### Alternate Data Streams

NTFS based file systems support the concept of alternate data streams. When this feature is used it behaves conceptually like files within the file.

**Note:** To demonstrate this, type the following at the command prompt:

```
echo plain > sample.txt
echo alternate > sample.txt:s
more < sample.txt
more < sample.txt:s
```

The first "more" will show only the text "plain", the same text that will be displayed if the file is

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

opened with a standard text editor, such as notepad. The second "more", which accesses the "s" stream of sample.txt will display the string "alternate".

For FileSets, if no stream is specified, then all streams are included. Each stream is a separate Entity entry in the baseline. The available attributes for streams are:

- **size**
- **Sha1**
- **Sha256**
- **Md5** (deprecated)
- **Contents**

The following example would include both streams from the demonstration above:

```
<include key="**/sample.txt" />
```

To include or exclude specific streams, the ":" notation is used. The following example matches only the "s" stream on sample.txt and not the main sample.txt stream:

```
<include key="**/sample.txt:s" />
```

Pattern matching is supported for the stream notation. The following example would include sample.txt, but exclude all of its alternate streams:

```
<include key="**/sample.txt" />
 <exclude key="**/sample.txt:*" />
```

## Meaning of "Key"

Key is a pattern to match against the path of the file relative to the directory specified by "base". This is a hierarchical pattern, with sections of the pattern separated by "/" matched against sections of the path separated by the file separator of the given OS

## Sub Elements

- **Include**
- **Exclude**

See "Integrity monitoring rules language" on page 645 for a general description of Include and Exclude for their allowed attributes and sub elements. Only information specific to includes and excludes relating to the FileSet Entity Set class are included here.

### Special attributes of Include and Exclude for FileSets:

**executable**

Determines if the file is executable. This does not mean that its permissions allow it to be executed. Instead the contents of the file are checked, as appropriate for platform, to determine if the file is an executable file.

> **Note:** This is a relatively expensive operation since it requires the Agent to open the file and examine the first kilobyte or two of its content looking for a valid executable image header. Opening and reading every file is much more expensive than simply scanning directories and matching file names based on wild card patterns, so any include and exclude rules using "executable" will result in slower scan times than those that do not use it.

## GroupSet

GroupSet represents a set of groups. Note these are local groups only.

### Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| onChange | Will be monitored in real time | No | false | true, false |

### Entity Set Attributes

These are the attributes of the entity that can be monitored:

- **Description:** (Windows only) The textual description of the group.
- **Group:** The group ID and name. The group name is part of the entity key, but it's still important to be able to monitor the group ID-name pairing in case groups are renamed and given new IDs. Operating systems generally enforce security based on its ID.

- **Members:** A comma separated list of the members of the group.
- **SubGroups:** (Windows only) A comma separated list of sub-groups of the group.

### Short Hand Attributes

- **Standard:** Group Members SubGroups

### Meaning of "Key"

The key is the group's name. This is not a hierarchical Entity Set. Patterns are applied only to the group name. As a result the "**" pattern is not applicable. The following example monitors the "Administrators" group for additions and deletions. (The "Member" attribute is included implicitly because it is a part of the STANDARD set, and no attributes are explicitly listed.)

```
<GroupSet>
 <include key="Administrators" />
 </GroupSet>
```

### Include and Exclude

See "Integrity monitoring rules language" on page 645 for a general description of Include and Exclude and their allowed attributes and sub elements.

## InstalledSoftwareSet

Represents a set of installed software. The "key" used to uniquely identify an installed application is platform-specific, but it is often a shorthand version of the application name or a unique numeric value.

On Windows, the key can be something readable like "FogBugz Screenshot_is1" or it can be a GUID like "{90110409-6000-11D3-8CFE-0150048383C9}". You can examine these by looking at the sub-keys of HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

On Linux the key is the RPM package name, as shown by the command:

```
rpm -qa --qf "%{NAME}\n"
```

On Solaris the key is the package name as shown by the **pkginfo** command.

On HPUX the key is the application name as shown by the command:

```
/usr/sbin/swlist -a name
```

## Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the computer where integrity monitoring is enabled.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| onChange | Will be monitored in real time | No | false | true, false |

## Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules. Presence of the attributes is dependent on both the platform and the application itself - installation programs do not necessarily populate all of the attributes.

- **Manufacturer:** The publisher or manufacturer of the application
- **Name:** The friendly name or display name of the application. (Not available on Linux.)
- **InstalledDate:** Date of installation. This is normally returned as YYYY-MM-DD [HH:MM:SS], but many installers on Windows format the date string in a different manner so this format is not guaranteed.
- **InstallLocation:** The directory where the application is installed. (Only available on Windows)
- **Parent:** For patches and updates, this gives the key name of this item's parent. Only available on Windows.
- **Size:** The estimated size of the application, if available. On Windows this attribute is read from the "EstimatedSize" registry value under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*. The value in that location is expressed in KB, so the Agent multiplies it by 1024 before returning the value. Note that not all Windows applications populate the EstimatedSize field in the registry.
- **Version:** The version of the installed application. On Windows this comes from the "DisplayVersion" registry value.

## Short Hand Attributes

These are the short hand attributes of the Entity and the attributes to which they resolve

- **STANDARD:** InstalledDate, Name, Version

## Meaning of "Key"

The key is the name of the installed software. This is not a hierarchical key, so the ** pattern does not apply. On Windows the key is often a GUID, especially for anything installed via the Windows Installer (aka MSI). Use the name="XXX" feature if you need to include or exclude based on the display name rather than the GUID.

The following example would monitor for the addition and deletion of new software.

```
<InstalledSoftwareSet>
 <include key="*"/>
 <attributes/>
 </InstalledSoftwareSet>
```

## Sub Elements

- **Include**
- **Exclude**

See "Integrity monitoring rules language" on page 645 for a general description of Include and Exclude for their allowed attributes and sub elements. Only information specific to includes and excludes relating to this EntitySet class are included here.

## Special attributes of Include and Exclude for InstalledSoftwareSets:

### name (Windows only)

Allows wildcard matching using ? and * on the display name of the application (the "name" attribute of the Entity). For example:

```
<InstalledSoftwareSet>
 <include name="Microsoft*"/>
 <InstalledSoftwareSet>
```

will match all installed applications whose display name (as shown by the Control Panel) starts with "Microsoft".

**manufacturer**

Allows wildcard matching using ? and * on the publisher or manufacturer of the application. For example:

```
<InstalledSoftwareSet>
 <include manufacturer="* Company "/>
 <InstalledSoftwareSet>
```

will match all installed applications whose manufacturer ends with " Company ".

## PortSet

Represents a set of listening ports.

### Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| onChange | Will be monitored in real time | No | false | true, false |

### Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules.

- **Created:** Windows only - XP SP2+ and Server 2003 SP1+ required. Returned by the GetExtendedTcpTable() or GetExtendedUdpTable() API. Indicates when the bind operation that created this TCP or UDP link occurred.
- **Listeners:** The number of active listeners on this protocol, IP address, and port number combination. This reflects the number of sockets bound-to and listening-on the given port, and may be greater than the number of processes listening on the port if processes bind multiple sockets to the port. This attribute has no value if only one socket is bound to the given port.

- **Path:** Windows only - XP SP2+ and Server 2003 SP1+ required. Gives the short name, if available, of the module that owns the port. On Windows this comes from the GetOwnerModuleFromXxxEntry() APIs. According to Microsoft documentation, the resolution of connection table entries to owner modules is a best practice. In a few cases, the owner module name returned can be a process name, such as "svchost.exe", a service name (such as "RPC"), or a component name, such as "timer.dll".
- **Process:** (Windows only - XP SP2+ and Server 2003 SP1+ required.) Gives the full path, if available, of the module that owns the port. On Windows this comes from the GetOwnerModuleFromXxxEntry() APIs. According to Microsoft documentation, the resolution of connection table entries to owner modules is a best practice.
- **ProcessId:** (Windows only - XP SP2+ and Server 2003 SP1+ required.) Gives the PID of the process that issued the bind for this port.
- **User:** (Linux only). Gives the user that owns the port.

## Meaning of "Key"

The key is in the following format:

<PROTOCOL>/<IP ADDRESS>/<PORT>

For example:

```
tcp/172.14.207.94/80
 udp/172.14.207.94/68
```

## IPV6

If the IP address is IPv6 the key is in the same format, but the protocol is TCP6 or UDP6 and the IP address is an IPv6 address as returned by the getnameinfo API:

```
tcp6/3ffe:1900:4545:3:200:f8ff:fe21:67cf/80
 udp6/3ffe:1900:4545:3:200:f8ff:fe21:67cf/68
```

## Matching of the Key

This is not a hierarchical key, so ** is not applicable. Unix-style glob matching is possible using * and ?. The following pattern matches port 80 on the IP addresses 72.14.207.90 through 72.14.207.99:

```
*/72.14.207.9?/80
```

The following pattern matches port 80 on the IP addresses 72.14.207.2, 72.14.207.20 through 72.14.207.29 as well as 72.14.207.200 through 72.14.207.255:

```
*/72.14.207.2*/80
```

The following pattern matches port 80 on any IP.

```
*/80
```

The following example would monitor for any change in the listening ports but ignore port 80 for TCP in IPv4 and IPv6:

```
<PortSet>
 <include key="*"/>
 <exclude key="tcp*/*/80"/>
 </PortSet>
```

## Sub Elements

- **Include**
- **Exclude**

See "Integrity monitoring rules language" on page 645 for a general description of Include and Exclude and their allowed attributes and sub elements. Only information specific to includes and excludes relating to this EntitySet class are included here.

## Special attributes of Include and Exclude for PortSets:

Various other attributes of the port may be used in include and exclude feature tests. These tests compare a value against the value of an attribute of the port; take note of the platform support for various attributes - not all attributes are available across platforms or even platform revisions, hence the use of these tests in include and exclude tags is of limited use. The feature tests support Unix glob-style wildcarding with * and ?, and there is no normalization of path separators or other characters - it is a simple match against the value of the attribute.

### Path

Checks for a wildcard match against the path attribute of the port. The following example would monitor ports owned by processes running the main IIS binary:

```
<PortSet>
 <include path="*\system32\inetsrv\inetinfo.exe"/>
 </PortSet>
```

### Process

Checks for a wildcard match against the process attribute of the port. The following example would monitor ports owned by anything running in a svchost.exe or outlook.* binary:

```
<PortSet>
 <include process="svchost.exe"/>
 <include process="outlook.*"/>
 </PortSet>
```

### User

Checks for a wildcard match against the user attribute of the port. The following example would monitor ports on a Unix system that were owned by the super-user (root):

```
<PortSet>
 <include user="root"/>
 </PortSet>
```

## ProcessSet

Represents a set of processes.

### Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| onChange | Will be monitored in real time | No | false | true, false |

### Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules.

- **CommandLine:** The full command-line as shown by "ps -f" (Unix), "ps w" (Linux), or Process Explorer (Windows).
- **Group:** The group under which the process is running. Under Unix this is the "effective" group ID of the process, which can change over time if the process drops privileges or otherwise switches its effective group credentials. On Windows this is the current Primary Group of the process as returned by the Win32 API GetTokenInformation with a TokenInformationClass of TokenPrimaryGroup. This is the default Primary Group SID for newly created objects. In addition to a Primary Group, processes typically have one or more group credentials associated with them. Those additional group credentials are not monitored by the Agent - they can be viewed on the "Security" tab of the process properties in Process Explorer.
- **Parent:** The PID of the process that created this process.
- **Path:** The full path to the binary of the process.On Windows, this comes from the GetModuleFileNameEx() API. On Linux it comes from reading the symlink /proc/{pid}/exe.
- **Process:** The short name of the process binary (no path). For example, for "c:\windows\notepad.exe" it would be "notepad.exe" and for "/usr/local/bin/httpd" it would be "httpd".
- **Threads:** The number of threads currently executing in the process.
- **User:** The user under which the process is running. Under Unix this is the "effective" user ID of the process, which can change over time if the process drops privileges or otherwise switches its effective user credentials.

## Short Hand Attributes

- **STANDARD:** CommandLine, Group, Parent, Path (where available), Process User

## Meaning of "Key"

The key is a combination of the "Process" attribute (the short name of the executable) and the PID. The PID is appended to the name with a path separator in between, ex. notepad.exe\1234 on Windows and httpd/1234 on Unix. The use of the path separator is to allow include or exclude matching of key="abc/*" to work as expected.

## Sub Elements

- **Include**
- **Exclude**

See "Integrity monitoring rules language" on page 645 for a general description of include for their allowed attributes and sub elements. Only information specific to includes and excludes relating to this EntitySet class are included here.

## Special attributes of Include and Exclude for ProcessSets:

The following example would monitor the set of running processes for notepad.exe regardless of the PID.

```
<ProcessSet>
 <include key="notepad.exe\*" />
 </ProcessSet>
```

Various other attributes of a process can be used in include and exclude feature tests. The feature tests support Unix glob-style wildcarding with * and ?, and there is no normalization of path separators or other characters - it is a simple glob-style match against the value of the attribute.

### CommandLine

Checks for a wildcard match against the commandLine attribute of the process. The following example would monitor any process whose command-line matches "*httpd *":

```
<ProcessSet>
 <include commandLine="*httpd *" />
 </ProcessSet>
```

### Group

Checks for a wildcard match against the group attribute of the process. The text version of the group name is used rather than the numeric form: use "daemon" rather than "2" to test for the daemon group on Linux. The following example would monitor any process running as one of the groups root, daemon, or lp:

```
<ProcessSet>
 <include group="root" />
```

```
 <include group="daemon" />
 <include group="lp" />
 </ProcessSet>
```

### Path

Checks for a wildcard match against the path attribute of the process. The path attribute is not available on some platforms. The following example would monitor any process whose binary resides under System32:

```
<ProcessSet>
 <include path="*\System32\*" />
 </ProcessSet>
```

### User

Checks for a wildcard match against the user attribute of the process. The text version of the user name is used rather than the numeric form: use "root" rather than "0" (zero) to test for the superuser on Unix. The following example would monitor any process running as one of the built in system users (ex. NT AUTHORITY\SYSTEM, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE):

```
<ProcessSet>
 <include user="NT AUTHORITY\*" />
 </ProcessSet>
```

## RegistryKeySet

The RegistryKeySet tag describes a set keys in the registry (Windows only).

### Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| base | Sets the base key of the RegistryKeySet. Everything else in the tag is relative to this key. The base must begin with one of the following registry branch names: HKEY_CLASSES_ROOT (or HKCR), | Yes | N/A | String values resolving to syntactically valid registry key path |

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| | HKEY_LOCAL_MACHINE (or HKLM),<br>HKEY_USERS (or HKU),<br>HKEY_CURRENT_CONFIG (or HKCC) | | | |

## Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules.

- **Owner**
- **Group**
- **Permissions**
- **LastModified** ("LastWriteTime" in Windows registry terminology)
- **Class**
- **SecurityDescriptorSize**

## Short Hand Attributes

- **STANDARD:** Group, Owner, Permissions, LastModified

## Meaning of "Key"

Registry Keys are stored hierarchically in the registry, much like directories in a file system. For the purpose of this language the "key path" to a key is considered to look like the path to a directory. For example the "key path" to the "Deep Security Agent" key of the Agent would be:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\Deep Security Agent
```

The "key" value for includes and excludes for the RegistryValueSet is matched against the key path. This is a hierarchical pattern, with sections of the pattern separated by "/" matched against sections of the key path separated by "\".

## Sub Elements

- **Include**
- **Exclude**

See "Integrity monitoring rules language" on page 645 for a general description of include for their allowed attributes and sub elements.

## RegistryValueSet

A set of Registry values (Windows only).

### Tag Attributes

These are XML attributes of the tag itself as opposed to the attributes of the entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| base | Sets the base key of the RegistryValueSet. Everything else in the tag is relative to this key. The base must begin with one of the registry branch names:<br>HKEY_CLASSES_ROOT (or HKCR),<br>HKEY_LOCAL_MACHINE (or HKLM),<br>HKEY_USERS (or HKU),<br>HKEY_CURRENT_CONFIG (or HKCC) | Yes | N/A | String values resolving to syntactically valid registry key |

### Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules:

- Size
- Type
- Sha1
- Sha256
- Md5 (deprecated)

### Short Hand Attributes

- **CONTENTS:** Resolves to the content hash algorithm set in **Computer or Policy editor**[1] > **Integrity Monitoring > Advanced**.
- **STANDARD:** Size, Type, Contents

### Meaning of "Key"

Registry Values are name-value pairs stored under a key in the registry. The key under which they are stored may in turn be stored under another key, very much like files and directories on a file system. For the purpose of this language the "key path" to a value is considered to look like the path to a file. For example, the "key path" to the InstallationFolder value of the Agent would be:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\Deep Security Agent\InstallationFolder
```

The "key" value for includes and excludes for the RegistryValueSet is matched against the key path. This is a hierarchical pattern, with sections of the pattern separated by "/" matched against sections of the key path separated by "\"

### Default Value

Each registry key has an unnamed or default value.

This value can be explicitly specified for inclusion and exclusion by using a trailing "/" in patterns. For example, "**/" will match all subordinate unnamed values, and "*Agent/**/" will match all unnamed values below a key matching "*Agent".

> **Note:** Registry value names can contain any printable character, including quotes, backslash, the "@" symbol, etc.

The Agent deals with this in Entity key names by using backslash as an escape character, but only backslashes themselves are escaped. It does this so that it can tell the difference between a

---

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

value name containing a backslash and a backslash that occurs as part of the registry path. This means that value names which end with a backslash character will match rules designed to match the default or unnamed value.

See the table below for example registry value names and the resulting Entity key.

| Value | Escaped Form | Example |
|---|---|---|
| Hello | Hello | HKLM\Software\Sample\Hello |
| "Quotes" | "Quotes" | HKLM\Software\Sample\"Quotes" |
| back\slash | back\\slash | HKLM\Software\Sample\back\\slash |
| trailing\ | trailing\\ | HKLM\Software\Sample\trailing\\ |
| | | HKLM\Software\Sample\ |
| @ | @ | HKLM\Software\Sample\@ |

### Sub Elements

- **Include**
- **Exclude**

See "Integrity monitoring rules language" on page 645 for a general description of Include and Exclude for their allowed attributes and sub elements.

## ServiceSet

The ServiceSet element represents a set of services (Windows only). Services are identified by the "service name", which is not the same as the "name" column shown in the Services administrative tool. The service name can be seen in the service properties and is often shorter than the value shown in the "name" column, which is actually the "Display Name" of the service. For example, the Agent has a service name of "ds_agent" and a display name of "Trend Micro Deep Security Agent".

### Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| onChange | Will be monitored in real time | No | false | true, false |

## Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules.

- **Permissions:** The service's security descriptor in SDDL format.
- **Owner:** User ID of the service owner
- **Group:** Group ID of the service owner
- **BinaryPathName:** The path plus optional command-line arguments that Windows uses to start the service.
- **DisplayName:** The "display name" of the service as shown in the properties panel of the service.
- **Description:** Description as it appears in the Services panel
- **State:** The current state of the service. One of: stopped, starting, stopping, running, continuePending, pausePending, paused
- **StartType:** How is the service started? One of: automatic, disabled, manual.
- **LogOnAs:** The name of the account that the service process will be logged on as when it runs.
- **FirstFailure:** Action to take the first time the service fails. Format is "delayInMsec,action", where action is one of None, Restart, Reboot, RunCommand.
- **SecondFailure:** Action to take the second time the service fails. Format is "delayInMsec,action", where action is one of None, Restart, Reboot, RunCommand.
- **SubsequentFailures:** Action to take if the service fails for a third or subsequent time. Format is "delayInMsec,action", where action is one of None, Restart, Reboot, RunCommand.
- **ResetFailCountAfter:** Time after which to reset the failure count to zero if there are no failures, in seconds.
- **RebootMessage:** Message to broadcast to server users before rebooting in response to the "Reboot" service controller action.
- **RunProgram:** Full command line of the process to execute in response to the RunCommand service controller action.
- **DependsOn:** Comma separated list of components that the service depends on

- **LoadOrderGroup:** The load ordering group to which this service belongs. The system startup program uses load ordering groups to load groups of services in a specified order with respect to the other groups. The list of load ordering groups is contained in the following registry value: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ServiceGroupOrder
- **ProcessId:** This is the numeric ID of the process that hosts the service. Many services may exist in a single Windows process, but for those that run in their own process, the monitoring of this attribute will allow the system to log service restarts.

### Short Hand Attributes

These are the short hand attributes of the Entity and the attributes to which they resolve

- **STANDARD**: Permissions, Owner, Group, BinaryPathName, Description, State, StartType, LogOnAs, FirstFailure, SecondFailure, SubsequentFailures, ResetFailCountAfter, RunProgram, DependsOn, LoadOrderGroup, ProcessId

### Meaning of "Key"

The key is the Service's name, which is not necessarily the same as the "name" column shown in the Services administrative tool (that tool shows the "display name" of the service). The service name can be seen in the service properties and is often shorter than the value shown in the "name" column.

**Note:** This is not a hierarchical Entity Set. Patterns are applied only to the service name. As a result the ** pattern is not applicable.

### Sub Elements

- **Include**
- **Exclude**

See "Integrity monitoring rules language" on page 645 for a general description of include for their allowed attributes and sub elements. Only information specific to includes and excludes relating to this Entity Set class are included here.

### Special attributes of Include and Exclude for ServiceSets:

#### state

Include or exclude based on whether the state of the service (stopped, starting, stopping, running, continuePending, pausePending, paused). The following example would monitor the set of running services for change:

```
<ServiceSet>
 <include state="running"/>
 </ServiceSet>
```

## UserSet

The UserSet element represents a set of users. On a Windows system it operates on users local to the system - the same users displayed by the "Local Users and Groups" MMC snap-in. Note that these are *local* users only if the DSA is running on something other than a domain controller. On a domain controller a UserSet element will enumerate all of the domain users, which may not be advisable for extremely large domains.

On Unix systems, the users monitored are whatever the "getpwent_r()" and "getspnam_r()" APIs have been configured to return.

### Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| onChange | Will be monitored in real time | No | false | true, false |

### Entity Set Attributes

These are the attributes of the entity that can be monitored:

### Common Attributes

- **cannotChangePassword:** True or false indicating if the user is permitted to change their password.

- **disabled:** True or false indicating if the account has been disabled. On Windows systems this reflects the "disabled" checkbox for the user. On Unix systems this will be true if the user's account has expired or if their password has expired and they've exceeded the inactivity grace period for changing it.
- **fullName:** The display name of the user.
- **groups:** A comma-separated list of the groups to which the user belongs.
- **homeFolder:** The path to the home folder or directory.
- **lockedOut:** True or false indicating if the user has been locked out, either explicitly or due to excessive failed password attempts.
- **passwordHasExpired:** True or false indicating if the user's password has expired. Note that on Windows this attribute is only available on Windows XP and newer operating systems.
- **passwordLastChanged:** The timestamp of the last time the user's password was changed. This is recorded by the DSA as the number of milliseconds since Jan 1 1970 UTC - Deep Security Manager renders the timestamp in local time based on this value. Note that on Unix platforms the resolution of this attribute is one day, so the time component of the rendered timestamp is meaningless.
- **passwordNeverExpires:** True or false indicating if the password does not expire.
- **user:** The name of the user as known to the operating system. For example, "Administrator" or "root".

### Windows-only Attributes

- **description:** The primary group the user belongs to.
- **homeDriveLetter:** The drive letter to which a network share is mapped as the user's home folder.
- **logonScript:** The path to a script that executes every time the user logs in.
- **profilePath:** A network path if roaming or mandatory Windows user profiles are being used.

## Linux-only Attributes

- **group:** The primary group the user belongs to.
- **logonShell:** The path to the shell process for the user.
- **passwordExpiredDaysBeforeDisabled:** The number of days after the user's password expires that the account is disabled.
- **passwordExpiry:** The date on which the user's account expires and is disabled.
- **passwordExpiryInDays:** The number of days after which the user's password must be changed.
- **passwordMinDaysBetweenChanges:** The minimum number of days permitted between password changes.
- **passwordWarningDays:** The number of days before the user's password is to expire that user is warned.

## Short Hand Attributes

- **Standard:**
  - cannotChangePassword
  - disabled
  - groups
  - homeFolder
  - passwordHasExpired
  - passwordLastChanged
  - passwordNeverExpires
  - user
  - logonScript (Windows-only)
  - profilePath (Windows-only)
  - group (Linux-only)
  - logonShell (Linux-only)

- passwordExpiryInDays (Linux-only)
- passwordMinDaysBetweenChanges (Linux-only)

### Meaning of "Key"

The key is the username. This is not a hierarchical EntitySet. Patterns are applied only to the user name. As a result the "**" pattern is not applicable.

The following example monitors for any user creations or deletions. (Note that attributes are explicitly excluded so group membership would not be tracked):

```
<UserSet>
 <Attributes/>
 <include key="*" />
 </UserSet>
```

The following example would track the creation and deletion of the "jsmith" account, along with any changes to the STANDARD attributes of the account (since the STANDARD set for this EntitySet is automatically included if no specific attribute list is included):

```
<UserSet>
 <include key="jsmith" />
 </UserSet>
```

### Sub Elements

### Include and Exclude

See "Integrity monitoring rules language" on page 645 for a general description of include for their allowed attributes and sub elements.

### Special attributes of Include and Exclude for UserSets

Various other attributes of the user may be used in include and exclude feature tests. These tests compare a value against the value of an attribute of the user; take note of the platform support for various attributes - not all attributes are available across platforms or even platform revisions, hence the use of these tests in include and exclude elements is of limited use. The

feature tests support Unix glob-style wildcarding with * and ?, and there is no normalization of path separators or other characters - it is a simple match against the value of the attribute.

- **Disabled:** Does true or false match the disabled attribute of the user. The following example monitors users with a primary group of either "users" or "daemon":

```
<UserSet>
 <include disabled="true"/>
 </UserSet>
```

- **Group:** Does a wildcard match against the primary group of the user. This test is only applicable on Unix systems. The following example would monitor users with a primary group of either "users" or "daemon".

```
<UserSet>
 <include group="users"/>
 <include group="daemon"/>
 </UserSet>
```

- **LockedOut:** Does a true or false match against the lockedOut attribute of the user.
- **PasswordHasExpired:** Does a true or false match against the passwordHasExpired attribute of the user.
- **PasswordNeverExpires:** Does a true or false match against the passwordNeverExpires attribute of the user.

## WQLSet

The WQLSet element describes a result set from a Windows Management Instrumentation WQL query statement. WQL allows SQL-like queries to be made against many different object classes, with the results forming a table of rows where each row represents an object and each column represents the value of a specific attribute of the object.

**Note:** Many WMI queries consume a large amount of time and computer resources. It is easy to inadvertently issue a query that takes several minutes to complete and returns thousands of rows. It is highly recommended that all queries be tested before use in a WQLSet using a program like PowerShell or WMI Explorer.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| namespace | Sets the namespace of the WMI query. | Yes | N/A | String values representing a valid WMI namespace.<br><br>The "root\cimv2" namespace is the one most commonly used when querying Windows operating system objects, but others such as "root\directory\LDAP" and "root\Microsoft\SqlServer\ComputerManagement" can be used. See here for a small script called GetNamespaces.vbs that enumerates the available WMI namespaces on a given host. |
| wql | A WQL query string. | Yes | N/A | A valid WQL string.<br><br>The query must include the __Path attribute for each returned object; the Agent uses the __Path attribute as the entity key when storing and reporting results, so each returned WMI object must include a __Path. If using a query string such as "SELECT * FROM ..." the __Path attribute will be available, but if using a more selective query such as "SELECT Name FROM ..." you must explicitly include __Path by writing the query as "SELECT __Path,Name FROM ...". |
| onChange | Whether the files returned should be monitored in real time. | No | false | true, false |
| provider | Optionally specifies an alternative WMI namespace provider to use. | No | none | RsopLoggingModeProvider<br><br>At present this is only required/supported for group policy queries, and "RsopLoggingModeProvider" is the only supported value. Group policy queries are special since it's recommended that the RsopLoggingModeProvider be used to create a snapshot of the policy data that is present on a computer. If you create a snapshot of the policy data, the query can be performed against a consistent set of data before the system overwrites or deletes it during a refresh of policy. Creating a snapshot actually creates a new WMI namespace, so when using provider="RsopLoggingModeProvider" in a WQLSet, the namespace attribute should specify the suffix to be added to the created namespace. For example, a typical temporary namespace created by the RsopLoggingModeProvider would be "\\.\Root\Rsop\NS71EF4AA3_FB96_465F_AC1C_DFCF9A3E9010". Specify namespace="Computer" to query "\\.\Root\Rsop\NS71EF4AA3_FB96_465F_AC1C_DFCF9A3E9010\Computer".<br><br>Since the temporary namespace is a one-time value, it hampers the ability of the Agent to detect changes since the value appears in the entity key. To avoid this, the Agent will remove the portion |

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| | | | | of the returned __Path value after \Rsop\ and up to the next backslash when the RsopLoggingModeProvider is used. Entity keys will therefore have prefixes like "\\.\Root\Rsop\Computer" rather than "\\.\Root\Rsop\NS71EF4AA3_FB96_465F_AC1C_DFCF9A3E9010\Computer" |
| timeout | Specifies a per-row timeout in milliseconds. | No | 5000 | 1-60000<br><br>The WMI query is performed in semisynchronous mode, where result rows are fetched one at a time and there is a timeout on the fetching of a single row. If this parameter is not specified, 5000 (5 seconds) is used as the timeout value. |

## Entity Set Attributes

Each "row" returned by the WQL query is treated as a single Entity for integrity monitoring purposes, with the returned columns representing the attributes of the entity. Since WMI/WQL is an open-ended specification, there is no set list of available or supported attributes. The query and the schema of the WMI object being queried will determine the attributes being monitored.

For example, the WQLSet:

```
<WQLSet namespace="Computer" wql="select * from RSOP_SecuritySettings where
precedence=1" provider="RsopLoggingModeProvider" />
```

will return attributes of:

```
ErrorCode, GPOID, KeyName, SOMID, Setting, Status, id, precedence
```

whereas a WQLSet that queries network adapters such as:

```
<WQLSet namespace="root\cimv2" wql="select * from Win32_NetworkAdapter where
AdapterTypeId = 0" />
```

will return attributes such as:

```
AdapterType, AdapterTypeId, Availability, Caption, ConfigManagerErrorCode,
ConfigManagerUserConfig, CreationClassName Description, DeviceID, Index, Installed,
MACAddress, Manufacturer, MaxNumberControlled, Name, PNPDeviceID,
PowerManagementSupported, ProductName, ServiceName, SystemCreationClassName,
SystemName, TimeOfLastReset
```

In order to reduce the load on the Agent, it is advisable to explicitly include only the attributes that require monitoring rather than use "select * ..." in queries. This also has the benefit that changes to the WMI schema to add or remove attributes will not be reported as changes to the object unless the attributes are part of the set being monitored. With "select * from Win32_Foobar", a patch to Windows that adds a new attribute to the Win32_Foobar object class would result in the next integrity scan reporting a change for every object of that class since a new attribute has appeared.

The following are some example WMI queries which return desirable Windows system entities.

Query for Windows mounted storage devices: (selecting for * will typically result in 80% returned attributes being null or duplicate values)

```
<WQLSet namespace="root\cimv2" wql="SELECT __
Path,DeviceID,VolumeName,VolumeSerialNumber,DriveType,FileSystem,Access,MediaType,S
ize,FreeSpace FROM Win32_LogicalDisk" />
```

To further the preceding query, the DriveType can be specified to isolate only certain types of mounted logical storage devices, such as type 2 which is a "Removable Disk": (like a removable USB storage drive)

```
<WQLSet namespace="root\cimv2" wql="SELECT __
Path,DeviceID,VolumeName,VolumeSerialNumber,DriveType,FileSystem,Access,MediaType,S
ize,FreeSpace FROM Win32_LogicalDisk WHERE DriveType=2" />
```

(See here for details on the Win32_LogicalDisk class)

**USB Storage Device notes:** U3 USB devices will mount both a type 2 "Removable Disk" device and a type 3 "Compact Disc" device. Also, the above query is for storage devices only. USB non-storage devices will not be included. USB memory card adapters may appear as a type 1 "No Root Directory" device. A badly or Windows incompatible USB storage device may appear as a type 1 "Unknown" device.

Query for all known System Directories where the Drive is "F:" for relevant attributes:

```
<WQLSet namespace="root\cimv2" wql="SELECT __
Path,CreationDate,LastAccessed,LastModified,Drive,Path,FileName,Caption,FileType,Re
adable,Writeable FROM Win32_Directory WHERE Drive='F:'" />
```

Query for all known System Files where the Drive is "F:" for relevant attributes:

```
<WQLSet namespace="root\cimv2" wql="SELECT __
Path,CreationDate,LastAccessed,LastModified,Drive,Path,FileName,Name,FileType,Reada
ble,Writeable FROM CIM_DataFile WHERE Drive='F:'" />
```

### Meaning of Key

The key is the "__Path" attribute of the returned WMI object, which is generally of the form:

```
SystemName\Namespace:WmiObjectClass.KeyAttribute=Value[,KeyAttribute=Value...]
```

Some examples:

```
\\TEST-DESK\root\cimv2:Win32_QuickFixEngineering.HotFixID="KB958215-
IE7",ServicePackInEffect="SP0"
 \\TEST-DESK\ROOT\Rsop\NSF49B36AD_10A3_4F20_9541_B4C471907CE7\Computer:RSOP_
RegistryValue.

Path="MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\Lega
lNoticeText",precedence=1
 \\TEST-DESK\root\cimv2:BRCM_NetworkAdapter.DeviceID="8"
```

### Include Exclude

See "Integrity monitoring rules language" on page 645 for a general description of "include" and "exclude" for their allowed attributes and sub elements.

For WQLSet, "include" and "exclude" sub elements should typically not be required. It is preferable to use WQL to specify the exact set of objects to be monitored since that limits the amount of work done by both the Agent and the host's WMI implementation.

The use of any include or exclude sub elements can only reduce the set of objects returned by the query; the WQL must be changed in order to return additional objects. If it is necessary to use include or exclude elements to further restrict the WQL results, "*"and "?" characters can be used as simple wildcards to match against values of the entity key.

## Analyze logs with log inspection

**Note:** For a list of operating systems where log inspection is supported, see "Supported features by platform" on page 77.

The log inspection protection module helps you identify important events that might be buried in your operating system and application logs. These events can be sent to a security information and event management (SIEM) system or centralized logging server for correlation, reporting, and archiving. All events are also securely collected in the Deep Security Manager. For more information about logging and forwarding events, see "Configure log inspection event forwarding and storage" on page 695.

The log inspection module lets you:

- Meet PCI DSS log monitoring requirements.
- Detect suspicious behavior.
- Collect events across heterogeneous environments containing different operating systems and diverse applications.
- View events such as error and informational events (disk full, service start, service shutdown, etc.).
- Create and maintain audit trails of administrator activity (administrator login or logout, account lockout, policy change, etc.).

To enable and configure log inspection, see "Set up log inspection" below.

The log inspection feature in Deep Security enables real-time analysis of third party log files. The log inspection rules and decoders provide a framework to parse, analyze, rank and correlate events across a wide variety of systems. As with intrusion prevention and integrity monitoring, log inspection content is delivered in the form of rules included in a security update. These rules provide a high level means of selecting the applications and logs to be analyzed. To configure and examine log inspection rules, see "Define a log inspection rule for use in policies" on page 696.

## Set up log inspection

To use log inspection, perform these basic steps:

1. "Turn on the log inspection module" on the next page
2. "Run a recommendation scan" on the next page

3. "Apply the recommended log inspection rules" on the next page
4. "Configure log inspection event forwarding and storage" on page 695

For an overview of the log inspection module, see "Analyze logs with log inspection" on page 691.

## Turn on the log inspection module

1. Go to **Policies**.
2. Double-click the policy for which you want to enable log inspection.
3. Click **Log Inspection > General**.
4. For **Log Inspection State**, select **On**.
5. Click **Save**.

## Run a recommendation scan

Rules should be set to gather security events relevant to your requirements. When improperly set, events for this feature can overwhelm the Deep Security database if too many log entries are triggered and stored. Run a recommendation scan on the computer for recommendations about which rules are appropriate to apply.

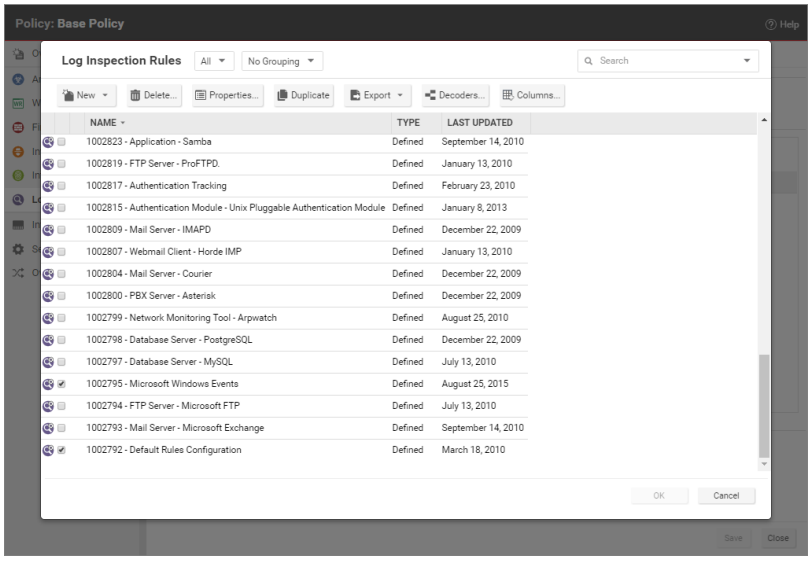
1. Go to **Computers** and double-click the appropriate computer.
2. Click **Log Inspection > General**.
3. For **Automatically implement Log Inspection Rule Recommendations (when possible)**, you can decide whether Deep Security should implement the rules it finds by selecting **Yes** or **No**.
4. In the **Recommendations** section, click **Scan For Recommendations**. Some log inspection rules written by Trend Micro require local configuration to function properly. If you assign one of these rules to your computers or one of these rules gets assigned automatically, an alert will be raised to notify you that configuration is required.

For more information about recommendation scans, see "Manage and run recommendation scans" on page 359.

## Apply the recommended log inspection rules

Deep Security ships with many pre-defined rules covering a wide variety of operating systems and applications. When you run a recommendation scan, you can choose to have Deep Security automatically implement the recommended rules, or you can choose to manually select and assign the rules by following the steps below:

1. Go to **Policies**.
2. Double-click the policy that you want to configure.
3. Click **Log Inspection > General**.
4. In the **Assigned Log Inspection Rules** section, the rules in effect for the policy are displayed. To add or remove log inspection rules, click **Assign/Unassign**.




5. Select or deselect the checkboxes for the rules you want to assign or unassign. You can edit the log inspection rule by right-clicking the rule and selecting **Properties** to edit the rule locally or **Properties (Global)** to apply the changes to all other policies that are using the rule. For more information, see "Examine a log inspection rule" on page 719.
6. Click **OK**.

Although Deep Security ships with log inspection rules for many common operating systems and applications, you also have the option to create your own custom rules. To create a custom rule, you can either use the "Basic Rule" template, or you can write your new rule in XML. For

information on how to create a custom rule, see "Define a log inspection rule for use in policies" on the next page.

## Configure log inspection event forwarding and storage

When a log inspection rule is triggered, an event is logged. To view these events, go to **Events & Reports > Log Inspection Events** or **Policy editor > Log Inspection > Log Inspection Events**. For more information on working with log inspection events, see "Log inspection events" on page 960.

Depending on the severity of the event, you can choose to send them to a syslog server (For information on enabling this feature, see "Forward Deep Security events to an external syslog or SIEM server " on page 814.) or to store events in the database by using the severity clipping feature.

There are two "severity clipping" settings available:

- **Send Agent events to syslog when they equal or exceed the following severity level:** This setting determines which events triggered by those rules get sent to the syslog server, if syslog is enabled.
- **Store events at the Agent for later retrieval by Deep Security Manager when they equal or exceed the following severity level:** This setting determines which log inspection events are kept in the database and displayed in the **Log Inspection Events** page.

To configure severity clipping:

1. Go to **Policies**.
2. Double-click the policy you want to configure.
3. Click **Log Inspection > Advanced**.
4. For **Send Agent/Appliance events to syslog when they equal or exceed the following severity level**, choose a severity level between **Low (0)** and **Critical (15)**.
5. For **Store events at the Agent/Appliance for later retrieval by DSM when they equal or exceed the following severity level**, choose a severity level between **Low (0)** and **Critical (15)**.
6. Click **Save**.

# Define a log inspection rule for use in policies

The OSSEC log inspection engine is integrated into Deep Security Agents and gives Deep Security the ability to inspect the logs and events generated by the operating system and applications running on the computer. Deep Security Manager ships with a standard set of OSSEC log inspection rules that you can assign to computers or policies. You can also create custom rules if there is no existing rule that fits your requirements.

Log Inspection Rules issued by Trend Micro are not editable (although you can duplicate them and then edit them.)

**Note:** Log Inspection Rules that are assigned to one or more computers or that are part of a policy cannot be deleted.

To create log inspection rules, perform these basic steps:


- "Create a new log inspection rule" below
- "Decoders" on page 698
- "Subrules" on page 700
- "Real world examples" on page 708
- "Log inspection rule severity levels and their recommended use" on page 717
- "strftime() conversion specifiers " on page 718
- "Examine a log inspection rule" on page 719


For an overview of the log inspection module, see "Analyze logs with log inspection" on page 691.

## Create a new log inspection rule

1. In the Deep Security Manager, go to **Policies** > **Common Objects** > **Rules** > **Log Inspection Rules**.
2. Click **New** > **New Log Inspection Rule**.
3. On the **General** tab, enter a name and an optional description for the rule.
4. The **Content** tab is where you define the rule. The easiest way to define a rule is to select

**Basic Rule** and use the options provided to define the rule. If you need further customization, you can select **Custom (XML)** to switch to an XML view of the rule that you are defining.

> **Note:** Any changes you make in the Custom (XML) view will be lost if you switch back to the Basic Rule view.

For further assistance in writing your own log inspection rules using the XML-based language, consult the OSSEC documentation or contact your support provider.

These options are available for the Basic Rule template:

- **Rule ID:** The Rule ID is a unique identifier for the rule. OSSEC defines 100000 - 109999 as the space for user-defined rules. Deep Security Manager will pre-populate the field with a new unique Rule ID.
- **Level:** Assign a level to the rule. Zero (0) means the rule never logs an event, although other rules that watch for this rule may fire.
- **Groups:** Assign the rule to one or more comma-separated groups. This can be useful when dependency is used because you can create rules that fire on the firing of a rule, or a rule that belongs to a specific group.
- **Rule Description:** Description of the rule.
- **Pattern Matching:** This is the pattern the rule will look for in the logs. The rule will be triggered on a match. Pattern matching supports Regular Expressions or simpler String Patterns. The "String Pattern" pattern type is faster than RegEx but it only supports three special operations:
  - **^ (caret)**: specifies the beginning of text
  - **$ (dollar sign)**: specifies the end of text
  - **| (pipe)**: to create a "OR" between multiple patterns

  For information on the regular expression syntax used by the Log Inspection module, see https://www.ossec.net/docs/syntax/regex.html.

- **Dependency:** Setting a dependency on another rule will cause your rule to only log an event if the rule specified in this area has also triggered.
- **Frequency** is the number of times the rule has to match within a specific time frame before the rule is triggered.
- **Time Frame** is the period of time in seconds within which the rule has to trigger a certain number of times (the frequency, above) to log an event.

Note: The **Content** tab only appears for log inspection rules that you create yourself. Log inspection rules issued by Trend Micro have a **Configuration** tab instead that displays the log inspection rule's configuration options (if any).

1. On the **Files** tab, type the full path to the file(s) you want your rule to monitor and specify the type of file it is.
2. On the **Options** tab, in the **Alert** section, select whether this rule triggers an alert in the Deep Security Manager.

   The **Alert Minimum Severity** setting is only used if you have written "multiple rules" within your rule - something that cannot be done using the Basic template. However, if after creating your rule using the Basic template, you edit the XML of the rule and add additional rules to the XML that have different severity levels, you can use the **Alert Minimum Severity Level** setting to set the minimum severity from the multiple rules that will trigger an Alert.

3. The **Assigned To** tab lists the policies and computers that are using this log inspection rule. Because you are creating a new rule, it has not been assigned yet.
4. Click **OK**. The rule is ready to be assigned to policies and computers.

## Decoders

A log inspection rule consists of a list of files to monitor for changes and a set of conditions to be met for the rule to trigger. When the log inspection engine detects a change in a monitored log file, the change is parsed by a decoder. Decoders parse the raw log entry into the following fields:

- **log:** the message section of the event
- **full_log:** the entire event
- **location:** where the log came from
- **hostname:** hostname of the vent source
- **program_name:** Program name. This is taken from the syslog header of the event
- **srcip:** the source IP address within the event
- **dstip:** the destination IP address within the event
- **srcport:** the source port number within the event
- **dstport:** the destination port number within the event
- **protocol:** the protocol within the event
- **action:** the action taken within the event
- **srcuser:** the originating user within the event
- **dstuser:** the destination user within the event
- **id:** any ID decoded as the ID from the event
- **status:** the decoded status within the event
- **command:** the command being called within the event
- **url:** the URL within the event
- **data:** any additional data extracted from the event
- **systemname:** the system name within the event

Rules examine this decoded data looking for information that matches the conditions defined in the rule.

If the matches are at a sufficiently high severity level, any of the following actions can be taken:

- An alert can be raised. (Configurable on the **Options** tab of the Log Inspection Rule's **Properties** window.)
- The event can be written to syslog. (Configurable in the **SIEM** area on **Administration > System Settings > Event Forwarding** tab.)

- The event can be sent to the Deep Security Manager. (Configurable in the **Log Inspection Syslog Configuration** setting on the **Policy or Computer Editor > Settings > Event Forwarding** tab.)

## Subrules

A single log inspection rule can contain multiple subrules. These subrules can be of two types: atomic or composite. An atomic rule evaluates a single event and a composite rule examines multiple events and can evaluate frequency, repetition, and correlation between events.

### Groups

Each rule, or grouping of rules, must be defined within a **<group></group>** element. The attribute name must contain the rules you want to be a part of this group. In the following example we have indicated that our group contains the syslog and sshd rules:

```
<group name="syslog,sshd,">
</group>
```

**Note:** Notice the trailing comma in the group name. Trailing commas are required if you intend to use the **<if_group></if_group>** tag to conditionally append another sub-rule to this one.

**Note:** When a set of log inspection rules are sent to an agent, the log inspection engine on the agent takes the XML data from each assigned rule and assembles it into what becomes essentially a single long log inspection rule. Some group definitions are common to all log inspection rules written by Trend Micro. For this reason Trend Micro has included a rule called "Default Rules Configuration" which defines these groups and which always gets assigned along with any other Trend Micro rules. (If you select a rule for assignment and haven't also selected the "Default Rules Configuration" rule, a notice will appear informing you that the rule will be assigned automatically.) *If you create your own log inspection rule and assign it to a Computer without assigning any Trend Micro-written rules, you must either copy the content of the "Default Rules Configuration" rule into your new rule, or also select the "Default Rules Configuration" rule for assignment to the Computer.*

## Rules, ID, and Level

A group can contain as many rules as you require. The rules are defined using the **<rule></rule>** element and must have at least two attributes, the **id** and the **level**. The **id** is a unique identifier for that signature and the **level** is the severity of the alert. In the following example, we have created two rules, each with a different rule ID and level:

```
<group name="syslog,sshd,">
       <rule id="100120" level="5">
       </rule>
       <rule id="100121" level="6">
       </rule>
</group>
```

**Note:** Custom rules must have ID values of 100,000 or greater.

You can define additional subgroups within the parent group using the **<group></group>** tag. This subgroup can reference any of the groups listed in the following table:

| Group Type | Group Name | Description |
|---|---|---|
| Reconnaissance | connection_attempt<br>web_scan<br>recon | Connection attempt<br>Web scan<br>Generic scan |
| Authentication Control | authentication_success<br>authentication_failed<br>invalid_login<br>login_denied<br>authentication_failures<br>adduser<br>account_changed | Success<br>Failure<br>Invalid<br>Login Denied<br>Multiple Failures<br>User account added<br>User Account changed or removed |
| Attack/Misuse | automatic_attack<br>exploit_attempt<br>invalid_access<br>spam<br>multiple_spam<br>sql_injection<br>attack<br>virus | Worm (nontargeted attack)<br>Exploit pattern<br>Invalid access<br>Spam<br>Multiple spam messages<br>SQL injection<br>Generic attack<br>Virus detected |
| Access Control | access_denied<br>access_allowed<br>unknown_resource<br>firewall_drop<br>multiple_drops<br>client_misconfig | Access denied<br>Access allowed<br>Access to nonexistent resource<br>Firewall drop<br>Multiple firewall drops<br>Client misconfiguration |

| Group Type | Group Name | Description |
|---|---|---|
| | client_error | Client error |
| Network Control | new_host<br>ip_spoof | New host detected<br>Possible ARP spoofing |
| System Monitor | service_start<br>system_error<br>system_shutdown<br>logs_cleared<br>invalid_request<br>promisc<br>policy_changed<br>config_changed<br>low_diskspace<br>time_changed | Service start<br>System error<br>Shutdown<br>Logs cleared<br>Invalid request<br>Interface switched to promiscuous mode<br>Policy changed<br>Configuration changed<br>Low disk space<br>Time changed |

**Note:** If event auto-tagging is enabled, the event will be labeled with the group name. Log inspection rules provided by Trend Micro make use of a translation table that changes the group to a more user-friendly version. So, for example, "login_denied" would appear as "Login Denied". Custom rules will be listed by their group name as it appears in the rule.

## Description

Include a **<description></description>** tag. The description text will appear in the event if the rule is triggered.

```
<group name="syslog,sshd,">
       <rule id="100120" level="5">
               <group>authentication_success</group>
               <description>SSHD testing authentication success</description>
       </rule>
       <rule id="100121" level="6">
               <description>SSHD rule testing 2</description>
       </rule>
</group>
```

## Decoded As

The **<decoded_as></decoded_as>** tag instructs the log inspection engine to only apply the rule if the specified decoder has decoded the log.

```
<rule id="100123" level="5">
       <decoded_as>sshd</decoded_as>
```

```
      <description>Logging every decoded sshd message</description>
</rule>
```

**Note:** To view the available decoders, go to the **Log Inspection Rule** page and click **Decoders.** Right-click on **1002791-Default Log Decoders** and select **Properties**. Go the **Configuration** tab and click **View Decoders**.

## Match

To look for a specific string in a log, use the **<match></match>**. Here is a Linux sshd failed password log:

```
 Jan 1 12:34:56 linux_server sshd[1231]: Failed password for invalid
       user jsmith from 192.168.1.123 port 1799 ssh2
```

Use the **<match></match>** tag to search for the "password failed" string.

```
<rule id="100124" level="5">
       <decoded_as>sshd</decoded_as>
       <match>^Failed password</match>
       <description>Failed SSHD password attempt</description>
</rule>
```

**Note:** Notice the regex caret ("^") indicating the beginning of a string. Although "Failed password" does not appear at the beginning of the log, the log inspection decoder will have broken up the log into sections. See "Decoders" on page 698 for more information. One of those sections is "log" which is the message part of the log as opposed to "full_log" which is the log in its entirety.

The following table lists supported regex syntax:

| Regex Syntax | Description |
|---|---|
| \w | A-Z, a-z, 0-9 single letters and numerals |
| \d | 0-9 single numerals |
| \s | single space |
| \t | single tab |
| \p | ()*+,-.:;<=>?[] |
| \W | not \w |
| \D | not \d |
| \S | not \s |
| \. | anything |

| Regex Syntax | Description |
|---|---|
| + | match one or more of any of the above (for example, \w+, \d+) |
| * | match zero or more of any of the above (for example, \w*, \d*) |
| ^ | indicates the beginning of a string (^somestring) |
| $ | specify the end of a string (somestring$) |
| \| | indicate an "OR" between multiple strings |

## Conditional Statements

Rule evaluation can be conditional upon other rules having been evaluated as true. The **<if_sid></if_sid>** tag instructs the log inspection engine to only evaluate this subrule if the rule identified in the tag has been evaluated as true. The following example shows three rules: 100123, 100124, and 100125. Rules 100124 and 100125 have been modified to be children of the 100123 rule using the **<if_sid></if_sid>** tag:

```
<group name="syslog,sshd,">
       <rule id="100123" level="2">
               <decoded_as>sshd</decoded_as>
               <description>Logging every decoded sshd message</description>
       </rule>
       <rule id="100124" level="7">
               <if_sid>100123</if_sid>
               <match>^Failed password</match>
               <group>authentication_failure</group>
               <description>Failed SSHD password attempt</description>
       </rule>
       <rule id="100125" level="3">
               <if_sid>100123</if_sid>
               <match>^Accepted password</match>
               <group>authentication_success</group>
               <description>Successful SSHD password attempt</description>
       </rule>
</group>
```

## Hierarchy of Evaluation

The **<if_sid></if_sid>** tag essentially creates a hierarchical set of rules. That is, by including an **<if_sid></if_sid>** tag in a rule, the rule becomes a child of the rule referenced by the **<if_sid></if_sid>** tag. Before applying any rules to a log, the log inspection engine assesses the **<if_sid></if_sid>** tags and builds a hierarchy of parent and child rules.

**Note:** The hierarchical parent-child structure can be used to improve the efficiency of your rules. If a parent rule does not evaluate as true, the log inspection engine will ignore the children of that parent.

**Note:** Although the **<if_sid></if_sid>** tag can be used to refer to subrules within an entirely different log inspection rule, you should avoid doing this because it makes the rule very difficult to review later on.

The list of available atomic rule conditional options is shown in the following table:

| Tag | Description | Notes |
|---|---|---|
| match | A pattern | Any string to match against the event (log). |
| regex | A regular expression | Any regular expression to match against the event(log). |
| decoded_as | A string | Any prematched string. |
| srcip | A source IP address | Any IP address that is decoded as the source IP address. Use "!" to negate the IP address. |
| dstip | A destination IP address | Any IP address that is decoded as the destination IP address. Use "!" to negate the IP address. |
| srcport | A source port number | Any source port (match format). |
| dstport | A destination port number | Any destination port (match format). |
| user | A username | Any username that is decoded as a username. |
| program_name | A program name | Any program name that is decoded from the syslog process name. |
| hostname | A system hostname | Any hostname that is decoded as a syslog hostname. |
| time | A time range in the format hh:mm - hh:mm or hh:mm am - hh:mm pm | The time range that the event must fall within for the rule to trigger. |
| weekday | A weekday (sunday, monday, tuesday, etc.) | Day of the week that the event must fall on for the rule to trigger. |
| id | An ID | Any ID that is decoded from the event. |
| url | A URL | Any URL that is decoded from the event. |

Use the **<if_sid>100125</if_sid>** tag to make this rule depend on the 100125 rule. This rule will be checked only for sshd messages that already matched the successful login rule.

```
<rule id="100127" level="10">
       <if_sid>100125</if_sid>
       <time>6 pm - 8:30 am</time>
       <description>Login outside business hours.</description>
       <group>policy_violation</group>
</rule>
```

## Restrictions on the Size of the Log Entry

The following example takes the previous example and adds the **maxsize** attribute which tells the log inspection engine to only evaluate rules that are less than the maxsize number of characters:

```
<rule id="100127" level="10" maxsize="2000">
       <if_sid>100125</if_sid>
       <time>6 pm - 8:30 am</time>
       <description>Login outside business hours.</description>
       <group>policy_violation</group>
</rule>
```

The following table lists possible atomic rule tree-based options:

| Tag | Description | Notes |
|---|---|---|
| if_sid | A rule ID | Adds this rule as a child rule of the rules that match the specified signature ID. |
| if_group | A group ID | Adds this rule as a child rule of the rules that match the specified group. |
| if_level | A rule level | Adds this rule as a child rule of the rules that match the specified severity level. |
| description | A string | A description of the rule. |
| info | A string | Extra information about the rule. |
| cve | A CVE number | Any Common Vulnerabilities and Exposures (CVE) number that you would like associated with the rule. |
| options | alert_by_email<br>no_email_alert<br>no_log | Additional rule options to indicate if the Alert should generate an e-mail, alert_by_email, should not generate an email, no_email_alert, or should not log anything at all, no_log. |

## Composite Rules

Atomic rules examine single log entries. To correlate multiple entries, you must use composite rules. Composite rules are supposed to match the current log with those already received. Composite rules require two additional options: the **frequency** option specifies how many times an event or pattern must occur before the rule generates an alert, and the **timeframe** option tells the log inspection engine how far back, in seconds, it should look for previous logs. All composite rules have the following structure:

```
<rule id="100130" level="10" frequency="x" timeframe="y">
</rule>
```

For example, you could create a composite rule that creates a higher severity alert after five failed passwords within a period of 10 minutes. Using the **<if_matched_sid></if_matched_sid>**

tag you can indicate which rule needs to be seen within the desired frequency and timeframe for your new rule to create an alert. In the following example, the **frequency** attribute is set to trigger when five instances of the event are seen and the **timeframe** attribute is set to specify the time window as 600 seconds.

The **<if_matched_sid></if_matched_sid>** tag is used to define which other rule the composite rule will watch:

```
<rule id="100130" level="10" frequency="5" timeframe="600">
       <if_matched_sid>100124</if_matched_sid>
       <description>5 Failed passwords within 10 minutes</description>
</rule>
```

There are several additional tags that you can use to create more granular composite rules. These rules, as shown in the following table, allow you to specify that certain parts of the event must be the same. This allows you to tune your composite rules and reduce false positives:

| Tag | Description |
|---|---|
| same_source_ip | Specifies that the source IP address must be the same. |
| same_dest_ip | Specifies that the destination IP address must be the same. |
| same_dst_port | Specifies that the destination port must be the same. |
| same_location | Specifies that the location (hostname or agent name) must be the same. |
| same_user | Specifies that the decoded username must be the same. |
| same_id | Specifies that the decoded id must be the same. |

If you wanted your composite rule to alert on every authentication failure, instead of a specific rule ID, you could replace the **<if_matched_sid></if_matched_sid>** tag with the **<if_matched_ group></if_matched_ group>** tag. This allows you to specify a category, such as **authentication_ failure**, to search for authentication failures across your entire infrastructure.

```
<rule id="100130" level="10" frequency="5" timeframe="600">
       <if_matched_group>authentication_failure</if_matched_group>
       <same_source_ip />
       <description>5 Failed passwords within 10 minutes</description>
</rule>
```

In addition to **<if_matched_sid></if_matched_sid>** and **<if_matched_group></if_matched_ group>** tags, you can also use the **<if_matched_regex></if_matched_regex>** tag to specify a regular expression to search through logs as they are received.

```
<rule id="100130" level="10" frequency="5" timeframe="600">
       <if_matched_regex>^Failed password</if_matched_regex>
       <same_source_ip />
       <description>5 Failed passwords within 10 minutes</description>
</rule>
```

## Real world examples

Deep Security includes many default log inspection rules for dozens of common and popular applications. Through Security Updates, new rules are added regularly. In spite of the growing list of applications supported by log inspection rules, you may find the need to create a custom rule for an unsupported or custom application.

In this section we will walk through the creation of a custom CMS (Content Management System) hosted on the Microsoft Windows Server IIS .Net platform with a Microsoft SQL Database as the data repository.

The first step is to identify the following application logging attributes:

1. Where does the application log to?
2. Which log inspection decoder can be used to decode the log file?
3. What is the general format of a log file message?

For our custom CMS example the answers are as follows:

1. Windows Event Viewer
2. Windows Event Log (eventlog)
3. Windows Event Log Format with the following core attributes:
    - Source: CMS
    - Category: None
    - Event: <Application Event ID>

The second step is to identify the categories of log events by application feature, and then organize the categories into a hierarchy of cascading groups for inspection. Not all inspected groups need to raise events; a match can be used as a conditional statement. For each group, identify the log format attributes which the rule can use as matching criteria. This can also be performed by inspecting all application logs for patterns and logical groupings of log events.

For example, the CMS application supports the following functional features which we will create log inspection rules for:

- CMS Application Log (Source: CMS)
  - Authentication (Event: 100 to 119)
    - User Login successful (Event: 100)
    - User Login unsuccessful (Event: 101)
    - Administrator Login successful (Event: 105)
    - Administrator Login unsuccessful (Event: 106)
  - General Errors (Type: Error)
    - Database error (Event: 200 to 205)
    - Runtime error (Event: 206-249)
  - Application Audit (Type: Information)
    - Content
      - New content added (Event: 450 to 459)
      - Existing content modified (Event: 460 to 469)
      - Existing content deleted (Event: 470 to 479)
    - Administration
      - User
        - New User created (Event: 445 to 446)
        - Existing User deleted (Event: 447 to 449)

This structure will provide you with a good basis for rule creation. Now to create a new log inspection rule in Deep Security Manager.

**To create the new CMS Log Inspection Rule:**

1. In the Deep Security Manager, go to **Policies > Common Objects > Rules > Log Inspection Rules** and click **New** to display the **New Log Inspection Rule Properties** window.
2. Give the new rule a name and a description, and then click the **Content** tab.

3. The quickest way to create a new custom rule is to start with a basic rule template. Select the **Basic Rule** radio button.
4. The **Rule ID** field will be automatically populated with an unused ID number of 100,000 or greater, the IDs reserved for custom rules.
5. Set the **Level** setting to **Low (0)**.
6. Give the rule an appropriate Group name. In this case, "cms".

7. Provide a short rule description.

General | Content | Files | Options | Assigned To

**Template**

- (•) Basic Rule
- ( ) Custom (XML)

**General Information**

Rule ID: 100000

Level: Low (0)

Groups (comma separated): cms

Rule Description: windows events for 'cms' group

**Pattern Matching**

Pattern to Match:

Pattern Type: String Pattern

**Dependency**

- (•) None
- ( ) Trigger event on the triggering of another rule:
- ( ) Trigger event on the triggering of any rule belonging to a specific group:

**Composite (optional)**

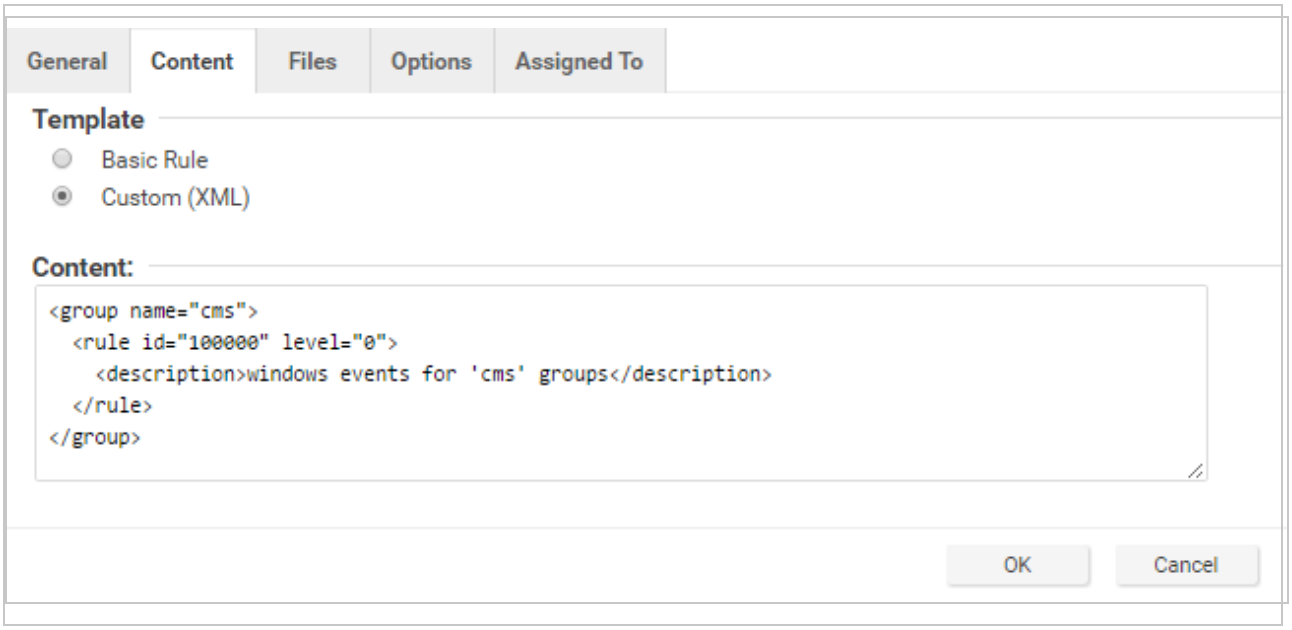
Only trigger if this rule matches its dependent rule the specified frequency of times in the specified time frame (in seconds).

Frequency (1 to 128):

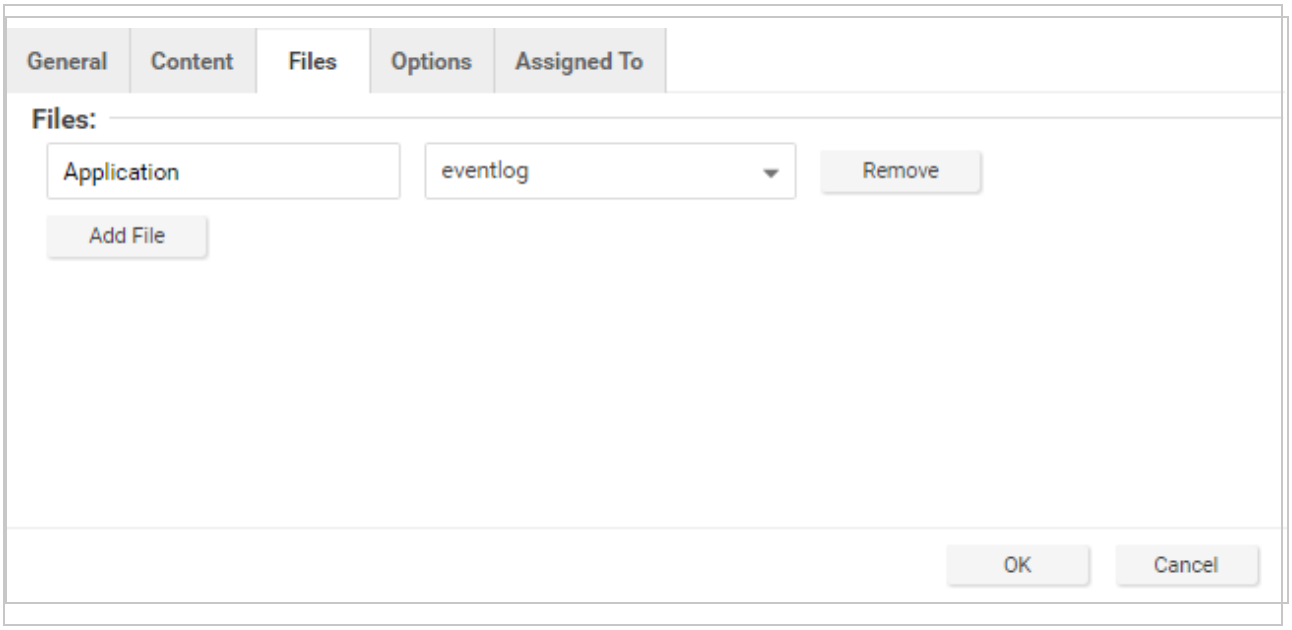
Time Frame (1 to 86400):

OK | Cancel

8. Now select the **Custom (XML)** option. The options you selected for your "Basic" rule will be converted to XML.




9. Click the **Files** tab and click the **Add File** button to add any application log files and log types which the rule will be applied to. In this case, "Application", and "eventlog" as the file type.




**Note:** **Eventlog** is a unique file type in Deep Security because the location and filename of the log files don't have to be specified. Instead, it is sufficient to type the log name as it

is displayed in the Windows Event Viewer. Other log names for the eventlog file type might be "Security", "System", "Internet Explorer", or any other section listed in the Windows Event Viewer. Other file types will require the log file's location and filename. (*C/C++ strftime()* conversion specifiers are available for matching on filenames. See the table below for a list of some of the more useful ones.)

10. Click **OK** to save the basic rule.
11. Working with the basic rule Custom (XML) created, we can begin adding new rules to the group based on the log groupings identified previously. We will set the base rule criteria to the initial rule. In the following example, the CMS base rule has identified Windows Event Logs with a Source attribute of "CMS":

```
<group name="cms">
       <rule id="100000" level="0">
               <category>windows</category>
               <extra_data>^CMS</extra_data>
               <description>Windows events from source 'CMS' group messages.</descriptio
       </rule>
```

12. Now we build up subsequent rules from the identified log groups. The following example identifies the authentication and login success and failure and logs by Event IDs.

```
<rule id="100001" level="0">
       <if_sid>100000</if_sid>
       <id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id>
       <group>authentication</group>
       <description>CMS Authentication event.</description>
</rule>

<rule id="100002" level="0">
       <if_group>authentication</if_group>
       <id>100</id>
       <description>CMS User Login success event.</description>
</rule>
<rule id="100003" level="4">
       <if_group>authentication</if_group>
       <id>101</id>
       <group>authentication_failure</group>
       <description>CMS User Login failure event.</description>
```

```
</rule>
<rule id="100004" level="0">
       <if_group>authentication</if_group>
       <id>105</id>
       <description>CMS Administrator Login success event.</description>
</rule>
<rule id="100005" level="4">
       <if_group>authentication</if_group>
       <id>106</id>
       <group>authentication_failure</group>
       <description>CMS Administrator Login failure event.</description>
</rule>
```

13. Now we add any composite or correlation rules using the established rules. The follow example shows a high severity composite rule that is applied to instances where the repeated login failures have occurred 5 times within a 10 second time period:

```
<rule id="100006" level="10" frequency="5" timeframe="10">
       <if_matched_group>authentication_failure</if_matched_group>
       <description>CMS Repeated Authentication Login failure event.</description>
</rule>
```

14. Review all rules for appropriate severity levels. For example, error logs should have a severity of level 5 or higher. Informational rules would have a lower severity.
15. Finally, open the newly created rule, click the **Configuration** tab and copy your custom rule XML into the rule field. Click **Apply** or **OK** to save the change.

Once the rule is assigned to a policy or computer, the log inspection engine should begin inspecting the designated log file immediately.

### The complete Custom CMS Log Inspection Rule:

```
<group name="cms">
        <rule id="100000" level="0">
               <category>windows</category>
               <extra_data>^CMS</extra_data>
               <description>Windows events from source 'CMS' group messages.</description>
       </rule>
        <rule id="100001" level="0">
               <if_sid>100000</if_sid>
               <id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id>
```

```
        <group>authentication</group>
        <description>CMS Authentication event.</description>
</rule>

<rule id="100002" level="0">
        <if_group>authentication</if_group>
        <id>100</id>
        <description>CMS User Login success event.</description>
</rule>

<rule id="100003" level="4">
        <if_group>authentication</if_group>
        <id>101</id>
        <group>authentication_failure</group>
        <description>CMS User Login failure event.</description>
</rule>

<rule id="100004" level="0">
        <if_group>authentication</if_group>
        <id>105</id>
        <description>CMS Administrator Login success event.</description>
</rule>

<rule id="100005" level="4">
        <if_group>authentication</if_group>
        <id>106</id>
        <group>authentication_failure</group>
        <description>CMS Administrator Login failure event.</description>
</rule>

<rule id="100006" level="10" frequency="5" timeframe="10">
        <if_matched_group>authentication_failure</if_matched_group>
        <description>CMS Repeated Authentication Login failure event.</description>
</rule>

<rule id="100007" level="5">
        <if_sid>100000</if_sid>
        <status>^ERROR</status>
        <description>CMS General error event.</description>
        <group>cms_error</group>
```

```
        </rule>

        <rule id="100008" level="10">
                <if_group>cms_error</if_group>
                <id>^200|^201|^202|^203|^204|^205</id>
                <description>CMS Database error event.</description>
        </rule>

        <rule id="100009" level="10">
                <if_group>cms_error</if_group>
                <id>^206|^207|^208|^209|^230|^231|^232|^233|^234|^235|^236|^237|^238|
                        ^239^|240|^241|^242|^243|^244|^245|^246|^247|^248|^249</id>
                <description>CMS Runtime error event.</description>
        </rule>

        <rule id="100010" level="0">
                <if_sid>100000</if_sid>
                <status>^INFORMATION</status>
                <description>CMS General informational event.</description>
                <group>cms_information</group>
        </rule>

        <rule id="100011" level="5">
                <if_group>cms_information</if_group>
                <id>^450|^451|^452|^453|^454|^455|^456|^457|^458|^459</id>
                <description>CMS New Content added event.</description>
        </rule>

        <rule id="100012" level="5">
                <if_group>cms_information</if_group>
                <id>^460|^461|^462|^463|^464|^465|^466|^467|^468|^469</id>
                <description>CMS Existing Content modified event.</description>
        </rule>

        <rule id="100013" level="5">
                <if_group>cms_information</if_group>
                <id>^470|^471|^472|^473|^474|^475|^476|^477|^478|^479</id>
                <description>CMS Existing Content deleted event.</description>
        </rule>
```

```
        <rule id="100014" level="5">
                <if_group>cms_information</if_group>
                <id>^445|^446</id>
                <description>CMS User created event.</description>
        </rule>

        <rule id="100015" level="5">
                <if_group>cms_information</if_group>
                <id>^447|449</id>
                <description>CMS User deleted event.</description>
        </rule>

</group>
```

## Log inspection rule severity levels and their recommended use

| Level | Description | Notes |
|---|---|---|
| Level 0 | Ignored, no action taken | Primarily used to avoid false positives. These rules are scanned before all the others and include events with no security relevance. |
| Level 1 | no predefined use | |
| Level 2 | System low priority notification | System notification or status messages that have no security relevance. |
| Level 3 | Successful or authorized events | Successful login attempts, firewall allow events, etc. |
| Level 4 | System low priority errors | Errors related to bad configurations or unused devices or applications. They have no security relevance and are usually caused by default installations or software testing. |
| Level 5 | User-generated errors | Missed passwords, denied actions, etc. These messages typically have no security relevance. |
| Level 6 | Low relevance attacks | Indicate a worm or a virus that provide no threat to the system such as a Windows worm attacking a Linux server. They also include frequently triggered IDS events and common error events. |
| Level 7 | no predefined use | |
| Level 8 | no predefined use | |
| Level 9 | Error from invalid source | Include attempts to login as an unknown user or from an invalid source. The message might have security relevance especially if repeated. They also include errors regarding the **admin** or **root** account. |
| Level 10 | Multiple user generated | Include multiple bad passwords, multiple failed logins, etc. They might indicate an attack, or it might be just that a user forgot his or her credentials. |

| Level | Description | Notes |
|---|---|---|
| | errors | |
| Level 11 | no predefined use | |
| Level 12 | High-importance event | Include error or warning messages from the system, kernel, etc. They might indicate an attack against a specific application. |
| Level 13 | Unusual error (high importance) | Common attack patterns such as a buffer overflow attempt, a larger than normal syslog message, or a larger than normal URL string. |
| Level 14 | High importance security event | Typically the result of the correlation of multiple attack rules and indicative of an attack. |
| Level 15 | Attack Successful | Very small chance of false positive. Immediate attention is necessary. |

## *strftime()* conversion specifiers

| Specifier | Description |
|---|---|
| %a | Abbreviated weekday name (e.g., Thu) |
| %A | Full weekday name (e.g., Thursday) |
| %b | Abbreviated month name (e.g., Aug) |
| %B | Full month name (e.g., August) |
| %c | Date and time representation (e.g., Thu Sep 22 12:23:45 2007) |
| %d | Day of the month (01 - 31) (e.g., 20) |
| %H | Hour in 24 h format (00 - 23) (e.g., 13) |
| %I | Hour in 12 h format (01 - 12) (e.g., 02) |
| %j | Day of the year (001 - 366) (e.g., 235) |
| %m | Month as a decimal number (01 - 12) (e.g., 02) |
| %M | Minute (00 - 59) (e.g., 12) |
| %p | AM or PM designation (e.g., AM) |
| %S | Second (00 - 61) (e.g., 55) |
| %U | Week number with the first Sunday as the first day of week one (00 - 53) (e.g., 52) |
| %w | Weekday as a decimal number with Sunday as 0 (0 - 6) (e.g., 2) |
| %W | Week number with the first Monday as the first day of week one (00 - 53) (e.g., 21) |
| %x | Date representation (e.g., 02/24/79) |
| %X | Time representation (e.g., 04:12:51) |
| %y | Year, last two digits (00 - 99) (e.g., 76) |
| %Y | Year (e.g., 2008) |
| %Z | Time zone name or abbreviation (e.g., EST) |
| %% | A % sign (e.g., %) |

More information can be found at the following websites:

https://secure.php.net/manual/en/function.strftime.php
www.cplusplus.com/reference/clibrary/ctime/strftime.html

## Examine a log inspection rule

Log inspection rules are found in the Deep Security Manager at **Policies > Common Objects > Rules > Log Inspection Rules**.

### Log inspection rule structure and the event matching process

This screen shot displays the contents of the **Configuration** tab of the Properties window of the "Microsoft Exchange" log inspection rule:

General | Configuration | Options | Assigned To

Configuration Options

Log Files to monitor:

Add

C:\Windows\system32\LogFiles\SMTPSVC1\ex%y%m%d.l

Remove

Type of Log File(s): syslog

This rule matches events decoded as: msexchange

3800 - Grouping of Exchange rules — Default - Ignore

3801 - E-mail RCPT is not valid (invalid account) — Default - Medium (5)

3851 - Multiple e-mail attempts to an invalid account — Default - High (10)

Frequency (1 to 128): 10

Time Frame (1 to 86400): 120 secs

Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400): 120 secs

3802 - E-mail 500 error code — Default - Medium (4)

3852 - Multiple e-mail 500 error code (spam) — Default - High (9)

Frequency (1 to 128): 12

Time Frame (1 to 86400): 120 secs

Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400): 240 secs

View Rules...

OK | Cancel | Apply

Here is the structure of the rule:

- 3800 - Grouping of Exchange Rules - Ignore
  - 3801 - Email rcpt is not valid (invalid account) - Medium (4)
    - 3851 - Multiple email attempts to an invalid account - High (9)
      - Frequency - 10
      - Time Frame - 120
      - Ignore - 120
  - 3802 - Email 500 error code - Medium (4)
    - 3852 - Email 500 error code (spam) - High (9)
      - Frequency - 12
      - Time Frame - 120
      - Ignore - 240

The log inspection engine will apply log events to this structure and see if a match occurs. For example, if an Exchange event occurs, and this event is an email receipt to an invalid account, the event will match line 3800 (because it is an Exchange event). The event will then be applied to line 3800's sub-rules: 3801 and 3802.

If there is no further match, this "cascade" of matches will stop at 3800. Because 3800 has a severity level of "Ignore", no log inspection event would be recorded.

However, an email receipt to an invalid account does match one of 3800's sub-rules: sub-rule 3801. Sub-rule 3801 has a severity level of "Medium(4)". If the matching stopped here, a log inspection event with a severity level of "Medium(4)" would be recorded.

But there is still another sub-rule to be applied to the event: sub-rule 3851. Sub-rule 3851 with its three attributes will match if the same event has occurred 10 times within the last 120 seconds. If so, a log inspection event with a severity "High(9)" is recorded. (The "Ignore" attribute tells sub-rule 3851 to ignore individual events that match sub-rule 3801 for the next 120 seconds. This is useful for reducing "noise".)

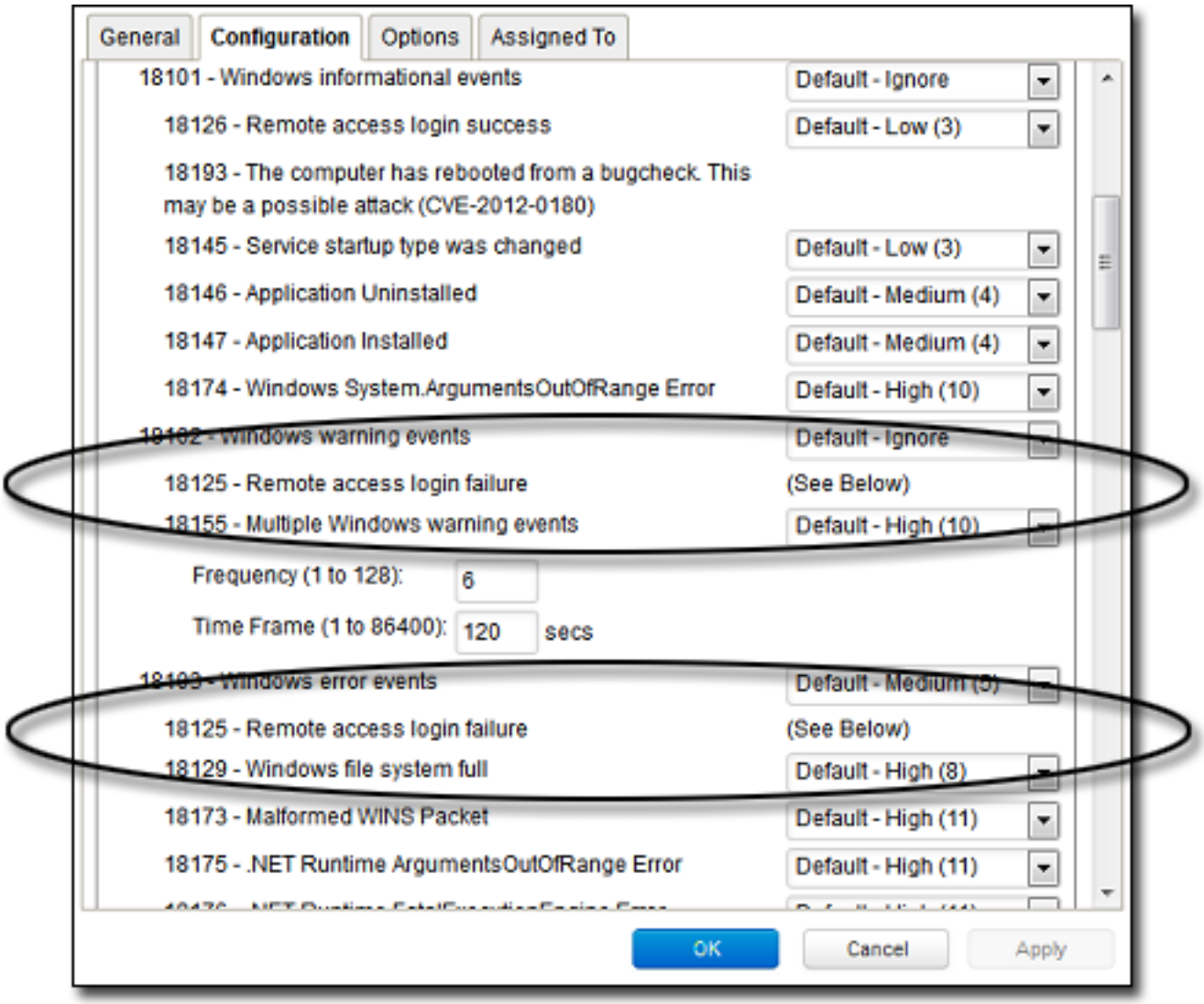
Assuming the parameters of sub-rule 3851 have been matched, a log inspection event with Severity "High(9)" is now recorded.

Looking at the Options tab of the Microsoft Exchange Rule, we see that Deep Security Manager will raise an alert if any sub-rules with a severity level of "Medium(4)" have been matched. Since this is the case in our example, the alert will be raised (if "Alert when this rule logs an event" is selected).

## Duplicate Sub-rules

Some log inspection rules have duplicate sub-rules. To see an example, open the "Microsoft Windows Events" rule and click on the **Configuration** tab. Note that sub-rule 18125 (Remote access login failure) appears under sub-rules 18102 and 18103. Also note that in both cases sub-rule 18125 does not have a severity value, it only says "See Below".

Instead of being listed twice, Rule 18125 is listed once at the bottom of the **Configuration** page:




# Block access to malicious URLs with web reputation

**Note:** For a list of operating systems where web reputation is supported, see "Supported features by platform" on page 77.

The web reputation module protects against web threats by blocking access to malicious URLs. Deep Security uses Trend Micro's Web security databases from Smart Protection Network sources to check the reputation of websites that users are attempting to access. The website's reputation is correlated with the specific web reputation policy enforced on the computer.

Depending on the security level being enforced, Deep Security will either block or allow access to the URL.

**Note:** The web reputation module does not block HTTPS traffic.

To enable and configure web reputation, perform the basic steps below:

1. "Turn on the web reputation module" below
2. "Switch between inline and tap mode" below
3. "Enforce the security level" on the next page
4. "Create exceptions" on page 726
5. "Configure the Smart Protection Server" on page 727
6. "Edit advanced settings" on page 728

To suppress messages that appear to users of agent computers, see "Configure notifications on the computer" on page 509

## Turn on the web reputation module

1. Go to **Policies**.
2. Double-click the policy for which you want to enable web reputation.
3. Click **Web Reputation > General**.
4. For **Web Reputation State**, select **On**.
5. Click **Save**.

## Switch between inline and tap mode

Web reputation uses the Deep Security Network Engine which can operate in one of two modes:

- **Inline:** Packet streams pass directly through the Deep Security network engine. All rules, therefore are applied to the network traffic before they proceed up the protocol stack
- **Tap mode:** Packet streams are replicated and diverted from the main stream.

In tap mode, the live stream is not modified. All operations are performed on the replicated stream. When in tap mode, Deep Security offers no protection beyond providing a record of events.

To switch between inline and tap mode, open the **Computer or Policy editor**[1] and go to **Settings > Advanced > Network Engine Mode**.

For more on the network engine, see "Test firewall rules before deploying them" on page 585.

## Enforce the security level

Web addresses that are known to be or are suspected of being malicious are assigned a **risk level** of:

- **Dangerous**: Verified to be fraudulent or known sources of threats
- **Highly suspicious**: Suspected to be fraudulent or possible sources of threats
- **Suspicious**: Associated with spam or possibly compromised

Security levels determine whether Deep Security will allow or block access to a URL, based on the associated risk level. For example, if you set the security level to low, Deep Security will only block URLs that are known to be web threats. As you set the security level higher, the web threat detection rate improves but the possibility of false positives also increases.

### To configure the security level:

1. Go to **Policies**.
2. Double-click the policy that you want to edit.
3. Click **Web Reputation > General**.
4. Select one of the following security levels:
    - **High**: Blocks pages that are:
        - Dangerous
        - Highly suspicious
        - Suspicious

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

- **Medium**: Blocks pages that are:
  - Dangerous
  - Highly Suspicious
- **Low**: Blocks pages that are:
  - Dangerous

5. Click **Save**.

## Create exceptions

You can override the block and allow behavior dictated by the Smart Protection Network's assessments with your lists of URLs that you want to block or allow.

**Note:** The **Allowed** list takes precedence over the **Blocked** list. URLs that match entries in the **Allowed** list are not checked against the **Blocked** list.

### To create URL exceptions:

1. Go to **Policies**.
2. Double-click the policy that you want to edit.
3. Click **Web Reputation > Exceptions**.
4. To allow URLs:
   a. Go to the **Allowed** section.
   b. In the blank under **URLs to be added to the Allowed list (one per line)**, enter your desired URL. Multiple URLs can be added at once but they must be separated by a line break.
   c. Select either:
      - **Allow URLs from the domain**: Allow all pages from the domain. Sub-domains are supported. Only include the domain (and optionally sub-domain) in the entry. For example, "example.com" and "another.example.com" are valid entries.
      - **Allow the URL:**: The URL as entered will be allowed. Wildcards are supported. For example, "example.com/shopping/coats.html", and "example.com/shopping/*" are valid entries.
   d. Click **Add**.

To block URLs:

a. Go to the **Blocked** section
b. In the blank under **URLs to be added to the Blocked list (one per line)**, enter your desired URL. Multiple URLs or keywords can be added at once but they must be separated by a line break.
c. Select either:
   - **Block URLs from the domain**: Block all pages from the domain. Sub-domains are supported. Only include the domain (and optionally sub-domain) in the entry. For example, "example.com" and "another.example.com" are valid entries.
   - **Block the URL**: The URL as entered will be blocked. Wildcards are supported. For example, "example.com/shopping/coats.html", and "example.com/shopping/*" are valid entries.
   - **Block URLs containing this keyword**: Any URL containing the keyword will be blocked.
d. Click **Add**.

5. Click **Save**.

## Configure the Smart Protection Server

Smart Protection Service for web reputation supplies web information required by the web reputation module. For more information, see Smart Protection Network - Global Threat Intelligence.

To configure Smart Protection Server:

1. Go to **Policies**.
2. Double-click the policy you'd like to edit.
3. Click **Web Reputation > Smart Protection**.
4. Select whether to connect directly to Trend Micro's Smart Protection service:
   a. Select **Connect directly to Global Smart Protection Service**.
   b. Optionally select **When accessing Global Smart Protection Service, use proxy**. Select **New** from the drop down menu and enter your desired proxy.

   Or to connect to one or more locally installed Smart Protection Servers:

a. Select **Use locally installed Smart Protection Server (ex: "http://[server]:5274")**.
b. Enter the Smart Protection Server URL into the field and click **Add**. To find the Smart Protection Server URL, do one of the following:
   - Log in to the Smart Protection Server, and in the main pane, look under **Real Time Status**. The Smart Protection Server's HTTP and HTTPS URLs are listed in the **Web Reputation** row. The HTTPS URL is only supported with 11.0 Deep Security Agents and up. If you have 10.3 or earlier agents, use the HTTP URL.

   Or

   - If you deployed the Smart Protection Server in AWS, go to the AWS **CloudFormation** service, select the check box next to the Smart Protection Server stack, and in the bottom pane, click the **Outputs** tab. The Smart Protection Server's HTTP and HTTPS URLs appear in the **WRSurl** and **WRSHTTPSurl** fields. The WRSHTTPSurl is only supported with 11.0 Deep Security Agents and up. If you have 10.3 or earlier agents, use the WRSurl URL.
c. Optionally select **When off domain, connect to global Smart Protection Service. (Windows only)**.

5. Click **Save**.

### Smart Protection Server Connection Warning

This option determines whether error events are generated and alerts are raised if a computer loses its connection to the Smart Protection Server. Select either **Yes** or **No** and click **Save**.

**Note:** If you have a locally installed Smart Protection Server, this option should be set to **Yes** on at least one computer so that you are notified if there is a problem with the Smart Protection Server itself.

## Edit advanced settings

### Blocking Page

When users attempt to access a blocked URL, they will be redirected to a blocking page. In the blank for **Link**, provide a link that users can use to request access to the blocked URL.

### Alert

Decide to raise an alert when a web reputation event is logged by selecting either **Yes** or **No**.

### Ports

Select specific ports to monitor for potentially harmful web pages from the drop down list next to **Ports to monitor for potentially harmful web pages**.

## Deep Security Best Practice Guide

The Deep Security 10.0 Best Practice Guide is intended to help you get the best productivity out of the product. It contains a collection of best practices that are based on knowledge gathered from previous enterprise deployments, lab validations, and lessons learned in the field. Examples and considerations in this document serve only as a guide and not a representation of strict design requirements. These guidelines do not apply in every environment but will help guide you through the decisions that you need in configuring Deep Security for optimum performance.

The Deep Security 11.0 Best Practice Guide is currently available in PDF format and includes the following:

- Deployment considerations and recommendations
- Upgrade guidelines and scenarios
- Sizing considerations and recommendations
- Recommended configurations to maximize system performance and reduce administrative overhead
- Best practice tips for VDI, private, and public cloud environments

# Maintain

## Check your license information

**Note:** Does not apply to a multi-tenant configuration that inherits licensing from the parent tenant.

Displays details about your Trend Micro Deep Security product licenses. Deep Security consists of six module packages:

- Anti-Malware and Web Reputation
- Firewall and Intrusion Prevention
- Integrity Monitoring
- Log Inspection
- Multi-Tenancy

Each module package can be licensed fully or for a trial basis. You can see an individual package's license status by clicking **View Details**. Contact Trend Micro if you wish to upgrade your license. If Trend Micro has provided you with a new activation code, click **Enter New Activation Code** and enter it there. Newly licensed features are immediately available.

When a license expires, existing functionality persists but updates are no longer delivered.

Alerts are raised if any module is about to expire or has expired.

## Licensing for Deep Security from AWS Marketplace

- **Deep Security** Marketplace metered billing allows you to only pay for the actual hours of protection that you use for each instance. The protection costs for each server are calculated based on the usage data that Deep Security sends to AWS Marketplace every hour. These costs are included on your monthly AWS bill.

  The pricing information is as follows:

| Instance Size | Example Instance Types | Cost of Protected Instance Per Hour (USD) |
|---|---|---|
| Medium or smaller | Amazon EC2: C1, M1, M3, T1, T2<br><br>Amazon WorkSpaces | $0.01 |
| Large | Amazon EC2: C3, C4, M1, M3, M4, R3, T2 | $0.03 |
| xLarge and bigger | Amazon EC2: C1, C3, C4, CC2, CG1, CR1, D2, G2, HI1, HS1, I2, M1, M2, M3, M4, R3 | $0.06 |

**Note:** Before you can launch the Marketplace metered billing version of Deep Security, you must configure the IAM role for the instance (see "Configure the IAM role for the Deep Security AMI from AWS Marketplace" on page 127).

- **Deep Security Bring-Your-Own-License (BYOL)** is for customers who have already obtained a license to use Deep Security from another source. This type of licensing works the same way as standard Deep Security licensing, described above.

**Note:** Deep Security from AWS Marketplace does not support the use of vCenter and the Deep Security Virtual Appliance (DSVA).

# Back up and restore your database

If you have a database backup, you can restore your Deep Security deployment if there is a catastrophic failure or if you move Deep Security Manager to another computer.

**Note:** The Deep Security Manager cannot initiate a backup of an Oracle database, a PostgreSQL database, or an Amazon RDS database. To back up your Oracle database, consult your Oracle documentation. To back up your PostgreSQL database, consult your PostgreSQL documentation. For RDS, follow the instructions provided by AWS for backing up your database to an S3 bucket. For example, see Amazon RDS for SQL Server - Support for Native Backup/Restore to Amazon S3.

## Microsoft SQL Server Database

You can back up databases using a scheduled task.

**Note:** Deep Security Manager cannot backup or restore an Oracle database. To backup or restore your Oracle database consult your Oracle documentation.

1. Go to **Administration > Scheduled Tasks**.
2. Click **New.**
3. Select **New Scheduled Task**.
4. Give a name to this task and select **Backup**.
5. To perform a one-time-only backup, select **Once Only** and enter a time (5 minutes from now, for example).
6. Select where to store the backup files.
7. Finish the wizard.
   A complete backup shouldn't take more than a minute or so to complete.

A "date-named" folder will be created in the backup location you specified. To restore this database, shut down the Trend Micro Deep Security Manager service (using the Services Microsoft Management Console), copy the backup folders into the corresponding folders of the install directory and restart Deep Security Manager.

If you are using a SQL Server database, a SQL Server database backup file named **[timestamp].dsmbackup** will be written to the backup folder specified in the scheduled task. For instructions on how to restore a SQL Server database refer to your SQL Server documentation.

## Restore the database only

1. Stop the Deep Security Manager service.
2. Restore the database.
   This must be a database from the same version number of the Deep Security Manager.
3. Start the Deep Security Manager service.
4. Verify contents restored.
5. Update all of the computers to ensure they have the proper configuration.

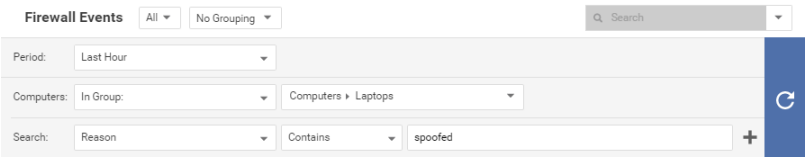
## Restore both the Deep Security Manager and the database

1. Remove any remnants of the lost or corrupted Deep Security Manager and database.
2. Install a fresh Deep Security Manager using a fresh or empty database.

3. Stop the Deep Security Manager service.
4. Restore the database over the freshly installed one, must be the same database name (Must be a database from the same version number of the Manager).
5. Start the Deep Security Manager service.
6. Verify contents restored.
7. Update all of the computers to ensure they have the proper configuration.

# Export objects in XML or CSV format

- **Events:** Go to one of the Events pages and use the Advanced Search options to filter the event data. For example, you could search for all firewall events for computers in the Computers > Laptops computer group that were logged within the last hour whose reason column contains the word spoofed.




  Click the submit button (with the right-facing arrow) to execute the "query". Then click**Export** to export the filtered data in CSV format. You can export all the displayed entries or just selected data. The exporting of logs in this format is primarily for integration with third-party reporting tools.

- **Computer Lists:** Computers lists can be exported in XML or CSV format from the **Computers** page. You might want to do this if you find you are managing too many computers from a single Deep Security Manager and are planning to set up a second Deep Security Manager to manage a collection of computers. Exporting a list of selected computers will save you the trouble of rediscovering all of the computers again and arranging them into groups.

  **Note:** Policy, firewall rule, and intrusion prevention rule settings will *not* be included. You will have to export your firewall rules, intrusion prevention rules, firewall stateful configurations, and policies as well and then reapply them to your computers.

- **Policies:** To export these in XML format, go to **Policies**.

  **Note:** When you export a selected policy to XML, any child policies the policy might have are included in the exported package. The export package contains all of the actual objects associated with the policy except: intrusion prevention rules, log inspection rules, integrity monitoring rules, and application types.

- **Firewall Rules:** Firewall rules can be exported to an XML or CSV file using the same searching and filtering techniques as above.
- **Firewall Stateful Configurations:** Firewall stateful configurations can be exported to an XML or CSV file using the same searching and filtering techniques as above.
- **Intrusion Prevention Rules:** Intrusion prevention rules can be exported to an XML or CSV file using the same searching and filtering techniques as above.
- **Integrity Monitoring Rules:** Integrity monitoring rules can be exported to an XML or CSV file using the same searching and filtering techniques as above.
- **Log Inspection Rules:** Log inspection rules can be exported to an XML or CSV file using the same searching and filtering techniques as above.
- **Other Common Objects :** All the reusable components common objects can be exported to an XML or CSV file the same way.

When exporting to CSV, only displayed column data is included. Use the Columns tool to change which data is displayed. Grouping is ignored so the data might not be in same order as on the screen.

## Import objects

To import each of the individual objects into Deep Security, next to **New** in the object page's toolbar, select **Import From File** .

# Restart the Deep Security Manager

## Linux

To restart the Deep Security Manager, open a CLI and run the following command:

```
sudo systemctl restart dsm_s
```

## Windows

To restart the Deep Security Manager, first log in to the Windows instance on which the Deep Security Manager is running and then follow the steps below for the "Windows desktop" below, the "Command prompt" below or "PowerShell" below:

### Windows desktop

1. Open the Windows Task Manager.
2. Click the **Services** tab.
3. Right click the **Trend Micro Deep Security Manager** service, and then click **Restart**.

### Command prompt

Open the command prompt (`cmd.exe`) and run the following commands:

1. `net stop "Trend Micro Deep Security Manager"`
2. `net start "Trend Micro Deep Security Manager"`

### PowerShell

Open PowerShell and run the following commands:

1. `Stop-Service 'Trend Micro Deep Security Manager'`
2. `Start-Service 'Trend Micro Deep Security Manager'`

# Upgrade Deep Security

## About upgrades

To ensure maximum protection, upgrade your software, security rules and malware patterns when updates are available. Upgrade types include:

- **Software update:** A package of new software such as the Deep Security Manager, Agent and Relay. See "Upgrade the Deep Security Manager AMI" on page 740 and "Update the Deep Security Agent" on page 738.
- **Security update:** An update to the security rules and malware patterns that Deep Security uses to identify potential threats. See "Get and distribute security updates" on page 743.

Relays distribute both software updates and security updates to your agents. Software updates (but not security updates) can alternatively be distributed by a local mirror web server.

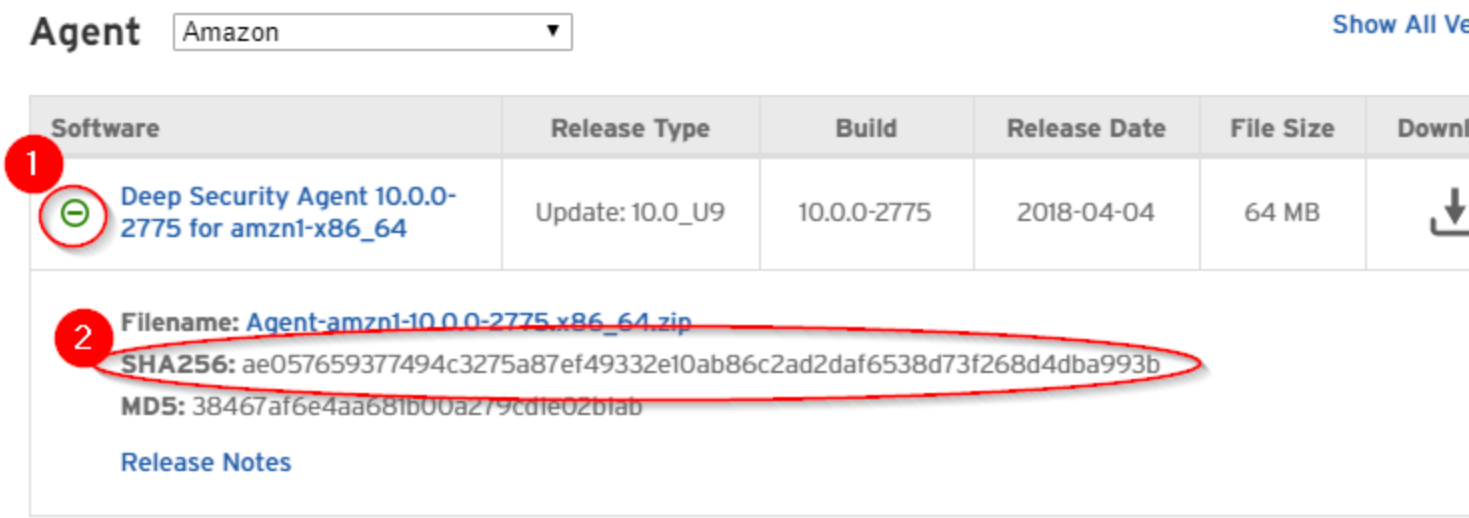
> **Warning:** All Deep Security Relays must be upgraded before upgrading the Deep Security Agent. Failure to do so may cause the relay upgrade to fail.

In this topic:


- "How agents validate the integrity of updates" below
- "How Deep Security Manager checks for software updates" on the next page


## How agents validate the integrity of updates

All security updates are verified for integrity by Deep Security using methods that include digital signatures and checksums (hashes) as well as other, non-disclosed methods. Software updates are digitally signed.



If you want to manually validate signatures or the checksums available on the Download Center, you can also use a tool such as:

- sha256sum (Linux)
- Checksum Calculator (Windows)
- jarsigner (Java Development Kit (JDK))

For example, you could enter this command to verify a download's signature:
`jarsigner -verify <filename>.zip`

## How Deep Security Manager checks for software updates

Deep Security Manager periodically connects to Trend Micro update servers to check for updates to software that you have imported into the Deep Security Manager database, such as:

- Deep Security Agent
- Deep Security Manager

The check is made against the local inventory, not against what is available on the Download Center. (There is a separate alert for new software on the Download Center.)

**Note:** Deep Security will only inform you of **minor** version updates-not major-of software. For example, if you have agent version **9.6.100**, and Trend Micro releases agent version **9.6.200**, an alert will tell you that software updates are available. However, if Trend Micro then releases agent version **10.0.xxx** (a major version difference) and you don't have any **10.0** agents in the database, no alert will appear (even though **10.0**is newer than **9.6.100**).

An alert on the manager will notify you that software updates are available. The "Trend Micro Download Center" section on **Administration > Updates > Software** also indicates whether there are updates available. Once you import (download) software into the Deep Security Manager database, you can upgrade the software in your deployment. See "Update the Deep Security Agent" on the next page.

**Tip:** To see *all* software packages that are available for download (even if you haven't imported it before), go to **Administration > Updates > Software > Download Center**.

To determine when the last check was performed, whether it was successful, or to manually initiate a check for updates, go to **Administration > Updates > Software** and view the "Deep Security" section. If you have configured a scheduled task to check for updates, the date and time of the next scheduled check is also listed here. See "Schedule Deep Security to perform tasks" on page 263.

When imported, software is stored in the Deep Security Manager database. Imported software is periodically replicated to relay-enabled agents.

## Update the Deep Security Agent

Software updates can be initiated via the Deep Security Manager, manually, or a third-party deployment system.

**Warning:** All Deep Security Relays must be upgraded before upgrading the Deep Security Agent. Failure to do so may cause the relay upgrade to fail.

In this topic:


- "Update available notifications" below
- "Initiate an agent update" on the next page
- "Manually upgrade the agent" on the next page


### Update available notifications

When a new agent software version is available, a message appears on **Alerts**.

1. In the alert, click **Show Details** and then click **View all out-of-date computers**.
   **Computers** opens with all computers showing a **Software Update Status** of **Out-of-Date**.
2. Continue with "Initiate an agent update" on the next page or "Manually upgrade the agent" on the next page.

## Initiate an agent update

**Tip:** Upgrade when the server is less busy.

On **Administration > Updates > Software**, the "Computers" section indicates whether any computers are running agents for which updates are available. The check is only performed against software that has been imported into Deep Security, not against software available from the Download Center. If any computers are out of date, either:

- To upgrade all out-of-date computers, click **Upgrade Agent / Appliance Software**.
- To upgrade a specific agent computer, go to **Computers** , select the computers that you want to upgrade, and click **Actions > Upgrade Agent Software**. You will be prompted to select the **Agent Version**. We recommend that you select the default **Use the latest version for platform (X.Y.Z.NNNN)**. Depending on your preference, select to **Upgrade Now** or **Use a Schedule for Upgrade** and specify the time window when the upgrade will be performed. If you choose to use a schedule, the manager will upgrade the agent to the specified version once; it does not continue to upgrade the agent to future versions.

**Note:** If you are using anti-malware on a Windows platform, the computer might require a reboot to complete the upgrade. If this is the case, a Reboot Required alert will be triggered, which you must dismiss manually after completing the reboot. You can also check the Agent Software Upgraded event or Virtual Appliance Upgraded event to see if a reboot is necessary. If you are using anti-malware, plan your upgrades during maintenance windows when reboots are possible.

## Manually upgrade the agent

Sometimes you may not be able to update the agent software from the Deep Security Manager because of connectivity restrictions, or you may prefer to deploy updates using a third-party system. If so, you can update the agent software using an installer that you have copied to the computer.

Download the new agent software either from the Download Center, or by exporting it from the Deep Security Manager (see "Get Deep Security Agent software" on page 177). Then run the installer. Method varies by operating system.

### Windows

1. Disable agent self-protection. To do this, on the Deep Security Manager, go to **Computer editor**[1] **> Settings > General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override.
2. Copy the agent installer to the computer.
3. Run the agent installer. It will detect the previous agent and perform the upgrade.

### Linux

1. Copy the agent installer to the computer.
2. Run the following command:
```
rpm -U <new agent installer rpm>
```

(The "-U" argument instructs the installer to perform an upgrade.)

## Upgrade the Deep Security Manager AMI

Before upgrading, verify that:

- Deep Security stores its data in an external database (embedded databases cannot be upgraded).
- You have a recent backup of the database (see Backing Up and Restoring Amazon RDS DB Instances). In the event of a catastrophic failure during the upgrade, there may be no way to recover without a backup.
- Deep Security Manager instances are behind an Elastic Load Balancer (ELB) or are using elastic IPs.

There are two options for upgrading your Deep Security Manager AMI:


- "Upgrade Deep Security Manager AMI 11.0 or later" on the next page
- "Manually upgrade your Deep Security Manager AMI" on the next page


[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

## Upgrade Deep Security Manager AMI 11.0 or later

If you are using Deep Security Manager AMI version 11.0 or later and see **A new version of Deep Security is available** in a banner at the top of the Deep Security Manager console, click **Upgrade Deep Security** in the banner to begin the upgrade process. A confirmation message appears, providing information about the upgrade. Click **Upgrade** to confirm that you want to continue.

The upgrade time depends on the number of Deep Security nodes you are running. It will take approximately 5 minutes per node. If there is a problem with the upgrade, an error message will appear. If the upgrade is successful, you will be redirected to the login page and the upgrade banner will no longer appear.

## Manually upgrade your Deep Security Manager AMI

1. Stop all Deep Security Manager instances: right-click the instance on the AWS console and select **Instance State > Stop**.
2. Deploy a new instance of Deep Security Manager using the latest version from the AWS Marketplace.
3. When the instance is running, go to **https://ip:8080**, enter the Instance ID, and click **Sign In**.
4. On the License Agreement tab, read and accept the terms of the license agreement and click **Next**.
5. On the Database tab, enter the configuration parameters of your existing Deep Security database and click **Next**.
6. On the Previous Version Check tab, click **Upgrade** and click **Next**.
7. On the Address and Ports tab, enter the hostname or IP address of the computer where Deep Security Manager is being installed and click **Next**.

   The Manager Address must be either a resolvable hostname, a fully qualified domain name, or an IP address. If DNS is not available in your environment or if some computers are unable to use DNS, a fixed IP address should be used instead of a hostname. You can also change the default port numbers.

8. On the Credentials tab, click **Next**.

The existing credentials will stay the same.

9. On the Review Settings tab, review the installation settings to ensure that they are correct and then click **Install**.

   The Deep Security Status page will show that the Deep Security Manager is being installed.

10. If you are using an ELB, add the new Deep Security Manager instance to the ELB list. Also add any relays to the list.
11. Log in to Deep Security Manager and delete the computer records for any old Deep Security Manager installations by clicking the **Computers** tab, selecting the record, and clicking **Delete** on the toolbar.
12. Delete old manager nodes by going to the **Administration** tab in Deep Security Manager, selecting **Manager Nodes** in the left-hand navigation menu, opening the **Properties** dialog for each old manager node (Status: "Offline (Upgrade Required)"), and clicking **Decommission**.
13. Double click on the newly added Deep Security Manager Computer Object and ensure it is Activated and has the correct policy assigned.
14. Delete your old Deep Security Manager instances by right-clicking on the instance from the AWS console and choosing **Instance State > Terminate**.

Please contact aws.marketplace@trendmicro.com if you have any questions or encounter any issues.

## Error: The installer could not establish a secure connection to the database server

When installing or upgrading Deep Security Manager, the following error message can occur if you are using Microsoft SQL Server as your Deep Security database:

*The installer could not establish a secure connection to the database server. Please upgrade or configure your database server to support TLS 1.2 encryption*.

The error message appears if the `java.security` file on the Deep Security Manager includes `TLSv1` and `TLSv1.1` in the `jdk.tls.disabledAlgorithms=` setting, which disables early TLS and only allows TLS 1.2. (The `java.security` file is set this way if you are doing a fresh install of

Deep Security Manager 11.1, where only TLS 1.2 is allowed, or if you are upgrading and previously enforced TLS 1.2.) During the upgrade or installation, the database drivers on the manager try to communicate with the SQL Server using TLS 1.2, and if your SQL Server version does not support TLS 1.2, you'll see this error.

To solve the problem, you must upgrade your SQL Server database to a version that supports TLS 1.2 and then retry the Deep Security Manager installation or upgrade. For a list of SQL Server versions that support TLS 1.2, see this Microsoft article.

## Get and distribute security updates

You must keep your Deep Security deployment up to date with the security updates that Deep Security uses to identify potential threats.

There are two types of security updates:

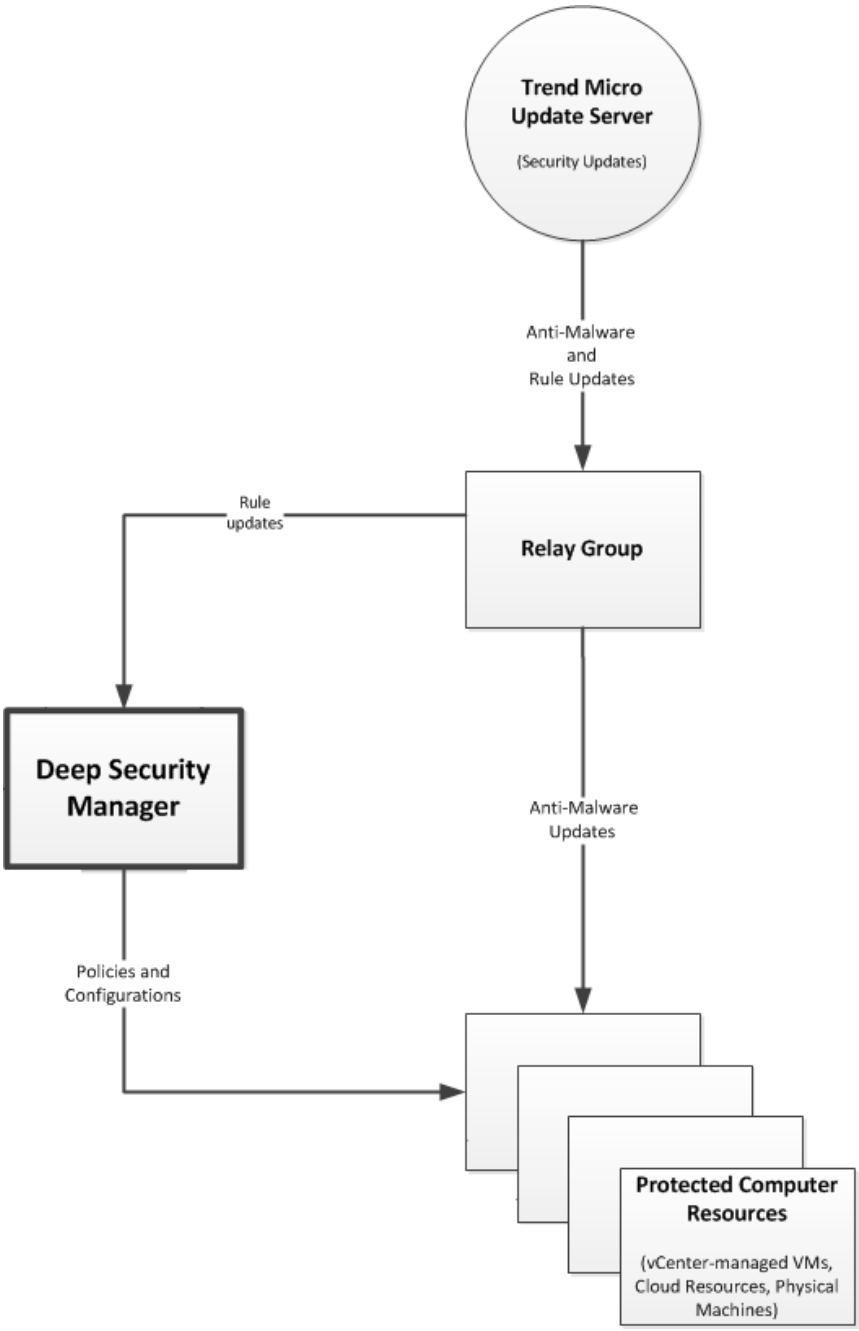
- **Pattern Updates** are used by the anti-malware module.
- **Rule Updates** are used by these modules:
  - Firewall
  - Intrusion Prevention
  - Integrity Monitoring
  - Log Inspection Security

Trend Micro releases new rule updates every Tuesday, with additional updates as new threats are discovered. You can get information about the latest updates from the Trend Micro Threat Encyclopedia.

To configure security updates, you will need to:

1. "Configure a security update source and settings" on page 745
2. Organize your relay-enabled agents into relay groups, assign relay groups to your agents and appliances, and configure relay settings for security and software updates. (See "Distribute security and software updates with relays" on page 234.)
3. "Perform security updates" on page 746
4. "Special case: configure updates on a relay-enabled agent in an air-gapped environment" on page 746

At any time, you can "Check your security update status" on page 747




**Note:** Alerts are raised if a rule update has been downloaded from Trend Micro and available for more than thirty minutes but computers have yet to be updated.

**Note:** Alerts are raised if a pattern update has been downloaded from Trend Micro and available for more than an hour but computers have yet to be updated.

## Configure a security update source and settings

1. Go to **Administration > System Settings > Updates**.
2. Set your **Primary Security Update Source**. By default this will be the **Trend Micro Update Server** accessed over the internet. Unless your support provider has told you to do otherwise, leave the setting as is. If you were given an alternative source for updates, enter the URL, including "http://" or "https://" in the **Other update source** box.
3. Normally, agents connect to a relay-enabled agent to get security updates. But if you have agents installed on roaming computers that are not always in contact with a Deep Security Manager or relay, you can select **Allow Agents/Appliances to download Pattern updates directly from Primary Security Update Source if Relays are not accessible** to allow agents to use the update source specified in the previous step when their relay group is not available.
4. Normally, the Deep Security Manager instructs agents or appliances to download pattern updates. When **Allow Agents/Appliances to download Pattern updates when Deep Security Manager is not accessible** is selected, even though an agent cannot communicate with the Deep Security Manager, it will continue to download updates from its configured source.

   **Tip:** You may want to deselect this option on computers where you do not want to risk a potentially problematic security update when the computer is not in contact with a manager and therefore possibly far away from any support services.

5. Trend Micro will occasionally issue an update to an existing Deep Security rule. The **Automatically apply Rule Updates to Policies** setting determines whether updated rules will automatically be applied to Deep Security policies. If this option is not selected, you will have to manually apply downloaded rule updates to policies from the **Administration > Updates > Security** page by clicking on the **Apply Rules to Policies** button.

   **Tip:** Updates to existing rules are either improvements to the efficiency of the rule or bug fixes. So although it's a good a idea to test new rules (either in detect-only mode or in a

test environment) before deploying them to a production environment, automatically applying updates to existing rules is usually a safe option.

**Note:** By default, changes to policies are automatically applied to computers. You can change this behavior by opening a **Computer or Policy editor**[1] > **Settings** > **General** window and changing the **Automatically send Policy changes to computers** setting in the **Send Policy Changes Immediately** area.

6. You can configure amount of time that can pass between an instruction to perform a security update being sent and the instruction being carried out before an alert is raised. Click **Administration** > **System Settings** > **Alerts** and change the value for **Length of time an Update can be pending before raising an Alert**.

## Perform security updates

The recommended way to check for security updates is to set up a "Check for Security Updates" scheduled task that performs a check on a regular basis. For details, see "Schedule Deep Security to perform tasks" on page 263

You can also manually initiate security updates:

- To perform security updates on specific agents, go to **Computers**, select the agent, then right-click and select **Actions** > **Download Security Update**.

## Special case: configure updates on a relay-enabled agent in an air-gapped environment

In a typical environment, at least one relay-enabled agent is configured and able to download updates from the Trend Micro Update Server and the rest of the agents and appliances connect to that relay-enabled agent for update distribution. However, if your relay-enabled agent cannot to connect to the Update Server over the Internet, you'll need to set up a relay in your

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

demilitarized zone (DMZ) that can obtain the security updates, which you can then copy to your air-gapped relays. For details, see "Configure agents that have no Internet access" on page 207.

## Check your security update status

The Security Updates Overview page (**Administration > Updates > Security**) displays the state of your security updates:

- **Trend Micro Update Server:** Indicates whether relays can connect to the Trend Micro Update Server to check for the latest security updates.
- **Deep Security:** Indicates when the last successful check and download were performed, and when the next schedule check will be performed.

  Tip: **All Relays are in sync** indicates that all relays are distributing the latest successfully downloaded pattern updates. Relays that are out of sync are usually in that state because they cannot communicate with Trend Update Servers. This could be because they are intentionally "air-gapped" and need to be manually updated or because of network connectivity problems. If any relays are out of sync, a link to those relays will be provided.

- **Computers:** Indicates whether any computers are out of date *with respect to the Pattern Updates being stored in the Relays*. You can click **Send Patterns to Computers** to instruct all computers to retrieve the latest pattern updates from their assigned relays.

### See details about pattern updates

The **Administration > Updates > Security > Patterns** page displays a list of the components that make up a pattern update. This page is displayed only when Deep Security has an active relay.

- **Component:** The type of update component.
- **Product Name:** The Deep Security product this component is intended for.
- **Platform:** The operating system for which the update is intended.
- **Current Version:** The version of the component within the Update currently downloaded from Trend Micro to Deep Security and being distributed by the relays and the Deep Security Manager.

- **Last Updated:** When the currently downloaded security update was retrieved from Trend Micro.

**Tip:** You can find the version numbers of the security update components in effect on a specific computer on **Computer Editor > Updates**.

## See details about rule updates

The **Administration > Updates > Security > Rules** page displays a list of the most recent Intrusion Prevention, Integrity Monitoring, and Log Inspection Rules that have been downloaded to the Deep Security Manager database.

From this page, you can:

- **View details about a rule update:** Select a rule update and click **View** to see details, including a list of the specific rules included in the update.
- **Roll back a rule update:** If a recent rule update has caused problems in your environment, you may want to roll back to a previous rule update. If you roll back to a previous update, all policies affected by the rollback will be immediately updated on *all computers using those policies*. Select the rule update that you want to roll back to and click **Rollback**. Deep Security Manager generates a summary of changes that will take place so that you can confirm the changes before finalizing the rollback.
- **Reapply the current rule set:** ✔ indicates that a rule update has been applied. To reapply that rule update to computers being protected by Deep Security, right-click the rule update and click **Reapply**.
- **Import a rule update:** Rule updates are automatically imported into Deep Security during the "Check for Security Updates" scheduled task, or when you click **Check for Updates and Download** on the **Administration > Updates > Security** page. The only time you might have to manually import a rule update is if your installation has no connectivity to the Trend Micro Update Servers or if you are asked to do so by your support provider.
- **Export a rule update:** Under normal circumstances you should not have to export a rule update unless asked to do so by your support provider.
- **Delete a rule update:** Click **Delete** to remove the selected rule update from the Deep Security Manager database.

**Tip:** You can configure the number of rule updates that are kept in the Deep Security Manager database by going to the **Administration > System Settings > Storage** tab.

**Tip:** If the relay functionality is enabled for a computer, the **Computer editor > Security Updates** page displays the components that the relay is currently distributing to the agents and appliances that rely on it for security updates. If the anti-malware module is enabled for a computer, the security updates page also displays the set of patterns that are in effect locally on this computer. From this page, you can also download or roll back security updates.

## Use a web server to distribute software updates

Deep Security software updates are normally hosted and distributed by relays. However, if you already have a web server, you can provide software updates via the web server instead of a relay. To do this, you must mirror the software repository of the relay on your web server.

**Note:** Although Deep Security Agents can download their *software* updates from the web server, at least one relay is still required to distribute *security* package updates such as anti-malware and IPS signatures (see "Get and distribute security updates" on page 743).

**Note:** Even though you are using your own web servers to distribute software, you must still go to **Administration > Updates > Software** and import software into the Deep Security Manager's database. Then you must ensure that your software web server contains the same software that has been imported into Deep Security Manager. Otherwise the alerts and other indicators that tell you about available updates will not function properly.

### Web server requirements

**Disk Space:** 20 GB

**Ports:** Web server and relay port numbers

### Copy the folder structure

Mirror the folder structure of the software repository folder on a relay-enabled agent. Methods vary by platform and network. For example, you could use `rsync` over SSH for a Linux computer

and network that allows SSH.

On Windows, the default location for the relay-enabled agent's software repository folder is:

```
C:\ProgramData\Trend Micro\Deep Security Agent\relay\www\dsa\
```

On Linux, the default location for the Relay's software repository folder is:

```
/var/opt/ds_agent/relay/www/dsa/
```

The structure of the folder is like this:

```
|-- dsa
|    |-- <Platform>.<Architecture>
|         |--  <Filename>
|         |--  <Filename>
|         |--  ...
|
|    |-- <Platform>.<Architecture>
|         |--  <Filename>
|         |--  <Filename>
|         |--  ...
```

For example:

```
|-- dsa
|    |--  CentOS_6.x86_64
|         |--   Feature-AM-CentOS_6-9.5.1-1097.x86_64.dsp
|         |--   Feature-DPI-CentOS_6-9.5.1-1097.x86_64.dsp
|         |--   Feature-FW-CentOS_6-9.5.1-1097.x86_64.dsp
|         |--   Feature-IM-CentOS_6-9.5.1-1097.x86_64.dsp
|         |--  ...
|
|    |--  RedHat_EL6.x86_64
|         |--   Agent-Core-RedHat_EL6-9.5.1-1306.x86_64.rpm
|         |--   Feature-AM-RedHat_EL6-9.5.1-1306.x86_64.dsp
|         |--   Feature-DPI-RedHat_EL6-9.5.1-1306.x86_64.dsp
|         |--   Feature-FW-RedHat_EL6-9.5.1-1306.x86_64.dsp
```

```
|         |--  ...
|         |--   Plugin-Filter_2_6_32_131_0_15_el6_x86_64-RedHat_
EL6-9.5.1-1306.x86_64.dsp
|         |--   Plugin-Filter_2_6_32_131_12_1_el6_x86_64-RedHat_
EL6-9.5.1-1306.x86_64.dsp
|         |--  ...
|
|    |-- Windows.x86_64
|         |--  Agent-Core-Windows-9.5.1-1532.x86_64.msi
|         |--  Agent-Core-Windows-9.5.1-1534.x86_64.msi
|         |--  Feature-AM-Windows-9.5.1-1532.x86_64.dsp
|         |--  Feature-AM-Windows-9.5.1-1534.x86_64.dsp
|         |--  Feature-DPI-Windows-9.5.1-1532.x86_64.dsp
|         |--  Feature-DPI-Windows-9.5.1-1534.x86_64.dsp
|         |--  ...
|         |--  Plugin-Filter-Windows-9.5.1-1532.x86_64.dsp
|         |--  Plugin-Filter-Windows-9.5.1-1534.x86_64.dsp
|         |--  ...
```

The example above shows only a few files and folders. Inside a complete `dsa` folder, there are more. If you need to save disk space or bandwidth, you don't need to mirror all of them. You're only required to mirror the files that apply to your computers' platforms.

## Configure agents to use the new software repository

When the mirror on the web server is complete, configure Deep Security Agents to get their software updates from your web server.

1. On Deep Security Manager, go to **Administration > System Settings > Updates**.
2. In the Software Updates section, enter the URL(s) of the mirror folder(s) on your web server (s).
3. Click **Save**.

**Note:** Verify that connectivity between agents and your web server is reliable. If the connection is blocked, agents will instead use the relay.

## Disable emails for New Pattern Update alerts

The "New Pattern Update is Downloaded and Available" alert is raised when a security update has not been applied to an agent one hour after Deep Security Manager has downloaded it. The one-hour time span is not configurable. The alert is sent via email when the alert is raised by default.

If you are receiving too many of these email alerts because one hour is not long enough to disperse the updates, you can disable email notifications for this alert. Instead, you can receive email messages for the "Computer Not Receiving Updates" alert for which you can configure the time that passes before the alert is raised.

1. To ensure that Deep Security Manager is configured to automatically download security updates, in Deep Security Manager, click **Administration > Scheduled Tasks**.
2. If there is no scheduled task of type Check for Security Updates, create one (see "Schedule Deep Security to perform tasks" on page 263).
3. Click **Administration > System Settings > Updates**. In the Rules section under Security Updates, make sure **Automatically apply Rule Updates to Policies** is selected.
   For Deep Security as a Service, rule updates are automatically applied by default.
4. Click **Alerts > Configure Alerts**.
5. In the Alert Configuration window, click the **New Pattern Update is Downloadable and Available** alert and then click **Properties**.
6. On the Alert Information window, deselect **Send Email to notify when this alert is raised** and then click **OK**.
7. Click the **Computer Not Receiving Updates** alert and then click **Properties**.
8. Make sure **Send Email to notify when this alert is raised** is selected, and click **OK**.
   The alert is raised when an update is pending for 7 days.
9. To raise the alert after a different amount of time has passed since the update was pending, click **Administration > System Settings > Alerts**.
10. In the alerts area, use the drop-down to select the period of time, and then click **Save**.

# Harden Deep Security

Deep Security as a Service and the Deep Security AMI from AWS Marketplace AMIs all run on Amazon Linux. The Deep Security team has hardened those products based on the Center for

Internet Security (CIS) standard for Amazon Linux.

Hardening involves making changes to secure the system and make it less vulnerable to attack. For Deep Security, the changes included updating the web installer so that it terminates after the Deep Security Manager is online, removing unnecessary software, and configuring system settings to use the principal of least privilege, wherever it is applicable.

Deep Security AMI from AWS Marketplace is also protected by a Deep Security Agent installed on the same host as the Deep Security Manager. The Agent has a default " Deep Security Manager" policy applied to it, which provides basic intrusion prevention rules and firewall rules that filter traffic to the Manager.

There are several measures you can take to increase the security of your Deep Security deployment.


- "Protect Deep Security Manager with an agent" below
- "Replace the Deep Security Manager SSL certificate" on page 756
- "Encrypt communication between the Deep Security Manager and the database" on page 763
- "Change the Deep Security Manager database password" on page 770
- "Enable Content Security Policy and HTTP Public Key Pinning" on page 772
- "Enforce user password rules" on page 773


## Protect Deep Security Manager with an agent

To protect the Deep Security Manager, install an Agent on its host computer and apply the Deep Security Manager policy.

1. Install an Agent on the same computer as the Manager.
2. On the **Computers** page, add the Manager's computer. Do not choose to apply a Policy at this time.
3. Double-click the new computer in the **Computers** page to display its **Details** window and go to **Intrusion Prevention > Advanced > SSL Configurations**.
4. A listing of the SSL Configurations for this computer will be displayed. Click **New** to start the wizard to create a new SSL Configuration.

5. Specify the interface used by the Manager. Click **Next**.
6. On the **Port** page, select whether to protect the Deep Security Manager GUI's port number. Click **Next**.
7. Specify whether SSL Intrusion Prevention analysis should take place on all IP addresses for this computer, or just one. (This feature can be used to set up multiple virtual computers on a single computer.)
8. Next, choose to "Use the SSL Credentials built into the Deep Security Manager". (This option only appears when creating an SSL Configuration for the Manager's computer.) Click **Next**.
9. Finish the wizard and close the **SSL Configuration** page.
10. Return to the computer's **Details** window. Apply the **Deep Security Manager Policy**, which includes the Firewall Rules and Intrusion Prevention Rules required to protect the Deep Security Manager's GUI port number.

You have now protected the Manager's computer and are now filtering the traffic (including SSL) to the Manager.

**Note:** After configuring the Agent to filter SSL traffic, you may notice that the Deep Security Agent will return several **Renewal Error** events. These are certificate renewal errors caused by the new SSL certificate issued by the Manager computer. To fix this, refresh the web page and reconnect to the Deep Security Manager's GUI.

The **Deep Security Manager** Policy has the basic Firewall Rules assigned to enable remote use of the Manager. Additional Firewall Rules may need to be assigned if the Manager's computer is being used for other purposes. The Policy also includes the Intrusion Prevention Rules in the **Web Server Common** Application Type. Additional Intrusion Prevention Rules can be assigned as desired.

Because the **Web Server Common** Application Type typically filters on the **HTTP** Port List and does not include the Deep Security Manager GUI's port number, it is added as an override to the ports setting in the **Intrusion Prevention Rules** page of the Policy's **Details** window.

For more information on SSL data inspection, see "Inspect SSL or TLS traffic" on page 573.

# Protect Deep Security Agent

If you have enabled manager-initiated communication (see "Agent-manager communication" on page 196for details), and by extension, manager-initiated activation, it is highly recommended that you bind the agent to a specific manager during this activation. For details, see the section below.

## Bind Deep Security Agent to a specific Deep Security Manager

If manager-initiated activation is enabled between Deep Security Agent and Deep Security Manager, Trend Micro strongly recommends that you protect the agent by allowing it to only be contacted by a known and specific manager during the activation. This configuration should be used if you are in an environment that might include malicious Deep Security Managers.

To bind the agent to a manager, you'll need to export the SSL certificate that is used for securing agent-manager communication, and then add it to the agent computer. Follow these instructions:

1. On the Deep Security Manager, export the Deep Security Manager SSL certificate by running this command:

```
dsm_c -action exportdsmcert -output ds_agent_dsm.crt [-tenantname TENANTNAME | -tenantid TENANTID]
```

where:

- `ds_agent_dsm.crt` must be specified exactly as shown (you cannot use another name). It is the name of the Deep Security Manager SSL certificate that is used to secure the communication between the agent and manager.
- `-tenantname` *`TENANTNAME`* is only required if you have a multi-tenant environment. *`TENANTNAME`* is replaced with the name of a tenant where agents are deployed.
- `-tenantid` *`TENANTID`* is an alternative to `-tentantname TENANTNAME`. *`TENANTID`* is replaced with the ID of a tenant where agents are deployed.
- To specify multiple tenants, see the last step of this procedure.
- For details on multi-tenancy, see "Set up a multi-tenant environment" on page 140.

2. On the computer that hosts the agent that you plan to activate, place the `ds_agent_dsm.crt` file in one of these locations:

- Windows: `%ProgramData%\Trend Micro\Deep Security Agent\dsa_core`
- Linux: `/var/opt/ds_agent/dsa_core`

3. If you have multiple tenants, run the command above for each tenant and then copy the certificate to each tenant's agents.
   Example:
   If you have two tenants, run:
   ```
   dsm_c -action exportdsmcert -output ds_agent_dsm.crt -tenantname TENANT1
   dsm_c -action exportdsmcert -output ds_agent_dsm.crt -tenantname TENANT2
   ```
   ...then copy:
   the first `ds_agent_dsm.crt` to agents controlled by TENANT1.
   the second `ds_agent_dsm.crt` to agents controlled by TENANT2.

You have now added the Deep Security Manager certificate to the agent. The agent now only accepts activations from the Deep Security Manager that owns the certificate. If you have tenants, the agent can only be activated by the tenant that was specified in the export command.

**Note:** After completing these steps, the agent enters a 'pre-activated' state. While in this state, operations initiated by other Deep Security Managers or by the agent's local `dsa_control` utility do not work properly, by design. After the agent is fully activated, all normal operation resumes.

**Note:** After resetting or deactivating an agent, the Deep Security Manager certificate is cleared, so the above steps must be re-applied.

## Replace the Deep Security Manager SSL certificate

Deep Security Manager creates a 10-year self-signed certificate for the connections between the Deep Security Manager console and users' web browsers. However, for added security, you can replace it with certificates from a trusted certificate authority (CA). (Such certificates are maintained after a Deep Security Manager upgrade.)

You will be working with the following two Deep Security Manager keystore files

- `<DSM_installation_folder>/jre/lib/security/cacerts`

  The `cacerts` file contains the Deep Security Manager trusted public keys for the CA server, intermediate CA server and the Deep Security application server.

- `<DSM_installation_folder>/.keystore`

  The `.keystore` file contains the certificate and private key for the Deep Security application server. To use your own certificate(s), you will need to import them to the `.keystore` file.

To replace the SSL certificate in a **Windows** environment you will need to:

1. "Create a new .keystore file and add your certificates to the cacerts file" on the next page
2. "Create a PKCS12 keychain file and import it into the new .keystore file" on page 759
3. "Configure Deep Security Manager to use the new .keystore file" on page 760

To replace the SSL certificate in a **Linux** environment you will need to:

1. "Create a new .keystore file and add your certificates to the cacerts file" on page 761
2. "Create a PKCS12 keychain file and import it into the new .keystore file" on page 762
3. "Configure the Deep Security Manager to use the new .keystore file" on page 763

**Note:** If you have enabled FIPS mode (see "FIPS 140-2 support" on page 1049), you will need to disable FIPS mode before replacing the certificate and then re-enable FIPS mode when you're finished.

## See your trusted certificates

Click **Administration > System Settings > Security > View Certificate List** to view a list of all security certificates accepted by Deep Security Manager.

# Replace the SSL certificate in a Windows environment

## Create a new .keystore file and add your certificates to the cacerts file

1. Create backups of the following files:
   - `<DSM_installation_folder>/jre/lib/security/cacerts`
   - `<DSM_installation_folder>/.keystore`
   - `<DSM_installation_folder>/configuration.properties`
2. Create a new `.keystore` file:

   ```
   "%ProgramFiles%\Trend Micro\Deep Security Manager\jre\bin\keytool.exe" -genkey -alias tomcat -keyalg RSA -dname cn=<Deep Security Manager server host name or FQDN> -storepass <keystore password>
   ```

3. Generate a certificate signing request file from the new `.keystore` file with the following commands:

   ```
   cd "%ProgramFiles%\Trend Micro\Deep Security Manager\jre\bin\"
   ```

   ```
   keytool.exe -certreq -keyalg RSA -alias tomcat -keystore %userprofile%\.keystore -storepass <keystore password> -file certrequest.csr
   ```

4. Send the `certrequest.csr` file to your CA for signing. Your CA will provide you with the following certificates:

   Root CA certificate: `rootCA.cer`

   Intermediate CA certificate: `intermediateCA.cer`

   Application server certificate: `dsm.cer`

5. Move the certificates and the new `.keystore` file into the `%userprofile%\certs\` directory.
6. Import the certificates into the `cacerts` file with the following commands:

   **Note:** The `cacerts` file requires a unique alias for each certificate. If you have multiple intermediate CA certificates, each one should have a unique alias (for example,

`intermd1`, `intermd2`, `intermd3`). You must import the certificates in the same order as that determined by your CA.

```
cd "%ProgramFiles%\Trend Micro\Deep Security Manager\jre\bin\"
```

```
keytool.exe -import -alias root -trustcacerts -file
%userprofile%\certs\rootCA.cer -keystore "%ProgramFiles%\Trend Micro\Deep
Security Manager\jre\lib\security\cacerts" -storepass changeit
```

```
keytool.exe -import -alias intermd1 -trustcacerts -file
%userprofile%\certs\intermediateCA.cer -keystore "%ProgramFiles%\Trend
Micro\Deep Security Manager\jre\lib\security\cacerts" -storepass changeit
```

```
keytool.exe -import -alias tomcat -trustcacerts -file
%userprofile%\certs\dsm.cer -keystore "%ProgramFiles%\Trend Micro\Deep
Security Manager\jre\lib\security\cacerts" -storepass changeit
```

## Create a PKCS12 keychain file and import it into the new .keystore file

To maintain the relationship between the certificates, you must create a PKCS12 keychain file and import the root CA, the intermediate CA and the application server certificates into it using openssl.

1. Generate the private key from the new `.keystore` file with the following commands:

```
cd %ProgramFiles%\Trend Micro\Deep Security Manager\jre\bin\
```

```
keytool.exe -importkeystore -srckeystore %userprofile%\certs\.keystore -
srcstorepass <keystore password> -deststoretype PKCS12 -destkeystore
%userprofile%\certs\keystore.p12 -storepass <p12 keystore password>
```

```
cd %ProgramFiles(x86)%\GnuWin32\bin\
```

```
openssl pkcs12 -in %userprofile%\certs\keystore.p12 -passin pass:<above p12
keystore password you specified> -nocerts -out %userprofile%\certs\private.pem
-passout pass:<private pem password>
```

```
openssl rsa -in %userprofile%\certs\private.pem -passin pass:<above private
pem password> -out %userprofile%\certs\private.key
```

2. Create a certificate for the keychain file from the root and intermediate CA certificates:

> **Note:** Combine the certificates in the order provided by your CA.

```
copy %userprofile%\certs\intermediateCA.cer+%userprofile%\certs\rootCA.cer
%userprofile%\certs\CAcertchain.cer
```

3. Create the PKCS12 keychain:

> **Note:** You will need to create the PKCS12 keychain in a Linux environment. At the time of this article's publication, there is an openssl bug in Windows that will cause openssl to crash if you use the `-name` option. As Java requires each key have an alias, you will not be able to import the PKCS12 keychain into the new `.keystore` file without using this option. Create the PKCS12 keychain In a Linux environment with the below command.

```
openssl pkcs12 -export -in ~/certs/dsm.cer -inkey ~/certs/private.key -
certfile ~/certs/CAcertchain.cer -out dsm.p12 -name tomcat -passout
pass:<keychain password>
```

4. Import the PKCS12 keychain into the new `.keystore` file:

```
cd %ProgramFiles%\Trend Micro\Deep Security Manager\jre\bin\
```

```
keytool.exe -importkeystore -srckeystore %userprofile%\certs\dsm.p12 -
srcstoretype pkcs12 -srcalias tomcat -srcstorepass <keychain password> -
destkeystore %userprofile%\certs\.keystore -storepass <keystore password> -
destalias tomcat
```

## Configure Deep Security Manager to use the new .keystore file

1. Overwrite the `.keystore` file in the Deep Security Manager installation directory with the new `.keystore` file:

> **Note:** Only the default `.keystore` file is kept when you upgrade Deep Security Manager. We recommend that you replace the existing `.keystore` file.

2. Open the `configuration.properties` file, find the `keystorekeystorePass=` parameter, and replace the value with the one you specified for the `<keystore password>` in step 2 of the "Create a new .keystore file and add your certificates to the cacerts file" on page 758 procedure.

3. Restart the Deep Security Manager service.
4. Open the Deep Security Manager console with `https://< Deep Security Manager server host name or FQDN>:4119` and make sure there is no certificate error message. The `<Deep`

`Security Manager server host name or FQDN>` should be the one used in step 2 of the "Create a new .keystore file and add your certificates to the cacerts file" on page 758 procedure.

## Replace the SSL certificate in a Linux environment

### Create a new .keystore file and add your certificates to the cacerts file

1. Create backups of the following files:

   `<DSM_installation_folder>/jre/lib/security/cacerts`

   `<DSM_installation_folder>/.keystore`

   `<DSM_installation_folder>/configuration.properties`

2. Create a new `.keystore` file:

   ```
   /opt/dsm/jre/bin/keytool -genkey -alias tomcat -keyalg RSA -dname cn=<Deep
   Security Manager server host name or FQDN> -storepass <keystore password>
   ```

3. Generate a certificate signing request file from the new `.keystore` file:

   ```
   /opt/dsm/jre/bin/keytool -certreq -keyalg RSA -alias tomcat -keystore
   ~/.keystore -storepass <keystore password> -file certrequest.csr
   ```

4. Send the `certrequest.csr` file to your CA for signing. Your CA will provide you with the following certificates:

   Root CA certificate: `rootCA.cer`

   Intermediate CA certificate: `intermediateCA.cer`

   Application server certificate: `dsm.cer`

5. Move the certificates and the new `.keystore` file into the `~/certs` directory.

6. Import the certificates into the `cacerts` file with the following commands:

   **Note:** The `cacerts` file requires a unique alias for each certificate. If you have multiple intermediate CA certificates, each one should have a unique alias (for example,

`intermd1`, `intermd2`, `intermd3`). You must import the certificates in the same order as that determined by your CA.

```
keytool -import -alias root -trustcacerts -file ~/certs/rootCA.cer -keystore
/opt/dsm/jre/lib/security/cacerts -storepass changeit
```

```
keytool -import -alias intermd1 -trustcacerts -file ~/certs/intermediateCA.cer -
keystore /opt/dsm/jre/lib/security/cacerts -storepass changeit
```

```
keytool -import -alias tomcat -trustcacerts -file ~/certs/dsm.cer -keystore
/opt/dsm/jre/lib/security/cacerts -storepass changeit
```

## Create a PKCS12 keychain file and import it into the new .keystore file

To maintain the relationship between the certificates, you must create a PKCS12 keychain file and import the root CA, the intermediate CA and the application server certificates into it using openssl.

1. Generate the private key from the new `.keystore` file with the following commands:

```
/opt/dsm/jre/bin/keytool -importkeystore -srckeystore ~/certs/.keystore -
srcstorepass <keystore password> -deststoretype PKCS12 -destkeystore
~/certs/keystore.p12 -storepass <p12 keystore password>
```

```
openssl rsa -in ~/certs/keystore.p12 -inform PKCS12 -passin pass:<above p12
keystore password you specified> -out ~/certs/private.key
```

2. Create a certificate for the keychain file from the root and intermediate CA certificates:

```
cat ~/certs/intermediateCA.cer ~/certs/rootCA.cer > ~/certs/CAcertchain.cer
```

**Note:** Combine the certificates in the order provided by your CA.

3. Create the PKCS12 keychain:

```
openssl pkcs12 -export -in ~/certs/dsm.cer -inkey ~/certs/private.key -
certfile ~/certs/CAcertchain.cer -out dsm.p12 -name tomcat -passout
pass:<keychain password>
```

4. Import the PKCS12 keychain into the new `.keystore` file:

```
/opt/dsm/jre/bin/keytool -importkeystore -srckeystore ~/certs/dsm.p12 -
srcstoretype pkcs12 -srcalias tomcat -srcstorepass <keychain password> -
destkeystore ~/certs/.keystore -storepass <keystore password> -destalias
tomcat
```

### Configure the Deep Security Manager to use the new .keystore file

1. Overwrite the `.keystore` file in the Deep Security Manager installation directory with the new `.keystore` file:

   ```
   cp ~/certs/.keystore /opt/dsm/.keystore
   ```

   **Note:** Only the default `.keystore` file is kept when you upgrade Deep Security Manager. We recommend that you replace the existing `.keystore` file.

2. Open the `configuration.properties` file, find the `keystorekeystorePass=` parameter, and replace the value with the one you specified for the `<keystore password>` in step 2 of the "Create a new .keystore file and add your certificates to the cacerts file" on page 758 procedure.

3. Restart the Deep Security Manager service.
4. Open the Deep Security Manager console with `https://< Deep Security Manager server host name or FQDN>:4119` and make sure there is no certificate error message. The `<Deep Security Manager server host name or FQDN>` should be the one used in step 2 of the "Create a new .keystore file and add your certificates to the cacerts file" on page 758 procedure.

## Encrypt communication between the Deep Security Manager and the database

Communication between the Deep Security Manager and the database is not encrypted by default. This is for performance reasons and because the channel between the manager and the database may already be secure (either they are running on the same computer or they are connected by crossover cable, a private network segment, or tunneling via IPSec).

However, if the communication channel between the Deep Security Manager and the database is not secure, you should encrypt the communications between them. Do this by editing the

`dsm.properties` file located in `\[Deep Security Manager install directory]\webclient\webapps\ROOT\WEB-INF\`

The instructions vary depending on the database you are using:

- "Microsoft SQL Server database (Linux)" below
- "Microsoft SQL Server (Windows)" on the next page
- "Oracle Database" on page 766
- "PostgreSQL" on page 767

**Note:** If you are running the Deep Security Manager in multi-node mode, these changes must be made on each node.

This section also provides information on "Running an agent on the database server" on page 768 and how to "Disable encryption between the manager and database" on page 768.

## Encrypt communication between the manager and database

### Microsoft SQL Server database (Linux)

1. Stop the Deep Security Manager service:

   ```
   # service dsm_s stop
   ```

2. Edit `/opt/dsm/webclient/webapps/ROOT/WEB-INF/dsm.properties` to add the following lines:

   ```
   database.SqlServer.encrypt=true
   database.SqlServer.trustServerCertificate=true
   ```

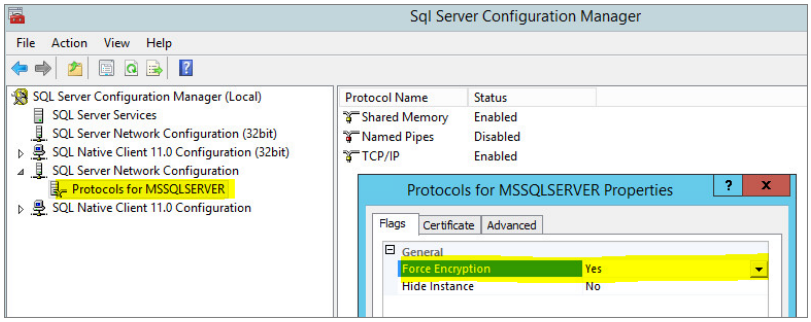
   **Note:** If you upgraded from Deep Security 10.1 or a previous version, and your connection to the database uses named pipes as the transport, add the following line instead:

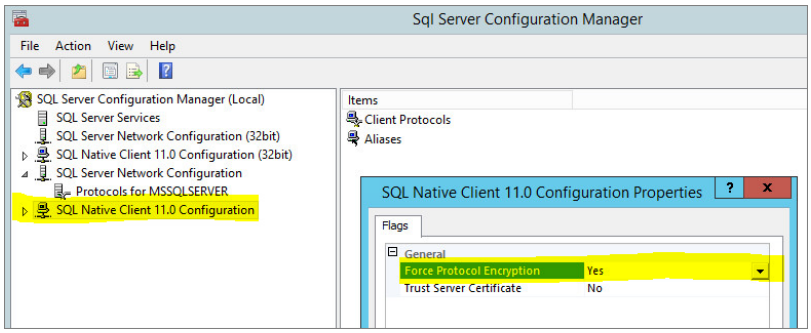
   ```
   database.SqlServer.ssl=require
   ```

3. If you upgraded from Deep Security 10.1 or a previous version, and your connection to the database uses named pipes as the transport, under `/opt/dsm`, create a file named `dsm_s.vmoptions` that contains the following line:

   ```
   -Djsse.enableCBCProtection=false
   ```

4. In the SQL Server Configuration Manager, enable "Force Encryption" in the protocol properties for the instance:




5. Start the Deep Security Manager service:

```
# service dsm_s start
```

For additional information, see Enable Encrypted Connections to the Database Engine on the Microsoft MSDN site.

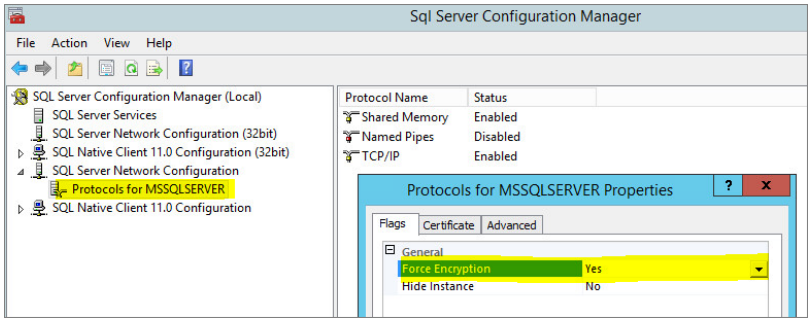
## Microsoft SQL Server (Windows)

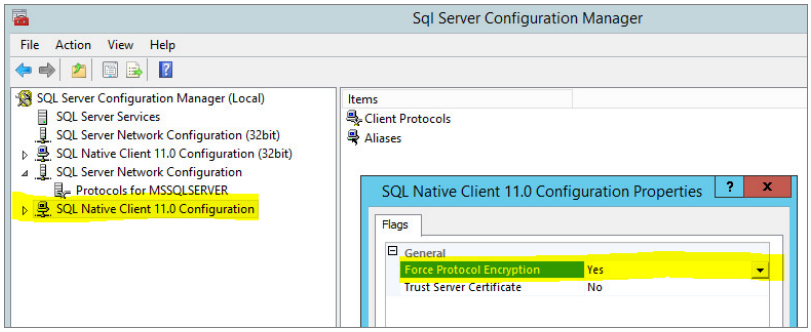
1. Stop the Deep Security Manager service.
2. Edit `\Program Files\Trend Micro\Deep Security Manager\webclient\webapps\ROOT\WEB-INF\dsm.properties` to add the following line:

```
database.SqlServer.encrypt=true
database.SqlServer.trustServerCertificate=true
```

> **Note:** If you upgraded from Deep Security 10.1 or a previous version, and your connection to the database uses named pipes as the transport, add the following line instead:
>
> `database.SqlServer.ssl=require`

3. If you upgraded from Deep Security 10.1 or a previous version, and your connection to the database uses named pipes as the transport, under `\Program Files\Trend Micro\Deep Security Manager`, create a file named `Deep Security Manager.vmoptions` that contains the following line:
   `-Djsse.enableCBCProtection=false`
4. In the SQL Server Configuration Manager, enable "Force Encryption" in the protocol properties for the instance:




5. Start the Deep Security Manager service.

For additional information, see Enable Encrypted Connections to the Database Engine on the Microsoft MSDN site.

## Oracle Database

1. Add the following lines to `dsm.properties` (example):

```
database.Oracle.oracle.net.encryption_types_client=(AES256)
database.Oracle.oracle.net.encryption_client=REQUIRED
database.Oracle.oracle.net.crypto_checksum_types_client=(SHA1)
```

```
database.Oracle.oracle.net.crypto_checksum_client=REQUIRED
```

2. Save and close the file. "Restart the Deep Security Manager" on page 734 service.

(All parameters prefixed with database.Oracle. will be passed to the Oracle driver.)

Possible values for the `encryption_types_client` are:

- AES256
- AES192
- AES128
- 3DES168
- 3DES112
- DES56C
- DES40C
- RC4_256
- RC4_128
- RC4_40
- RC4_56

Possible values for `crypto_checksum_types_client` are:

- MD5
- SHA1

For additional options consult: https://docs.oracle.com/cd/B28359_01/java.111/b31224/clntsec.htm

## PostgreSQL

1. Turn on SSL in PostgreSQL. For information, on how to do this for an on-premise PostgreSQL database, see Secure TCP/IP Connections with SSL. For an Amazon RDS for PostgreSQL, see Using SSL with a PostgreSQL DB Instance.
2. Stop the Trend Micro Deep Security Manager service.
3. In the `dsm.properties` file, add the following line:

```
database.PostgreSQL.connectionParameters=ssl=true
```

4. Restart the Trend Micro Deep Security Manager service.
5. To check that the manager is connecting using TLS, use the following query and check the SSL column:

```
select a.client_addr, a.application_name, a.usename, s.* from pg_stat_ssl s
join pg_stat_activity a using (pid) where a.datname='<Deep Security database
name>';
```

## Running an agent on the database server

Encryption should be enabled if you are using an agent to protect the database. When you perform a security update, the Deep Security Manager stores new intrusion prevention rules in the database. The rule names themselves will almost certainly generate false positives as they get parsed by the agent if the data is not encrypted.

## Disable encryption between the manager and database

If you have encrypted communication between Deep Security Manager and the database, you will need to disable the encryption before performing an upgrade to Deep Security Manager.

### Microsoft SQL Server database (Linux)

1. Stop the Deep Security Manager service:

```
# service dsm_s stop
```

2. Edit the `/opt/dsm/webclient/webapps/ROOT/WEB-INF/dsm.properties` to remove the following lines:

```
database.SqlServer.encrypt=true
database.SqlServer.trustServerCertificate=true
```

> **Note:** If you upgraded from Deep Security 10.1 or a previous version, and your connection to the database uses named pipes as the transport, remove the following line instead:
>
> `database.SqlServer.ssl=require`

3. In the SQL Server Configuration Manager, disable "Force Encryption" in the protocol properties for the instance:
4. Start the Deep Security Manager service:

```
# service dsm_s start
```

## Microsoft SQL Server (Windows)

1. Stop the Deep Security Manager service.
2. Edit `\Program Files\Trend Micro\Deep Security Manager\webclient\webapps\ROOT\WEB-INF\dsm.properties` to remove the following lines:

   ```
   database.SqlServer.encrypt=true
   database.SqlServer.trustServerCertificate=true
   ```

   **Note:** If you upgraded from Deep Security 10.1 or a previous version, and your connection to the database uses named pipes as the transport, remove the following line instead:

   ```
   database.SqlServer.ssl=require
   ```

3. In the SQL Server Configuration Manager, disable "Force Encryption" in the protocol properties for the instance:
4. Start the Deep Security Manager service.

## Oracle Database

1. Remove the following lines from `dsm.properties` (example):

   ```
   database.Oracle.oracle.net.encryption_types_client=(AES256)
   database.Oracle.oracle.net.encryption_client=REQUIRED
   database.Oracle.oracle.net.crypto_checksum_types_client=(SHA1)
   database.Oracle.oracle.net.crypto_checksum_client=REQUIRED
   ```

2. Save and close the file. Stop and restart the Deep Security Manager service.

## PostgreSQL

1. Stop the Trend Micro Deep Security Manager service.
2. In the `dsm.properties` file, remove the following line:

   ```
   database.PostgreSQL.connectionParameters=ssl=true
   ```

3. Restart the Trend Micro Deep Security Manager service.

# Change the Deep Security Manager database password

Your organization's security policies may require that you periodically change the password that Deep Security Manager uses to access the database.

- "Change your Microsoft SQL Server password" below
- "Change your Oracle password" on the next page
- "Change your PostgreSQL password" on the next page

## Change your Microsoft SQL Server password

1. On Windows, stop the Trend Micro Deep Security Manager service on each of your Deep Security Manager instances.

   On Linux, the command to stop the service is:

   ```
   # service dsm_s stop
   ```

2. Use SQL Server Management Studio to change the SQL user password.
3. On each Deep Security Manager instance, modify the `/opt/dsm/webclient/webapps/ROOT/WEB-INF/dsm.properties` file to specify the new password. When you open this file, you will see an obfuscated value for the password, similar to this:

   ```
   database.SqlServer.password=$1$4ec04f9550e0bf378fa6b1bc9698d0bbc59ac010bfef7ea1
   e6e47f30394800b1a9554fe206a3ee9ba5f774d205ba03bb86c91c0664c7f05f8c467e03e0d8ebbe
   ```

   Overwrite that value with your new password (the new password will be obfuscated when the service restarts):

   ```
   Database.SqlServer.password=NEW PASSWORD GOES HERE
   ```

4. On Windows, start the Trend Micro Deep Security Manager service on each of your Deep Security Manager instances.

   On Linux, the command to start the service is:

   ```
   # service dsm_s start
   ```

## Change your Oracle password

1. On Windows, stop the Trend Micro Deep Security Manager service on each of your Deep Security Manager instances.

   On Linux, the command to stop the service is:

   ```
   # service dsm_s stop
   ```

2. Use your Oracle tools to change the password.
3. On each Deep Security Manager instance, modify the `/opt/dsm/webclient/webapps/ROOT/WEB-INF/dsm.properties` file to specify the new password. When you open this file, you will see an obfuscated value for the password, similar to this:

   ```
   database.Oracle.password=$1$4ec04f9550e0bf378fa6b1bc9698d0bbc59ac010bfef7ea1e6e
   47f30394800b1a9554fe206a3ee9ba5f774d205ba03bb86c91c0664c7f05f8c467e03e0d8ebbe
   ```

   Overwrite that value with your new password (the new password will be obfuscated when the service restarts):

   ```
   Database.Oracle.password=NEW PASSWORD GOES HERE
   ```

4. On Windows, start the Trend Micro Deep Security Manager service on each of your Deep Security Manager instances.

   On Linux, the command to start the service is:

   ```
   # service dsm_s start
   ```

## Change your PostgreSQL password

1. On Windows, stop the Trend Micro Deep Security Manager service on each of your Deep Security Manager instances.

   On Linux, the command to stop the service is:

   ```
   # service dsm_s stop
   ```

2. Follow instructions from your PostgreSQL documentation to change the password.

3. On each Deep Security Manager instance, modify the `/opt/dsm/webclient/webapps/ROOT/WEB-INF/dsm.properties` file to specify the new password. When you open this file, you will see an obfuscated value for the password, similar to this:

   ```
   database.PostgreSQL.password=$1$4ec04f9550e0bf378fa6b1bc9698d0bbc59ac010bfef7ea1e6e47f30394800b1a9554fe206a3ee9ba5f774d205ba03bb86c91c0664c7f05f8c467e03e0d8ebbe
   ```

   Overwrite that value with your new password (the new password will be obfuscated when the service restarts):

   ```
   Database.PostgreSQL.password=NEW PASSWORD GOES HERE
   ```

4. On Windows, start the Trend Micro Deep Security Manager service on each of your Deep Security Manager instances.

   On Linux, the command to start the service is:

   ```
   # service dsm_s start
   ```

# Enable Content Security Policy and HTTP Public Key Pinning

Enabling Content Security Policy and HTTP Public Key Pinning in the Deep Security Manager can provide additional protection against cross-site scripting attacks and fraudulent certificates.

**Note:** In multi-tenant mode, the Content Security Policy and HTTP Public Key Pin Policy settings are only available to the primary tenant.

## Add a content security policy or public key pin policy

1. Go to **Administration** > **System Settings** > **Security**.
2. Enter your Content Security Policy or HTTP Public Key Pin Policy directives in the corresponding field.

   **Note:** Before you enable your policies, test them by selecting the **Report Only** option and verifying that the policy violation reports are correct.

   **Tip:** You can enter individual policy directives on separate lines.

3. Click **Save** at the bottom of the page.

## Reset your configuration

If you experience trouble while configuring your content security policy or public key pin policy and cannot correct it in the Deep Security Manager, SSH into the Deep Security Manager and run the corresponding commands to reset your configuration(s):

### Content security policy

```
dsm_c -action changesetting -name settings.configuration.contentSecurityPolicy -value ""
```

```
dsm_c -action changesetting -name settings.configuration.contentSecurityPolicyReportOnly -value "true"
```

### Public key pin policy

```
dsm_c -action changesetting -name settings.configuration.publicKeyPinPolicy -value ""
```

```
dsm_c -action changesetting -name settings.configuration.publicKeyPinPolicyReportOnly -value "true"
```

# Enforce user password rules

You can specify password requirements for Deep Security Manager passwords, and other settings related to user authentication.

## Specify password requirements

> **Note:** For greater security, enforce stringent password requirements: minimum 8 characters, include both numbers and letters, use upper and lower case, include non-alphanumeric characters, and expire regularly.

Go to **Administration > System Settings > Security**. In the **User Security** section, you can change these settings:

- **Session idle timeout:** Specify the period of inactivity after which a user will be required to sign in again.

- **Maximum session duration:** Maximum length of time that a user can be signed into the Deep Security Manager before they'll be required to sign in again.
- **Number of incorrect sign-in attempts allowed (before lock out):** The number of times an individual user (i.e. with a specific username) can attempt to sign in with an incorrect password before they are locked out. Only a user with "Can Edit User Properties" rights can unlock a locked-out user (see "Define roles for users" on page 995).

  **Note:** If a user gets locked out for a particular reason (too many failed sign-in attempts, for example), and no user remains with the sufficient rights to unlock that account, please contact Trend Micro for assistance.

- **Number of concurrent sessions allowed per User:** Maximum number of simultaneous sessions allowed per user.

  **Note:** A note about being signed in as two users at once: Remember that Firefox sets session cookies on a per-process basis, and not on a per-window basis. This means that if for some reason you want to be signed in as two users at the same time, you will either have to use two different browsers (if one of them is Firefox), or sign in from two separate computers.

- **Action when concurrent session limit is exceeded:**Specifies what happens when a user reaches the maximum number of concurrent sessions.
- **User password expires:** Number of days that passwords are valid. You can also set passwords to never expire.
- **User password minimum length:** The minimum number of characters required in a password.
- **User password requires both letters and numbers:** Letters (a-z, A-Z) as well as numbers (0-9) must be used as part of the password.
- **User password requires both upper and lower case characters:** Upper and lower case characters must be used.
- **User password requires non-alphanumeric characters:** Passwords must include non-alphanumeric characters.

- **Send email when a user's password is about the expire:** Before a user's password expires, they will receive an email message. To use this feature, you must "Configure SMTP settings for email notifications" on page 176.

### Use another identity provider for sign-on

You can also configure Deep Security to use SAML single sign-on. For details, see "Getting started with SAML single sign-on" on page 1015.

### Add a message to the Deep Security Manager Sign In page

On the **Administration > System Settings > Security** page, use **Sign-In Page Message** to enter text that will be displayed on the Deep Security Manager's sign in page.

### Present users with terms and conditions

You can configure Deep Security Manager so that users must agree to terms and conditions before they can sign in to the Deep Security Manager.

To enable this feature, select **User must agree to the terms and conditions** on the **Administration > System Settings > Security** page. In the two text boxes, enter a title and the list of terms and conditions that will be displayed when a user clicks the **Terms and Conditions** link on the Sign In page.

### Other Security settings

The **Administration > System Settings > Security** page also enables you to:

- "Manage trusted certificates" on page 216
- "Enable Content Security Policy and HTTP Public Key Pinning" on page 772

## Set up multi-factor authentication

The Deep Security Manager allows you the option to use multi-factor authentication (MFA). MFA is a method of access control requiring more than a user name and password that is recommended as a best practice.

In this article:

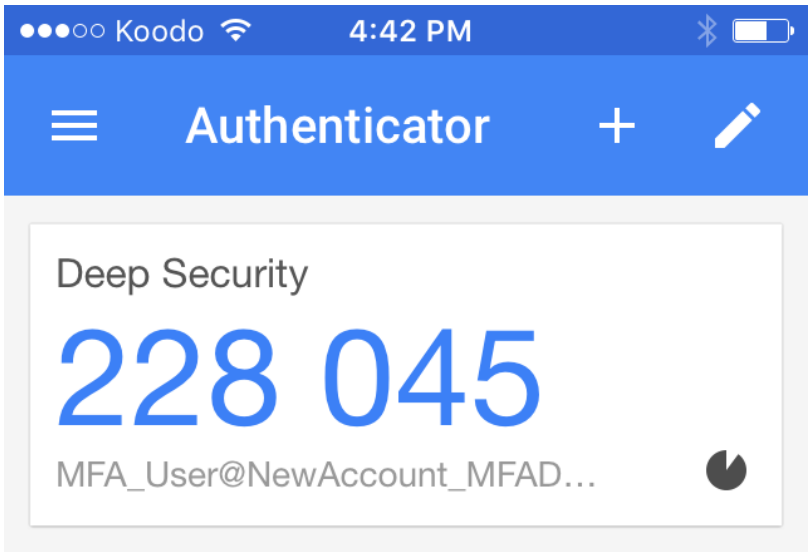

- "Enable multi-factor authentication" below
- "Disable multi-factor authentication" on page 778
- "Supported multi-factor authentication (MFA) applications" on page 778
- "Troubleshooting MFA" on page 779


## Enable multi-factor authentication

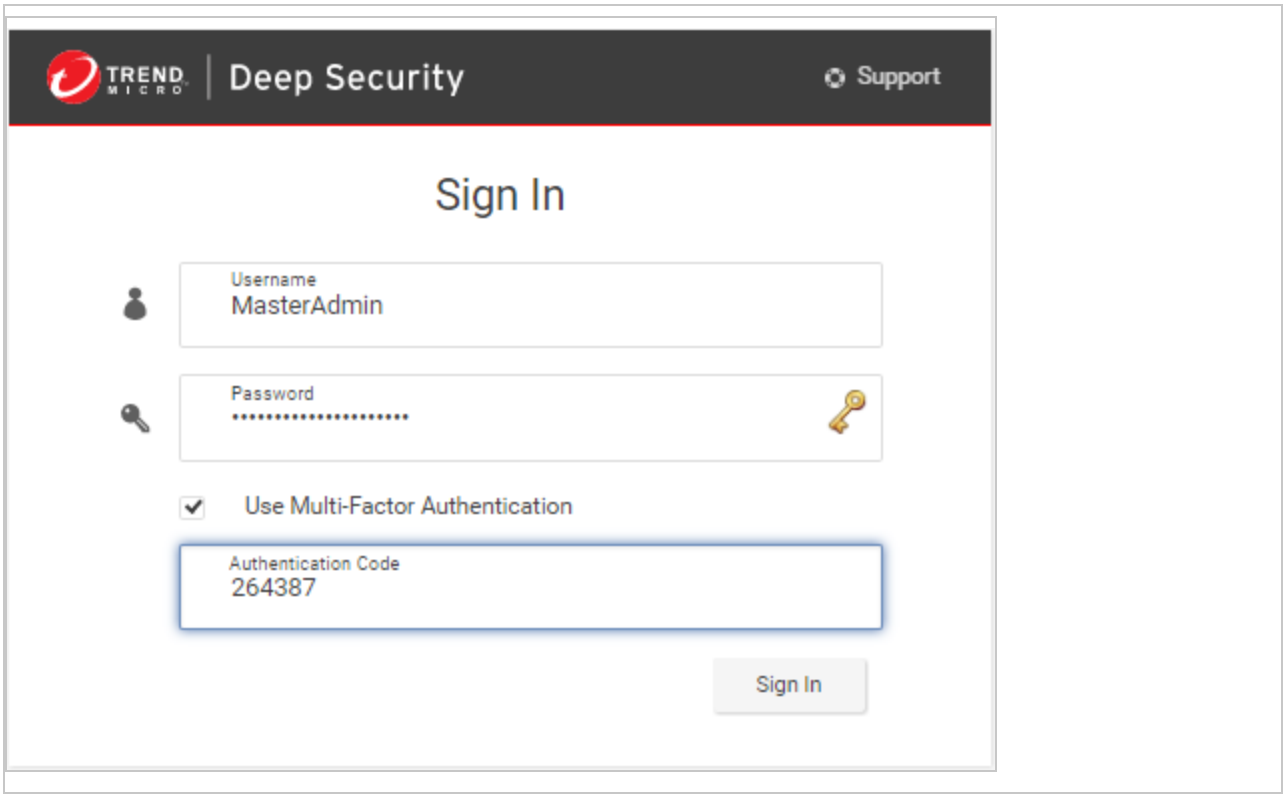
1. In Deep Security Manager, select **User Properties** from the menu under your user name in the upper-right corner.
2. On the **General** tab, click the **Enable MFA** button. This will open the **Enable Multi-Factor Authentication** wizard to guide you through the rest of the process.
3. The first screen of the wizard will remind you to install a compatible virtual MFA application, such as Google Authenticator. For more information, see "Supported multi-factor authentication (MFA) applications" on page 778 at the bottom of this article.
4. If your device supports scanning QR codes, you can use your camera to configure your MFA application and click **Next**.

   Otherwise, you can choose **My device does not support scanning QR codes. Show secret key for manual time-based configuration**.

5. Enter the **Authentication Code** (without the space), for example: 228045.



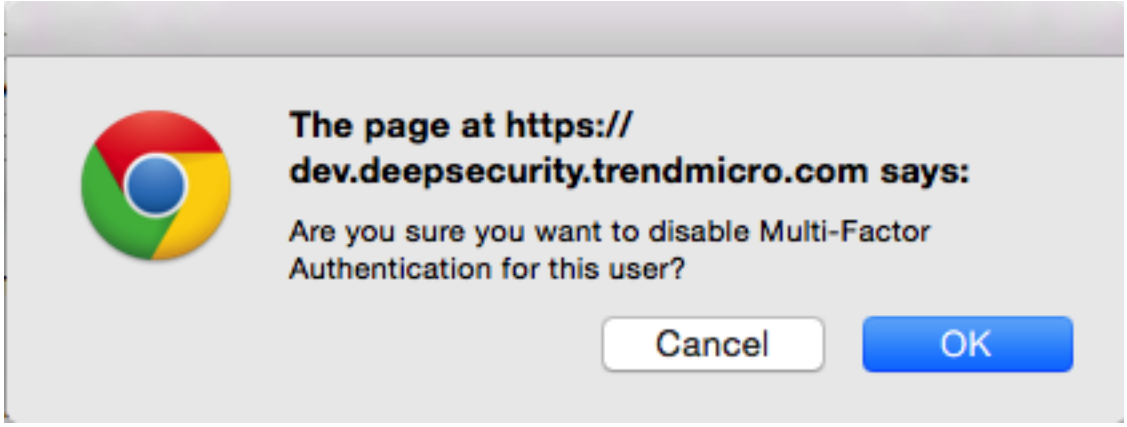

6. If the authorization code is correct, MFA will be enabled for your account and you will be required to enter a new MFA code each time you sign in.



## Disable multi-factor authentication

1. In the Deep Security Manager, select **User Properties** from the menu under your user name in the upper-right corner.

2. On the **General** tab, click the **Disable MFA** button.
3. Click **OK** on the confirmation screen to disable MFA.




4. Your user properties screen displays with a note to indicate the changes to MFA. Click **OK** to close the screen.

## Supported multi-factor authentication (MFA) applications

The following smartphones and applications are actively supported for MFA. However, any application implementing an RFC 6238 compliant Time-base One-time Password Algorithm should work.

| Smartphone | MFA App |
|---|---|
| Android | Google Authenticator, Duo |
| iPhone | Google Authenticator, Duo |
| Blackberry | Google Authenticator |

# Troubleshooting MFA

## What if my MFA is enabled but not working?

The most common source of MFA login issues is caused by the time on your Deep Security Manager being out of sync with your device.

Follow the instructions below for your chosen operating system to make sure the time is properly synced:

**If your Deep Security Manager is Linux:**

Check that NTP is working correctly by entering `ntpstat` in the command line. To view the current system time and date, enter `date`.

**If your Deep Security Manager is Windows:**

Check that the Windows Time Service is working correctly. To view the current system time and date, enter `time` and `date` in the command line.

## What if my MFA device is lost or stops working?

If your MFA device is lost, destroyed, or stops working, you'll need to have MFA disabled for your account in order to be able to sign in.

1. Get in touch with the person who provided you with your sign in credentials and ask them to follow the instructions in "Disable multi-factor authentication" on the previous page. (You'll then be able to sign in with just your user name and password.)
2. After you've signed in, change your password.
3. Follow the instructions for "Enable multi-factor authentication" on page 776.

If you are the only administrative user for a Deep Security as a Service account, contact technical support (sign in Deep Security as a Service, and click **Support** in the top right-hand corner) for assistance in temporarily deactivating MFA for your account.

# Manage AWS regions

## Add an Amazon Web Services region

If the Amazon Web Services (AWS) region hosting your EC2 resources does not appear when you try to add a cloud account using the **Add AWS Cloud Account** wizard, manually add the region.

1. On the server that is hosting Deep Security Manager, enter the command:
   `dsm_c -action addregion -region REGION -display DISPLAY -endpoint ENDPOINT`

   where the parameters are:

| Parameter | Description | Example |
|---|---|---|
| REGION | The Amazon Web Services identifier for the region. | `ca-east-1` |
| DISPLAY | The display string to use for the region in the **Add AWS Cloud Account** wizard. | Canada East (Ottawa) |
| ENDPOINT | The fully-qualified domain name of the Amazon Elastic Compute Cloud (EC2) endpoint to use for the region. | `ec2.ca-east-1.amazonaws.com` |

   **Note:** If Deep Security Manager is running on a Linux server, you must run the command with `sudo` or use a superuser account such as root.

2. If the specific AWS region requires that you import a trusted certificate (most don't), see "Manage trusted certificates" on page 216.

## Viewing your Amazon Web Services regions

You can view any AWS regions that you have added using the CLI.

On the server that is hosting Deep Security Manager, enter the command:

```
dsm_c -action listregions
```

**Note:** If Deep Security Manager is running on a Linux server, you must run the command with `sudo` or use a superuser account such as root.

## Removing an Amazon Web Services region

You can delete any AWS regions that you have added using the CLI. Any existing cloud accounts for the region will continue to work unless you remove them, but administrators won't be able to create new cloud accounts for the region.

1. On the server that is hosting Deep Security Manager, enter the command:

   ```
   dsm_c -action listregions
   ```

2. Find the identifier for the that you want to remove.
3. Enter the command:

   ```
   dsm_c -action removeregion -region REGION
   ```

   The `REGION` parameter is required.

| Parameter | Description | Example |
|---|---|---|
| REGION | The Amazon Web Services identifier for the region. | `ca-east-1` |

**Note:** If Deep Security Manager is running on a Linux server, you must run the command with `sudo` or use a superuser account such as root.

# Configure alerts

Alerts are generated when Deep Security requires your attention, such as an administrator-issued command failing, or a hard disk running out of space. Deep Security includes a pre-defined set of alerts (for a list, see "Predefined alerts" on page 903). Additionally, when you create protection module rules, you can configure them to generate alerts if they are triggered.

There are several ways to see which alerts have been triggered:

- They're displayed in the "Alert Status" dashboard widget in Deep Security Manager.
- They're displayed on the Alerts page in Deep Security Manager (see "View alerts in Deep Security Manager" on the next page).
- You can get an email notification when an alert is triggered (see "Set up email notification for alerts" on page 783.)

- You can generate alert reports (see "Generate reports about alerts and other activity" on page 786).

Unlike security events and system events, alerts are not purged from the database after a period of time. Alerts remain until they are dismissed, either manually or automatically.

## View alerts in Deep Security Manager

The **Alerts** page in Deep Security Manager displays all alerts that have been triggered, but not yet responded to. You can display alerts in a summary view that groups similar alerts together, or in list view, which lists all alerts individually. To switch between the two views, use the menu next to "Alerts" in the page's title. You can also sort the alerts by time or by severity.

In summary view, expanding an Alert panel (by clicking **Show Details**) displays all the computers (or users) that have generated that particular alert. Clicking the computer will display the computer's **Details** window. If an alert applies to more than five computers, an ellipsis ("...") appears after the fifth computer. Clicking the ellipsis displays the full list. Once you have taken the appropriate action to deal with an alert, you can dismiss the alert by selecting the check box next to the target of the alert and clicking **Dismiss**. (In list view, right-click the alert to see the list of options in the context menu.)

Alerts that can't be dismissed (like "Relay Update Service Not Available") will be dismissed automatically when the condition no longer exists.

**Note:** In cases where an alert condition occurs more than once on the same computer, the alert will show the timestamp of the first occurrence of the condition. If the alert is dismissed and the condition reoccurs, the timestamp of the first re-occurrence will be displayed.

**Tip:** Use the Computers filtering bar to view only alerts for computers in a particular computer group, with a particular policy, etc.

Unlike security events and system events, alerts are not purged from the database after a period of time. Alerts remain until they are dismissed, either manually or automatically.

## Configure alert settings

To configure the settings for individual alerts, go to the **Alerts** page in Deep Security Manager and click **Configure Alerts**. This displays a list of all alerts. A green check mark next to an alert indicates that it is enabled. An alert will be triggered if the corresponding situation occurs, and it will appear in the Deep Security Manager.

You can select an alert and click **Properties** to change other settings for the alert, such as the severity level and email notification settings.

## Set up email notification for alerts

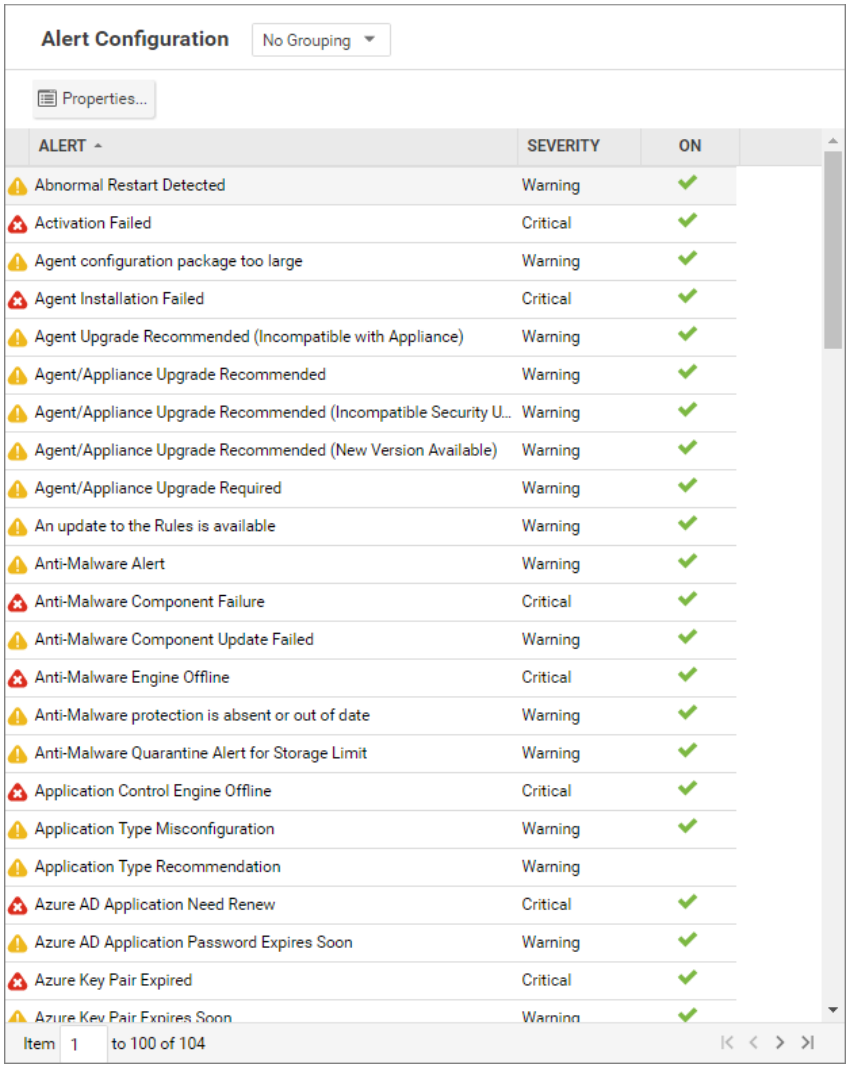
Deep Security Manager can send emails to specific users when selected alerts are triggered.

To enable email notifications:

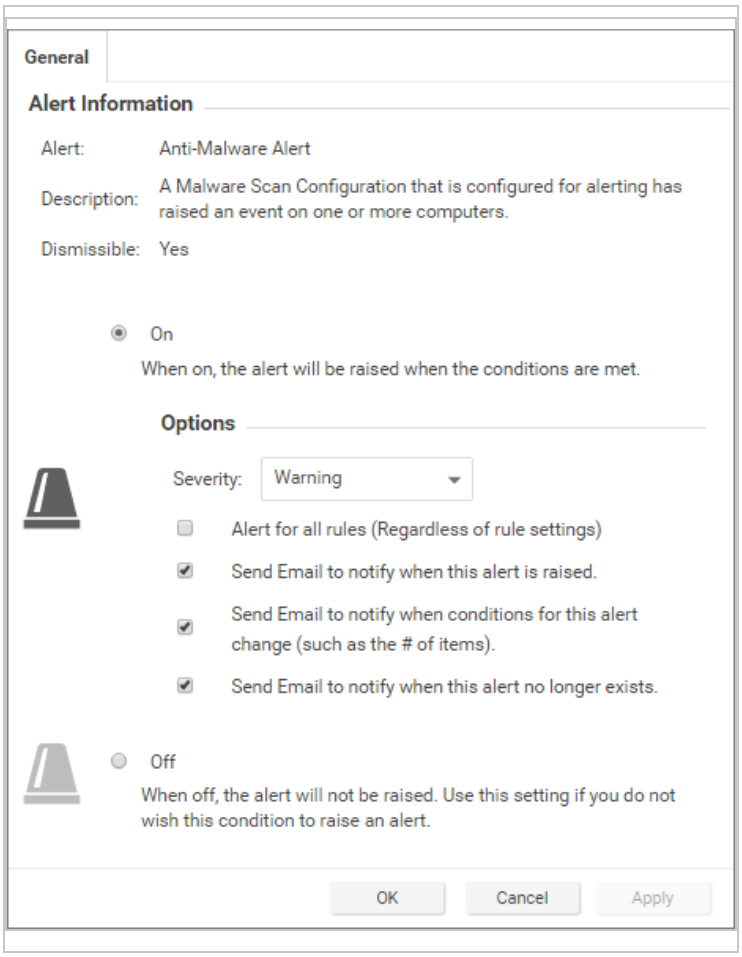
1. Give Deep Security Manager access to an SMTP mail server (see "Configure SMTP settings for email notifications" on page 176).
2. Specify which alerts cause email notifications to be sent. For example, you can send email only for the most critical alerts. Most alerts send email notifications by default. (see "Turn alert emails on or off" on the next page).
3. Specify who will receive email notifications. You can configure user accounts so that they receive alert emails (see "Configure an individual user to receive alert emails" on page 785). You can also configure alerts to specify the email account of a user or a distribution list. With this option, email is sent regardless of the configuration of the user accounts (see "Configure recipients for all alert emails" on page 785).

## Turn alert emails on or off

1. Go to the **Alerts** page and click **Configure Alerts** to display the list of alerts.




2. A green check mark next to an alert indicates that it is enabled. An alert will be triggered if the corresponding situation occurs, and appear in the Deep Security Manager GUI. If you also want to receive email about the alert, double-click on an alert to display its Properties window, then select at least one of the "Send Email" check boxes.




## Configure an individual user to receive alert emails

1. Go to **Administration** > **User Management** > **Users** and double-click a user account to display its Properties window.
2. On the **Contact Information** tab, enter an email address and select **Receive Alert Emails**.

## Configure recipients for all alert emails

**Note:** All alert emails will be sent to this address or email distribution list, even if the recipients have not been set up in their user account properties to receive email notifications.

1. Go to **Administration** > **System Settings** > **Alerts**.
2. For **Alert Email Address - The email address to which all alert emails should be sent**, provide an email address or a distribution list email address.

# Generate reports about alerts and other activity

Deep Security Manager produces reports in PDF or RTF formats. Most of the reports have configurable parameters such as date range or reporting by computer group. Parameter options will be disabled for reports to which they don't apply. You can set up a one-time report (see "Set up a single report" below) or set up a schedule to run a report on a regular basis (see "Set up a recurring report " on page 789).

## Set up a single report

1. In the Deep Security Manager, go to the **Events & Reports** tab and then in the left pane, click **Generate Reports**. Go to the **Single Report** tab.
2. In the **Report** list, select the type of report that you want to generate. Depending on which protection modules you are using, these reports may be available:
   - **Alert Report:** List of the most common alerts
   - **Anti-Malware Report:** List of the top 25 infected computers
   - **Attack Report:** Summary table with analysis activity, divided by mode
   - **AWS Metered Billing Report:** Summary table of AWS Metered Billing consumption in hours per day by instance size and deployment type
   - **Computer Report:** Summary of each computer listed on the Computers tab
   - **DPI Rule Recommendation Report:** Intrusion prevention rule recommendations. This report can be run for only one security policy or computer at a time.
   - **Firewall Report:** Record of firewall rule and stateful configuration activity
   - **Forensic Computer Audit Report:** Configuration of an agent on a computer
   - **Integrity Monitoring Baseline Report:** Baseline of the host(s) at a particular time, showing Type, Key, and Fingerprinted Date.
   - **Integrity Monitoring Detailed Change Report:** Details about the changes detected

- **Integrity Monitoring Report:** Summary of the changes detected
- **Intrusion Prevention Report:** Record of intrusion prevention rule activity
- **Log Inspection Detailed Report:** Details of log data that has been collected
- **Log Inspection Report:** Summary of log data that has been collected
- **Recommendation Report:** Record of recommendation scan activity
- **Security Module Usage Cumulative Report:** Current computer usage of protection modules, including a cumulative total and the total in blocks of 100
- **Security Module Usage Report:** Current computer usage of protection modules
- **Summary Report:** Consolidated summary of Deep Security activity
- **Suspicious Application Activity Report:** Information about suspected malicious activity
- **System Event Report:** Record of system (non-security) activity
- **System Report:** Overview of computers, contacts, and users
- **User and Contact Report:** Content and activity detail for users and contacts
- **Web Reputation Report:** List of computers with the most web reputation events

3. Select the **Format** for the report, either PDF or RTF. (The "Security Module Usage Report" and "Security Module Usage Cumulative Report" are exceptions and are always output as CSV files.)
4. You can also add an optional **Classification** to PDF or RTF reports: BLANK, TOP SECRET, SECRET, CONFIDENTIAL, FOR OFFICIAL USE ONLY, LAW ENFORCEMENT SENSITIVE (LES), LIMITED DISTRIBUTION, UNCLASSIFIED, INTERNAL USE ONLY.
5. You can use the **Tag Filter** area to filter the report data using event tags (if you have selected a report that contains event data). Select **All** for all events, **Untagged** for only untagged events, or select **Tag(s)** and specify one or more tags to include only those events with your selected tag(s).

   **Note:** If you apply multiple contradicting tags, the tags will counteract each other, rather than combine. For example, if you select "User Signed In" and "User Signed Out", there will be no system events.

6. You can use the **Time Filter** area to set a time filter for any period for which records exist. This is useful for security audits. Time filter options:
   - **Last 24 Hours:** Includes events from the past 24 hours, starting and ending at the top of the hour. For example if you generate a report on December 5th at 10:14am, you will get a report for events that occurred between December 4th at 10:00am and December 5th at 10:00am.
   - **Last 7 Days:** Includes events from the past week. Weeks start and end at midnight (00:00). For example if you generate a report on December 5th at 10:14am, you will get a report for events that occurred between November 28th at 0:00am and December 5th at 0:00am.
   - **Previous Month:** Includes events from the last full calendar month, starting and ending at midnight (00:00). For example, if you select this option on November 15, you will receive a report for events that occurred between midnight October 1 to midnight November 1.
   - **Custom Range:** Enables you to specify your own date and time range for the report. In the report, the start time may be changed to midnight if the start date is more than two days ago.
   - Note: Reports use data stored in counters. Counters are data aggregated periodically from Events. Counter data is aggregated on an hourly basis for the most recent three days. Data from the current hour is not included in reports. Data older than three days is stored in counters that are aggregated on a daily basis. For this reason, the time period covered by reports for the last three days can be specified at an hourly level of granularity, but beyond three days, the time period can only be specified on a daily level of granularity.
7. In the **Computer Filter** area, select the computers whose data will be included in the report.
   - **All Computers:** Every computer in Deep Security Manager
   - **My Computers:** If the signed in user has restricted access to computers based on their user role's rights settings, these are the computers the signed in User has view access right to.
   - **In Group:** The computers in a Deep Security group.

- **Using Policy:** The computers using a specific protection Policy.
- **Computer:** A single computer.

> **Note:** To generate a report on specific computers from multiple computer groups, create a user who has viewing rights only to the computers in question and then either create a scheduled task to regularly generate an "All Computers" report for that user or sign in as that user and run an "All Computers" report. Only the computers to which that user has viewing rights will be included in the report.

8. In the **Encryption** area, you can protect the report with the password of the currently signed in user or with a new password for this report only:
   - **Disable Report Password:** Report is not password protected.
   - **Use Current User's Report Password:** Use the current user's PDF report password. To view or modify the user's PDF report password, go to **Administration > User Management > Users > Properties > Settings > Reports**.
   - **Use Custom Report Password:** Create a one-time-only password for this report. The password does not have any complexity requirements.

## Set up a recurring report

Recurring reports are scheduled tasks that periodically generate and distribute reports to any number of users and contacts.

To set up a recurring report, go to the **Events & Reports** tab and then in the left pane, click **Generate Reports**. Go to the **Recurring Reports** tab and click **New**. The New Scheduled Task wizard opens and will step you through the configuration process. Most of the options are identical to those for single reports, with the exception of Time Filter:

- **Last [N] Hour(s):** When [N] is less than 60, the start and end times will be at the top of the specified hour. When [N] is more than 60, hourly data is not available for the beginning of the time range, so the start time in the report will be changed to midnight (00:00) of the start day.
- **Last [N] Day(s):** Includes data from midnight [N] days ago to midnight of the current day.
- **Last [N] Week(s):** Includes events from the last [N] weeks, starting and ending at midnight (00:00).
- **Last [N] Month(s):** Includes events from the last [N] full calendar month, starting and ending at midnight (00:00). For example, if you select "Last 1 Month(s)" on November 15, you will receive a report for events that occurred between midnight October 1 to midnight November 1.

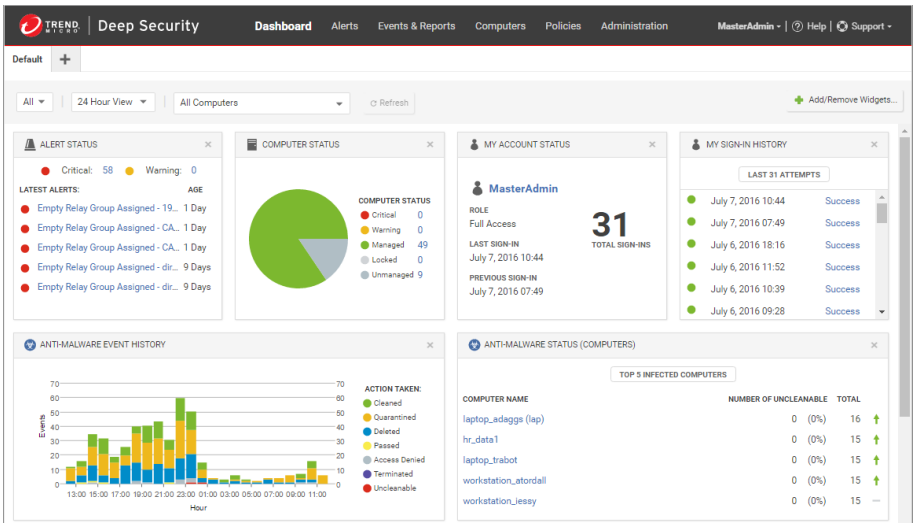
**Note:** Reports use data stored in counters. Counters are data aggregated periodically from events. Counter data is aggregated on an hourly basis for the most recent three days. Data from the current hour is not included in reports. Data older than three days is stored in counters that are aggregated on a daily basis. For this reason, the time period covered by reports for the last three days can be specified at an hourly level of granularity, but beyond three days, the time period can only be specified on a daily level of granularity.

For more information on scheduled tasks, see the "Schedule Deep Security to perform tasks" on page 263.

# Customize the dashboard

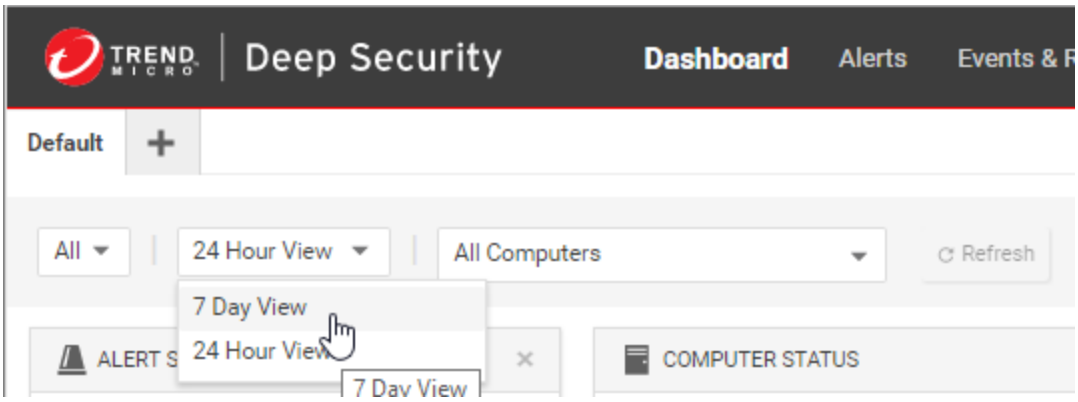
The dashboard is the first page that appears after you log into Deep Security Manager.

Each user can customize the contents and layout of their dashboard. Deep Security Manager automatically saves your settings, and will remember your dashboard the next time that you log in. You can also configure the data's time period, and which computer's or computer group's data is displayed.



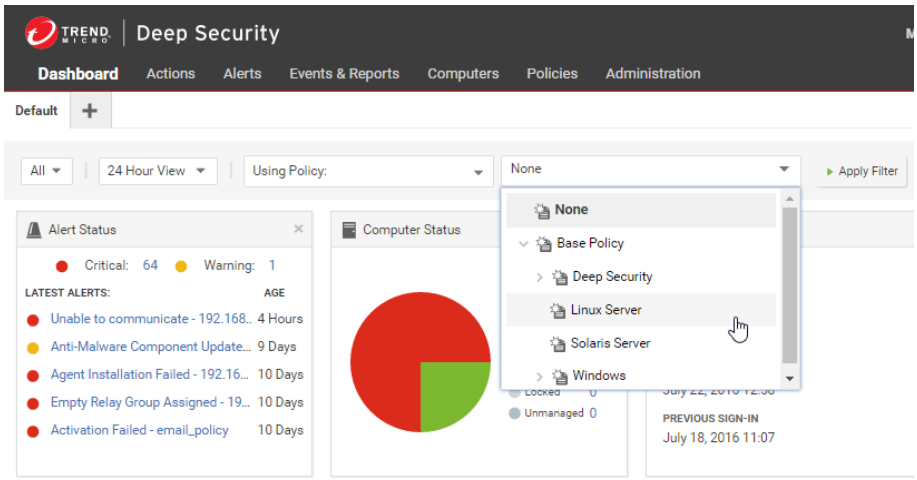

## Date and time range

The dashboard can display data from either the last 24 hours, or the last seven days.




## Computers and computer groups

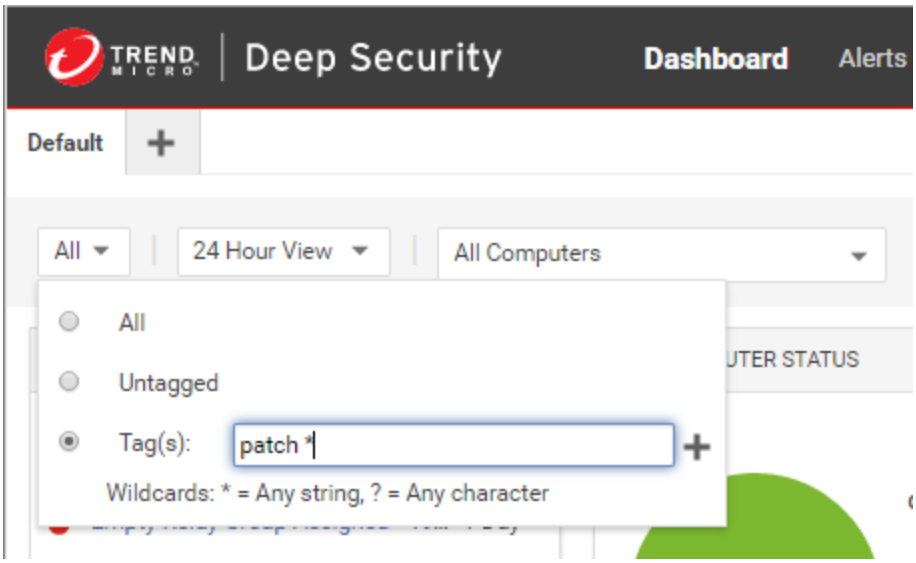
Use the **Computer** menu to filter the displayed data to display only data from specific computers. For example, only those using the **Linux Server** security policy:




## Filter by tags

In Deep Security, a **Tag** is a unit of meta-data that you can apply to an Event in order to create an additional attribute for the Event that is not originally contained within the Event itself. Tags can be used to filter Events in order to simplify the task of Event monitoring and management. A typical use of tagging is to distinguish between Events that require action and those that have been investigated and found to be benign.

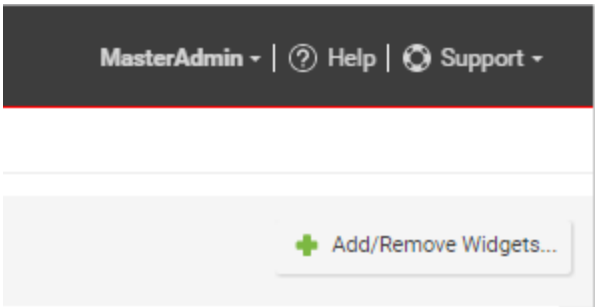
The data displayed in the Dashboard can be filtered by tags:




For more information on tagging see "Apply tags to identify and group events" on page 804.

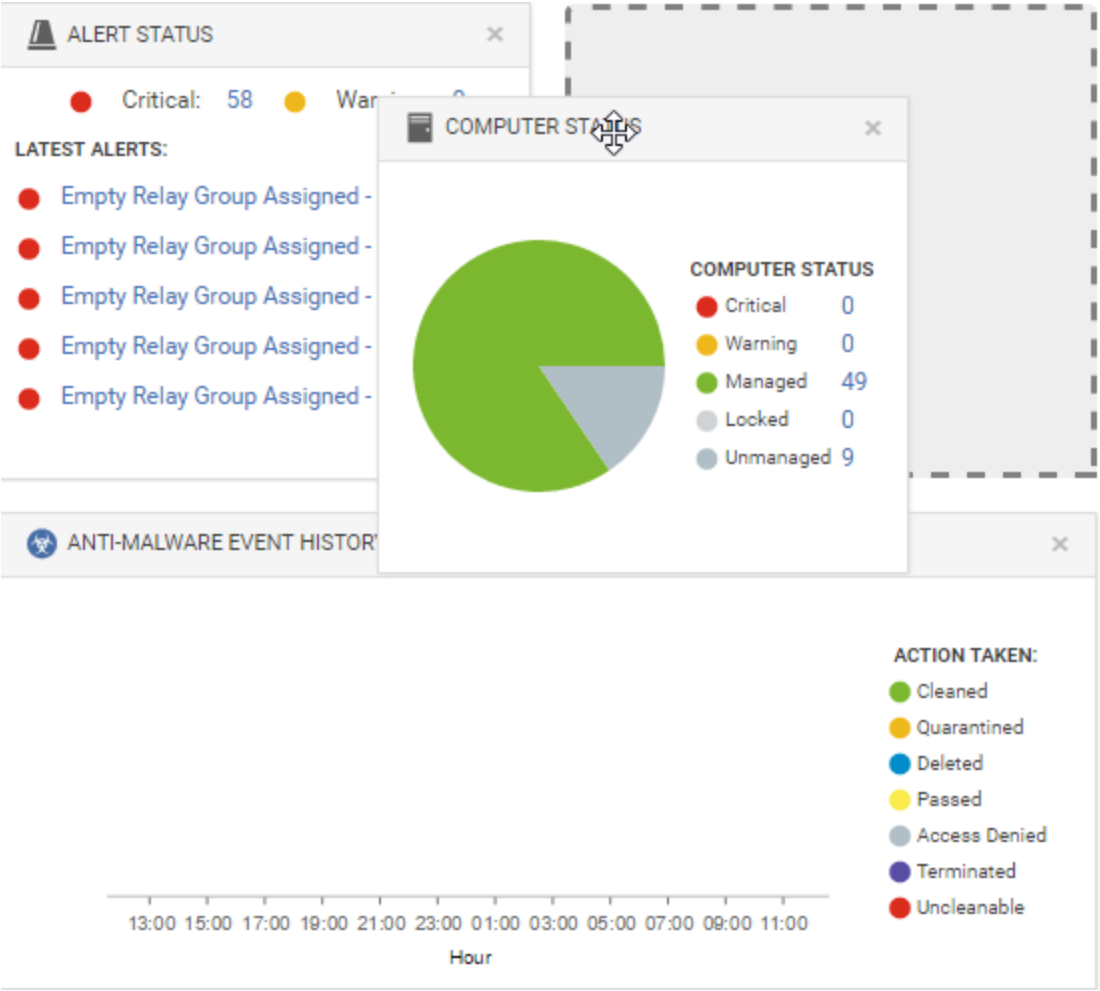
## Select dashboard widgets

Click **Add/Remove Widgets** to display the widget selection window and choose which widgets to display.



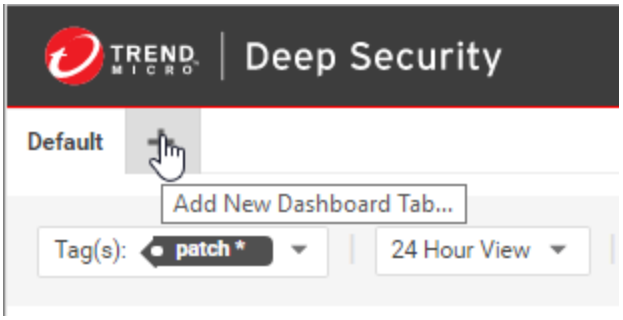

## Change the layout

The selected widgets can be moved around the dashboard by dragging them by their title bar. Move the widget over an existing one and they will exchange places. (The widget that is about to be displaced will temporarily gray out.)




## Save and manage dashboard layouts

You can create multiple dashboard layouts and save them as separate tabs. Your Dashboard settings and layouts will not be visible to other Users after you sign out. To create a new Dashboard tab, click the "plus" symbol to the right of the last tab on the Dashboard:



# Event collection in Deep Security

Deep Security Agents record when a protection module rule or condition is triggered (a "security event"). Agents and Deep Security Manager also record when administrative or system-related events occur (a "system event"), such as an administrator logging in, or agent software being upgraded. Event data is used to populate the various reports and graphs in Deep Security Manager.

To view events, go to **Events & Reports** tab in Deep Security Manager.

## Where are event logs on the agent?

Location varies by the computer's operating system. On Windows, event logs are stored in this location:

```
C:\Program Data\Trend Micro\Deep Security Agent\Diag
```

On Linux, event logs are stored here:

```
/var/opt/ds_agent/diag
```

**Note:** These locations only contain standard-level logs; diagnostic debug-level logs have a different location. For performance reasons, debug-level logging is not enabled by default. You should only enable debug logging if diagnosing an issue with Trend Micro technical support, and make sure to disable debug logging when you are done. For more information, see Enabling detailed logging on Deep Security Agent (DSA).

## When are events sent to the manager?

Most events that take place on a computer are sent to the Deep Security Manager during the next heartbeat operation except the following, which will be sent right away if communication settings allow relays/agents/appliances to initiate communication:

- Smart Scan Server is offline
- Smart Scan Server is back online
- Integrity Monitoring scan is complete

- Integrity Monitoring baseline created
- Unrecognized elements in an Integrity Monitoring Rule
- Elements of an Integrity Monitoring Rule are unsupported on the local platform
- Abnormal restart detected
- Low disk space warning
- Log Inspection offline
- Log Inspection back online
- Reconnaissance scan detected (if the setting is enabled in **Computer or Policy editor**[1] > **Firewall > Reconnaissance**

## How long are events stored?

Once collected by the Deep Security Manager, events are kept for a period of time, which is specified on the **Administration** > **System Settings** > **Storage** page. For details, see "Log and event storage best practices" on page 799.

## System events

All the Deep Security system events are listed and can be configured on the **Administration > System Settings > System Events** tab. You can set whether to record the individual events and whether to forward them to a SIEM system. For details on system events, see "System events" on page 918.

## Security events

Each protection module generates events when rules are triggered or other configuration conditions are met. Some of this security event generation is configurable. For information on specific types of security events, refer to these articles:

---

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

- "Anti-malware events" on page 942
- "View and restore identified malware" on page 526
- "Firewall events" on page 944
- "Integrity monitoring events" on page 957
- "Intrusion prevention events" on page 953
- "Log inspection events" on page 960
- "Web reputation events" on page 962


The firewall stateful configuration in effect on a computer can be modified to enable or disable TCP, UDP, and ICMP event logging. To edit the properties of a stateful firewall configuration, go to **Policies > Common Objects > Other > Firewall Stateful Configurations**. The logging options are in the **TCP**, **UDP**, and **ICMP** tabs of the firewall stateful configuration's **Properties** window. For more information about firewall events, see "Firewall events" on page 944.

## See the events associated with a policy or computer

The **Policy editor**[1] and the**Computer editor** [2]both have **Events** tabs for each protection module. The policy editor displays events associated with the current policy. The computer editor displays events specific to the current computer.

## View details about an event

To see details about an event, double-click it.

The **General** tab displays:

- **Time:** The time according to the system clock on the computer hosting the Deep Security Manager.

[1]To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).
[2]To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

- **Level:** The severity level of event that occurred. Event levels include **Info**, **Warning**, and **Error**.
- **Event ID:** The event type's unique identifier.
- **Event:** The name of the event (associated with the event ID.)
- **Target:** The system object associated with the event will be identified here. Clicking the object's identification will display the object's properties sheet.
- **Event Origin:** The Deep Security component from which the event originated.
- **Action Performed By:** If the event was initiated by a user, that user's username will be displayed here. Clicking the username will display the **User Properties** window.
- **Manager:** The hostname of the Deep Security Manager computer.
- **Description:** If appropriate, the specific details of what action was performed to trigger this event are displayed here.

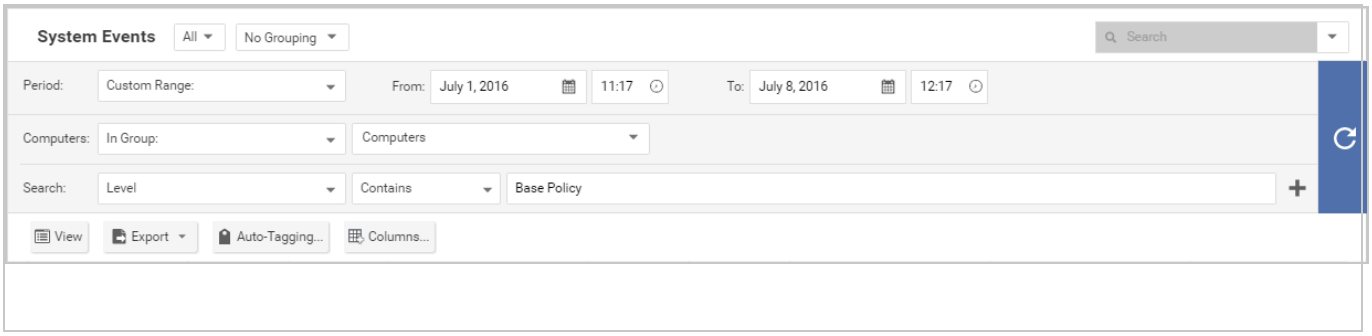
The **Tags** tab displays tags that have been attached to this event. For more information on event tagging, see **Policies > Common Objects > Other > Tags**, and "Apply tags to identify and group events" on page 804.

## Filter the list to search for an event

The **Period** toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The **Computers** toolbar lets you organize the display of event log entries by computer groups or computer policies.

Clicking **Search > Open Advanced Search** toggles the display of the advanced search bar.



Clicking the "Add Search Bar" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the "Submit Request" button (at the right of the toolbars with the right-arrow on it).

## Export events

You can export displayed events to a CSV file. (Paging is ignored, all pages will be exported.) You have the option of exporting the displayed list or the selected items.

## Improve logging performance

Here are some suggestions to help maximize the performance of event collection:

- Reduce or disable log collection for computers that are not of interest.
- Consider reducing the logging of firewall rule activity by disabling some logging options in the firewall stateful configuration **Properties** window. For example, disabling the UDP logging will eliminate the "Unsolicited UDP" log entries.

## Log and event storage best practices

Best practices for log and event data storage depend on the data compliance regulations you must meet, such as PCI and HIPAA. Also consider optimizing the use of your database. Storing too much data may affect database performance and size requirements.

If you're storing too much data in your database, these symptoms may occur:

- Error messages that systems may be experiencing loss of database activity
- Inability to import software updates
- General slow-down in Deep Security

To avoid those symptoms:

1. Store system events according to the compliance standard requirement.
2. Forward system and security events to external storage. See "Forward Deep Security

events to an external syslog or SIEM server " on page 814. Then you can reduce how long events are kept in the local database.

3. Set thresholds in the log inspection module for event storage or event forwarding. **Severity clipping** allows you to send events to a Syslog server (if enabled) or to store events based on the severity level of the log inspection rule. See "Configure log inspection event forwarding and storage" on page 695.

Default local storage settings are in the table below. To change these settings, go to **Administration > System Settings > Storage**. To delete software versions or older rule updates, go to **Administration > Updates > Software > Local or Administration > Updates > Security > Rules**.

**Tip:** To reduce database disk space usage, forward events to an external Syslog server or SIEM and reduce the local event retention time. Only keep counters locally.

| Data type settings | Data pruning default setting |
|---|---|
| Automatically delete Anti-Malware Events older than | 7 Days |
| Automatically delete Web Reputation Events older than: | 7 Days |
| Automatically delete Firewall Events older than: | 7 Days |
| Automatically delete Intrusion Prevention Events older than: | 7 Days |
| Automatically delete Integrity Monitoring Events older than: | 7 Days |
| Automatically delete Log Inspection Events older than: | 7 Days |
| Automatically delete Application Control Events older than: | 7 Days |
| Automatically delete System Events older than: | 13 Weeks |
| Automatically delete Server Logs older than: | 7 Days |
| Automatically delete Counters older than: | 13 Weeks |
| Number of older software versions to keep per platform:* | 5 |
| Number of older Rule Updates to keep: | 10 |

* If multi-tenancy is enabled, this setting will not be available.

> **Note:** If using a PostgreSQL database, old events might not be pruned immediately. PostgreSQL maintenance jobs periodically remove the old events' database partitions. Pruning will occur during the next scheduled job.

*Events* are records of individual events. They populate the **Events** pages.

*Counters* are the number of times individual events have occurred. They populate the dashboard widgets (number of firewall events over the last 7 days, etc.) and the reports.

*Server log files* are from Deep Security Manager's web server. They don't include event logs from agents installed on your network's web servers.

## Troubleshooting

During troubleshooting, it may be useful to increase the logging level and record more detailed events.

Increased logging can significantly increase disk space usage. Reduce the logging level again when you have finished troubleshooting.

1. Open the **Computer or Policy editor**[1].
2. Go to **Settings > General > Logging Level**.
3. Choose whether to inherit the logging override settings from the policy assigned to this computer (**Inherited**), to not override logging settings (**Do Not Override**), to log all triggered firewall rules (**Full Firewall Event Logging**), to log all triggered intrusion prevention rules (**Full Intrusion Prevention Event Logging**), or to log all triggered rules (**Full Logging**).
4. Click **Save** .

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

## Limit log file sizes

You can set the maximum size of each individual log file and how many of the most recent files are kept. Event log files will be written to until they reach the maximum allowed size, at which point a new file will be created and written to until it reaches the maximum size and so on. Once the maximum number of files is reached, the oldest will be deleted before a new file is created. Event log entries usually average around 200 bytes in size and so a 4 MB log file will hold about 20,000 log entries. How quickly your log files fill up depends on the number of rules in place.

1. Open the **Computer or Policy editor**[1] for the policy that you want to configure.
2. Go to **Settings > Advanced > Events**.
3. Configure these properties:
   - **Maximum size of the event log files (on Agent/Appliance):** Maximum size that the log file can reach before a new log file is created.
   - **Number of event log files to retain (on Agent/Appliance):** Maximum number of log files that will be kept. Once the maximum number of log files is reached, the oldest file will be deleted before a new one is created.
   - **Do Not Record Events with Source IP of:** This option is useful if you don't want Deep Security to make record events for traffic from certain trusted computers.

     **Note:** The following three settings let you fine tune event aggregation. To save disk space, Deep Security Agents and Appliances will take multiple occurrences of identical events and aggregate them into a single entry and append a "repeat count", a "first occurrence" timestamp, and a "last occurrence" timestamp. To aggregate event entries, Deep Security Agents and Appliances need to cache the entries in memory and then write them to disk.

   - **Cache Size:** Determines how many types of events to track at any given time. Setting a value of 10 means that 10 types of events will be tracked (with a repeat count, first

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

occurrence timestamp, and last occurrence timestamp). When a new type of event occurs, the oldest of the 10 aggregated events will be flushed from the cache and written to disk.

- **Cache Lifetime:** Determines how long to keep a record in the cache before flushing it to disk. If this value is 10 minutes and nothing else causes the record to be flushed, any record that reaches an age of 10 minutes gets flushed to disk.
- **Cache Stale time:** Determines how long to keep a record whose repeat count has not been recently incremented. If Cache Lifetime is 10 minutes and Cache Staletime is two minutes, an event record which has gone two minutes without being incremented will be flushed and written to disk.

> **Note:** Regardless of the above settings, the cache is flushed whenever events are sent to the Deep Security Manager.

4. Click **Save**.

## Event logging tips

- On computers that are less important, modify the amount of logs collected. This can be done in the **Events** and **Advanced Network Engine Options** areas on the **Computer or Policy editor**[1] > **Settings** > **Advanced** tab.
- Consider reducing the event logging of firewall rule activity by disabling the event logging options in the firewall stateful configuration. (For example, if you disable UDP logging, it will eliminate unsolicited UDP log entries.)
- For intrusion prevention rules, the best practice is to log only dropped packets. If you log packet modifications, it may cause too many log entries.
- For intrusion prevention rules, only include packet data (an option in the intrusion prevention rule's **Properties** window) when you are interested in examining the behavior of a specific attack. Packet data increases log sizes, so it shouldn't be used for everything.

---

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

# Apply tags to identify and group events

Deep Security enables you to create tags that you can use to identify and sort events. For example, you might use tags to separate events that are benign from those that require further investigation. You can use tags to create customized dashboards and reports.

Although you can use event tagging for a variety of purposes, it was designed to ease the burden of event management. After you have analyzed an event and determined that it is benign, you can look through the event logs of the computer (and any other similarly configured and tasked computers) to find similar events and apply the same label to them, eliminating the need to analyze each event individually.

To view tags that are currently in use, go to **Policies > Common Objects > Other > Tags**.

**Note:** Tags do not alter the data in the events themselves, nor do they allow users to delete events. They are simply extra attributes provided by the manager.

You can perform tagging the following ways:

- "Manual tagging" below lets you tag specific events as needed.
- "Auto-tagging" on the next page lets you use an existing event as the model for auto-tagging similar events on the same or other computers. You define the parameters for "similarity" by selecting which event attributes have to match the model event attributes for a tag to be applied.
- "Trusted source tagging" on page 807 lets you auto-tag integrity monitoring events based on their similarity to known-good events from a trusted source.

**Note:** An important difference between standard tagging and trusted source tagging is that "Run on Existing Events Now" can only be done with standard event tagging

## Manual tagging

1. Go to **Events & Reports > Events** and select an event list. Right-click the event (or select multiple events and right-click) and select **Add Tag(s)**.

2. Type a name for the tag. Deep Security Manager will suggest matching names of existing tags as you type.
3. Select **The Selected [Event Type] Event**. Click **Next**.
4. Enter some optional comments and click **Finish**.

In the events list, you can see your tag in the **TAG(S)** column.

## Auto-tagging

Deep Security Manager enables you to define rules that apply the same tag to similar events automatically. To view existing saved auto-tagging rules, click **Auto-Tagging** in the menu bar on any **Events** page. You can run saved rules manually from this page.

1. Go to **Events & Reports > Events** and select an event list. Right-click a representative event and select **Add Tag(s)**.
2. Type a name for the tag. Deep Security Manager will suggest matching names of existing tags as you type.
3. Select **Apply to selected and similar [Event Type] Events** and click **Next**.
4. Select the computers where you want to auto-tag events and click **Next**. When applying tags to system events, this page is skipped.
5. Select which attributes will be examined to determine whether events are similar. For the most part, the attribute options are the same as the information displayed in the columns of the **Events** list pages. When you have selected which attributes to include in the event selection process, click **Next**.
6. On the next page, specify when events should be tagged. If you select **Existing [Event Type] Events**, you can select **Apply Auto-Tag Rule now** to apply the auto-tagging rule immediately, or **Apply Auto-Tag Rule in the background** to have it run in the background at a lower priority. Select **Future [Event Type] Events** to apply the auto-tagging rule to events that will happen in the future. You can also save the auto-tagging rule by selecting **Save Auto-Tag Rule** and optionally entering a name. Click **Next**.
7. Review the summary of your auto-tagging rule and click **Finish**.

In the events list, you can see that your original event and all similar events have been tagged

**Note:** Event tagging only occurs after events have been retrieved from the agents or appliances to the Deep Security Manager database.

## Set the precedence for an auto-tagging rule

Once an auto-tagging rule is created, you can assign it a **Precedence** value. If the auto-tagging rule has been configured to run on future events, the rule's precedence determines the order in which all auto-tagging rules are applied to incoming events. For example, you can have a rule with a precedence value of "1" that tags all "User Signed In" events as "suspicious", and a rule with a precedence value of "2" that removes the "suspicious" tag from all "User Signed In" events where the target (user) is you. This will result in a "suspicious" tag being applied to all future "User Signed In" events where the user is not you.

1. In an events list, click **Auto-Tagging** to display a list of saved auto-tagging rules.
2. Right-click an auto-tagging rule and select **Details**.
3. In the **General** tab, select a **Precedence** for the rule.

## Auto-tagging log inspection events

Log inspection events are auto-tagged based upon their grouping in the log file structure. This simplifies and automates the processing of log inspection events within Deep Security Manager. You can use auto-tagging to automatically apply tags for the log inspection groups. Log inspection rules have groups associated with them in the rules. For example:

```
<rule id="18126" level="3">
 <if_sid>18101</if_sid>
 <id>^20158</id>
 <description>Remote access login success</description>
 <group>authentication_success,</group>
 </rule>

 <rule id="18127" level="8">
 <if_sid>18104</if_sid>
 <id>^646|^647</id>
 <description>Computer account changed/deleted</description>
<group>account_changed,</group>
 </rule>
```

Each group name has a "friendly" name string associated with it. In the above example, "authentication_success" would be "Authentication Success", "account_changed" would be

"Account Changed". When this checkbox is set, the friendly names are automatically added as a tag for that event. If multiple rules trigger, multiple tags will be attached to the event.

## Trusted source tagging

**Note:** Trusted source event tagging can only be used with events generated by the integrity monitoring protection module.

The integrity monitoring module allows you to monitor system components and associated attributes on a computer for changes. ("Changes" include creation and deletion as well as edits.) Among the components that you can monitor for changes are files, directories, groups, installed software, listening port numbers, processes, registry keys, and so on.

Trusted source event tagging is designed to reduce the number of events that need to be analyzed by automatically identifying events associated with authorized changes.

In addition to auto-tagging similar events, the integrity monitoring module allows you to tag events based on their similarity to events and data found on **Trusted Sources**. A trusted source can be either:

1. A **local trusted computer**,
2. The **Trend Micro Certified Safe Software Service**, or
3. A **trusted common baseline**, which is a set of file states collected from a group of computers.

### Local trusted computer

A trusted computer is a computer that will be used as a "model" computer that you know will only generate benign or harmless events. A "target" computer is a computer that you are monitoring for unauthorized or unexpected changes. The auto-tagging rule examines events on target computers and compares them to events from the trusted computer. If any events match, they are tagged with the tag defined in the auto-tagging rule.

You can establish auto-tagging rules that compare events on protected computers to events on a trusted computer. For example, a planned rollout of a patch can be applied to the trusted computer. The events associated with the application of the patch can be tagged as "Patch X".

Similar events raised on other systems can be auto-tagged and identified as acceptable changes and filtered out to reduce the number of events that need to be evaluated.

## How does Deep Security determine whether an event on a target computer matches an event on a trusted source computer?

Integrity monitoring events contain information about transitions from one state to another. In other words, events contain *before* and *after* information. When comparing events, the auto-tagging engine will look for matching before and after states; if the two events share the same before and after states, the events are judged to be a match and a tag is applied to the second event. This also applies to creation and deletion events.

**Note:** Remember that when using a trusted computer for trusted source event tagging, the events being tagged are events generated by integrity monitoring rules. This means that the integrity monitoring rules that are generating events on the target computer must also be running on the trusted source computer.

**Note:** Trusted source computers must be scanned for malware before applying trusted source event tagging.

**Note:** Utilities that regularly make modifications to the content of files on a system (prelinking on Linux, for example) can interfere with trusted source event tagging.

## Tag events based on a local trusted computer

1. Make sure the trusted computer is free of malware by running a full anti-malware scan.
2. Make sure the computer(s) on which you want to auto-tag events are running the same (or some of the same) integrity monitoring rules as the trusted source computer.
3. In Deep Security Manager, go to **Events & Reports > Integrity Monitoring Events** and click **Auto-Tagging** in the toolbar.
4. In the **Auto-Tag Rules (Integrity Monitoring Events)** window, click **New Trusted Source** to display the **Tag Wizard**.
5. Select **Local Trusted Computer** and click **Next**.
6. From the list, select the computer that will be the trusted source and click **Next**.
7. Specify one or more tags to apply to events on target computers when they match events on this trusted source computer. Click **Next**.

> **Note:** You can enter the text for a new tag or select from a list of existing tags.

8. Identify the target computers whose events will be matched to those of the trusted source. Click **Next**.
9. Optionally, give the rule a name and click **Finish**.

### Tag events based on the Trend Micro Certified Safe Software Service

The Certified Safe Software Service is an allow of known-good file signatures maintained by Trend Micro. This type of trusted source tagging will monitor target computers for file-related integrity monitoring events. When an event has been recorded, the file's signature (after the change) is compared to Trend Micro's list of known good file signatures. If a match is found, the event is tagged.

1. In Deep Security Manager, go to **Events & Reports > Integrity Monitoring Events** and click **Auto-Tagging** in the toolbar.
2. In the **Auto-Tag Rules (Integrity Monitoring Events)** window, click **New Trusted Source** to display the **Tag Wizard**.
3. Select **Certified Safe Software Service** and click **Next**.
4. Specify one or more tags to apply to events on target computers when they match the Certified Safe Software Service. Click **Next**.
5. Identify the target computers whose events will be matched to the Certified Safe Software Service. Click **Next**.
6. Optionally, give the rule a name and click **Finish**.

### Tag events based on a trusted common baseline

The trusted common baseline method compares events within a group of computers. A group of computers is identified and a common baseline is generated based on the files and system states targeted by the integrity monitoring rules in effect on the computers in the group. When an integrity monitoring event occurs on a computer within the group, the signature of the file after the change is compared to the common baseline. If the file's new signature has a match elsewhere in the common baseline, a tag is applied to the event. In trusted computer method, the before and after states of an integrity monitoring event are compared, but in the trusted common baseline method, only the after state is compared.

**Note:** This method relies on all the computers in the common group being secure and free of malware. A full anti-malware scan should be run on all the computers in the group before the common baseline is generated.

**Note:** When an integrity monitoring baseline is generated for a computer, Deep Security will first check if that computer is part of a trusted common baseline group. If it is, it will include the computer's baseline data in the trusted common baseline for that group. For this reason, the trusted common baseline auto-tagging rule must be in place before any integrity monitoring rules have been applied to the computers in the common baseline group.

1. Make sure all the computers that will be in the group that will make up the trusted common baseline are free of malware by running a full anti-malware scan on them.
2. In Deep Security Manager, go to **Events & Reports > Integrity Monitoring Events** and click **Auto-Tagging** in the toolbar.
3. In the **Auto-Tag Rules (Integrity Monitoring Events)** window, click **New Trusted Source** to display the **Tag Wizard**.
4. Select **Trusted Common Baseline** and click **Next**.
5. Specify one or more tags to apply to events when they have a match in the trusted common baseline and click **Next**.
6. Identify the computers to include in the group used to generate the trusted common baseline. Click **Next**.
7. Optionally, give this rule a name and click **Finish**.

### Delete a tag

1. In an events list, right-click the events with the tag you want to delete, and select **Remove Tag(s)**.
2. Select the tag you'd like to remove. Choose to remove the tag from **The Selected [Event Type] Event** or to **Apply to selected similar [Event Type] Events.** Click **Next**.
3. Enter some optional comments and click **Finish**.

## Reduce the number of logged events

To reduce the number of events being logged, the Deep Security Manager can be configured to operate in one of several **Advanced Logging Policy** modes. These modes are set in the

**Computer or Policy editor**[1] on the **Settings > Advanced > Advanced Network Engine Settings** area.

The following table lists the types of events that are ignored in four of the more complex Advanced Logging Policy modes:

| Mode | Ignored Events |
|---|---|
| **Stateful and Normalization Suppression** | Out Of Connection<br>Invalid Flags<br>Invalid Sequence<br>Invalid ACK<br>Unsolicited UDP<br>Unsolicited ICMP<br>Out Of Allowed Policy<br>Dropped Retransmit |
| **Stateful, Normalization, and Frag Suppression** | Out Of Connection<br>Invalid Flags<br>Invalid Sequence<br>Invalid ACK<br>Unsolicited UDP<br>Unsolicited ICMP<br>Out Of Allowed Policy<br>CE Flags<br>Invalid IP<br>Invalid IP Datagram Length<br>Fragmented<br>Invalid Fragment Offset<br>First Fragment Too Small<br>Fragment Out Of Bounds<br>Fragment Offset Too Small<br>IPv6 Packet<br>Max Incoming Connections<br>Max Outgoing Connections<br>Max SYN Sent<br>License Expired<br>IP Version Unknown<br>Invalid Packet Info<br>Maximum ACK Retransmit<br>Packet on Closed Connection<br>Dropped Retransmit |

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| Mode | Ignored Events |
| --- | --- |
| **Stateful, Frag, and Verifier Suppression** | Out Of Connection<br>Invalid Flags<br>Invalid Sequence<br>Invalid ACK<br>Unsolicited UDP<br>Unsolicited ICMP<br>Out Of Allowed Policy<br>CE Flags<br>Invalid IP<br>Invalid IP Datagram Length<br>Fragmented<br>Invalid Fragment Offset<br>First Fragment Too Small<br>Fragment Out Of Bounds<br>Fragment Offset Too Small<br>IPv6 Packet<br>Max Incoming Connections<br>Max Outgoing Connections<br>Max SYN Sent<br>License Expired<br>IP Version Unknown<br>Invalid Packet Info<br>Invalid Data Offset<br>No IP Header<br>Unreadable Ethernet Header<br>Undefined<br>Same Source and Destination IP<br>Invalid TCP Header Length<br>Unreadable Protocol Header<br>Unreadable IPv4 Header<br>Unknown IP Version<br>Maximum ACK Retransmit<br>Packet on Closed Connection<br>Dropped Retransmit |
| **Tap Mode** | Out Of Connection<br>Invalid Flags<br>Invalid Sequence<br>Invalid ACK<br>Maximum ACK Retransmit<br>Packet on Closed Connection<br>Dropped Retransmit |

# Rank events to quantify their importance

The ranking system provides a way to quantify the importance of events. By assigning "asset values" to computers, and assigning severity or risk values to rules, the importance ("rank") of an event is calculated by multiplying the two values together. This allows you to sort events by rank.

## Web reputation event risk values

Risk values for web reputation events are linked to the three levels of risk used by the web reputation settings on the **General** tab of the **Web Reputation** page:

- **Dangerous:** corresponds to "A URL that has been confirmed as fraudulent or a known source of threats."
- **Highly Suspicious:** corresponds to "A URL that is suspected to be fraudulent or a known source of threats."
- **Suspicious:** corresponds to "A URL that is associated with spam or possibly compromised."
- **Blocked by Administrator:** A URL that is on the Web Reputation Service **Blocked** list.
- **Untested:** A URL that does not have a risk level.

## Firewall rule severity values

Severity values for firewall rules are linked to their actions: Deny, Log Only, and Packet Rejection. (The latter refers to packets rejected because of a firewall stateful configuration setting.) Use this panel to edit the severity values which will be multiplied by a computer's asset value to determine the rank of a firewall event. (A firewall rule's actions can be viewed and edited in the rule's **Properties** window.)

## Intrusion prevention rule severity values

Intrusion prevention rule severity values are linked to their severity levels: Critical, High, Medium, Low, or Error. Use this panel to edit their values which will be multiplied by a computer's asset value to determine the rank of an intrusion prevention event. An intrusion prevention rule's severity setting can be viewed in the rule's **Properties** window.

### Integrity monitoring rule severity values

Integrity monitoring rule severity values are linked to their severity levels: Critical, High, Medium, or Low. Use this panel to edit their values which will be multiplied by a computer's asset value to determine the rank of an integrity monitoring event. An integrity monitoring rule's severity can be viewed in the rule's **Properties** window.

### Log inspection rule severity values

Log inspection rule severity values are linked to their severity levels: Critical, High, Medium, or Low. Use this panel to edit their values which will be multiplied by a computer's asset value to determine the rank of a log inspection event. A log inspection rule's severity level can be viewed and edited from the rule's **Properties** window.

### Asset values

Asset values are not associated with any of their other properties like intrusion prevention rules or firewall rules. Instead, asset values are properties in themselves. A computer's asset value can be viewed and edited from the computer's **Details** window. To simplify the process of assigning asset values, you can predefine some values that will appear in the **Asset Importance** list in the first page of the computer's **Details** window. To view existing predefined computer asset values, click the **View Asset Values** button in this panel. The **Asset Values** window displays the predefined settings. These values can be changed, and new ones can be created. (New settings will appear in the list for all computers.)

## Forward Deep Security events to an external syslog or SIEM server

**Note:** If you want to publish events to Amazon SNS, see "Access events with Amazon SNS" on page 864.

Deep Security records two types of events:

- **System events:** Administrative or system-related events such as an administrator logging in or agent software being upgraded. These events are generated by the Deep Security Manager.
- **Security events:** Recorded when a protection module rule or condition is triggered. These events are generated by the Deep Security Agent.

You can configure Deep Security to forward both types of events to an external syslog or Security Information and Event Management (SIEM) server. The content and format of the log messages differs slightly depending on whether they are sent by the Deep Security Manager or from an agent computer. For more information on the format, see "Syslog message formats" on page 821

The two different types of events that can be forwarded have to be configured separately:

- "Forward system events to a syslog or SIEM server" below
- "Forward security events to a syslog or SIEM server" on the next page

**Note:** Deep Security still records all system and security events and display them in reports and graphs in the Deep Security Manager even if you enable event forwarding to a syslog or SIEM server.

**Tip:** If you are using Splunk as your syslog or SIEM server, consider using the Deep Security app for Splunk, which provides dashboards and saved searches.

## Forward system events to a syslog or SIEM server

1. Go to **Administration > System Settings > Event Forwarding**.
2. In the **Forward System Events to a remote computer (via Syslog) using configuration** list, select an existing syslog configuration or select **New** and define a new configuration (for details, see "Define a syslog configuration" on page 817.)
3. Click **Save**.

## Forward security events to a syslog or SIEM server

Security events are generated by the agents for each protection module. You have two options for forwarding these types of events:

- "Forward security events directly from agent computers to a syslog or SIEM server" below
- "Forward security events from the agent computers via the Deep Security Manager" on the next page

If you want to use TLS to send secure syslog messages, they must be sent via the Deep Security Manager. Syslog messages sent directly from the agent use UDP and are sent as clear text.

**Note:** The best practice is to use a high-level parent policy to propagate configuration settings throughout your environment. Like with other settings in Deep Security, you can override event forwarding settings for specific policies or computers (see "Policies, inheritance, and overrides" on page 354.)

### Forward security events directly from agent computers to a syslog or SIEM server

1. Go to **Policies**.
2. Double-click the policy you want to use for computers to forward events directly to a syslog server.
3. Go to **Settings > Event Forwarding**.
4. Under **Event Forwarding Frequency (from the Agent/Appliance)**, specify how often events are sent from the agent or appliance to the syslog or SIEM server.
5. Under **Event Forwarding Configuration (from the Agent/Appliance)**, specify the syslog configuration to use for each protection module. The options are:
   - Inherited (*configuration name*): The behavior is being inherited from a parent policy or computer
   - None: Events are not forwarded
   - *Syslog configuration name*: Events are forwarded to the specified syslog configuration. To see details about the configuration or edit it, click **Edit**. The configuration must have **Transport** set to "UDP" and **Agents should forward logs** set to "Directly to the Syslog server".

- New: Enables you to define a new configuration (for details, see "Define a syslog configuration" below.) The configuration must have **Transport** set to "UDP" and **Agents should forward logs** set to "Directly to the Syslog server".

6. Click **Save.**

### Forward security events from the agent computers via the Deep Security Manager

When you choose to forward events via the Deep Security Manager, the manager collects the events at every heartbeat (**Settings > General > Heartbeat Interval**.)

1. Go to **Policies**.
2. Double-click the policy you want to use for computers to forward security events via the Deep Security Manager.
3. Go to **Settings > Event Forwarding**.
4. Under **Event Forwarding Configuration (from the Agent/Appliance)**, specify the syslog configuration to use for each protection module. The options are:
   - Inherited (*configuration name*): The behavior is being inherited from a parent policy or computer
   - None: Events are not forwarded
   - *Syslog configuration name*: Events are forwarded to the specified syslog configuration. To see details about the configuration or edit it, click **Edit**. The configuration must have **Agents should forward logs** set to "Via the Deep Security Manager".
   - New: Enables you to define a new configuration (for details, see "Define a syslog configuration" below.) The configuration must have **Agents should forward logs** set to "Via the Deep Security Manager".
5. Click **Save.**

## Define a syslog configuration

You can define a syslog configuration and assign it to system events, security events, or both. You can define as many syslog configurations as you need.

To see any existing syslog configurations, go to **Policies > Common Objects > Other > Syslog Configurations**. From that page, you can add or edit configurations. You can also import and export configurations.

**Note:** If you configured syslog or SIEM server settings prior to January 26th, 2017, they have been converted to syslog configurations and appear on the **Syslog Configurations** page. Any identical configurations are merged together.

To add a new configuration:

1. Click **New > New Configuration**.
2. On the **General** tab:
   - **Name:** Meaningful name that identifies the configuration. The name must be unique.
   - **Description:** Optional description of the configuration.
   - **Log Source Identifier**: When syslog messages are sent to a syslog or SIEM server, they include a reported hostname that identifies the source of the messages. If you leave the Log Source Identifier setting empty and you are running a multi-node Deep Security Manager, each node sends a different hostname as the identifier. If you want to use the same identifier for each manager node (to treat the syslog messages as if they all come from the same source), you can specify a common Log Source Identifier. Note that syslog messages sent directly from the Deep Security Agent to a syslog or SIEM server use the reported computer hostname and cannot use the Log Source Identifier instead.
   - **Server Name:** Hostname or IP address to which events should be sent. The syslog or SIEM server and any routers, firewalls, and security groups must allow inbound traffic from the Deep Security Manager for event forwarding to work.

     **Note:** If you are going to forward events directly from the Deep Security Agent, traffic from the agent must also be allowed.

   - **Server Port:** UDP or TLS port to which events should be sent. For UDP, this is usually port 514. For TLS, it's usually port 6514. For more information, see "Port numbers" on page 96.
   - **Event Format:** The format of the log message. For more information on formats, see "Syslog message formats" on page 821

> **Note:** The LEEF format is only supported for messages sent from the Deep Security Manager. Basic Syslog format is not supported by the anti-malware, web reputation, integrity monitoring, and application control protection modules.

- **Transport:** UDP or TLS. Security events sent directly from the agent must be sent with UDP. System events and security events sent via the manager can be sent via UDP or TLS (which is the newer version of SSL). If you select UDP, the events are sent in clear text. If you select TLS, the events are sent encrypted over TLS 1.2, 1.1, or 1.0. (TLS is not supported as a transport mode when operating in FIPS mode. See "FIPS 140-2 support" on page 1049.) Syslog messages are limited to 64 KB if they are transferred over UDP. If the message is longer, data may be truncated.
- **Facility:** The type of program or process that is logging the message.
- **Agents should forward logs:** This setting applies when forwarding security events. You can choose to send the syslog messages **Directly to the Syslog server** or **Via the Deep Security Manager**.

> **Note:** When either LEEF or TLS is selected, this option is hard-coded to **Via the Deep Security Manager**.

3. If you selected TLS as the transport mechanism, perform these additional steps:

   - If your syslog or SIEM server is configured to require TLS client authentication, you'll need to provide the Deep Security Manager's TLS certificate. Do the following: Click the **Credentials** tab and supply the Deep Security Manager certificate's **Private Key**, **Certificate**, and **Certificate Chain** (if required) in PEM format (also known as base64 encoded format).The syslog or SIEM server may or may not accept a self-signed certificate. Consult its documentation for details.

   - Click **Test Connection**.

   - An **Accept Server Certificate?** message appears if the syslog or SIEM server certificate is not yet known to Deep Security Manager. The message shows the contents of the certificate. Review it and click **OK**. The certificate is added to the

manager's Deep Security list, under **Administration > System Settings > Security**. Deep Security Manager accepts self-signed certificates as long as they pass standard validation such as expiry checks.

- Click **Test Connection** again to establish a TLS connection using the certificate you just accepted. (See this article on the TLS handshake for details on how the TLS session is established.) You see a pass or fail message at the top of the manager.

## Troubleshooting

### "Failed to Send Syslog Message" alert

If there is a problem with your syslog configuration, you might see this alert:

```
Failed to Send Syslog Message
The Deep Security Manager was unable to forward messages to a Syslog Server.
Unable to forward messages to a Syslog Server
```

The alert also contains a link to the affected syslog configuration. Click the link to open the configuration and then click the **Test Connection** button to get more troubleshooting information. An indication that the connection was successful or an error message that provides more detailed information on what's causing the problem is displayed.

### Can't edit syslog configurations

If you can see the syslog configurations but can't edit them, the role associated with your account might not have the appropriate rights. An administrator who is able to configure roles can check your rights by going to **Administration > User Management**. Then select your name and click **Properties**. On the **Other Rights** tab, the **Syslog Configurations** setting controls your ability to edit syslog configurations. For more information on users and roles, see "Create and manage users" on page 989.

### Can't see the syslog configuration sections of Deep Security Manager

If you can't see the syslog configurations UI in Deep Security Manager, you may be a tenant in a multi-tenant environment where the primary tenant has disabled this feature or configured it for you.

### Syslog not transferred due to an expired certificate

If you set up TLS client authentication and the certificate expires, syslog messages are not sent to the syslog server. To fix this problem, obtain a new certificate, update the syslog configuration with the new certificate values, test the connection, and then save the configuration.

### Syslog not delivered due to an expired or changed server certificate

If the syslog server's certificate has expired or changed, open the syslog configuration and click the **Test Connection** button. You are prompted to accept the new certificate.

## Syslog or SIEM servers used for testing

Deep Security has been tested with the Enterprise version of these products:

- Splunk 6.5.1
- IBM QRadar 7.2.8 Patch 3 (with the TLS protocol patch, PROTOCOL-TLSSyslog-7.2-20170104125004.noarch)
- HP ArcSight 7.2.2 (with a TLS Syslog-NG connector created using the ArcSight-7.2.2.7742.0-Connector tool)

## Syslog message formats

Common Event Format (CEF) and Log Event Extended Format (LEEF) log message formats are slightly different. For example, the "Source User" column in the GUI corresponds to a field named "suser" in CEF; in LEEF, the same field is named "usrName" instead. Log message fields also vary by whether the event originated on the agent or Deep Security Manager and which feature created the log message.

**Note:** If your syslog messages are being truncated, it may be because you're using User Datagram Protocol (UDP). To prevent truncation, transfer your syslog messages over Transport Layer Security (TLS) instead. For instructions on switching to TLS, see "Define a syslog configuration" on page 817.

**Note:** Basic syslog format is not supported by the anti-malware, web reputation, integrity monitoring, and application control protection modules.

If the syslog messages are sent from the Manager, there are several differences. In order to preserve the original hostname (the source of the event), a new extension ("dvc" or "dvchost") is present. "dvc" is used if the hostname is an IPv4 address; "dvchost" is used for hostnames and IPv6 addresses. Additionally, the extension "TrendMicroDsTags" is used if the events are tagged (This applies only to auto-tagging with run on future, since events are forwarded via syslog only as they are collected by the manager). The product for logs relayed through the Manager will still read " Deep Security Agent"; however, the product version is the version of the Manager.

## CEF syslog message format

All CEF events include dvc=IPv4 Address or dvchost=Hostname (or the IPv6 address) for the purposes of determining the original source of the event. This extension is important for events sent from a virtual appliance or the manager, since in this case the syslog sender of the message is not the originator of the event.

**Base CEF format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

To determine whether the log entry comes from the Deep Security Manager or a Deep Security Agent, look at the "Device Product" field:

**Sample CEF Log Entry:** Jan 18 11:07:53 dsmhost CEF:0|Trend Micro|**Deep Security Manager**|<DSM version>|600|Administrator Signed In|4|suser=Master...

> **Note:** Events that occur on a VM that is protected by a virtual appliance, but that don't have an in-guest agent, will still be identified as coming from an agent.

To further determine what kind of rule triggered the event, look at the "Signature ID" and "Name" fields:

**Sample Log Entry:** Mar 19 15:19:15 root CEF:0|Trend Micro|Deep Security Agent|<DSA version>|**123**|**Out Of Allowed Policy**|5|cn1=1...

The "Signature ID" value indicates what kind of event has been triggered:

| Signature IDs | Description |
|---|---|
| 10 | Custom intrusion prevention (IPS) rule |

| Signature IDs | Description |
|---|---|
| 20 | Log-only firewall rule |
| 21 | Deny firewall rule |
| 30 | Custom integrity monitoring rule |
| 40 | Custom log inspection rule |
| 100-7499 | System events |
| 100-199 | Policy firewall rule and firewall stateful configuration |
| 200-299 | IPS internal errors |
| 300-399 | SSL/TLS events |
| 500-899 | IPS normalization |
| 1,000,000-1,999,999 | Trend Micro IPS rule. The signature ID is the same as the IPS rule ID. |
| 2,000,000-2,999,999 | Integrity monitoring rule. The signature ID is the integrity monitoring rule ID + 1,000,000. |
| 3,000,000-3,999,999 | Log inspection rule. The signature ID is the log inspection rule ID + 2,000,000. |
| 4,000,000-4,999,999 | Anti-malware events. Currently, only these signature IDs are used:<br>• 4,000,000<br>• 4,000,001<br>• 4,000,002<br>• 4,000,003<br>• 4,000,010<br>• 4,000,011<br>• 4,000,012<br>• 4,000,013<br>• 4,000,020<br>• 4,000,030 |
| 5,000,000-5,999,999 | Web reputation events. Currently, only these signature IDs are used:<br>• 5,000,000<br>• 5,000,001 |
| 6,000,000-6,999,999 | Application control events. Currently, only these signature IDs are used:<br>• 6,001,100<br>• 6,001,200<br>• 6,002,100<br>• 6,002,200 |

**Note:** Log entries don't always have all CEF extensions described in the event log format tables below. CEF extensions also may not be always in the same order. If you are using regular expressions (regex) to parse the entries, make sure your expressions do not depend on each key-value pair to exist, or to be in a specific order.

**Note:** Syslog messages are limited to 64 KB by the syslog protocol specification. If the message is longer, data may be truncated. The basic syslog format is limited to 1 KB.

## LEEF 2.0 syslog message format

**Base LEEF 2.0 format:** LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

**Sample LEEF 2.0 Log Entry (DSM System Event Log Sample):** LEEF:2.0|Trend Micro|Deep Security Manager|<DSA version>|192|cat=System name=Alert Ended desc=Alert: CPU Warning Threshold Exceeded\nSubject: 10.201.114.164\nSeverity: Warning sev=3 src=10.201.114.164 usrName=System msg=Alert: CPUWarning Threshold Exceeded\nSubject: 10.201.114.164\nSeverity:Warning TrendMicroDsTenant=Primary

## Events originating in the Manager

### System event log format

**Base CEF Format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

**Sample CEF Log Entry:** CEF:0|Trend Micro|Deep Security Manager|<DSM version>|600|User Signed In|3|src=10.52.116.160 suser=admin target=admin msg=User signed in from 2001:db8::5

**Base LEEF 2.0 format:** LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

**Sample LEEF 2.0 Log Entry:** LEEF:2.0|Trend Micro|Deep Security Manager|<DSA version>|192|cat=System name=Alert Ended desc=Alert: CPU Warning Threshold Exceeded\nSubject: 10.201.114.164\nSeverity: Warning sev=3 src=10.201.114.164 usrName=System msg=Alert: CPU Warning Threshold Exceeded\nSubject: 10.201.114.164\nSeverity: Warning TrendMicroDsTenant=Primary

**Note:** LEEF format uses a reserved "sev" key to show severity and "name" for the Name value.

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| src | src | Source IP Address | Deep Security Manager IP address. | src=10.52.116.23 |
| suser | usrName | Source User | Deep Security Manager administrator's account. | suser=MasterAdmin |
| target | target | Target Entity | The subject of the event. It can be the administrator account logged into Deep Security Manager, or a computer. | target=MasterAdmin<br>target=server01 |
| targetID | targetID | Target Entity ID | The identifier added in the manager. | targetID=1 |
| targetType | targetType | Target Entity Type | The event target entity type. | targetType=Host |
| msg | msg | Details | Details of the system event. May contain a verbose description of the event. | msg=User password incorrect for username MasterAdmin on an attempt to sign in from 127.0.0.1<br>msg=A Scan for Recommendations on computer (localhost) has completed... |
| TrendMicroDsTags | TrendMicroDsTags | Event Tags | Deep Security event tags assigned to the event | TrendMicroDsTags=suspicious |
| TrendMicroDsTenant | TrendMicroDsTenant | Tenant Name | Deep Security tenant | TrendMicroDsTenant=Primary |
| TrendMicroDsTenantId | TrendMicroDsTenantId | Tenant ID | Deep Security tenant ID | TrendMicroDsTenantId=0 |
| None | sev | Severity | The severity of the event. 1 is the least severe; 10 is the most severe. | sev=3 |
| None | cat | Category | Event category | cat=System |
| None | name | Name | Event name | name=Alert Ended |
| None | desc | Description | Event description | desc:Alert: CPU Warning Threshold Exceeded |

## Events originating in the agent

### Anti-malware event format

**Base CEF format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

**Sample CEF Log Entry:** CEF:0|Trend Micro|Deep Security Agent|<DSA version>|4000000|Eicar_test_file|6|cn1=1 cn1Label=Host ID dvchost=hostname cn2=205 cn2Label=Quarantine File Size cs6=ContainerImageName | ContainerName | ContainerID cs6Label=Container filePath=C:\\Users\\trend\\Desktop\\eicar.exe act=Delete msg=Realtime TrendMicroDsMalwareTarget=N/A TrendMicroDsMalwareTargetType=N/TrendMicroDsFileMD5=44D88612FEA8A8F36DE82E1278ABB02F TrendMicroDsFileSHA1=3395856CE81F2B7382DEE72602F798B642F14140 TrendMicroDsFileSHA256=275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F TrendMicroDsDetectionConfidence=95 TrendMicroDsRelevantDetectionNames=Ransom_CERBER.BZC;Ransom_CERBER.C;Ransom_CRYPNISCA.SM

**Base LEEF 2.0 format:** LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

**Sample LEEF Log Entry:** LEEF: 2.0|Trend Micro|Deep Security Agent|<DSA version>|4000030|cat=Anti-Malware name=HEU_AEGIS_CRYPT desc=HEU_AEGIS_CRYPT sev=6 cn1=241 cn1Label=Host ID dvc=10.0.0.1 TrendMicroDsTags=FS TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 filePath=C:\\Windows\\System32\\virus.exe act=Terminate msg=Realtime TrendMicroDsMalwareTarget=Multiple TrendMicroDsMalwareTargetType=File System TrendMicroDsFileMD5=1947A1BC0982C5871FA3768CD025453E#011 TrendMicroDsFileSHA1=5AD084DDCD8F80FBF2EE3F0E4F812E812DEE60C1#011 TrendMicroDsFileSHA256=25F231556700749F8F0394CAABDED83C2882317669DA2C01299B45173482FA6E TrendMicroDsDetectionConfidence=95 TrendMicroDsRelevantDetectionNames=Ransom_CERBER.BZC;Ransom_CERBER.C;Ransom_CRYPNISCA.SM

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| cn1 | cn1 | Host Identifier | The agent computer's internal unique identifier. | cn1=1 |
| cn1Label | cn1Label | Host | The name | cn1Label=Host ID |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | ID | label for the field cn1. | |
| cn2 | cn2 | File Size | The size of the quarantine file. This extension is included only when the "direct forward" from agent /appliance is selected. | cn2=100 |
| cn2Label | cn2Label | File Size | The name label for the field cn2. | cn2Label=Quarantine File Size |
| cs3 | cs3 | Infected Resource | The path of the spyware item. This field is only for spyware detection events. | cs3=C:\test\atse_samples\SPYW_Test_Virus.exe |
| cs3Label | cs3Label | Infected Resource | The name label for the field cs3. This field is only for spyware detection events. | cs3Label=Infected Resource |
| cs4 | cs4 | Resource Type | Resource Type values: 10=File | cs4=10 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | s and Directories<br>11=System Registry<br>12=Internet Cookies<br>13=Internet URL Shortcut<br>14=Programs in Memory<br>15=Program Startup Areas<br>16=Browser Helper Object<br>17=Layered | |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | Service Provider<br><br>18=Hosts File<br>19=Windows Policy Settings<br><br>20=Browser<br>23=Windows Shell Setting<br>24=IE Downloaded Program Files<br>25=Add/Remove Programs<br>26=Services | |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | other=Other<br><br>For example, if there's a spyware file named spy.exe that creates a registry run key to keep its persistence after system reboot, there will be two items in the spyware report: the item | |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | for spy.exe has cs4=10 (Files and Directories), and the item for the run key registry has cs4=11 (System Registry).<br>This field is only for spyware detection events. | |
| cs4Label | cd4Label | Resource Type | The name label for the field cs4. This field is only for spyware detection events. | cs4Label=Resource Type |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| cs5 | cs5 | Risk Level | Risk level values:<br>0=Very Low<br>25=Low<br>50=Medium<br>75=High<br>100=Very High<br>This field is only for spyware detection events. | cs5=25 |
| cs5Label | cs5Label | Risk Level | The name label for the field cs5. This field is only for spyware detection events. | cs5Label=Risk Level |
| cs6 | cs6 | Container | The image name of the Docker container, | cs6=ContainerImageName \| ContainerName \| ContainerID |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | container name, and container ID where the malware was detected. | |
| cs6Label | cs6Label | Container | The name label for the field cs6. | cs6Label=Container |
| filePath | filePath | File Path | The location of the malware file. | filePath=C:\\Users\\Mei\\Desktop\\virus.exe |
| act | act | Action | The action performed by the anti-malware engine. Possible values are: Deny Access, Quarantine, Delete, Pass, Clean, Terminate, and Unspecified. | act=Clean<br>act=Pass |
| msg | msg | Message | The type of scan. Possible values are: Realtime, | msg=Realtime<br>msg=Scheduled |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | Scheduled, and Manual. | |
| dvc | dvc | Device address | The IPv4 address for cn1.<br>Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.) | dvc=10.1.144.199 |
| dvchost | dvchost | Device hostname | The hostname or IPv6 address for cn1.<br>Does not appear | dvchost=www.example.com<br>dvchost=fe80::f018:a3c6:20f9:afa6%5 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | if the source is an IPv4 address. (Uses dvc field instead.) | |
| TrendMicroDsTags | TrendMicroDsTags | Events tags | Deep Security event tags assigned to the event | TrendMicroDsTags=suspicious |
| TrendMicroDsTenant | TrendMicroDsTenant | Tenant name | Deep Security tenant | TrendMicroDsTenant=Primary |
| TrendMicroDsTenantId | TrendMicroDsTenantId | Tenant ID | Deep Security tenant ID | TrendMicroDsTenantId=0 |
| TrendMicroDsMalwareTarget | TrendMicroDsMalwareTarget | Target(s) | The file, process, or registry key (if any) that the malware was trying to affect. If the malware was | TrendMicroDsMalwareTarget=N/A<br>TrendMicroDsMalwareTarget=C:\\Windows\\System32\\cmd.exe<br>TrendMicroDsMalwareTarget=HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings<br>TrendMicroDsMalwareTarget=Multiple |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | trying to affect more than one, this field will contain the value "Multiple."<br>Only suspicious activity monitoring and unauthorized change monitoring have values for this field. | |
| TrendMicroDsMalwareTargetType | TrendMicroDsMalwareTargetType | Target Type | The type of system resourc | TrendMicroDsMalwareTargetType=N/A<br>TrendMicroDsMalwareTargetType=Exploit<br>TrendMicroDsMalwareTargetType=File System<br>TrendMicroDsMalwareTargetType=Process<br>TrendMicroDsMalwareTargetType=Registry |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | e that this malware was trying to affect, such as the file system, a process, or Windows registry.<br>Only suspicious activity monitoring and unauthorized change monitoring have values for this field. | |
| TrendMicroDsFileMD5 | TrendMicroDsFileMD5 | File MD5 | The MD5 hash of | TrendMicroDsFileMD5=1947A1BC0982C5871FA3768CD025453E |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | the file | |
| TrendMicroDsFileSHA1 | TrendMicroDsFileSHA1 | File SHA 1 | The SHA1 hash of the file | TrendMicroDsFileSHA1=5AD084DDCD8F80FBF2EE3F0E4F812E812DEE60C1 |
| TrendMicroDsFileSHA256 | TrendMicroDsFileSHA256 | File SHA 256 | The SHA256 hash of the file | TrendMicroDsFileSHA256=25F231556700749F8F0394CAABDED83C2882317669DA2C01299B45173482FA6E |
| TrendMicroDsDetectionConfidence | TrendMicroDsDetectionConfidence | Threat Probability | Indicates how closely (in %) the file matched the malware model | TrendMicroDsDetectionConfidence=95 |
| TrendMicroDsRelevantDetectionNames | TrendMicroDsRelevantDetectionNames | Probable Threat Type | Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats (separate by semicolon";" ) | TrendMicroDsRelevantDetectionNames=Ransom_CERBER.BZC;Ransom_CERBER.C;Ransom_CRYPNISCA.SM |
| None | sev | Severity | The severity of the event. 1 is the least severe; 10 is the most | sev=6 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | severe. | |
| None | cat | Category | Category | cat=Anti-Malware |
| None | name | Name | Event name | name=SPYWARE_KEYL_ACTIVE |
| None | desc | Description | Event description. Anti-malware uses the event name as the description. | desc=SPYWARE_KEYL_ACTIVE |

## Application control event format

**Base CEF format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

**Example CEF Log Entry:** `CEF: 0|Trend Micro|Deep Security Agent|10.2.229|6001200|AppControl detectOnly|6|cn1=202 cn1Label=Host ID dvc=192.168.33.128 TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 fileHash=80D4AC182F97D2AB48EE4310AC51DA5974167C596D133D64A83107B9069745E0 suser=root suid=0 act=detectOnly filePath=/home/user1/Desktop/Directory1//heartbeatSync.sh fsize=20 aggregationType=0 repeatCount=1 cs1=notWhitelisted cs1Label=actionReason cs2=0CC9713BA896193A527213D9C94892D41797EB7C cs2Label=sha1 cs3=7EA8EF10BEB2E9876D4D7F7E5A46CF8D cs3Label=md5`

**Base LEEF 2.0 format:** LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

**Example LEEF Log Entry:** `LEEF:2.0|Trend Micro|Deep Security Agent|10.0.2883|60|`cat=AppControl name=blocked desc=blocked sev=6 cn1=2 cn1Label=Host ID dvc=10.203.156.39 TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 fileHash=E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855 suser=root suid=0 act=blocked filePath=/bin/my.jar fsize=123857 aggregationType=0 repeatCount=1 cs1=notWhitelisted cs1Label=actionReason

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| cn1 | cn1 | Host Identifier | The agent computer's internal unique identifier. | cn1=2 |
| cn1Label | cn1Label | Host ID | The name label for the field cn1. | cn1Label=Host ID |
| cs1 | cs1 | Reason | The reason why application control performed the specified action, such as "notWhitelisted" (the software did not have a matching rule, and application control was configured to block unrecognized software). | cs1=notWhitelisted |
| cs1Label | cs1Label | | The name label for the field cs1. | cs1Label=actionReason |
| cs2 | cs2 | | If it was calculated, the SHA-1 hash of the file. | cs2=156F4CB711FDBD668943711F853FB6DA89581AAD |
| cs2Label | cs2Label | | The name label for the field cs2. | cs2Label=sha1 |
| cs3 | cs3 | | If it was calculated, the MD5 hash of the file. | cs3=4E8701AC951BC4537F8420FDAC7EFBB5 |
| cs3Label | cs3Label | | The name label for the | cs3Label=md5 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | field cs3. | |
| act | act | Action | The action performed by the application control engine. Possible values are: Blocked, Allowed. | act=blocked |
| dvc | dvc | Device address | The IPv4 address for cn1.<br>Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.) | dvc=10.1.1.10 |
| dvchost | dvchost | Device host name | The hostname or IPv6 address for cn1.<br>Does not appear if the source is an IPv4 address. | dvchost=www.example.com<br>dvchost=2001:db8::5 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | (Uses dvc field instead.) | |
| suid | suid | User ID | The account ID number of the user name. | suid=0 |
| suser | suser | User Name | The name of the user account that installed the software on the protected computer. | suser=root |
| TrendMicroDsTenant | TrendMicroDsTenant | Tenant name | Deep Security tenant name. | TrendMicroDsTenant=Primary |
| TrendMicroDsTenantId | TrendMicroDsTenantId | Tenant ID | Deep Security tenant ID number. | TrendMicroDsTenantId=0 |
| fileHash | fileHash | File hash | The SHA 256 hash that identifies the software file. | fileHash=E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855 |
| filePath | filePath | File Path | The location of the malware file. | filePath=/bin/my.jar |
| fsize | fsize | File Size | The file size in bytes. | fsize=16 |
| aggregationType | aggregationType | Aggregation Type | An integer that indicates how the event is aggregated:<br>• 0: | aggregationType=2 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | The event is not aggregated<br>• 1: The event is aggregated based on file name, path, and event type.<br>• 2: The event is aggregated base | |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | d on event type.<br><br>For information, about event aggregation, see "View application control event logs" on page 472. | |
| repeatCount | repeatCount | Repeat Count | The number of occurrences of the event. Non-aggregated events have a value of 1. Aggregated events have a value of 2 or more. | repeatCount=4 |
| None | sev | Severity | The severity of the event. 1 is the least severe; 10 is the most severe. | sev=6 |
| None | cat | Category | Category | cat=AppControl |
| None | name | Name | Event name | name=blocked |
| None | desc | Descrip | Event | desc=blocked |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | tion | description. Application control uses the action as the description. | |

Firewall event log format

**Base CEF format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

**Sample CEF Log Entry:** CEF:0|Trend Micro|Deep Security Agent|<DSA version>|20|Log for TCP Port 80|0|cn1=1 cn1Label=Host ID dvc=hostname act=Log dmac=00:50:56:F5:7F:47 smac=00:0C:29:EB:35:DE TrendMicroDsFrameType=IP src=192.168.126.150 dst=72.14.204.147 out=1019 cs3=DF MF cs3Label=Fragmentation Bits proto=TCP spt=49617 dpt=80 cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=1 TrendMicroDsPacketData=AFB...

**Sample LEEF Log Entry:** LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|21|cat=Firewall name=Remote Domain Enforcement (Split Tunnel) desc=Remote Domain Enforcement (Split Tunnel) sev=5 cn1=37 cn1Label=Host ID dvchost=www.example.com TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=Deny dstMAC=67:BF:1B:2F:13:EE srcMAC=78:FD:E7:07:9F:2C TrendMicroDsFrameType=IP src=10.0.110.221 dst=105.152.185.81 out=177 cs3= cs3Label=Fragmentation Bits proto=UDP srcPort=23 dstPort=445 cnt=1

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| act | act | Action | | act=Log<br>act=Deny |
| cn1 | cn1 | Host Identifier | The agent computer's internal unique identifier. | cn1=113 |
| cn1Label | cn1Label | Host ID | The name label for the field cn1. | cn1Label=Host ID |
| cnt | cnt | Repeat Count | The number of times this | cnt=8 |

| CEF Extension Field | LEEF Extension Field | Name | Descriptio n | Examples |
|---|---|---|---|---|
| | | | event was sequentially repeated. | |
| cs2 | cs2 | TCP Flags | | cs2=0x10 ACK<br>cs2=0x14 ACK RST |
| cs2Label | cs2Label | TCP Flags | The name label for the field cs2. | cs2Label=TCP Flags |
| cs3 | cs3 | Packet Fragmentatio n Information | | cs3=DF<br>cs3=MF<br>cs3=DF MF |
| cs3Label | cs3Label | Fragmentatio n Bits | The name label for the field cs3. | cs3Label=Fragmentation Bits |
| cs4 | cs4 | ICMP Type and Code | (For the ICMP protocol only) The ICMP type and code, delimited by a space. | cs4=11 0<br>cs4=8 0 |
| cs4Label | cs4Label | ICMP | The name label for the field cs4. | cs4Label=ICMP Type and Code |
| dmac | dstMAC | Destination MAC Address | MAC address of the destination computer's network interface. | dmac= 00:0C:29:2F:09:B3 |
| dpt | dstPort | Destination Port | (For TCP and UDP protocol only) Port number of the destination computer's connection or session. | dpt=80<br>dpt=135 |
| dst | dst | Destination IP Address | IP address of the destination computer. | dst=192.168.1.102<br>dst=10.30.128.2 |
| in | in | Inbound Bytes Read | (For inbound connections only) Number of inbound bytes read. | in=137<br>in=21 |
| out | out | Outbound | (For outbound | out=216 |

| CEF Extension Field | LEEF Extension Field | Name | Descriptio n | Examples |
|---|---|---|---|---|
| | | Bytes Read | connections only) Number of outbound bytes read. | out=13 |
| proto | proto | Transport protocol | Name of the transport protocol used. | proto=tcp<br>proto=udp<br>proto=icmp |
| smac | srcMAC | Source MAC Address | MAC address of the source computer's network interface. | smac= 00:0E:04:2C:02:B3 |
| spt | srcPort | Source Port | (For TCP and UDP protocol only) Port number of the source computer's connection or session. | spt=1032<br>spt=443 |
| src | src | Source IP Address | IP address of the source computer. | src=192.168.1.105<br>src=10.10.251.231 |
| TrendMicroDsFrameTyp e | TrendMicroDsFrameTyp e | Ethernet frame type | Connection ethernet frame type. | TrendMicroDsFrameType=IP<br>TrendMicroDsFrameType=ARP<br>TrendMicroDsFrameType=RevARP<br>TrendMicroDsFrameType=NetBEUI |
| TrendMicroDsPacketDat a | TrendMicroDsPacketDat a | Packet data | | TrendMicroDsPacketData=AA...BA\= |
| dvc | dvc | Device address | The IPv4 address for cn1.<br>Does not appear if the source is an IPv6 address or hostname. | dvc=10.1.144.199 |

| CEF Extension Field | LEEF Extension Field | Name | Descriptio n | Examples |
|---|---|---|---|---|
| | | | (Uses dvchost instead.) | |
| dvchost | dvchost | Device host name | The hostname or IPv6 address for cn1.<br>Does not appear if the source is an IPv4 address. (Uses dvc field instead.) | dvchost=exch01.example.com<br>dvchost=2001:db8::5 |
| TrendMicroDsTags | TrendMicroDsTags | Event Tags | Deep Security event tags assigned to the event | TrendMicroDsTags=suspicious |
| TrendMicroDsTenant | TrendMicroDsTenant | Tenant Name | Deep Security tenant | TrendMicroDsTenant=Primary |
| TrendMicroDsTenantId | TrendMicroDsTenantId | Tenant ID | Deep Security tenant ID | TrendMicroDsTenantId=0 |
| None | sev | Severity | The severity of the event. 1 is the least severe; 10 is the most severe. | sev=5 |
| None | cat | Category | Category | cat=Firewall |
| None | name | Name | Event name | name=Remote Domain Enforcement (Split Tunnel) |
| None | desc | Description | Event description. Firewall events use the event name as | desc=Remote Domain Enforcement (Split Tunnel) |

| CEF Extension Field | LEEF Extension Field | Name | Descriptio n | Examples |
|---|---|---|---|---|
| | | | the description. | |

## Integrity monitoring log event format

**Base CEF format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

**Sample CEF Log Entry:** CEF:0|Trend Micro|Deep Security Agent|<DSA version>|30|New Integrity Monitoring Rule|6|cn1=1 cn1Label=Host ID dvchost=hostname act=updated filePath=c:\\windows\\message.dll suser=admin msg=lastModified,sha1,size

**Base LEEF 2.0 format:** LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

**Sample LEEF Log Entry:** LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|2002779|cat=Integrity Monitor name=Microsoft Windows - System file modified desc=Microsoft Windows - System file modified sev=8 cn1=37 cn1Label=Host ID dvchost=www.example.com TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=updated suser=admin

| CEF Extension Field | LEEF Extension Field | Name | Descriptio n | Examples |
|---|---|---|---|---|
| act | act | Action | The action detected by the integrity rule. Can contain: created, updated, detected or renamed. | act=created act=deleted |
| cn1 | cn1 | Host Identifier | The agent computer's internal unique identifier. | cn1=113 |
| cn1Label | cn1Label | Host ID | The name label for the field cn1. | cn1Label=Host ID |
| filePath | filePath | Target Entity | The integrity | filePath=C:\WINDOWS\system32\drivers\etc\hosts |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | rule target entity. May contain a file or directory path, registry key, etc. | |
| suser | suser | Source User | Deep Security Manager administrator's account. | suser=MasterAdmin |
| msg | msg | Attribute changes | (For "renamed" action only) A list of changed attribute names. If "Relay via Manager" is selected, all event action types include a full description. | msg=lastModified,sha1,size |
| oldfilePath | oldfilePath | Old target entity | (For "renamed" action only) The previous integrity rule target entity to capture the rename action from the previous target entity to the new, which is recorded in the filePath field. | oldFilePath=C:\WINDOWS\system32\logfiles\ds_agent.log |
| dvc | dvc | Device address | The IPv4 address for cn1. | dvc=10.1.144.199 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.) | |
| dvchost | dvchost | Device host name | The hostname or IPv6 address for cn1.<br>Does not appear if the source is an IPv4 address. (Uses dvc field instead.) | dvchost=www.example.com<br>dvchost=2001:db8::5 |
| TrendMicroDsTags | TrendMicroDsTags | Events tags | Deep Security event tags assigned to the event | TrendMicroDsTags=suspicious |
| TrendMicroDsTenant | TrendMicroDsTenant | Tenant name | Deep Security tenant | TrendMicroDsTenant=Primary |
| TrendMicroDsTenantId | TrendMicroDsTenantId | Tenant ID | Deep Security tenant ID | TrendMicroDsTenantId=0 |
| None | sev | Severity | The severity of the event. | sev=8 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | 1 is the least severe; 10 is the most severe. | |
| None | cat | Category | Category | cat=Integrity Monitor |
| None | name | Name | Event name | name=Microsoft Windows - System file modified |
| None | desc | Description | Event description. Integrity monitoring uses the event name as the description. | desc=Microsoft Windows - System file modified |

## Intrusion prevention event log format

**Base CEF format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

**Sample CEF Log Entry:** CEF:0|Trend Micro|Deep Security Agent|<DSA version>|1001111|Test Intrusion Prevention Rule|3|cn1=1 cn1Label=Host ID dvchost=hostname dmac=00:50:56:F5:7F:47 smac=00:0C:29:EB:35:DE TrendMicroDsFrameType=IP src=192.168.126.150 dst=72.14.204.105 out=1093 cs3=DF MF cs3Label=Fragmentation Bits proto=TCP spt=49786 dpt=80 cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=1 act=IDS:Reset cn3=10 cn3Label=Intrusion Prevention Packet Position cs5=10 cs5Label=Intrusion Prevention Stream Position cs6=8 cs6Label=Intrusion Prevention Flags TrendMicroDsPacketData=R0VUIC9zP3...

**Base LEEF 2.0 format:** LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

**Sample LEEF Log Entry:** LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|1000940|cat=Intrusion Prevention name=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities desc=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities sev=10 cn1=6 cn1Label=Host ID dvchost=exch01 TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 dstMAC=55:C0:A8:55:FF:41 srcMAC=CA:36:42:B1:78:3D TrendMicroDsFrameType=IP src=10.0.251.84 dst=56.19.41.128 out=166 cs3= cs3Label=Fragmentation Bits proto=ICMP srcPort=0 dstPort=0 cnt=1 act=IDS:Reset cn3=0

cn3Label=DPI Packet Position cs5=0 cs5Label=DPI Stream Position cs6=0 cs6Label=DPI Flags

| CEF Extension Field | LEEF Extension Field | Name | Descriptio n | Examples |
|---|---|---|---|---|
| act | act | Action | (IPS rules written before Deep Security version 7.5 SP1 could additionally perform Insert, Replace, and Delete actions. These actions are no longer performed. If an older IPS Rule is triggered which still attempts to perform those actions, the event will indicate that the rule was applied in detect-only mode.) | act=Block |
| cn1 | cn1 | Host Identifier | The agent computer's internal unique identifier. | cn1=113 |
| cn1Label | cn1Label | Host ID | The name label for the field cn1. | cn1Label=Host ID |
| cn3 | cn3 | Intrusion Prevention Packet Position | Position within packet of data that triggered the event. | cn3=37 |
| cn3Label | cn3Label | Intrusion Prevention Packet Position | The name label for the field cn3. | cn3Label=Intrusion Prevention Packet Position |
| cnt | cnt | Repeat Count | The number of times this | cnt=8 |

| CEF Extension Field | LEEF Extension Field | Name | Descriptio n | Examples |
|---|---|---|---|---|
| | | | event was sequentially repeated. | |
| cs1 | cs1 | Intrusion Prevention Filter Note | (Optional) A note field which can contain a short binary or text note associated with the payload file. If the value of the note field is all printable ASCII characters, it will be logged as text with spaces converted to underscores. If it contains binary data, it will be logged using Base-64 encoding. | cs1=Drop_data |
| cs1Label | cs1Label | Intrusion Prevention Note | The name label for the field cs1. | cs1Label=Intrusion Prevention Note |
| cs2 | cs2 | TCP Flags | (For the TCP protocol only) The raw TCP flag byte followed by the URG, ACK, PSH, RST, SYN and FIN fields may be present if the TCP header was set. | cs2=0x10 ACK<br>cs2=0x14 ACK RST |
| cs2Label | cs2Label | TCP Flags | The name label for the field cs2. | cs2Label=TCP Flags |

| CEF Extension Field | LEEF Extension Field | Name | Descriptio n | Examples |
|---|---|---|---|---|
| cs3 | cs3 | Packet Fragmentatio n Information | | cs3=DF<br>cs3=MF<br>cs3=DF MF |
| cs3Label | cs3Label | Fragmentatio n Bits | The name label for the field cs3. | cs3Label=Fragmentation Bits |
| cs4 | cs4 | ICMP Type and Code | (For the ICMP protocol only) The ICMP type and code stored in their respective order delimited by a space. | cs4=11 0<br>cs4=8 0 |
| cs4Label | cs4Label | ICMP | The name label for the field cs4. | cs4Label=ICMP Type and Code |
| cs5 | cs5 | Intrusion Prevention Stream Position | Position within stream of data that triggered the event. | cs5=128<br>cs5=20 |
| cs5Label | cs5Label | Intrusion Prevention Stream Position | The name label for the field cs5. | cs5Label=Intrusion Prevention Stream Position |
| cs6 | cs6 | Intrusion Prevention Filter Flags | A combined value that includes the sum of the flag values:<br><br>1 - Data truncated - Data could not be logged.<br>2 - Log Overflow - Log overflowed after this log.<br>4 - Suppressed - Logs threshold suppressed after this log.<br>8 - Have Data - Contains | The following example would be a summed combination of 1 (Data truncated) and 8 (Have Data):<br>cs6=9 |

| CEF Extension Field | LEEF Extension Field | Name | Descriptio n | Examples |
|---|---|---|---|---|
| | | | packet data 16 - Reference Data - References previously logged data. | |
| cs6Label | cs6Label | Intrusion Prevention Flags | The name label for the field cs6. | cs6=Intrusion Prevention Filter Flags |
| dmac | dstMAC | Destination MAC Address | Destination computer network interface MAC address. | dmac= 00:0C:29:2F:09:B3 |
| dpt | dstPort | Destination Port | (For TCP and UDP protocol only) Destination computer connection port. | dpt=80<br>dpt=135 |
| dst | dst | Destination IP Address | Destination computer IP Address. | dst=192.168.1.102<br>dst=10.30.128.2 |
| in | in | Inbound Bytes Read | (For inbound connections only) Number of inbound bytes read. | in=137<br>in=21 |
| out | out | Outbound Bytes Read | (For outbound connections only) Number of outbound bytes read. | out=216<br>out=13 |
| proto | proto | Transport protocol | Name of the connection transport protocol used. | proto=tcp<br>proto=udp<br>proto=icmp |
| smac | srcMAC | Source MAC Address | Source computer network interface MAC address. | smac= 00:0E:04:2C:02:B3 |
| spt | srcPort | Source Port | (For TCP and UDP protocol | spt=1032<br>spt=443 |

| CEF Extension Field | LEEF Extension Field | Name | Descriptio n | Examples |
|---|---|---|---|---|
| | | | only) Source computer connection port. | |
| src | src | Source IP Address | Source computer IP Address. | src=192.168.1.105<br>src=10.10.251.231 |
| TrendMicroDsFrameTyp e | TrendMicroDsFrameTyp e | Ethernet frame type | Connection ethernet frame type. | TrendMicroDsFrameType=IP<br>TrendMicroDsFrameType=ARP<br>TrendMicroDsFrameType=RevARP<br>TrendMicroDsFrameType=NetBEUI |
| TrendMicroDsPacketDat a | TrendMicroDsPacketDat a | Packet data | | TrendMicroDsPacketData=AA...BA\= |
| dvc | dvc | Device address | The IPv4 address for cn1.<br>Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.) | dvc=10.1.144.199 |
| dvchost | dvchost | Device host name | The hostname or IPv6 address for cn1.<br>Does not appear if | dvchost=www.example.com<br>dvchost=2001:db8::5 |

| CEF Extension Field | LEEF Extension Field | Name | Descriptio n | Examples |
|---|---|---|---|---|
| | | | the source is an IPv4 address. (Uses dvc field instead.) | |
| TrendMicroDsTags | TrendMicroDsTags | Event tags | Deep Security event tags assigned to the event | TrendMicroDsTags=Suspicious |
| TrendMicroDsTenant | TrendMicroDsTenant | Tenant name | Deep Security tenant name | TrendMicroDsTenant=Primary |
| TrendMicroDsTenantId | TrendMicroDsTenantId | Tenant ID | Deep Security tenant ID | TrendMicroDsTenantId=0 |
| None | sev | Severity | The severity of the event. 1 is the least severe; 10 is the most severe. | sev=10 |
| None | cat | Category | Category | cat=Intrusion Prevention |
| None | name | Name | Event name | name=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities |
| None | desc | Description | Event description. Intrusion prevention events use the event name as the description. | desc=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities |

## Log inspection event format

**Base CEF format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

**Sample CEF Log Entry:** CEF:0|Trend Micro|Deep Security Agent|<DSA version>|3002795|Microsoft Windows Events|8|cn1=1 cn1Label=Host ID dvchost=hostname cs1Label=LI Description cs1=Multiple Windows Logon Failures fname=Security src=127.0.0.1

duser=(no user) shost=WIN-RM6HM42G65V msg=WinEvtLog Security: AUDIT_FAILURE (4625): Microsoft-Windows-Security-Auditing: (no user): no domain: WIN-RM6HM42G65V: An account failed to log on. Subject: ..

**Base LEEF 2.0 format:** LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

**Sample LEEF Log Entry:** LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|3003486|cat=Log Inspection name=Mail Server - MDaemon desc=Server Shutdown. sev=3 cn1=37 cn1Label=Host ID dvchost=exch01.example.com TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 cs1=Server Shutdown. cs1Label=LI Description fname= shost= msg=

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| cn1 | cn1 | Host Identifier | The agent computer's internal unique identifier. | cn1=113 |
| cn1Label | cn1Label | Host ID | The name label for the field cn1. | cn1Label=Host ID |
| cs1 | cs1 | Specific Sub-Rule | The Log Inspection sub-rule which triggered this event. | cs1=Multiple Windows audit failure events |
| cs1Label | cs1Label | LI Description | The name label for the field cs1. | cs1Label=LI Description |
| duser | duser | User Information | (If parse-able username exists) The name of the target user initiated the log entry. | duser=(no user)<br>duser=NETWORK SERVICE |
| fname | fname | Target entity | The log inspection rule target entity. May contain a file or directory path, registry key, etc. | fname=Application<br>fname=C:\Program Files\CMS\logs\server0.log |
| msg | msg | Details | Details of the log inspection event. May contain a verbose description of the detected log event. | msg=WinEvtLog: Application: AUDIT_FAILURE(20187): pgEvent: (no user): no domain: SERVER01: Remote login failure for user 'xyz' |
| shost | shost | Source Hostname | Source computer hostname. | shost=webserver01.corp.com |
| src | src | Source IP Address | Source computer IP address. | src=192.168.1.105<br>src=10.10.251.231 |
| dvc | dvc | Device address | The IPv4 address for cn1. | dvc=10.1.144.199 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.) | |
| dvchost | dvchost | Device host name | The hostname or IPv6 address for cn1.<br>Does not appear if the source is an IPv4 address. (Uses dvc field instead.) | dvchost=www.example.com<br>dvchost=2001:db8::5 |
| TrendMicroDsTags | TrendMicroDsTags | Events tags | Deep Security event tags assigned to the event | TrendMicroDsTags=suspicious |
| TrendMicroDsTenant | TrendMicroDsTenant | Tenant name | Deep Security tenant | TrendMicroDsTenant=Primary |
| TrendMicroDsTenantId | TrendMicroDsTenantId | Tenant ID | Deep Security tenant ID | TrendMicroDsTenantId=0 |
| None | sev | Severity | The severity of the event. 1 is the least severe; 10 is the most severe. | sev=3 |
| None | cat | Category | Category | cat=Log Inspection |
| None | name | Name | Event name | name=Mail Server - MDaemon |
| None | desc | Description | Event description. | desc=Server Shutdown |

## Web reputation event format

**Base CEF format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

**Sample CEF Log Entry:** CEF:0|Trend Micro|Deep Security Agent|<DSA version>|5000000|WebReputation|5|cn1=1 cn1Label=Host ID dvchost=hostname request=example.com msg=Blocked By Admin

**Base LEEF 2.0 format:** LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

**Sample LEEF Log Entry:** LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|5000000|cat=Web Reputation name=WebReputation desc=WebReputation sev=6 cn1=3 cn1Label=Host ID dvchost=exch01.example.com TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 request=http://yw.olx5x9ny.org.it/HvuauRH/eighgSS.htm msg=Suspicious

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| cn1 | cn1 | Host Identifier | The agent computer's internal unique identifier. | cn1=1 |
| cn1Label | cn1Label | Host ID | The name label for the field cn1. | cn1Label=Host ID |
| request | request | Request | The URL of the request. | request=http://www.example.com/index.php |
| msg | msg | Message | The type of action. Possible values are: Realtime, Scheduled, and Manual. | msg=Realtime<br>msg=Scheduled |
| dvc | dvc | Device address | The IPv4 address for cn1.<br><br>Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.) | dvc=10.1.144.199 |

| CEF Extension Field | LEEF Extension Field | Name | Descriptio n | Examples |
|---|---|---|---|---|
| dvchost | dvchost | Device host name | The hostname or IPv6 address for cn1.<br>Does not appear if the source is an IPv4 address. (Uses dvc field instead.) | dvchost=www.example.com<br>dvchost=2001:db8::5 |
| TrendMicroDsTags | TrendMicroDsTags | Events tags | Deep Security event tags assigned to the event | TrendMicroDsTags=suspicious |
| TrendMicroDsTenant | TrendMicroDsTenant | Tenant name | Deep Security tenant | TrendMicroDsTenant=Primary |
| TrendMicroDsTenantI d | TrendMicroDsTenantI d | Tenant ID | Deep Security tenant ID | TrendMicroDsTenantId=0 |
| None | sev | Severity | The severity of the event. 1 is the least severe; 10 is the most severe. | sev=6 |
| None | cat | Category | Category | cat=Web Reputation |
| None | name | Name | Event name | name=WebReputation |
| None | desc | Descriptio n | Event description. Web reputation uses the event name as the description. | desc=WebReputation |

# Configure Red Hat Enterprise Linux to receive event logs

## Set up a Syslog on Red Hat Enterprise Linux 6 or 7

The following steps describe how to configure rsyslog on Red Hat Enterprise Linux 6 or 7 to receive logs from Deep Security.

1. Log in as root
2. Execute:

   ```
   vi /etc/rsyslog.conf
   ```
3. Uncomment the following lines near the top of the `rsyslog.conf` to change them from:

   ```
   #$ModLoad imudp
   #$UDPServerRun 514

   #$ModLoad imtcp
   #$InputTCPServerRun 514
   ```

   to

   ```
   $ModLoad imudp
   $UDPServerRun 514

   $ModLoad imtcp
   $InputTCPServerRun 514
   ```
4. Add the following two lines of text to the end of the `rsyslog.conf`:
   - `#Save Deep Security Manager logs to DSM.log`
   - `Local4.* /var/log/DSM.log`

   **Note:** You may need to replace `Local4` with another value, depending on your Manager settings.
5. Save the file and exit
6. Create the `/var/log/DSM.log` file by typing `touch /var/log/DSM.log`
7. Set the permissions on the DSM log so that syslog can write to it
8. Save the file and exit

9. Restart syslog:
   - On Red Hat Enterprise Linux 6: `service rsyslog restart`
   - On Red Hat Enterprise Linux 7: `systemctl restart rsyslog`

When Syslog is functioning you will see logs populated in: `/var/log/DSM.log`

### Set up a Syslog on Red Hat Enterprise Linux 5

The following steps describe how to configure Syslog on Red Hat Enterprise Linux to receive logs from Deep Security.

1. Log in as root
2. Execute:

   `vi /etc/syslog.conf`
3. Add the following two lines of text to the end of the `syslog.conf` :
   - `#Save Deep Security Manager logs to DSM.log`
   - `Local4.* /var/log/DSM.log`

   **Note:** You may need to replace `Local4` with another value, depending on your Manager settings.
4. Save the file and exit
5. Create the `/var/log/DSM.log` file by typing `touch /var/log/DSM.log`
6. Set the permissions on the DSM log so that syslog can write to it
7. Execute:

   `vi /etc/sysconfig/syslog`
8. Modify the line " `SYSLOGD_OPTIONS` " and add a " `-r` " to the options
9. Save the file and exit
10. Restart syslog: `/etc/init.d/syslog restart`

When Syslog is functioning you will see logs populated in: `/var/log/DSM.log`

## Access events with Amazon SNS

If you have an AWS account, you can take advantage of the Amazon Simple Notification Service (SNS) to publish notifications about Deep Security events and deliver them to subscribers. For details about SNS, see https://aws.amazon.com/sns/.

To set up Amazon SNS:

1. "Create an AWS user" below.
2. "Create an Amazon SNS topic" on the next page.
3. "Enable SNS" on the next page.
4. "Create subscriptions" on page 867.

See the sections below for details on how to perform these tasks.

## Create an AWS user

In order to use Amazon SNS with Deep Security, you need to create an AWS user with the appropriate permissions for SNS. Note the access key and secret key for the user, because you will need that information for step 3, below.

The AWS user will need the "sns:Publish" permission on all SNS topics that Deep Security will publish to. This is an example of a policy with this permission:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": [
            "sns:Publish"
         ],
         "Effect": "Allow",
         "Resource": "*"
      }
   ]
}
```

If you want to limit publishing rights to a single topic, you can replace `"Resource":"*"` with `"Resource":"TOPIC ARN"`.

For more information, see Controlling User Access to Your AWS Account and Special Information for Amazon SNS Policies in the Amazon AWS documentation.

## Create an Amazon SNS topic

In AWS, create an SNS topic where the events will be published. For instructions on how to create an Amazon SNS topic, see "Create a Topic" in the Amazon SNS documentation. Note the SNS Topic ARN because you will need this information in step 3, below.

## Enable SNS

1. In the Deep Security Manager, go to **Administration** > **System Settings** > **Event Forwarding**.
2. In the Amazon SNS section, select **Publish Events to Amazon Simple Notification Service**.
3. Enter this information:
   - **Access Key:** The access key of the AWS user you created in section 1.
   - **Secret Key:** The secret key of the AWS user you created in section 1.
   - **SNS Topic ARN:** The SNS Topic ARN that events will be sent to. This is the ARN that you noted in section 2.
4. Select the types of events that you want to forward to SNS.

   Selecting the events automatically generates a JSON SNS configuration.

5. (Optional) You can also click **Edit JSON SNS configuration** to edit the JSON SNS configuration directly if you want to filter the events in greater detail and configure the forwarding instructions for each filter. For details on the configuration language, see "JSON SNS configuration" on the next page.

   **Note:** If you edit the JSON, the event check boxes will become unavailable. If you want to select or deselect any of the event check boxes, you can click **Revert to basic SNS configuration**, but any customizations you have made to the JSON SNS configuration will be discarded.

6. Click **Save**.

## Create subscriptions

Now that SNS is enabled and events are being published to the topic, go to the Amazon SNS console and subscribe to the topic to access the events. There are several ways that you can subscribe to events, including email, SMS, and Lambda endpoints.

**Note:** Lambda is not available in all AWS regions.

## JSON SNS configuration

For instructions on how to enable the forwarding of events to Amazon SNS topics, see "Access events with Amazon SNS" on page 864. If you opt to directly edit the JSON SNS configuration, this page provides details on how to do it.

The configuration language used to define which events are sent to which topics is modeled after Amazon's Policy language for SNS, described in the Amazon documentation.

The configuration is a special JSON-encoded document that says which conditions an event must meet in order to be published to a topic. A basic configuration looks like:

```
{
  "Version": "2014-09-24",
  "Statement": [statement1, statement2, ...]
}
```

### Version

The **Version** element specifies the version of the configuration language. The only currently valid value is the string "2014-09-24"

```
"Version": "2014-09-24",
```

### Statement

The **Statement** element is an array of individual statements. Each individual statement is a distinct JSON object giving the SNS topic to send to if an event meets given conditions.

```
"Statement": [{...}, {...}, ...]
```

An individual statement has the form

```
{
  "Topic": "destination topic",
  "Condition": {conditions event must meet to be published to the
destination topic}
}
```

## Topic

The **Topic** element must be the Amazon Resource Name of the SNS Topic to publish to.

```
"Topic": "arn:aws:sns:us-east-1:012345678901:myTopic"
```

## Condition

The **Condition** element is the most complex part of the configuration. It contains one or more conditions an event must match in order to be published to the topic. Each condition may itself contain multiple key-value pairs, and some conditions support multiple values for each key. The keys in conditions are the names of properties from events.

```
"Condition": {
  "ConditionName": {
    "key1": [value1, value2],
    "key2": value3
  },
  "ConditionName2": {
    "key3": [value4]
  },
  ...
}
```

Possible condition names and their syntax are described below.

### Bool

The **Bool** condition performs Boolean matching. To match, an event must have a property with the desired Boolean value. If the property in the event exists but is not itself a Boolean value, the property is tested as follows:

- Numbers equal to 0 evaluate to false. Numbers not equal to 0 evaluate to true.
- Empty strings and the special strings "false" and "0" evaluate to false. Other strings evaluate to true.
- Any other property value in an event cannot be converted to a Boolean and will not match.

Allows for multiple values? No

The following example shows a configuration that publishes events that have a "DetectOnly" property with a value false:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "Bool": {
          "DetectOnly": false
        }
      }
    }
  ]
}
```

### Exists

The **Exists** condition tests for the existence or non-existence of a property in an event. The value of the property is not considered.

Allows for multiple values? No

The following example shows a configuration that publishes events when the event has the property "Severity" but does not have the property "Title":

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "Exists": {
          "Severity": true,
          "Title": false
        }
      }
    }
  ]
}
```

## IpAddress

The **IpAddress** condition tests the value of an event's property is an IP address in a range given in CIDR format, or exactly equals a single IP address.

Allows for multiple values? Yes

The following example shows a configuration that publishes events when the event has the property "DestinationIP" with an IP address in the range 64.23.0.0/16, or to 216.104.20.189:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
```

```
          "IpAddress": {
            "DestinationIP": ["64.23.0.0/16", "216.104.20.189"]
          }
        }
      }
    ]
  }
```

### NotIpAddress

The **NotIpAddress** condition tests the value of an event's property is not an IP address in any of the specified IP address ranges.

Allows for multiple values? Yes

The following example shows a configuration that publishes events when the event has the property "DestinationIP" with an IP address not in the range 10.0.0.0/8:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NotIpAddress": {
          "DestinationIP": "10.0.0.0/8"
        }
      }
    }
  ]
}
```

### NumericEquals

The **NumericEquals** condition tests the numeric value of an event's property equals one or more desired values. If the property in the event exists but is not itself a numeric value, the property is tested as follows:

- Strings are converted to numbers. Strings that cannot be converted to numbers will not match.
- Any other property value in an event cannot be converted to a number and will not match.

Allows for multiple values? Yes

The following example shows a configuration that publishes events when the event has the property "Protocol" with the value 6 or 17:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericEquals": {
          "Protocol": [6, 17]
        }
      }
    }
  ]
}
```

### NumericNotEquals

The **NumericNotEquals** condition tests the numeric value of an event's property is not equal to any one of an undesired set of values.

Allows for multiple values? Yes

The following example shows a configuration that publishes events when the event has the property "Protocol" not equal to 6, and the property "Risk" not equal to 2 or 3:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericNotEquals": {
          "Protocol": 6,
          "Risk" : [2, 3]
        }
      }
    }
  ]
}
```

### NumericGreaterThan

The **NumericGreaterThan** condition tests the numeric value of an event's property is strictly greater than a desired value. If the property in the event exists but is not itself a numeric value it is converted to a number as described for NumericEquals.

Allows for multiple values? No

The following example shows a configuration that publishes events when the event has the property "Protocol" with the value greater than 6:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericGreaterThan": {
```

```
            "Protocol": 6
          }
        }
      }
    ]
  }
```

### NumericGreaterThanEquals

The **NumericGreaterThanEquals** condition tests the numeric value of an event's property is greater than or equal to a desired value. If the property in the event exists but is not itself a numeric value it is converted to a number as described for NumericEquals.

Allows for multiple values? No

The following example shows a configuration that publishes events when the event has the property "Number" with a value greater than or equal to 600:

```
  {
    "Version": "2014-09-24",
    "Statement": [
      {
        "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
        "Condition": {
          "NumericGreaterThanEquals": {
            "Number": 600
          }
        }
      }
    ]
  }
```

### NumericLessThan

The **NumericLessThan** condition tests the numeric value of an event's property is strictly less than a desired value. If the property in the event exists but is not itself a numeric value it is converted to a number as described for NumericEquals.

Allows for multiple values? No

The following example shows a configuration that publishes events when the event has the property "Number" with a value greater than 1000:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericLessThan": {
          "Number": 1000
        }
      }
    }
  ]
}
```

### NumericLessThanEquals

The **NumericLessThanEquals** condition tests the numeric value of an event's property is less than or equal to a desired value. If the property in the event exists but is not itself a numeric value it is converted to a number as described for NumericEquals.

Allows for multiple values? No

The following example shows a configuration that publishes events when the event has the property "Number" with a value less than or equal to 500:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericLessThanEquals": {
          "Number": 500
        }
      }
    }
  ]
}
```

### StringEquals

The **StringEquals** condition tests the string value of an event's property is strictly equal to or more desired values.

Allows for multiple values? Yes

The following example shows a configuration that publishes events when the event has the property "EventType" equal to "SystemEvent" and property "TargetType" equal to "User" or "Role":

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringEquals": {
          "EventType": ["SystemEvent"],
          "TargetType" : ["User", "Role"]
        }
```

```
        }
      }
    ]
  }
```

### StringNotEquals

The **StringNotEquals** condition tests the string value of an event's property does not equal any of an undesired set of values.

Allows for multiple values? Yes

The following example shows a configuration that publishes events when the event has the property "EventType" not equal to "PacketLog" or "IntegrityEvent":

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringNotEquals": {
          "EventType": ["PacketLog", "IntegrityEvent"]
        }
      }
    }
  ]
}
```

### StringEqualsIgnoreCase

The **StringEqualsIgnoreCase** condition is the same as the StringEquals condition, except string matching is performed in a case-insensitive manner.

### StringNotEqualsIgnoreCase

The **StringNotEqualsIgnoreCase** condition is the same as the StringNotEquals condition, except string matching is performed in a case-insensitive manner.

### StringLike

The **StringLike** condition tests the string value of an event's property is equal to or more desired values, where the desired values may include the wildcard '*' to match any number of characters or '?' to match a single character. String comparisons are case-sensitive.

Allows for multiple values? Yes

The following example shows a configuration that publishes events when the event has the property "Title" which contains the string "User" or "Role":

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringLike": {
          "Title": ["*User*", "*Role*"]
        }
      }
    }
  ]
}
```

### StringNotLike

The **StringNotLike** condition tests that the string value of an event's property is not equal to any of an undesired set of values, where the values may include the wildcard '*' to match any number of characters or '?' to match a single character. String comparisons are case-sensitive.

Allows for multiple values? Yes

The following example shows a configuration that publishes all events except the "System Settings Saved" event:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringNotLike": {
          "Title":"System Settings Saved"
        }
      }
    }
  ]
}
```

The next example shows a configuration that publishes events when the event has the property "Title" that does not start with "User" and does not end with "Created":

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringNotLike": {
          "Title": ["User*", "*Created"]
        }
      }
    }
  ]
}
```

## Event Description

When published to Amazon SNS, events are sent as simple JSON objects encoded as strings. The properties in the objects are the elements of the event, and the values of the properties are typically strings or numbers. This section describes the properties that events can have and what values these properties can take.

### Event Data Types

Properties in an event will be one of the data types described in the following table:

| Data Type | Description |
|---|---|
| Boolean | The value will be the JSON `true` or `false` value. |
| Integer | The value will be a JSON `int` value. Deep Security does not output floating point numbers in events. Note that integer types in events are *not* guaranteed to fit in 32 bit integers. |
| Integer (enum) | The value will be a JSON `int` value, with the additional restriction that it can only be one of a limited set of enumerated values. |
| String | The value will be a JSON `string` value. |
| String (Date) | The value will be a date and time encoded in a JSON `string` value. Dates are encoded using ISO 8601 format YYYY-MM-DDThh:mm:ss.sssZ, always using 'Z' for the time zone designator and including three digits for sub-seconds. See the W3C note on date and time formats for more details about this encoding. |
| String (IP) | The value will be an IPv4 or IPv6 address encoded in a JSON `string` value. |
| String (MAC) | The value will be a JSON `string` value, with the additional restriction that it will contain a network MAC address. |
| String (URL) | The value will be a JSON `string` value, with the additional restriction that it will contain a URL. |
| String (enum) | The value will be a JSON `string` value, with the additional restriction that it can only be one of a limited set of enumerated values. |

## Event Properties

This section describes all the properties that may be seen in an event. Note that events will not necessarily contain all of the properties that are listed as applicable for the event type; in some circumstances a property will not apply and will not be present in the JSON object.

| Property Name | Data Type | Description | Applies To Event Type (s) |
|---|---|---|---|
| Action | Integer (enum) | Action taken for intrusion prevention event. 0=Unknown, 1=Deny, 2=Reset, 3=Insert, 4=Delete, 5=Replace, 6=Log Only, 0x81=Detect Only: Deny, 0x82=Detect Only: Reset, 0x83=Detect Only: Insert, 0x84=Detect Only: Delete, 0x85=Detect Only: Replace. | Intrusion prevention events |
| Action | Integer (enum) | Action taken for firewall event. "Detect Only" values show what would have happened if the rule had been enabled. 0=Unknown, 1=Deny, 6=Log Only, 0x81=Detect Only: Deny. | Firewall events |
| ActionBy | String | The name of the Deep Security Manager User who performed the event, or "System" if the event was not generated by a User. | System events |
| ActionString | String | Conversion of Action to a readable string. | Firewall events, intrusion prevention events |
| AdministratorID | Integer | Unique identifier of the Deep Security User who performed an action. Events generated by the system and not by a user will not have an identifier. | System events |
| ApplicationType | String | Name of the Application Type associated with the Intrusion Prevention Rule, if available. | Intrusion prevention events |
| Change | Integer (enum) | What type of change was made to a file, process, registry key, etc. for an integrity monitoring event. 1=Created, 2=Updated, 3=Deleted, 4=Renamed. | Integrity events, integrity events |

| Property Name | Data Type | Description | Applies To Event Type (s) |
|---|---|---|---|
| ContainerID | String | ID of the Docker container where the malware was found. | Anti-malware events |
| ContainerImageName | String | Image name of the Docker container where the malware was found. | Anti-malware events |
| ContainerName | String | Name of the Docker container where the malware was found. | Anti-malware events |
| Description | String | Description of the change made to the entity (created, deleted, updated) along with details about the attributes changed. | Integrity events |
| Description | String | Brief description of what happened during an event. | System events |
| DestinationIP | String (IP) | The IP Address of the destination of a packet. | Firewall events, intrusion prevention events |
| DestinationMAC | String (MAC) | The MAC Address of the destination of a packet. | Firewall events, intrusion prevention events |
| DestinationPort | Integer | The network port number a packet was sent to. | Firewall events, intrusion prevention events |
| DetectionCategory | Integer (enum) | The detection category for a web reputation event. 12=User Defined, 13=Custom, 91=Global. | Web reputation events |
| DetectOnly | Boolean | Whether or not the event was returned with the Detect Only flag turned on. If true, this indicates that the URL was not blocked, but access was detected. | Web reputation events |

| Property Name | Data Type | Description | Applies To Event Type (s) |
|---|---|---|---|
| Direction | Integer (enum) | Network packet direction. 0=Incoming, 1=Outgoing. | Firewall events, intrusion prevention events |
| DirectionString | String | Conversion Direction to a readable string. | Firewall events, intrusion prevention events |
| DriverTime | Integer | The time the log was generated as recorded by the driver. | Firewall events, intrusion prevention events |
| EndLogDate | String (Date) | The last log date recorded for repeated events. Will not be present for events that did not repeat. | Firewall events, intrusion prevention events |
| EngineType | Integer | The anti-malware engine type. | Anti-malware events |
| EngineVersion | String | The anti-malware engine version. | Anti-malware events |
| EntityType | String (enum) | The type of entity an integrity monitoring event applies to. One of: Directory, File, Group, InstalledSoftware, Port, Process, RegistryKey, RegistryValue, Service, User, Wql | Integrity events |
| ErrorCode | Integer | Error code for malware scanning events. If non-zero the scan failed, and the scan action and scan result fields contain more details. | Anti-malware events |
| EventID | Integer | The identifier of the event. Identifiers are unique per event type, but events of different types may share the same identifier. For example, it is possible for events | All event types |

| Property Name | Data Type | Description | Applies To Event Type (s) |
|---|---|---|---|
| | | with EventType firewall and ips to have EventID equal to 1. The combination of EventID, EventType and TenantID are required to completely identify an event in Deep Security. Note that this property is not related to the "Event ID" property of a System Event in the Deep Security Manager. | |
| EventType | String (enum) | The type of the event. One of: "SystemEvent", "PacketLog", "PayloadLog", "AntiMalwareEvent", "WebReputationEvent", "IntegrityEvent", "LogInspectionEvent". | All event types |
| Flags | String | Flags recorded from a network packet; a space-separated list of strings. | Firewall events, intrusion prevention events |
| Flow | Integer (enum) | Network connection flow. Possible values: -1=Not Applicable, 0=Connection Flow, 1=Reverse Flow | Firewall events, intrusion prevention events |
| FlowString | String | Conversion of Flow to a readable string. | Firewall events, intrusion prevention events |
| Frame | Integer (enum) | Frame type. -1=Unknown, 2048=IP, 2054=ARP, 32821=REVARP, 33169=NETBEUI, 0x86DD=IPv6 | Firewall events, intrusion prevention events |
| FrameString | String | Conversion of Frame to a readable string. | Firewall events, intrusion prevention events |

| Property Name | Data Type | Description | Applies To Event Type (s) |
|---|---|---|---|
| HostAgentVersion | String | The version of the agent protecting the computer where the event was detected. | Anti-malware events, web reputation events, integrity events, log inspection events, firewall events, intrusion prevention events |
| HostAssetValue | Integer | The asset value assigned to the computer at the time the event was generated. | Anti-malware events, web reputation events, integrity events, log inspection events, firewall events, intrusion prevention events |
| HostGroupID | Integer | The unique identifier of the Computer Group of the computer where the event was detected. | Anti-malware events, web reputation events, integrity events, log inspection events, firewall events, intrusion prevention events |
| HostGroupName | String | The name of the Computer Group of the computer | Anti-malware |

| Property Name | Data Type | Description | Applies To Event Type (s) |
|---|---|---|---|
| | | where the event was detected. Note that Computer Group names may not be unique. | events, web reputation events, integrity events, log inspection events, firewall events, intrusion prevention events |
| HostID | Integer | Unique identifier of the computer the event applies to. | Anti-malware events, web reputation events, integrity events, log inspection events, firewall events, intrusion prevention events |
| HostInstanceID | String | The cloud instance ID of the computer where the event was detected. This property will only be set for computers synchronized with a Cloud Connector. | Anti-malware events, web reputation events, integrity events, log inspection events, firewall events, intrusion prevention events |
| Hostname | String | Name of the computer on which the event was generated. | Anti-malware events, web |

| Property Name | Data Type | Description | Applies To Event Type (s) |
|---|---|---|---|
| | | | reputation events, integrity events, log inspection events, firewall events, intrusion prevention events |
| HostOS | String | The Operating System running on the computer where the event was detected. | Anti-malware events, web reputation events, integrity events, log inspection events, firewall events, intrusion prevention events |
| HostOwnerID | String | The cloud account ID of the computer where the event was detected. This property will only be set for computers synchronized with a Cloud Connector. | Anti-malware events, web reputation events, integrity events, log inspection events, firewall events, intrusion prevention events |
| HostSecurityPolicyID | Integer | The unique identifier of the Security Policy applied to the computer where the event was detected. | Anti-malware events, web reputation |

| Property Name | Data Type | Description | Applies To Event Type (s) |
|---|---|---|---|
| | | | events, integrity events, log inspection events, firewall events, intrusion prevention events |
| HostSecurityPolicyName | String | The name of the Security Policy applied to the computer where the event was detected. Note that Security Policy names may not be unique. | Anti-malware events, web reputation events, integrity events, log inspection events, firewall events, intrusion prevention events |
| HostVCUUID | String | The vCenter UUID of the computer the event applies to, if known. | Anti-malware events, web reputation events, integrity events, log inspection events, firewall events, intrusion prevention events |
| InfectedFilePath | String | Path of the infected file in the case of malware detection. | Anti-malware events |
| InfectionSource | String | The name of the computer that's the source of a | Anti-malware |

| Property Name | Data Type | Description | Applies To Event Type (s) |
|---|---|---|---|
| | | malware infection, if known. | events |
| Interface | String (MAC) | MAC address of the network interface sending or receiving a packet. | Firewall events, intrusion prevention events |
| IPDatagramLength | Integer | The length of the IP datagram. | Intrusion prevention events |
| IsHash | String | The SHA-1 content hash (hexadecimal encoded) of the file after it was modified. | Integrity events |
| Key | String | The file or registry key an integrity event refers to. | Integrity events |
| LogDate | String (Date) | The date and time the event was recorded. For Agent-generated events (Firewall, IPS, etc.) the date is the date the event was recorded by the Agent, not the time the event was sent to Deep Security Manager. | All event types |
| MajorVirusType | Integer (enum) | The classification of malware detected. 0=Joke, 1=Trojan, 2=Virus, 3=Test, 4=Spyware, 5=Packer, 6=Generic, 7=Other | Anti-malware events |
| MajorVirusTypeString | String | Conversion of MajorVirusType to a readable string. | Anti-malware events |
| MalwareName | String | The name of the malware detected. | Anti-malware events |
| MalwareType | Integer (enum) | The type of malware detected. 1=General malware, 2=Spyware. General malware events will have an InfectedFilePath, spyware events will not. | Anti-malware events |
| ManagerNodeID | Integer | Unique identifier of the Deep Security Manager Node where the event was generated. | System events |
| ManagerNodeName | String | Name of the Deep Security Manager Node where the | System |

| Property Name | Data Type | Description | Applies To Event Type (s) |
|---|---|---|---|
| | | event was generated. | events |
| Number | Integer | System events have an additional ID that identifies the event. Note that in the Deep Security Manager, this property appears as "Event ID". | System events |
| Origin | Integer (enum) | The origin of the event. -1=Unknown, 0=Agent, 1=In-VM guest agent, 2=Appliance, 3=Deep Security Manager | All event types |
| OriginString | String | Conversion of Origin to a readable string. | All event types |
| OSSEC_Action | String | OSSEC action | Log inspection events |
| OSSEC_Command | String | OSSEC command | Log inspection events |
| OSSEC_Data | String | OSSEC data | Log inspection events |
| OSSEC_Description | String | OSSEC description | Log inspection events |
| OSSEC_DestinationIP | String | OSSEC dstip | Log inspection events |
| OSSEC_DestinationPort | String | OSSEC dstport | Log inspection events |
| OSSEC_ DestinationUser | String | OSSEC dstuser | Log inspection events |

| Property Name | Data Type | Description | Applies To Event Type (s) |
|---|---|---|---|
| OSSEC_FullLog | String | OSSEC full log | Log inspection events |
| OSSEC_Groups | String | OSSEC groups result (e.g. syslog,authentication_failure) | Log inspection events |
| OSSEC_Hostname | String | OSSEC hostname. This is the name of the host as read from a log entry, which is not necessarily the same as the name of the host on which the event was generated. | Log inspection events |
| OSSEC_ID | String | OSSEC id | Log inspection events |
| OSSEC_Level | Integer (enum) | OSSEC level. An integer in the range 0 to 15 inclusive. 0-3=Low severity, 4-7=Medium severity, 8-11=High severity, 12-15=Critical severity. | Log inspection events |
| OSSEC_Location | String | OSSEC location | Log inspection events |
| OSSEC_Log | String | OSSEC log | Log inspection events |
| OSSEC_ProgramName | String | OSSEC program_name | Log inspection events |
| OSSEC_Protocol | String | OSSEC protocol | Log inspection events |
| OSSEC_RuleID | Integer | OSSEC rule id | Log inspection events |

| Property Name | Data Type | Description | Applies To Event Type (s) |
|---|---|---|---|
| OSSEC_SourceIP | Integer | OSSEC srcip | Log inspection events |
| OSSEC_SourcePort | Integer | OSSEC srcport | Log inspection events |
| OSSEC_SourceUser | Integer | OSSEC srcuser | Log inspection events |
| OSSEC_Status | Integer | OSSEC status | Log inspection events |
| OSSEC_SystemName | Integer | OSSEC systemname | Log inspection events |
| OSSEC_URL | Integer | OSSEC url | Log inspection events |
| PacketData | Integer | Hexadecimal encoding of captured packet data, if the rule was configured to capture packet data. | Intrusion prevention events |
| PacketSize | Integer | The size of the network packet. | Firewall events |
| PatternVersion | Integer (enum) | The malware detection pattern version. | Anti-malware events |
| PayloadFlags | Integer | Intrusion Prevention Filter Flags. A bitmask value that can include the following flag values: 1 - Data truncated - Data could not be logged. 2 - Log Overflow - Log overflowed after this log. 4 - Suppressed - Logs threshold suppressed after this log. 8 - Have Data - Contains packet data. 16 - Reference Data - References previously logged data. | Intrusion prevention events |

| Property Name | Data Type | Description | Applies To Event Type (s) |
|---|---|---|---|
| PosInBuffer | Integer | Position within packet of data that triggered the event. | Intrusion prevention events |
| PosInStream | Integer | Position within stream of data that triggered the event. | Intrusion prevention events |
| Process | String | The name of the process that generated the event, if available. | Integrity events |
| Protocol | Integer (enum) | The numerical network protocol identifier. -1=Unknown, 1=ICMP, 2=IGMP, 3=GGP, 6=TCP, 12=PUP, 17=UDP, 22=IDP, 58=ICMPv6, 77=ND, 255=RAW | Firewall events, Intrusion prevention events |
| ProtocolString | String | Conversion of Protocol to a readable string. | Firewall events, intrusion prevention events |
| Rank | Integer | The numerical rank of the event; the product of the computer's assigned asset value and the severity value setting for an event of this severity. | Integrity events, log inspection events, firewall events, intrusion prevention events |
| Reason | String | Name of the Firewall Rule that caused the event, or a mapping of Status to String if the event was not caused by a Rule. | Firewall events |
| Reason | String | Name of Integrity Rule that caused this event, if known. | Integrity events |
| Reason | String | Name of the Anti-Malware configuration that caused the event, if known. | Anti-malware events |

| Property Name | Data Type | Description | Applies To Event Type (s) |
|---|---|---|---|
| Reason | String | Name of the Intrusion Prevention Rule that caused the event, or a mapping of Status to String if the event was not caused by a Rule. | Intrusion prevention events |
| RepeatCount | Integer | The number of times this event was sequentially repeated. A repeat count of 1 indicates the event was only observed once and did not repeat. | Firewall events, intrusion prevention events |
| Risk | Integer (enum) | Translated risk level of the URL accessed. 2=Suspicious, 3=Highly Suspicious, 4=Dangerous, 5=Untested, 6=Blocked by Administrator | Web reputation events |
| RiskLevel | Integer | The raw risk level of the URL from 0 to 100. Will not be present if the URL was blocked because it was blocked by a block rule. | Web reputation events |
| RiskString | String | Conversion of Risk to a readable string. | Web reputation events |
| ScanAction1 | Integer | Scan action 1. Scan action 1 & 2 and scan result actions 1 & 2 and ErrorCode are combined to form the single "summaryScanResult". | Anti-malware events |
| ScanAction2 | Integer | Scan action 2. | Anti-malware events |
| ScanResultAction1 | Integer | Scan result action 1. | Anti-malware events |
| ScanResultAction2 | Integer | Scan result action 2. | Anti-malware events |
| ScanResultString | String | Malware scan result, as a string. A combination of ScanAction 1 and 2, ScanActionResult 1 and 2, and ErrorCode. | Anti-malware events |
| ScanType | Integer (enum) | Malware scan type that created the event. 0=Real-Time, 1=Manual, 2=Scheduled, 3=Quick Scan | Anti-malware events |

| Property Name | Data Type | Description | Applies To Event Type (s) |
|---|---|---|---|
| ScanTypeString | String | Conversion of ScanType to a readable string. | Anti-malware events |
| Severity | Integer | 1=Info, 2=Warning, 3=Error | System events |
| Severity | Integer (enum) | 1=Low, 2=Medium, 3=High, 4=Critical | Integrity events, intrusion prevention events |
| SeverityString | String | Conversion of Severity to a readable string. | System events, integrity events, intrusion prevention events |
| SeverityString | String | Conversion of OSSEC_Level to a readable string. | Log inspection events |
| SourceIP | String (IP) | The IP address of the source of a packet. | Firewall events, intrusion prevention events |
| SourceMAC | String (MAC) | The MAC Address of the source of a packet. | Firewall events, intrusion prevention events |
| SourcePort | Integer | The network port number a packet was sent from. | Firewall events, intrusion prevention events |

| Property Name | Data Type | Description | Applies To Event Type (s) |
|---|---|---|---|
| Status | Integer | If this event was not generated by a specific Firewall Rule then this status is one of approximately 50 hard-coded rules, e.g. 123=Out Of Allowed Policy | Firewall events |
| Status | Integer | If this event was not generated by a specific IPS Rule then this status is one of approximately 50 hard-coded reasons, e.g. -504=Invalid UTF8 encoding | Intrusion prevention events, intrusion prevention events |
| Tags | String | Comma-separated list of tags that have been applied to the event. This list will only include tags that are automatically applied when the event is generated. | All event types |
| TargetID | Integer | Unique identifier of the target of the event. This identifier is unique for the targets of the same type within a tenant. It is possible for target IDs to be reused across different types, for example, both a Computer and a Policy may have target ID 10. | System events |
| TargetIP | String (IP) | IP Address that was being contacted when a Web Reputation Event was generated. | Web reputation events |
| TargetName | String | The name of the target of the event. The target of a system event can be many things, including computers, policies, users, roles, and tasks. | System events |
| TargetType | String | The type of the target of the event. | System events |
| TenantID | Integer | Unique identifier of the tenant that generated the event. | All event types |
| TenantName | String | Name of the tenant that generated the event. | All event types |
| Title | String | Title of the event. | System events |

| Property Name | Data Type | Description | Applies To Event Type (s) |
|---|---|---|---|
| URL | String (URL) | The URL being accessed that generated the event. | Web reputation events |
| User | String | The user account that was the target of an integrity monitoring event, if known. | Integrity events |

## Example events in JSON format

The following is an example of a system event:


```
{
  "ActionBy": "System",
  "Description": "A request has been made to synchronize
computers with Cloud Account: Amazon",
  "EventID": 4947,
  "EventType": "SystemEvent",
  "LogDate": "2014-10-29T13:13:38.500Z",
  "ManagerNodeID": 41,
  "ManagerNodeName": "192.168.0.1",
  "Number": 1906,
  "Origin": 3,
  "OriginString": "Manager",
  "Severity": 1,
  "SeverityString": "Info",
  "Tags": "",
  "TargetID": 1,
  "TargetName": "Amazon -  US East (Virginia)",
  "TargetType": "Cloud",
  "TenantID": 1984,
  "TenantName": "Planet Express",
  "Title": "Cloud Provider Synchronization Requested"
```

```
}
```


The following is an example of an integrity monitoring event:


```
{
  "Change": 4,
  "ChangeString": "Renamed",
  "Description": "No description is available.",
  "EventID": 2187499,
  "EventType": "IntegrityEvent",
  "HostAgentVersion": "9.0.0.883",
  "HostAssetValue": 1,
  "HostGroupID": 2,
  "HostGroupName": "Intranet",
  "HostID": 2,
  "Hostname": "hr_data2",
  "HostOS": "Microsoft Windows Server 2008 R2",
  "HostSecurityPolicyID": 9,
  "HostSecurityPolicyName": "Windows Server 2008",
  "Key": "C:\\Windows\\system32\\explorer.exe -\u003e
C:\\Windows\\system32\\explorer2.exe",
  "LogDate": "2014-10-29T13:18:08.380Z",
  "Origin": 0,
  "OriginString": "Agent",
  "Process": "",
  "Rank": 50,
  "Reason": "1002777 - Microsoft Windows - System configuration
file modified",
  "Severity": 3,
  "SeverityString": "High",
  "Tags": "",
  "TenantID": 0,
  "TenantName": "Primary",
```

```
    "Type": "File"
  }
```

## Example Configurations

This section gives some SNS configuration examples for different scenarios.

### Send all critical intrusion prevention events to an SNS topic

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericEquals": {
          "Severity": 4
        },
        "StringEquals" : {
          "EventType" : "PayloadLog"
        }
      }
    }
  ]
}
```

### Send different events to different SNS topics

This example shows sending all system events to one topic and all integrity monitoring events to a different topic.

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-
```

```
1:012345678901:systemEventsTopic",
      "Condition": {
        "StringEquals" : {
          "EventType" : "SystemEvent"
        }
      }
    },
    {
      "Topic": "arn:aws:sns:us-east-
1:012345678901:integrityTopic",
      "Condition": {
        "StringEquals" : {
          "EventType" : "IntegrityEvent"
        }
      }
    }
  ]
}
```

## Multiple statements vs. multiple conditions

If you create multiple statements for the same SNS topic, those statements are evaluated as if they are joined by "or". If a statement contains multiple conditions, those conditions are evaluated as if they are joined by "and".

### Multiple statements

This is an example of what not to do. The first statement says to forward all events other than "System Settings Saved". The second statement says to forward all "System Settings Saved" events. The result is that all events will be forwarded because any event will match either the condition in the first statement **or** the one in the second statement:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
```

```
        "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
        "Condition": {
          "StringNotLike" : {
            "Title" : "System Settings Saved"
          }
        }
      },
      {
        "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
        "Condition": {
          "StringLike" : {
            "Title" : "System Settings Saved"
          }
        }
      }
    ]
  }
```

### Multiple conditions

This is another example of what not to do. The first condition says to forward all events other than "System Settings Saved". The second condition says to forward all "System Settings Saved" events. The result is that no events will be forwarded because no events will match both the condition in the first statement **and** the one in the second statement:

```
  {
    "Version": "2014-09-24",
    "Statement": [
      {
        "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
        "Condition": {
          "StringNotLike" : {
            "Title" : "System Settings Saved"
          },
          "StringLike" : {
```

```
            "Title" : "System Settings Saved"
          }
        }
      }
    ]
  }
```

# DevOps, automation and scaling

## DevOps, automation and scaling

To support DevOps workflows, Deep Security offers APIs to automate, monitor, and manage security throughout the release lifecycle. (See "Use the Deep Security API to automate tasks" on page 261.)

To accelerate integration with popular DevOps tools, we've provided the following resources in Github for Chef, Puppet, and Ansible:

- https://github.com/deep-security/puppet
- https://github.com/deep-security/chef
- https://github.com/deep-security/ansible

These resources provide a starting point to integrate Deep Security with your specific deployment, including agent deployment and configuration and support for elastic workloads.

Deep Security also offers many other ways to speed up the protection of your computers and other resources:

- "Schedule Deep Security to perform tasks" on page 263
- "Automatically perform tasks when a computer is added or changed" on page 266
- "AWS Auto Scaling and Deep Security" on page 271
- "Use deployment scripts to add and protect computers" on page 281
- "Automatically assign policies by AWS instance tags" on page 285
- "Command-line basics" on page 244

In addition, Deep Security provides the ability to forward events to SIEMs such as Spunk, QRadar, ArcSight, as well as Amazon SNS. For details, see:

- "Forward Deep Security events to an external syslog or SIEM server " on page 814
- "Access events with Amazon SNS" on page 864

## Forward system events to a remote computer via SNMP

Deep Security supports SNMP for forwarding system events to a computer from Deep Security Manager. On Windows, the MIB file ("DeepSecurity.mib") is located in \Trend Micro\Deep Security Manager\util. On Linux, the default location is /opt/dsm/util.

## Lists of events and alerts

The following sections list all of the Deep Security alerts and events you could encounter.

- "Predefined alerts" below
- "Agent events" on page 914
- "System events" on page 918
- "Anti-malware events" on page 942
- "Firewall events" on page 944
- "Intrusion prevention events" on page 953
- "Integrity monitoring events" on page 957
- "Log inspection events" on page 960

### Predefined alerts

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| Abnormal Restart Detected | Warning | Yes | An abnormal restart has been detected on the computer. This condition may be caused by a variety of conditions. If the agent/appliance is suspected as the root cause then the diagnostics package (located in the Support section of the Computer Details dialog) should be invoked. |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| Activation Failed | Critical | No | This may indicate a problem with the agent/appliance, but it also can occur if agent self-protection is enabled. On the Deep Security Manager, go to **Computer editor**[1] > **Settings** > **General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override. |
| A Deep Security Relay cannot download security components | Critical | No | A Deep Security Relay can't successfully download security components. This might be due to network connectivity issues or misconfigurations in Deep Security Manager under **Administration > System Settings > Updates**. Check your network configurations (for example, the proxy settings of the relay group) and **System Settings**, and then manually initiate an update on the relay using the **Download Security Update** option on the **Administration > Updates > Software** page. |
| Agent configuration package too large | Warning | Yes | This is usually caused by too many firewall and intrusion prevention rules being assigned. Run a recommendation scan on the computer to determine if any rules can be safely unassigned. |
| Agent Installation Failed | Critical | Yes | The agent failed to install successfully on one or more computers. Those computers are currently unprotected. You must reboot the computers which will automatically restart the agent install program.<br><br>This may indicate a problem with the agent/appliance, but it also can occur if agent self-protection is enabled. On the Deep Security Manager, go to **Computer editor**[2] > **Settings** > **General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override. |
| Agent Upgrade Recommended (Incompatible with Appliance) | Warning | No | Deep Security Manager has detected a computer with a version of the agent that is not compatible with the appliance. The appliance will always filter network traffic in this configuration resulting in redundant protection. (Deprecated in 9.5) |

[1]To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2]To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| Agent/Appliance Upgrade Recommended | Warning | No | The Deep Security Manager has detected an older agent/appliance version on the computer that does not support all available features. An upgrade of the agent/appliance software is recommended. (Deprecated in 9.5) |
| Agent/ApplianceUpgrade Recommended (Incompatible Security Update(s)) | Warning | No | Deep Security Manager has detected a computer with a version of the agent/appliance that is not compatible with one or more security updates assigned to it. An upgrade of the agent/appliance software is recommended. |
| Agent/ApplianceUpgrade Recommended (New Version Available) | Warning | No | Deep Security Manager has detected one or more computers with a version of the agent/appliance that is older than the latest version imported into the manager. An upgrade of the agent/appliance software is recommended. |
| Agent/Appliance Upgrade Required | Warning | No | Deep Security Manager has detected a computer with a version of the agent/appliance that is not compatible with this version of the manager. An upgrade of the agent/appliance software is required. |
| An update to the Rules is available | Warning | No | Updated rules have been downloaded but not applied to your policies. To apply the rules, go to **Administration** > **Updates** > **Security** and in the **Rule Updates** column, click **Apply Rules to Policies**. |
| Anti-Malware Alert | Warning | Yes | A malware scan configuration that is configured for alerting has raised an event on one or more computers. |
| Anti-Malware Component Failure | Critical | Yes | An anti-malware component failed on one or more computers. See the event descriptions on the individual computers for specific details. |
| Anti-Malware Component Update Failed | Warning | No | One or more agent or relay failed to update anti-malware components. See the affected computers for more information. |
| Anti-Malware Engine Offline | Critical | No | The agent or appliance has reported that the anti-malware engine is not responding. Please check the system events for the computer to determine the cause of the failure. |
| Anti-Malware protection is absent or out of date | Warning | No | The agent on this computer has not received its initial anti-malware protection package, or its anti-malware protection is out of date. Make sure a relay is available and that the agent has been properly configured to communicate with it. To configure relays and other update options, go to Administration > System Settings > Updates. |
| Anti-malware module maximum disk space used to store identified files exceeded | Warning | Yes | The Anti-Malware module was unable to analyze or quarantine a file because the maximum disk space used to store identified files was reached. To change the maximum disk space for identified files setting, open the computer or policy editor and go to the Anti-malware > Advanced tab. |
| Application Control Ruleset is incompatible with agent version | Critical | No | An application control ruleset could not be assigned to one or more computers because the ruleset is not supported by the installed version of the agent. Typically, the problem is that a |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | hash-based ruleset (which is compatible only with Deep Security Agent 11.0 or newer) has been assigned to an older Deep Security Agent. Deep Security Agent 10.x supports only file-based rulesets. (For details, see "Differences in how Deep Security Agent 10.x and 11.x compare files" on page 462.) To fix this issue, upgrade the Deep Security Agent to version 11.0 or newer. Alternatively, if you are using local rulesets, reset application control for the agent. Or if you are using a shared ruleset, use a shared ruleset that was created with Deep Security 10.x until all agents using the shared ruleset are upgraded to Deep Security Agent 11.0 or newer. |
| Application Type Misconfiguration | Warning | No | Misconfiguration of application types may prevent proper security coverage. |
| Application Type Recommendation | Warning | Yes | Deep Security Manager has determined that a computer should be assigned an application type. This could be because an agent was installed on a new computer and vulnerable applications were detected, or because a new vulnerability has been discovered in an installed application that was previously thought to be safe. To assign the application type to the computer, open the 'Computer Details' dialog box, click on 'Intrusion Prevention Rules', and assign the application type. |
| Maintenance Mode Active | Warning | No | Maintenance mode is currently active for application control on one or more computers. While this mode is active, application control continues to enforce block rules (if you selected **Block unrecognized software until it is explicitly allowed**), but will allow software updates, and automatically add them to the inventory part of the ruleset. When the software update is finished for each computer, disable maintenance mode so that unauthorized software is not accidentally added to the ruleset. |
| Census, Good File Reputation, and Predictive Machine Learning Service Disconnected | | | Disconnected from Census, Good File Reputation, and Predictive Machine Learning Service. Please see the event details below for possible solutions.<br><br>Refer to "Warning: Census, Good File Reputation, and Predictive Machine Learning Service Disconnected" on page 985 for troubleshooting tips. |
| Certified Safe Software Service Offline | Warning | No | A Deep Security Manager node cannot connect to the Trend Micro Certified Safe Software Service to perform file signature comparisons for the integrity monitoring module. A locally cached database will be used until connectivity is restored. Make sure the manager node has internet connectivity and that proxy settings (if any) are correct. |
| Clock Change Detected | Warning | Yes | A clock change has been detected on the computer. Unexpected clock changes may indicate a problem on the computer and |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | should be investigated before the alert is dismissed. |
| Cloud Computer Not Managed as Part of Cloud Account | Warning | Yes | An agent was activated on one or more Amazon WorkSpace but WorkSpaces are not enabled for your AWS account. To enable WorkSpaces, click 'Edit AWS Account' above, and select the 'Include Amazon WorkSpaces' check box. Your WorkSpace(s) are moved into the WorkSpaces folder of the AWS Account, and are billed at a lower hourly rate (if you are using hourly billing). |
| Communications Problem Detected | Warning | Yes | A communications problem has been detected on the computer. Communications problems indicate that the computer cannot initiate communication with the Deep Security Manager(s) because of network configuration or load reasons. Please check the system events in addition to verifying communications can be established to the Deep Security Manager(s) from the computer. The cause of the issue should be investigated before the alert is dismissed. |
| Computer Not Receiving Updates | Warning | No | These computer(s) have stopped receiving updates. Manual intervention may be required. |
| Computer Reboot Required | Critical | Yes | The agent software upgrade was successful, but the computer must be rebooted for the install to be completed. The computer(s) should be manually updated before the alert is dismissed. |
| Computer Reboot Required for Anti-Malware Protection | Critical | No | The anti-malware protection on the agent has reported that the computer needs to be rebooted. Please check the system events for the computer to determine the reason for the reboot. |
| Configuration Required | Warning | No | One or more computers are using a policy that defines multiple interface types where not all interfaces have been mapped. |
| Connection to Filter Driver Failure | Critical | No | An appliance has reported a failure connecting to the filter driver. This may indicate a configuration issue with the filter driver running on the ESXi or with the appliance. The appliance must be able to connect to the filter driver in order to protect guests. The cause of the issue should be investigated and resolved. |
| CPU Critical Threshold Exceeded | Critical | No | The CPU critical threshold has been exceeded. |
| CPU Warning Threshold Exceeded | Warning | No | The CPU warning threshold has been exceeded. |
| Duplicate Computer Detected | Warning | Yes | A duplicate computer has been activated or imported. Please remove the duplicate computer and reactivate the original computer if necessary. |
| Duplicate Unique Identifiers Detected | Warning | No | Duplicate UUIDs have been detected. Please remove the duplicate UUID. |
| Empty Relay Group Assigned | Critical | No | These computers have been assigned an empty relay group. Assign a different relay group to the computers or add relays to the empty relay group(s). |
| Events Suppressed | Warning | Yes | The agent/appliance encountered an unexpectedly high volume of events. As a result, one or more events were not recorded (suppressed) to prevent a potential denial of service. Check the firewall events to determine the cause of the suppression. |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| Events Truncated | Warning | Yes | Some events were lost because the data file grew too large for the agent/appliance to store. This may have been caused by an unexpected increase in the number of events being generated, or the inability of the agent/appliance to send the data to the Deep Security Manager. For more information, see the properties of the "Events Truncated" system event on the computer. |
| Files Could Not Be Scanned for Malware | Warning | No | Files could not be scanned for malware because the file path exceeded the maximum file path length limit or the directory depth exceeded the maximum directory depth limit. Please check the system events for the computer to determine the reason. |
| Firewall Engine Offline | Critical | No | The agent/appliance has reported that the firewall engine is offline. Please check the status of the engine on the agent/appliance. |
| Firewall Rule Alert | Warning | Yes | A firewall rule that is selected for alerting has been encountered on one or more computers. |
| Firewall Rule Recommendation | Warning | Yes | Deep Security Manager has determined that a computer on your network should be assigned a firewall rule. This could be because an agent was installed on a new computer and vulnerable applications were detected, or because a new vulnerability has been discovered in an installed application that was previously thought to be safe. To assign the firewall rule to the computer, open the 'Computer Details' dialog box, click on the 'Firewall Rules' node, and assign the firewall rule. |
| Heartbeat Server Failed | Warning | No | The heartbeat server failed to start properly. This may be due to a port number conflict. Agents/appliances will not be able to contact the manager until this problem is resolved. To resolve this problem ensure that another service is not using the port number reserved for use by the heartbeat server and "Restart the Deep Security Manager" on page 734 service. If you do not wish to use the heartbeat you can turn this alert off in the Alert Configuration section. |
| Incompatible Agent/Appliance Version | Warning | No | Deep Security Manager has detected a more recent agent/appliance version on the computer that is not compatible with this version of the manager. An upgrade of the manager software is recommended. |
| Insufficient Disk Space | Warning | Yes | The agent/appliance has reported that it was forced to delete an old log file to free up disk space for a new log file. Please immediately free up disk space to prevent loss of intrusion prevention, firewall and agent/appliance events. See "Warning: Insufficient disk space" on page 988. |
| Integrity Monitoring Engine Offline | Critical | No | The agent/appliance has reported that the integrity monitoring engine is not responding. Please check the system events for the computer to determine the cause of the failure. |
| Integrity Monitoring information collection | Warning | No | The rate at which integrity monitoring information is collected has been temporarily delayed due to an increased amount of integrity |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| has been delayed | | | monitoring data. During this time the baseline and integrity event views may not be current for some computers. This alert will be dismissed automatically once integrity monitoring data is no longer being delayed. |
| Integrity Monitoring Rule Alert | Warning | Yes | An integrity monitoring rule that is selected for alerting has been encountered on one or more computers. |
| Integrity Monitoring Rule Compilation Error | Critical | No | An error was encountered compiling an integrity monitoring rule on a computer. This may result in the integrity monitoring rule not operating as expected. |
| Integrity Monitoring Rule Recommendation | Warning | Yes | Deep Security Manager has determined that a computer on your network should be assigned an integrity monitoring rule. To assign the integrity monitoring rule to the computer, open the 'Computer Details' dialog box, click on the 'Integrity Monitoring > Integrity Monitoring Rules' node, and assign the integrity monitoring rule. |
| Integrity Monitoring Rule Requires Configuration | Warning | No | An integrity monitoring rule that requires configuration before use has been assigned to one or more computers. This rule will not be sent to the computer(s). Open the integrity monitoring rule properties and select the Configuration tab for more information. |
| Integrity Monitoring Trusted Platform Module Not Enabled | Warning | Yes | Trusted platform module not enabled. Please ensure the hardware is installed and the BIOS setting is correct. |
| Integrity Monitoring Trusted Platform Module Register Value Changed | Warning | Yes | Trusted platform module register value changed. If you have not modified the ESXi hypervisor configuration this may represent an attack. |
| Intrusion Prevention Engine Offline | Critical | No | The agent/appliance has reported that the intrusion prevention engine is offline. Please check the status of the engine on the agent/appliance. |
| Intrusion Prevention Rule Alert | Warning | Yes | An intrusion prevention rule that is selected for alerting has been encountered on one or more computers. |
| Intrusion Prevention Rule Recommendation | Warning | Yes | Deep Security Manager has determined that a computer on your network should be assigned an intrusion prevention rule. This could be because an agent was installed on a new computer and vulnerable applications were detected, or because a new vulnerability has been discovered in an installed application that was previously thought to be safe. To assign the intrusion prevention rule to the computer, open the 'Computer Details' dialog box, click on 'Intrusion Prevention Rules', and assign the intrusion prevention rule. |
| Intrusion Prevention Rule Removal Recommendation | Warning | Yes | Deep Security Manager has determined that a computer on your network has an intrusion prevention rule assigned to it that is not required. This could be because a vulnerable application was uninstalled, an existing vulnerability was patched, or the rule was unnecessarily assigned to begin with. To unassign the intrusion prevention rule from the computer, open the 'Computer Details' dialog box, click on Intrusion Prevention > Intrusion Prevention |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | Rules, and clear the checkbox next to the intrusion prevention rule. |
| Intrusion Prevention Rule Requires Configuration | Warning | No | An intrusion prevention rule that requires configuration before use has been assigned to one or more computers. This rule will not be sent to the computer(s). Open the intrusion prevention rule properties and select the Configuration tab for more information. |
| Log Inspection Engine Offline | Critical | No | The agent/appliance has reported that the log inspection engine has failed to initialize. Please check the system events for the computer to determine the cause of the failure. |
| Log Inspection Rule Alert | Warning | Yes | A log inspection rule that is selected for alerting has been encountered on one or more computers. |
| Log Inspection Rule Recommendation | Warning | Yes | Deep Security Manager has determined that a computer on your network should be assigned a log inspection rule. To assign the log inspection rule to the computer, open the 'Computer Details' dialog box, click on the 'Log Inspection > Log Inspection Rules' node, and assign the log inspection rule. |
| Log Inspection Rule Requires Configuration | Warning | No | A log inspection rule that requires configuration before use has been assigned to one or more computers. This rule will not be sent to the computer(s). Open the Log Inspection Rule properties and select the Configuration tab for more information. |
| Low Disk Space | Warning | No | A Deep Security Manager Node has less than 10% remaining disk space. Please free space by deleting old or unnecessary files, or add more storage capacity. |
| Manager Offline | Warning | No | A Deep Security Manager node is offline. It is possible the computer has a hardware or software problem, or has simply lost network connectivity. Please check the status of the manager's computer. |
| Manager Time Out of Sync | Critical | No | The clock on each manager node must be synchronized with the clock on the database. If the clocks are too far out of sync (more than 30 seconds) the manager node will not perform its tasks correctly. Synchronize the clock on your manager node with the clock on the database. |
| Memory Critical Threshold Exceeded | Critical | No | The memory critical threshold has been exceeded. |
| Memory Warning Threshold Exceeded | Warning | No | The memory warning threshold has been exceeded. |
| Multiple Activated Appliances Detected | Warning | Yes | The appliance has reported that multiple connections have been made to the filter driver on the same ESXi. This indicates that there may be multiple activated Appliances running on the same ESXi, which is not supported. The cause of the issue should be investigated before the alert is dismissed. |
| Network Engine Mode Incompatibility | Warning | No | Setting "Network Engine Mode" to "Tap" is only available on agent versions 5.2 or higher. Review and update the agent's configuration or upgrade the agent to resolve the incompatibility. |
| New Pattern Update is | Warning | No | New patterns are available as part of a security update. The |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| Downloaded and Available | | | patterns have been downloaded to Deep Security but have not yet been applied to your computers. To apply the update to your computers, go to the Administration > Updates > Security page. |
| New Rule Update is Downloaded and Available | Warning | No | New rules are available as part of a security update. The rules have been downloaded to Deep Security but have not yet been applied to policies and sent to your computers. To apply the update and send the updated policies to your computers, go to the Administration > Updates > Security page. |
| Newer Version of Deep Security Manager is Available | Warning | No | A new version of the Deep Security Manager is available. Download the latest version from the Trend Micro Download Center at http://downloadcenter.trendmicro.com/ |
| Newer Versions of Software Available | Warning | No | New software is available. Software can be downloaded from the Download Center. |
| Number of Computers exceeds database limit | Warning | No | The number of activated computers has exceeded the recommended limit for an embedded database. Performance will degrade rapidly if more computers are added and it is strongly suggested that another database option (Oracle or SQL Server) be considered at this point. Please contact Trend Micro for more information on upgrading your database. |
| Protection Module Licensing Expired | Warning | Yes | The protection module license has expired. |
| Protection Module Licensing Expires Soon | Warning | No | The protection module licensing will expire soon. You can remove this alert by changing your license on the Administration > Licenses page. |
| Recommendation | Warning | Yes | Deep Security Manager has determined that the security configuration of one of your computers should be updated. To see what changes are recommended, open the **Computer editor**[1] and look through the module pages for warnings of unresolved recommendations. In the Assigned Rules area, click **Assign/Unassign** to display the list of available rules and then filter them using the "Show Recommended for Assignment" viewing filter option. (Select "Show Recommended for Unassignment" to display rules that can safely be unassigned.) |
| Reconnaissance Detected: Computer OS Fingerprint Probe | Warning | Yes | The agent or appliance detected an attempt to identify the computer operating system via a "fingerprint" probe. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the computer's events to see the details of the probe and see "Warning: Reconnaissance Detected" on page 986. |
| Reconnaissance Detected: Network or Port Scan | Warning | Yes | The agent or appliance detected network activity typical of a network or port scan. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the computer's |

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | events to see the details of the probe and see "Warning: Reconnaissance Detected" on page 986. |
| Reconnaissance Detected: TCP Null Scan | Warning | Yes | The agent or appliance detected a TCP "Null" scan. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the computer's events to see the details of the probe and see "Warning: Reconnaissance Detected" on page 986. |
| Reconnaissance Detected: TCP SYNFIN Scan | Warning | Yes | The agent or appliance detected a TCP "SYNFIN" scan. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the computer's events to see the details of the probe and see "Warning: Reconnaissance Detected" on page 986. |
| Reconnaissance Detected: TCP Xmas Scan | Warning | Yes | The agent or appliance detected a TCP "Xmas" scan. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the computer's events to see the details of the probe and see "Warning: Reconnaissance Detected" on page 986. |
| Scheduled Malware Scan Missed | Warning | No | Scheduled malware scan tasks were initiated on computers that already had pending scan tasks. This may indicate a scanning frequency that is too high. Consider lowering the scanning frequency, or selecting fewer computers to scan during each scheduled scan job. |
| Send Policy Failed | Critical | No | Inability to send policy may indicate a problem with the agent/appliance. Please check the affected computers. |
| Smart Protection Server Connection Failed | Warning | Yes | Failed to connect to a Smart Protection Server. This could be due to a configuration issue, or due to network connectivity. |
| Software Package Not Found | Critical | No | An agent software package is required for the proper operation of one or more virtual appliance(s). Please import a Red Hat Enterprise Linux 6 (64 bit) agent software package with the correct version for each appliance. If the required version is not available then please import the latest package and upgrade the appliance to match. |
| Software Updates Available for Import | Warning | No | New software is available. To import new software to Deep Security, go to Administration > Updates > Software > Download Center. |
| Unable to communicate | Critical | No | Deep Security Manager has been unable to query the agent/appliance for its status within the configured period. Please check your network configuration and the affected computer's connectivity. |
| Unable to Upgrade the Agent Software | Warning | Yes | Deep Security Manager was unable to upgrade the agent software on the computer. |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | This may indicate a problem with the agent/appliance, but it also can occur if agent self-protection is enabled. On the Deep Security Manager, go to **Computer editor**[1] > **Settings** > **General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override. |
| Unrecognized Software Detected | Warning | No | During ongoing file system monitoring, application control detected that new software had been installed, and it did not match any configured allow or block rule. If your system administrators did not install the software, and no other users have permissions to install software, this could indicate a security compromise. If the software tries to launch, depending on your lockdown configuration at that time, it may or may not be allowed to execute. |
| Unresolved software change limit | Critical | No | Software changes detected on the file system exceeded the maximum amount. Application control will continue to enforce existing rules, but will not record any more changes, and it will stop displaying any of that computer's software changes. You must resolve and prevent excessive software change. |
| Upgrade of the Deep Security Manager Software Recommended (Incompatible Security Update(s)) | Warning | No | Deep Security Manager has detected a computer that is using security updates that are not compatible with the current version of Deep Security Manager. An upgrade of Deep Security Manager software is recommended. |
| Upgrade of the Filter Driver Recommended (New Version Available) | Warning | No | Deep Security Manager has detected one or more ESXi Servers with a version of the filter driver that does not match the latest version available. An upgrade of the filter driver is recommended. |
| User Locked Out | Warning | No | Users can be locked out manually, by repeated incorrect sign-in attempts, if their password expires, or if they have been imported but not yet unlocked. |
| User Password Expires Soon | Warning | No | The password expiry setting is enabled and one or more users have passwords that will expire within the next 7 days. |
| Virtual Appliance is Incompatible With Filter Driver | Warning | No | The appliance is incompatible with the filter driver. Please ensure both are upgraded to their latest versions. |
| Virtual Machine | Warning | No | One or more of the virtual machines monitored by a Deep |

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| Interfaces Out of Sync | | | Security Virtual Appliance has reported that its interfaces are out of sync with the filter driver. This means that the appliance may not be properly monitoring the virtual machine's interfaces. The virtual machine may require manual intervention such as a configuration change, or a restart, to correct the issue. |
| Virtual Machine Moved to Unprotected ESXi Server | Warning | Yes | A virtual machine was moved to an ESXi Server that does not have an activated Deep Security Virtual Appliance. |
| Virtual Machine Unprotected after move to another ESXi | Warning | Yes | A virtual machine that was appliance-protected has been unprotected during or after it was moved to another ESXi. This may be due to an appliance reboot or power off during the move, or it may indicate a configuration issue. The cause of the issue should be investigated before the alert is dismissed. |
| VMware Tools Not Installed | Critical | Yes | A protected virtual machine in an NSX environment does not have VMware Tools installed. VMware Tools is required to protect virtual machines in an NSX environment. |
| Web Reputation Event Alert | Warning | Yes | A web reputation event has been encountered on one or more computers that are selected for alerting. |
| WorkSpaces Disabled for AWS Account | Warning | Yes | An agent was activated on one or more Amazon WorkSpaces but WorkSpaces are not enabled for your AWS account. To enable WorkSpaces, click 'Edit AWS Account' above, and select the 'Include Amazon WorkSpaces' check box. Your WorkSpace(s) will be moved into the WorkSpaces folder of the AWS account, and billed at a lower hourly rate, if you are using hourly billing. |

## Agent events

| ID | Severity | Event | Notes |
|---|---|---|---|
| **Special Events** | | | |
| 0 | Error | Unknown Agent/Appliance Event | |
| **Driver-Related Events** | | | |
| 1000 | Error | Unable To Open Engine | |
| 1001 | Error | Engine Command Failed | |
| 1002 | Warning | Engine List Objects Error | |
| 1003 | Warning | Remove Object Failed | |
| 1004 | Error | Driver Upgrade Stalled | |
| 1005 | Warning | Upgrading Driver | |
| 1006 | Warning | Driver Upgrade Requires Reboot | |
| 1007 | Warning | Driver Upgrade Succeeded | |
| 1008 | Error | Kernel Unsupported | |
| **Configuration-Related Events** | | | |

| ID | Severity | Event | Notes |
|---|---|---|---|
| 2000 | Info | Policy Sent | |
| 2001 | Warning | Invalid Firewall Rule Assignment | |
| 2002 | Warning | Invalid Firewall Stateful Configuration | |
| 2003 | Error | Save Security Configuration Failed | |
| 2004 | Warning | Invalid Interface Assignment | |
| 2005 | Warning | Invalid Interface Assignment | |
| 2006 | Warning | Invalid Action | |
| 2007 | Warning | Invalid Packet Direction | |
| 2008 | Warning | Invalid Rule Priority | |
| 2009 | Warning | Unrecognized IP Format | |
| 2010 | Warning | Invalid Source IP List | |
| 2011 | Warning | Invalid Source Port List | |
| 2012 | Warning | Invalid Destination IP List | |
| 2013 | Warning | Invalid Destination Port List | |
| 2014 | Warning | Invalid Schedule | |
| 2015 | Warning | Invalid Source MAC List | |
| 2016 | Warning | Invalid Destination MAC List | |
| 2017 | Warning | Invalid Schedule Length | |
| 2018 | Warning | Invalid Schedule String | |
| 2019 | Warning | Unrecognized IP Format | |
| 2020 | Warning | Object Not Found | |
| 2021 | Warning | Object Not Found | |
| 2022 | Warning | Invalid Rule Assignment | |
| 2050 | Warning | Firewall Rule Not Found | |
| 2075 | Warning | Traffic Stream Not Found | |
| 2076 | Warning | Intrusion Prevention Rule Not Found | |
| 2077 | Warning | Pattern List Not Found | |
| 2078 | Warning | Traffic Stream Conversion Error | |
| 2080 | Warning | Conditional Firewall Rule Not Found | |
| 2081 | Warning | Conditional Intrusion Prevention Rule Not Found | |
| 2082 | Warning | Empty Intrusion Prevention Rule | |
| 2083 | Warning | Intrusion Prevention Rule XML Rule Conversion Error | |
| 2085 | Error | Security Configuration Error | |
| 2086 | Warning | Unsupported IP Match Type | |
| 2087 | Warning | Unsupported MAC Match Type | |
| 2088 | Warning | Invalid SSL Credential | |
| 2089 | Warning | Missing SSL Credential | |
| **Hardware-Related Events** | | | |
| 3000 | Warning | Invalid MAC Address | |
| 3001 | Warning | Get Event Data Failed | |
| 3002 | Warning | Too Many Interfaces | |

| ID | Severity | Event | Notes |
|---|---|---|---|
| 3003 | Error | Unable To Run External Command | |
| 3004 | Error | Unable To Read External Command Output | |
| 3005 | Error | Operating System Call Error | |
| 3006 | Error | Operating System Call Error | |
| 3007 | Error | File Error | |
| 3008 | Error | Machine-Specific Key Error | |
| 3009 | Error | Unexpected Agent/Appliance Shutdown | |
| 3010 | Error | Agent/Appliance Database Error | |
| 3300 | Warning | Get Event Data Failed | Linux error. |
| 3302 | Warning | Get Security Configuration Failed | Linux error. |
| 3303 | Error | File Mapping Error | Linux error. File type error. |
| 3600 | Error | Get Windows System Directory Failed | |
| 3601 | Warning | Read Local Data Error | Windows error. |
| 3602 | Warning | Windows Service Error | Windows error. |
| 3603 | Error | File Mapping Error | Windows error. File size error. |
| 3700 | Warning | Abnormal Restart Detected | Windows error. |
| 3701 | Info | System Last Boot Time Change | Windows error. |
| **Communications-Related Events** | | | |
| 4000 | Warning | Invalid Protocol Header | Content length out of range. |
| 4001 | Warning | Invalid Protocol Header | Content length missing. |
| 4002 | Info | Command Session Initiated | |
| 4003 | Info | Configuration Session Initiated | |
| 4004 | Info | Command Received | |
| 4011 | Warning | Failure to Contact Manager | |
| 4012 | Warning | Heartbeat Failed | |
| **Agent-Related Events** | | | |
| 5000 | Info | Agent/Appliance Started | |
| 5001 | Error | Thread Exception | |
| 5002 | Error | Operation Timed Out | |
| 5003 | Info | Agent/Appliance Stopped | |
| 5004 | Warning | Clock Changed | |
| 5005 | Info | Agent/Appliance Auditing Started | |
| 5006 | Info | Agent/Appliance Auditing Stopped | |
| 5007 | Info | Appliance Protection Change | |
| 5008 | Warning | Filter Driver Connection Failed | |
| 5009 | Info | Filter Driver Connection Success | |
| 5010 | Warning | Filter Driver Informational Event | |
| 5100 | Info | Protection Module Deployment Started | |
| 5101 | Info | Protection Module Deployment Succeeded | |
| 5102 | Error | Protection Module Deployment Failed | |
| 5103 | Info | Protection Module Download Succeeded | |

| ID | Severity | Event | Notes |
|---|---|---|---|
| 5104 | Info | Protection Module Disablement Started | |
| 5105 | Info | Protection Module Disablement Succeeded | |
| 5106 | Error | Protection Module Disablement Failed | |
| 5107 | Info | Agent Self-Protection enabled | |
| 5108 | Info | Agent Self-Protection disabled | |
| **Logging-Related Events** | | | |
| 6000 | Info | Log Device Open Error | |
| 6001 | Info | Log File Open Error | |
| 6002 | Info | Log File Write Error | |
| 6003 | Info | Log Directory Creation Error | |
| 6004 | Info | Log File Query Error | |
| 6005 | Info | Log Directory Open Error | |
| 6006 | Info | Log File Delete Error | |
| 6007 | Info | Log File Rename Error | |
| 6008 | Info | Log Read Error | |
| 6009 | Warning | Log File Deleted Due To Insufficient Space | |
| 6010 | Warning | Events Were Suppressed | |
| 6011 | Warning | Events Truncated | |
| 6012 | Error | Insufficient Disk Space | See "Warning: Insufficient disk space" on page 988. |
| 6013 | Warning | Agent configuration package too large | |
| **Attack-, Scan-, and Probe-Related Events** | | | |
| 7000 | Warning | Computer OS Fingerprint Probe | |
| 7001 | Warning | Network or Port Scan | |
| 7002 | Warning | TCP Null Scan | |
| 7003 | Warning | TCP SYNFIN Scan | |
| 7004 | Warning | TCP Xmas Scan | |
| **Download Security Update Events** | | | |
| 9050 | Info | Update of Anti-Malware Component on Agent Succeeded | |
| 9051 | Error | Update of Anti-Malware Component on Agent Failed | |
| 9100 | Info | Security Update Successful | |
| 9101 | Error | Security Update Failure | |
| 9102 | Error | Security Update Failure | Specific information recorded in error message. |
| **Relay Events** | | | |
| 9103 | Info | Relay Web Server Disabled | |
| 9104 | Info | Relay Web Server Enabled | |
| 9105 | Error | Enable Relay Web Server Failed | |
| 9106 | Error | Disable Relay Web Server Failed | |
| 9107 | Error | Relay Web Server failed | |
| 9108 | Info | Unable to Connect to Update Source | |

| ID | Severity | Event | Notes |
|---|---|---|---|
| 9109 | Error | Component Update Failure | |
| 9110 | Error | Anti-Malware license is expired | |
| 9111 | Info | Security Update Rollback Success | |
| 9112 | Error | Security Update Rollback Failure | |
| 9113 | Info | Relay Replicated All Packages | |
| 9114 | Error | Relay Failed to Replicate All Packages | |
| **Integrity Scan Status Events** | | | |
| 9201 | Info | Integrity Scan Started | |
| 9203 | Info | Integrity Scan Terminated Abnormally | |
| 9204 | Info | Integrity Scan Paused | |
| 9205 | Info | Integrity Scan Resumed | |
| 9208 | Warning | Integrity Scan failed to start | |
| 9209 | Warning | Integrity Scan Stalled | |
| **Smart Protection Server Status Events** | | | |
| 9300 | Warning | Smart Protection Server Disconnected for Web Reputation | See "Troubleshoot "Smart Protection Server disconnected" errors" on page 965. |
| 9301 | Info | Smart Protection Server Connected for Web Reputation | See "Troubleshoot "Smart Protection Server disconnected" errors" on page 965. |

## System events

To view system events, go to **Events & Reports > Events**.

Depending on whether it's a system configuration change or security incident, each log will appear in either the **System Events** sub-menu, or the sub-menu corresponding to the event's protection module, such as **Anti-Malware Events**.

These events sometimes also appear in the Status column on **Computers**.

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 0 | Error | Unknown Error | |
| 100 | Info | Deep Security Manager Started | |
| 101 | Info | License Changed | |
| 102 | Info | Trend Micro Deep Security Customer Account Changed | |
| 103 | Warning | Check For Updates Failed | |
| 104 | Warning | Automatic Software Download Failed | |
| 105 | Warning | Scheduled Rule Update Download and Apply Failed | |
| 106 | Info | Scheduled Rule Update Downloaded and Applied | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 107 | Info | Rule Update Downloaded and Applied | |
| 108 | Info | Script Executed | |
| 109 | Error | Script Execution Failed | |
| 110 | Info | System Events Exported | |
| 111 | Info | Firewall Events Exported | |
| 112 | Info | Intrusion Prevention Events Exported | |
| 113 | Warning | Scheduled Rule Update Download Failed | |
| 114 | Info | Scheduled Rule Update Downloaded | |
| 115 | Info | Rule Update Downloaded | |
| 116 | Info | Rule Update Applied | |
| 117 | Info | Deep Security Manager Shutdown | |
| 118 | Warning | Deep Security Manager Offline | |
| 119 | Info | Deep Security Manager Back Online | |
| 120 | Error | Heartbeat Server Failed | The server within Deep Security Manager that listens for incoming agent heartbeats did not start. Check that the manager's incoming heartbeat port number is not in use by another application on the server. Once the port is free, the manager's heartbeat server should bind to it, and this error should be fixed. |
| 121 | Error | Scheduler Failed | |
| 122 | Error | Manager Message Thread Failed | An internal thread has failed. There is no resolution for this error. If it persists, please contact customer support. |
| 123 | Info | Deep Security Manager Forced Shutdown | |
| 124 | Info | Rule Update Deleted | |
| 130 | Info | Credentials Generated | |
| 131 | Warning | Credential Generation Failed | |
| 140 | Info | Discover Computers | |
| 141 | Warning | Discover Computers Failed | |
| 142 | Info | Discover Computers Requested | |
| 143 | Info | Discover Computers Canceled | |
| 150 | Info | System Settings Saved | |
| 151 | Info | Software Added | |
| 152 | Info | Software Deleted | |
| 153 | Info | Software Updated | |
| 154 | Info | Software Exported | |
| 155 | Info | Software Platforms Changed | |
| 160 | Info | Authentication Failed | |
| 161 | Info | Rule Update Exported | |
| 162 | Info | Log Inspection Events Exported | |
| 163 | Info | Anti-Malware Event Exported | |
| 164 | Info | Security Update Successful | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 165 | Error | Security Update Failed | |
| 166 | Info | Check for New Software Success | |
| 167 | Error | Check for New Software Failed | |
| 168 | Info | Manual Security Update Successful | |
| 169 | Error | Manual Security Update Failed | |
| 170 | Error | Manager Available Disk Space Too Low | The manager does not have enough free disk space to function and will shut down. Either expand the disk space or delete unused files to free some disk space, then "Restart the Deep Security Manager" on page 734. |
| 171 | Info | Anti-Malware Spyware Item Exported | |
| 172 | Info | Web Reputation Events Exported | |
| 173 | Info | Anti-Malware Identified Files List Exported | |
| 174 | Info | Anti-Malware Unauthorized Change Targeted Item Exported | |
| 180 | Info | Alert Type Updated | |
| 190 | Info | Alert Started | |
| 191 | Info | Alert Changed | |
| 192 | Info | Alert Ended | |
| 197 | Info | Alert Emails Sent | |
| 198 | Warning | Alert Emails Failed | An alert email could not be sent. Verify that your SMTP settings are correct. |
| 199 | Error | Alert Processing Failed | The current alert status could be inaccurate because an alert was not completely processed. If the problem persists, contact your support provider. |
| 248 | Info | Software Update: Disable Relay Requested | |
| 249 | Info | Software Update: Enable Relay Requested | |
| 250 | Info | Computer Created | |
| 251 | Info | Computer Deleted | |
| 252 | Info | Computer Updated | |
| 253 | Info | Policy Assigned to Computer | |
| 254 | Info | Computer Moved | |
| 255 | Info | Activation Requested | |
| 256 | Info | Send Policy Requested | |
| 257 | Info | Locked | |
| 258 | Info | Unlocked | |
| 259 | Info | Deactivation Requested | |
| 260 | Info | Scan for Open Ports | |
| 261 | Warning | Scan for Open Ports Failed | |
| 262 | Info | Scan for Open Ports Requested | |
| 263 | Info | Scan for Open Ports Canceled | |
| 264 | Info | Agent Software Upgrade Requested | |
| 265 | Info | Agent Software Upgrade Cancelled | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 266 | Info | Warnings/Errors Cleared | |
| 267 | Info | Check Status Requested | |
| 268 | Info | Get Events Requested | |
| 269 | Info | Computer Added to Cloud Connector | |
| 270 | Error | Computer Creation Failed | |
| 271 | Info | Agent Software Upgrade Timed Out | |
| 272 | Info | Appliance Software Upgrade Timed Out | |
| 273 | Info | Security Update: Security Update Check and Download Requested | |
| 274 | Info | Security Update: Security Update Rollback Requested | |
| 275 | Warning | Duplicate Computer | |
| 276 | Info | Update: Summary Information | |
| 280 | Info | Computers Exported | |
| 281 | Info | Computers Imported | |
| 286 | Info | Computer Log Exported | |
| 287 | Info | Relay Group Assigned to Computer | |
| 290 | Info | Group Added | |
| 291 | Info | Group Removed | |
| 292 | Info | Group Updated | |
| 293 | Info | Interface Renamed | |
| 294 | Info | Computer Bridge Renamed | |
| 295 | Info | Interface Deleted | |
| 296 | Info | Interface IP Deleted | |
| 297 | Info | Recommendation Scan Requested | |
| 298 | Info | Recommendations Cleared | |
| 299 | Info | Asset Value Assigned to Computer | |
| 300 | Info | Recommendation Scan Completed | |
| 301 | Info | Agent Software Deployment Requested | |
| 302 | Info | Agent Software Removal Requested | |
| 303 | Info | Computer Renamed | |
| 305 | Info | Scan for Integrity Requested | |
| 306 | Info | Rebuild Baseline Requested | |
| 307 | Info | Cancel Update Requested | |
| 308 | Info | Integrity Monitoring Rule Compile Issue | |
| 309 | Info | Integrity Monitoring Rule Compile Issue Resolved | |
| 310 | Info | Directory Added | |
| 311 | Info | Directory Removed | |
| 312 | Info | Directory Updated | |
| 320 | Info | Directory Synchronization | |
| 321 | Info | Directory Synchronization Finished | |
| 322 | Error | Directory Synchronization Failed | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 323 | Info | Directory Synchronization Requested | |
| 324 | Info | Directory Synchronization Cancelled | |
| 325 | Info | User Synchronization | Synchronization of the user accounts with Microsoft Active Directory has been started. |
| 326 | Info | User Synchronization Finished | Synchronization of the user accounts with Microsoft Active Directory has completed. |
| 327 | Error | User Synchronization Failed | |
| 328 | Info | User Synchronization Requested | |
| 329 | Info | User Synchronization Cancelled | |
| 330 | Info | SSL Configuration Created | |
| 331 | Info | SSL Configuration Deleted | |
| 332 | Info | SSL Configuration Updated | |
| 333 | Info | Host Merge Finished | |
| 334 | Error | Host Merge Failed | |
| 350 | Info | Policy Created | |
| 351 | Info | Policy Deleted | |
| 352 | Info | Policy Updated | |
| 353 | Info | Policies Exported | |
| 354 | Info | Policies Imported | |
| 355 | Info | Scan for Recommendations Canceled | |
| 360 | Info | VMware vCenter Added | |
| 361 | Info | VMware vCenter Removed | |
| 362 | Info | VMware vCenter Updated | |
| 363 | Info | VMware vCenter Synchronization | |
| 364 | Info | VMware vCenter Synchronization Finished | |
| 365 | Error | VMware vCenter Synchronization Failed | |
| 366 | Info | VMware vCenter Synchronization Requested | |
| 367 | Info | VMware vCenter Synchronization Cancelled | |
| 368 | Warning | Interfaces Out of Sync | Interfaces reported by the Deep Security Virtual Appliance are different than the interfaces reported by the vCenter. This can typically be resolved by rebooting the VM. |
| 369 | Info | Interfaces in Sync | |
| 370 | Info | Filter Driver Installed | |
| 371 | Info | Filter Driver Removed | The VMware ESXi server has been restored to the state it was in before the filter driver software was installed. |
| 372 | Info | Filter Driver Upgraded | |
| 373 | Info | Virtual Appliance Deployed | |
| 374 | Info | Virtual Appliance Upgraded | |
| 375 | Warning | Virtual Appliance Upgrade Failed | |
| 376 | Warning | Virtual Machine Moved to Unprotected ESXi | |
| 377 | Info | Virtual Machine Moved to Protected ESXi | |
| 378 | Warning | Virtual Machine unprotected after move to | A VM was moved to an ESXi where there is no Deep |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | another ESXi | Security Virtual Appliance. |
| 379 | Info | Virtual Machine unprotected after move to another ESXi Resolved | |
| 380 | Error | Filter Driver Offline | The filter driver on an ESXi server is offline. Use the VMware vCenter console to troubleshoot problems with the hypervisor and the ESXi. |
| 381 | Info | Filter Driver Back Online | |
| 382 | Info | Filter Driver Upgrade Requested | |
| 383 | Info | Appliance Upgrade Requested | |
| 384 | Warning | Prepare ESXi Failed | |
| 385 | Warning | Filter Driver Upgrade Failed | |
| 386 | Warning | Removal of Filter Driver from ESXi Failed | |
| 387 | Error | Connection to Filter Driver Failure | |
| 388 | Info | Connection to Filter Driver Success | |
| 389 | Error | Multiple Activated Appliances Detected | |
| 390 | Info | Multiple Activated Appliances Detected Resolved | |
| 391 | Error | Network Settings Out of Sync With vCenter Global Settings | |
| 392 | Info | Network Settings in Sync With vCenter Global Settings | |
| 393 | Error | Anti-Malware Engine Offline | The anti-malware protection module is not functioning. This is probably because the VMware environment does not meet the requirements. See "System requirements" on page 69. |
| 394 | Info | Anti-Malware Engine Back Online | |
| 395 | Error | Virtual Appliance is Incompatible With Filter Driver | |
| 396 | Info | Virtual Appliance is Incompatible With Filter Driver Resolved | |
| 397 | Warning | VMware NSX Callback Authentication Failed | |
| 398 | Error | VMware Tools Not Installed | |
| 399 | Info | VMware Tools Not Installed Resolved | |
| 410 | Info | Firewall Rule Created | |
| 411 | Info | Firewall Rule Deleted | |
| 412 | Info | Firewall Rule Updated | |
| 413 | Info | Firewall Rule Exported | |
| 414 | Info | Firewall Rule Imported | |
| 420 | Info | Firewall Stateful Configuration Created | |
| 421 | Info | Firewall Stateful Configuration Deleted | |
| 422 | Info | Firewall Stateful Configuration Updated | |
| 423 | Info | Firewall Stateful Configuration Exported | |
| 424 | Info | Firewall Stateful Configuration Imported | |
| 460 | Info | Application Type Created | An administrator configured a new IPS network |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | | application definition. |
| 461 | Info | Application Type Deleted | An administrator removed an IPS network application definition. |
| 462 | Info | Application Type Updated | An administrator changed an existing IPS network application definition. |
| 463 | Info | Application Type Exported | An administrator downloaded an IPS network application definition. |
| 464 | Info | Application Type Imported | An administrator uploaded an IPS network application definition. |
| 470 | Info | Intrusion Prevention Rule Created | |
| 471 | Info | Intrusion Prevention Rule Deleted | |
| 472 | Info | Intrusion Prevention Rule Updated | |
| 473 | Info | Intrusion Prevention Rule Exported | |
| 474 | Info | Intrusion Prevention Rule Imported | |
| 480 | Info | Integrity Monitoring Rule Created | |
| 481 | Info | Integrity Monitoring Rule Deleted | |
| 482 | Info | Integrity Monitoring Rule Updated | |
| 483 | Info | Integrity Monitoring Rule Exported | |
| 484 | Info | Integrity Monitoring Rule Imported | |
| 490 | Info | Log Inspection Rule Created | |
| 491 | Info | Log Inspection Rule Deleted | |
| 492 | Info | Log Inspection Rule Updated | |
| 493 | Info | Log Inspection Rule Exported | |
| 494 | Info | Log Inspection Rule Imported | |
| 495 | Info | Log Inspection Decoder Created | |
| 496 | Info | Log Inspection Decoder Deleted | |
| 497 | Info | Log Inspection Decoder Updated | |
| 498 | Info | Log Inspection Decoder Exported | |
| 499 | Info | Log Inspection Decoder Imported | |
| 505 | Info | Context Created | |
| 506 | Info | Context Deleted | |
| 507 | Info | Context Updated | |
| 508 | Info | Context Exported | |
| 509 | Info | Context Imported | |
| 510 | Info | IP List Created | |
| 511 | Info | IP List Deleted | |
| 512 | Info | IP List Updated | |
| 513 | Info | IP List Exported | |
| 514 | Info | IP List Imported | |
| 520 | Info | Port List Created | |
| 521 | Info | Port List Deleted | |
| 522 | Info | Port List Updated | |
| 523 | Info | Port List Exported | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 524 | Info | Port List Imported | |
| 525 | Info | Scan Cache Configuration Created | |
| 526 | Info | Scan Cache Configuration Exported | |
| 530 | Info | MAC List Created | |
| 531 | Info | MAC List Deleted | |
| 532 | Info | MAC List Updated | |
| 533 | Info | MAC List Exported | |
| 534 | Info | MAC List Imported | |
| 540 | Info | Proxy Created | |
| 541 | Info | Proxy Deleted | |
| 542 | Info | Proxy Updated | |
| 543 | Info | Proxy Exported | |
| 544 | Info | Proxy Imported | |
| 550 | Info | Schedule Created | |
| 551 | Info | Schedule Deleted | |
| 552 | Info | Schedule Updated | |
| 553 | Info | Schedule Exported | |
| 554 | Info | Schedule Imported | |
| 560 | Info | Scheduled Task Created | |
| 561 | Info | Scheduled Task Deleted | |
| 562 | Info | Scheduled Task Updated | |
| 563 | Info | Scheduled Task Manually Executed | |
| 564 | Info | Scheduled Task Started | |
| 565 | Info | Backup Finished | |
| 566 | Error | Backup Failed | |
| 567 | Info | Sending Outstanding Alert Summary | |
| 568 | Warning | Failed To Send Outstanding Alert Summary | |
| 569 | Warning | Email Failed | An e-mail notification could not be sent. Verify that your SMTP settings are correct. |
| 570 | Info | Sending Report | |
| 571 | Warning | Failed To Send Report | |
| 572 | Error | Invalid Report Jar | |
| 573 | Info | Asset Value Created | |
| 574 | Info | Asset Value Deleted | |
| 575 | Info | Asset Value Updated | |
| 576 | Error | Report Uninstall Failed | |
| 577 | Error | Report Uninstalled | |
| 578 | Warning | Integrity Monitoring Rules Require Configuration | |
| 580 | Warning | Application Type Port List Misconfiguration | |
| 581 | Warning | Application Type Port List Misconfiguration Resolved | |
| 582 | Warning | Intrusion Prevention Rules Require | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Configuration | |
| 583 | Info | Intrusion Prevention Rules Require Configuration Resolved | |
| 584 | Warning | Application Types Require Configuration | IPS rules require network application definitions, and cannot correctly scan traffic until you define them. |
| 585 | Info | Integrity Monitoring Rules Require Configuration Resolved | |
| 586 | Warning | Log Inspection Rules Require Configuration | |
| 587 | Info | Log Inspection Rules Require Configuration Resolved | |
| 588 | Warning | Log Inspection Rules Require Log Files | |
| 589 | Info | Log Inspection Rules Require Log Files Resolved | |
| 590 | Warning | Scheduled Task Unknown Type | |
| 591 | Info | Relay Group Created | |
| 592 | Info | Relay Group Updated | |
| 593 | Info | Relay Group Deleted | |
| 594 | Info | Event-Based Task Created | |
| 595 | Info | Event-Based Task Deleted | |
| 596 | Info | Event-Based Task Updated | |
| 597 | Info | Event-Based Task Triggered | |
| 600 | Info | User Signed In | |
| 601 | Info | User Signed Out | |
| 602 | Info | User Timed Out | |
| 603 | Info | User Locked Out | |
| 604 | Info | User Unlocked | |
| 608 | Error | User Session Validation Failed | Deep Security Manager could not confirm that a session was initiated after successful authentication. The user will be redirected to the login page, and asked to re-authenticate. This could be normal if the authenticated session list was cleared. |
| 609 | Error | User Made Invalid Request | Deep Security Manager received invalid request to access audit data (events). Access was denied. |
| 610 | Info | User Session Validated | |
| 611 | Info | User Viewed Firewall Event | |
| 613 | Info | User Viewed Intrusion Prevention Event | |
| 615 | Info | User Viewed System Event | |
| 616 | Info | User Viewed Integrity Monitoring Event | |
| 617 | Info | User Viewed Log Inspection Event | |
| 618 | Info | User Viewed Identified File Detail | |
| 619 | Info | User Viewed Anti-Malware Event | |
| 620 | Info | User Viewed Web Reputation Event | |
| 621 | Info | User Signed In As Tenant | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 622 | Info | Access from Primary Tenant Enabled | |
| 623 | Info | Access from Primary Tenant Disabled | |
| 624 | Info | Access from Primary Tenant Allowed | |
| 625 | Info | Access from Primary Tenant Revoked | |
| 626 | Info | Access from Primary Tenant Expired | |
| 630 | Info | Syslog Configuration Created | |
| 631 | Info | Syslog Configuration Deleted | |
| 632 | Info | Syslog Configuration Updated | |
| 633 | Info | Syslog Configuration Exported | |
| 634 | Info | Syslog Configuration Imported | |
| 650 | Info | User Created | |
| 651 | Info | User Deleted | |
| 652 | Info | User Updated | |
| 653 | Info | User Password Set | |
| 660 | Info | Role Created | |
| 661 | Info | Role Deleted | |
| 662 | Info | Role Updated | |
| 663 | Info | Roles Imported | |
| 664 | Info | Roles Exported | |
| 670 | Info | Contact Created | |
| 671 | Info | Contact Deleted | |
| 672 | Info | Contact Updated | |
| 700 | Info | Agent Software Installed | |
| 701 | Error | Agent Software Installation Failed | |
| 702 | Info | Credentials Generated | |
| 703 | Error | Credential Generation Failed | |
| 704 | Info | Activated | |
| 705 | Error | Activation Failed | This can occur if agent self-protection is enabled. On the Deep Security Manager, go to **Computer editor**[1] > **Settings** > **General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override. |
| 706 | Info | Software Update: Agent Software Upgraded | |
| 707 | Warning | Software Update: Agent Software Upgrade Failed | This can occur if agent self-protection is enabled. On the Deep Security Manager, go to **Computer editor**[2] > **Settings** > **General**. In **Agent Self** |

[1]To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2]To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | | **Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override. |
| 708 | Info | Deactivated | |
| 709 | Error | Deactivation Failed | |
| 710 | Info | Events Retrieved | |
| 711 | Info | Agent Software Deployed | |
| 712 | Error | Agent Software Deployment Failed | This can occur if agent self-protection is enabled. On the Deep Security Manager, go to **Computer editor**[1] **> Settings > General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override. |
| 713 | Info | Agent Software Removed | |
| 714 | Error | Agent Software Removal Failed | This can occur if agent self-protection is enabled. On the Deep Security Manager, go to **Computer editor**[2] **> Settings > General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override. |
| 715 | Info | Agent/Appliance Version Changed | |
| 716 | Info | Reactivation Attempted by Unknown Agent | An agent that is currently unknown to the Deep Security Manager has attempted reactivation. This usually happens when a computer was deleted from Deep Security Manager without first removing the agent on the computer. For more information, see the 'Reactivation Attempted by Unknown Agent' section in Agent settings. |
| 720 | Info | Policy Sent | Agent/Appliance updated. |
| 721 | Error | Send Policy Failed | |
| 722 | Warning | Get Interfaces Failed | |
| 723 | Info | Get Interfaces Failure Resolved | |

[1]To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2]To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 724 | Warning | Insufficient Disk Space | An agent detected low disk space. Free space on the Agent's host. See "Warning: Insufficient disk space" on page 988. |
| 725 | Warning | Events Suppressed | |
| 726 | Warning | Get Agent/Appliance Events Failed | Manager was unable to retrieve Events from Agent/Appliance. This error does not mean that the data was lost on the Agent/Appliance. This error is normally caused by a network interruption while events are being transferred. Clear the error and run a "Check Status" to retry the operation. |
| 727 | Info | Get Agent/Appliance Events Failure Resolved | |
| 728 | Error | Get Events Failed | Manager was unable to retrieve audit data from Agent/Appliance. This error does not mean that the data was lost on the Agent/Appliance. This error is normally caused by a network interruption while events are being transferred. Clear the error and run a "Get Events Now" to retry the operation. |
| 729 | Info | Get Events Failure Resolved | |
| 730 | Error | Offline | Manager cannot communicate with Computer. Usually, however, the offline Agent is still protecting the computer with its last configured settings. See Computer and Agent/Appliance Status and ""Offline" agent" on page 1097. |
| 731 | Info | Back Online | |
| 732 | Error | Firewall Engine Offline | The Firewall Engine is offline and traffic is flowing unfiltered. This is normally due to an error during installation or verification of the driver on the computer's OS platform. Check the status of the network driver at the computer to ensure it is properly loaded. |
| 733 | Info | Firewall Engine Back Online | |
| 734 | Warning | Computer Clock Change | A clock change has occurred on the Computer which exceeds the maximum allowed specified in **Computer or Policy editor**[1] > Settings > General > Heartbeat area. Investigate what has caused the clock change on the computer. |
| 735 | Warning | Misconfiguration Detected | The Agent's configuration does not match the configuration indicated in the Manager's records. This is typically because of a recent backup restoration of the Manager or the Agent. |

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | | Unanticipated misconfiguration warnings should be investigated. |
| 736 | Info | Check Status Failure Resolved | |
| 737 | Error | Check Status Failed | See "Error: Check Status Failed" on page 981. |
| 738 | Error | Intrusion Prevention Engine Offline | The Intrusion Prevention Engine is offline and traffic is flowing unfiltered. This is normally due to an error during installation or verification of the driver on the computer's OS platform. Check the status of the network driver at the computer to ensure it is properly loaded. |
| 739 | Info | Intrusion Prevention Engine Back Online | |
| 740 | Error | Agent/Appliance Error | |
| 741 | Warning | Abnormal Restart Detected | |
| 742 | Warning | Communications Problem | The Agent is having problems communicating its status to Manager. It usually indicates network or load congestion in the Agent --> Manager direction. Further investigation is warranted if the situation persists |
| 743 | Info | Communications Problem Resolved | |
| 745 | Warning | Events Truncated | |
| 748 | Error | Log Inspection Engine Offline | |
| 749 | Info | Log Inspection Engine Back Online | |
| 750 | Warning | Last Automatic Retry | |
| 755 | Info | Deep Security Manager Version Compatibility Resolved | |
| 756 | Warning | Deep Security Manager Upgrade Recommended (Incompatible Security Update(s)) | |
| 760 | Info | Agent/Appliance Version Compatibility Resolved | |
| 761 | Warning | Agent/Appliance Upgrade Recommended | |
| 762 | Warning | Agent/Appliance Upgrade Required | |
| 763 | Warning | Incompatible Agent/Appliance Version | |
| 764 | Warning | Agent/Appliance Upgrade Recommended (Incompatible Security Update(s)) | |
| 765 | Error | Computer Reboot Required | |
| 766 | Warning | Network Engine Mode Configuration Incompatibility | |
| 767 | Warning | Network Engine Mode Version Incompatibility | |
| 768 | Warning | Network Engine Mode Incompatibility Resolved | |
| 770 | Warning | Agent/Appliance Heartbeat Rejected | |
| 771 | Warning | Contact by Unrecognized Client | |
| 780 | Info | Recommendation Scan Failure Resolved | |
| 781 | Warning | Recommendation Scan Failure | See "Troubleshooting: Recommendation Scan |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | | Failure" on page 368. |
| 782 | Info | Rebuild Baseline Failure Resolved | |
| 783 | Warning | Rebuild Baseline Failure | |
| 784 | Info | Security Update: Security Update Check and Download Successful | |
| 785 | Warning | Security Update: Security Update Check and Download Failed | |
| 786 | Info | Scan For Change Failure Resolved | |
| 787 | Warning | Scan For Change Failure | |
| 790 | Info | Agent-Initiated Activation Requested | |
| 791 | Warning | Agent-Initiated Activation Failure | |
| 792 | Info | Manual Malware Scan Failure Resolved | |
| 793 | Warning | Manual Malware Scan Failure | A Malware Scan has failed. Use the VMware vCenter console to check the status of the VM on which the scan failed. |
| 794 | Info | Scheduled Malware Scan Failure Resolved | |
| 795 | Warning | Scheduled Malware Scan Failure | A scheduled Malware Scan has failed. Use the VMware vCenter console to check the status of the VM on which the scan failed. |
| 796 | Warning | Scheduled Malware Scan Task has been Missed | This occurs when a scheduled Malware Scan is initiated on a computer when a previous scan is still pending. This typically indicates that Malware Scans are being scheduled too frequently. |
| 797 | Info | Malware Scan Cancellation Failure Resolved | |
| 798 | Warning | Malware Scan Cancellation Failure | A Malware Scan cancellation has failed. Use the VMware vCenter console to check the status of the VM on which the scan failed. |
| 799 | Warning | Malware Scan Stalled | A Malware Scan has stalled. Use the VMware vCenter console to check the status of the VM on which the scan stalled. |
| 800 | Info | Alert Dismissed | |
| 801 | Info | Error Dismissed | |
| 804 | Error | Intrusion Prevention Rule Compiler Failed | |
| 805 | Error | Intrusion Prevention Rules Failed to Compile | |
| 806 | Error | Intrusion Prevention Rules Failed to Compile | |
| 850 | Warning | Reconnaissance Detected: Computer OS Fingerprint Probe | See "Warning: Reconnaissance Detected" on page 986 |
| 851 | Warning | Reconnaissance Detected: Network or Port Scan | See "Warning: Reconnaissance Detected" on page 986 |
| 852 | Warning | Reconnaissance Detected: TCP Null Scan | See "Warning: Reconnaissance Detected" on page 986 |
| 853 | Warning | Reconnaissance Detected: TCP SYNFIN Scan | See "Warning: Reconnaissance Detected" on page 986 |
| 854 | Warning | Reconnaissance Detected: TCP Xmas Scan | See "Warning: Reconnaissance Detected" on page 986 |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 900 | Info | Deep Security Manager Audit Started | |
| 901 | Info | Deep Security Manager Audit Shutdown | |
| 902 | Info | Deep Security Manager Installed | |
| 903 | Warning | License Related Configuration Change | |
| 910 | Info | Diagnostic Package Generated | |
| 911 | Info | Diagnostic Package Exported | |
| 912 | Info | Diagnostic Package Uploaded | |
| 913 | Error | Automatic Diagnostic Package Error | |
| 914 | Info | Identified File Deletion Succeeded | |
| 915 | Info | Identified File Deletion Failed | |
| 916 | Info | Identified File Download Succeeded | |
| 917 | Info | Identified File Download Failed | |
| 918 | Info | Identified File Administration Utility Download Succeeded | |
| 919 | Info | Identified File Not Found | |
| 920 | Info | Usage Information Generated | |
| 921 | Info | Usage Information Package Exported | |
| 922 | Info | Usage Information Package Uploaded | |
| 923 | Error | Usage Information Package Error | |
| 924 | Warning | File cannot be analyzed or quarantined (VM maximum disk space used to store identified files exceeded) | The Anti-Malware module was unable to analyze or quarantine a file because the VM maximum disk space used to store identified files was reached. To change the maximum disk space for identified files setting, open the computer or policy editor and go to the Anti-malware > Advanced tab. |
| 925 | Warning | File cannot be analyzed or quarantined (maximum disk space used to store identified files exceeded) | The Anti-Malware module was unable to analyze or quarantine a file because the maximum disk space used to store identified files was reached. To change the maximum disk space for identified files setting, open the computer or policy editor and go to the Anti-malware > Advanced tab. |
| 926 | Warning | Smart Protection Server Disconnected for Smart Scan | See "Troubleshoot "Smart Protection Server disconnected" errors" on page 965. |
| 927 | Info | Smart Protection Server Connected for Smart Scan | |
| 928 | Info | Identified File Restoration Succeeded | |
| 929 | Warning | Identified File Restoration Failed | |
| 930 | Info | Certificate Accepted | |
| 931 | Info | Certificate Deleted | |
| 932 | Warning | Smart Protection Server Disconnected for Web Reputation | See "Troubleshoot "Smart Protection Server disconnected" errors" on page 965. |
| 933 | Info | Smart Protection Server Connected for Web Reputation | |
| 934 | Info | Software Update: Anti-Malware Windows Platform Update Successful | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 935 | Error | Software Update: Anti-Malware Windows Platform Update Failed | |
| 936 | Info | Submission of identified file to Deep Discovery Analyzer succeeded | |
| 937 | Info | Submission of identified file to Deep Discovery Analyzer failed | |
| 938 | Info | Identified File Submission Queued | |
| 940 | Info | Auto-Tag Rule Created | |
| 941 | Info | Auto-Tag Rule Deleted | |
| 942 | Info | Auto-Tag Rule Updated | |
| 943 | Info | Tag Deleted | |
| 944 | Info | Tag Created | |
| 945 | Warning | Census, Good File Reputation, and Predictive Machine Learning Service Disconnected | |
| 946 | Info | Census, Good File Reputation, and Predictive Machine Learning Service Connected | |
| 970 | Info | Command Line Utility Started | |
| 978 | Info | Command Line Utility Failed | |
| 979 | Info | Command Line Utility Shutdown | Deep Security Manager was manually stopped. |
| 980 | Info | System Information Exported | |
| 990 | Info | Manager Node Added | |
| 991 | Info | Manager Node Decommissioned | |
| 992 | Info | Manager Node Updated | |
| 995 | Info | Connection to the Certified Safe Software Service has been restored | |
| 996 | Warning | Unable to connect to the Certified Safe Software Service | |
| 997 | Error | Tagging Error | |
| 998 | Error | System Event Notification Error | |
| 999 | Error | Internal Software Error | |
| 1101 | Error | Plug-in Installation Failed | |
| 1102 | Info | Plug-in Installed | |
| 1103 | Error | Plug-in Upgrade Failed | |
| 1104 | Info | Plug-in Upgraded | |
| 1105 | Error | Plug-in Start Failed | |
| 1106 | Error | Plug-in Uninstall Failed | |
| 1107 | Info | Plug-in Uninstalled | |
| 1108 | Info | Plug-in Started | |
| 1109 | Info | Plug-in Stopped | |
| 1110 | Error | Software Package Not Found | |
| 1111 | Info | Software Package Found | |
| 1500 | Info | Malware Scan Configuration Created | |
| 1501 | Info | Malware Scan Configuration Deleted | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 1502 | Info | Malware Scan Configuration Updated | |
| 1503 | Info | Malware Scan Configuration Exported | |
| 1504 | Info | Malware Scan Configuration Imported | |
| 1505 | Info | Directory List Created | |
| 1506 | Info | Directory List Deleted | |
| 1507 | Info | Directory List Updated | |
| 1508 | Info | Directory List Exported | |
| 1509 | Info | Directory List Imported | |
| 1510 | Info | File Extension List Created | |
| 1511 | Info | File Extension List Deleted | |
| 1512 | Info | File Extension List Updated | |
| 1513 | Info | File Extension List Exported | |
| 1514 | Info | File Extension List Imported | |
| 1515 | Info | File List Created | |
| 1516 | Info | File List Deleted | |
| 1517 | Info | File List Updated | |
| 1518 | Info | File List Exported | |
| 1519 | Info | File List Imported | |
| 1520 | Info | Manual Malware Scan Pending | |
| 1521 | Info | Manual Malware Scan Started | |
| 1522 | Info | Manual Malware Scan Completed | |
| 1523 | Info | Scheduled Malware Scan Started | |
| 1524 | Info | Scheduled Malware Scan Completed | |
| 1525 | Info | Manual Malware Scan Cancellation In Progress | |
| 1526 | Info | Manual Malware Scan Cancellation Completed | |
| 1527 | Info | Scheduled Malware Scan Cancellation In Progress | |
| 1528 | Info | Scheduled Malware Scan Cancellation Completed | |
| 1529 | Info | Manual Malware Scan Paused | |
| 1530 | Info | Manual Malware Scan Resumed | |
| 1531 | Info | Scheduled Malware Scan Paused | |
| 1532 | Info | Scheduled Malware Scan Resumed | |
| 1533 | Info | Computer reboot required for Anti-Malware cleanup task | |
| 1534 | Error | Computer reboot required for Anti-Malware protection | |
| 1536 | Info | Quick Malware Scan Pending | |
| 1537 | Info | Quick Malware Scan Started | |
| 1538 | Info | Quick Malware Scan Completed | |
| 1539 | Info | Quick Malware Scan Cancellation In Progress | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 1540 | Info | Quick Malware Scan Cancellation Completed | |
| 1541 | Info | Quick Malware Scan Paused | |
| 1542 | Info | Quick Malware Scan Failure Resolved | |
| 1543 | Warning | Quick Malware Scan Failure | |
| 1544 | Info | Quick Malware Scan Resumed | |
| 1545 | Info | Files could not be scanned for malware | Anti-malware could not scan a file because its file path exceeded the maximum number of characters. Maximum file path length varies by OS and file system. To prevent this problem, try moving the file to a directory path and file name with fewer characters. |
| 1546 | Info | Files could not be scanned for malware | Anti-malware could not scan a file because its location exceeded the maximum directory depth. To prevent this problem, try reducing the number of layers of nested directories. |
| 1550 | Info | Web Reputation Settings Updated | |
| 1551 | Info | Malware Scan Configuration Updated | |
| 1552 | Info | Integrity Configuration Updated | |
| 1553 | Info | Log Inspection Configuration Updated | |
| 1554 | Info | Firewall Stateful Configuration Updated | |
| 1555 | Info | Intrusion Prevention Configuration Updated | |
| 1600 | Info | Relay Group Update Requested | |
| 1601 | Info | Relay Group Update Success | |
| 1602 | Error | Relay Group Update Failed | |
| 1603 | Info | Security Update: Security Update Rollback Success | |
| 1604 | Warning | Security Update: Security Update Rollback Failure | |
| 1605 | Info | Successfully send file back up command to host | |
| 1606 | Warning | Failed to send file back up command to host | |
| 1607 | Info | Successfully back up file | |
| 1608 | Error | Failed to back up file | |
| 1650 | Warning | Anti-Malware protection is not enabled or is out of date | |
| 1651 | Info | Anti-Malware module is ready | |
| 1660 | Info | Rebuild Baseline Started | |
| 1661 | Info | Rebuild Baseline Paused | |
| 1662 | Info | Rebuild Baseline Resumed | |
| 1663 | Warning | Rebuild Baseline Failure | |
| 1664 | Warning | Rebuild Baseline Stalled | |
| 1665 | Info | Rebuild Baseline Completed | |
| 1666 | Info | Scan for Integrity Started | |
| 1667 | Info | Scan for Integrity Paused | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 1668 | Info | Scan for Integrity Resumed | |
| 1669 | Warning | Scan for Integrity Failure | |
| 1670 | Warning | Scan for Integrity Stalled | |
| 1671 | Info | Scan for Integrity Completed | |
| 1675 | Error | Integrity Monitoring Engine Offline | |
| 1676 | Info | Integrity Monitoring Engine Back Online | |
| 1677 | Error | Trusted Platform Module Error | |
| 1678 | Info | Trusted Platform Module Register Values Loaded | |
| 1679 | Warning | Trusted Platform Module Register Values Changed | |
| 1680 | Info | Trusted Platform Module Checking Disabled | |
| 1681 | Info | Trusted Platform Module Information Unreliable | |
| 1700 | Info | No Agent Detected | |
| 1800 | Error | Deep Security Protection Module Failure | |
| 1900 | Info | Cloud Account Added | |
| 1901 | Info | Cloud Account Removed | |
| 1902 | Info | Cloud Account Updated | |
| 1903 | Info | Cloud Account Synchronization In Progress | |
| 1904 | Info | Cloud Account Synchronization Finished | |
| 1905 | Error | Cloud Account Synchronization Failed | |
| 1906 | Info | Cloud Account Synchronization Requested | |
| 1907 | Info | Cloud account Synchronization Cancelled | |
| 1908 | Info | AWS Account Synchronization Requested | |
| 1909 | Info | AWS Account Synchronization Finished | |
| 1910 | Error | AWS Account Synchronization Failed | |
| 1911 | Info | AWS Account Added | |
| 1912 | Info | AWS Account Removed | |
| 1913 | Info | AWS Account Updated | |
| 1914 | Info | Azure Account Added | |
| 1915 | Info | Azure Account Removed | |
| 1916 | Info | Azure Account Updated | |
| 1917 | Info | Azure Account Synchronization Finished | |
| 1918 | Error | Azure Account Synchronization Failed | |
| 1919 | Info | Azure Account Synchronization Requested | |
| 1921 | Info | vCloud Account Added | |
| 1922 | Info | vCloud Account Removed | |
| 1923 | Info | vCloud Account Updated | |
| 1924 | Info | vCloud Account Synchronization Finished | |
| 1925 | Error | vCloud Account Synchronization Failed | |
| 1926 | Info | vCloud Account Synchronization Requested | |
| 1927 | Info | Upgrade Connector to AWS Account | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Requested | |
| 1928 | Warning | AWS Account Update Failed | |
| 1929 | Info | Upgrade Connector to AWS Account Finished | |
| 1950 | Info | Tenant Created | |
| 1951 | Info | Tenant Deleted | |
| 1952 | Info | Tenant Updated | |
| 1953 | Info | Tenant Database Server Created | |
| 1954 | Info | Tenant Database Server Deleted | |
| 1955 | Info | Tenant Database Server Updated | |
| 1957 | Error | Tenant Initialization Failure | |
| 1958 | Info | Tenant Features Updated | |
| 2000 | Info | Scan Cache Configuration Object Added | |
| 2001 | Info | Scan Cache Configuration Object Removed | |
| 2002 | Info | Scan Cache Configuration Object Updated | |
| 2200 | Info | Software Update: Anti-Malware Module Installation Started | |
| 2201 | Info | Software Update: Anti-Malware Module Installation Successful | |
| 2202 | Warning | Software Update: Anti-Malware Module Installation Failed | |
| 2203 | Info | Software Update: Anti-Malware Module Download Successful | |
| 2204 | Info | Security Update: Pattern Update on Agents/Appliances Successful | |
| 2205 | Warning | Security Update: Pattern Update on Agents/Appliances Failed | |
| 2300 | Info | Software Update: Web Reputation Module Installation Started | |
| 2301 | Info | Software Update: Web Reputation Module Installation Successful | |
| 2302 | Warning | Software Update: Web Reputation Module Installation Failed | |
| 2303 | Info | Software Update: Web Reputation Download Successful | |
| 2400 | Info | Software Update: Firewall Module Installation Started | |
| 2401 | Info | Software Update: Firewall Module Installation Successful | |
| 2402 | Warning | Software Update: Firewall Module Installation Failed | |
| 2403 | Info | Software Update: Firewall Module Download Successful | |
| 2500 | Info | Software Update: Intrusion Prevention Module Installation Started | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 2501 | Info | Software Update: Intrusion Prevention Module Installation Successful | |
| 2502 | Warning | Software Update: Intrusion Prevention Module Installation Failed | |
| 2503 | Info | Software Update: Intrusion Prevention Module Download Successful | |
| 2600 | Info | Software Update: Integrity Monitoring Module Installation Started | |
| 2601 | Info | Software Update: Integrity Monitoring Module Installation Successful | |
| 2602 | Warning | Software Update: Integrity Monitoring Module Installation Failed | |
| 2603 | Info | Software Update: Integrity Monitoring Module Download Successful | |
| 2700 | Info | Software Update: Log Inspection Module Installation Started | |
| 2701 | Info | Software Update: Log Inspection Module Installation Successful | |
| 2702 | Warning | Software Update: Log Inspection Module Installation Failed | |
| 2703 | Info | Software Update: Log Inspection Module Download Successful | |
| 2800 | Info | Software Update: Software Automatically Downloaded | |
| 2801 | Error | Software Update: Unable to retrieve Download Center inventory | |
| 2802 | Error | Software Update: Unable to download software from Download Center | |
| 2803 | Info | Online Help Update Started | |
| 2804 | Info | Online Help Update Ended | |
| 2805 | Info | Online Help Update Success | |
| 2806 | Warning | Online Help Update Failed | |
| 2803 | Info | Online Help Update Started | |
| 2804 | Info | Online Help Update Ended | |
| 2805 | Info | Online Help Update Success | |
| 2806 | Warning | Online Help Update Failed | |
| 2900 | Info | Software Update: Relay Module Installation Started | |
| 2901 | Info | Software Update: Relay Module Installation Successful | |
| 2902 | Warning | Software Update: Relay Module Installation Failed | |
| 2903 | Info | Software Update: Relay Module Download Successful | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 2904 | Info | VMware NSX Synchronization Finished | |
| 2905 | Error | VMware NSX Synchronization Failed | |
| 2906 | Info | Agent Self-Protection enabled | |
| 2907 | Info | Agent Self-Protection disabled | |
| 2908 | Info | Agent Self-Protection enabled | |
| 2909 | Info | Agent Self-Protection disabled | |
| 2915 | Info | Data migration complete | |
| 2916 | Warning | Data migration finished with error | |
| 2920 | Info | Querying report from DDAn Finished | |
| 2921 | Error | Querying report from DDAn Failed | |
| 2922 | Info | Submission to Deep Discovery Analyzer processed | |
| 2923 | Error | File submission to Deep Discovery Analyzer Failed | |
| 2924 | Info | Security Update: Suspicious Object Check and Update Successful | |
| 2925 | Error | Security Update: Suspicious Object Check and Update Failed | |
| 2926 | Warning | Submission to Deep Discovery Analyzer queued | |
| 2930 | Info | File back up pending | |
| 2931 | Info | Smart Folder Added | |
| 2932 | Info | Smart Folder Removed | |
| 2933 | Info | Smart Folder Updated | |
| 2934 | Error | Failed to send Amazon SNS message | |
| 2935 | Info | System resumed sending SNS messages | |
| 7000 | Info | Application Control Events Exported | An administrator downloaded application control event logs in CSV format. |
| 7007 | Info | User Viewed Application Control Event | An administrator dismissed an application control alert. This is normal unless your system has been compromised by an intruder that has gained an administrator login. |
| 7008 | Error | Application Control Engine Offline | An agent's application control engine failed to come online. This could happen if you have enabled application control on a computer whose kernel is not supported. |
| 7009 | Info | Application Control Engine Online Again | An agent's application control engine started. |
| 7010 | Info | Application Control Configuration Updated | Deep Security Manager updated the application control settings on an agent. |
| 7011 | Info | Software Update: Application Control Module Installation Started | The agent received a policy from Deep Security Manager where application control was selected, but detected that it did not have the application control engine installed or needed to update it, so it began to download it. This is normal when you enable application control on a computer for the first time, or |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | | when it has been disabled while application control engine updates were released. |
| 7012 | Info | Software Update: Application Control Module Installation Successful | The agent installed the application control engine. The application control engine is also used by the integrity monitoring feature. |
| 7013 | Error | Software Update: Application Control Module Installation Failed | The agent could not install the application control engine. This is not normal. |
| 7014 | Info | Software Update: Application Control Module Download Successful | The agent finished downloading the application control engine. |
| 7015 | Info | Application Control Ruleset Updated | The API was used to allow or block software. This message does not occur when administrators perform the same action in the GUI. |
| 7020 | Info | Application Control Ruleset Retrieved | The API uploaded a computer's initial allow rules to Deep Security Manager. |
| 7021 | Info | Application Control Ruleset Build Started | The application control engine was enabled, and the agent detected that it did not have any allow rules for that computer, so it began to build initial rules based on the currently installed software. This is normal when you enable application control for the first time. This message does not occur when you use the API to replace the allow rules. |
| 7022 | Info | Application Control Ruleset Build Completed | The agent finished building the initial allow rules for that computer. After this, any new software that is detected which is not in the allow or block rules will, if configured, cause and alert. |
| 7023 | Error | Application Control Ruleset Build Failed | The agent could not build the initial allow rules for that computer. This is not normal. |
| 7024 | Info | Application Control Ruleset Updated | An administrator allowed or blocked software in the **Actions** tab, or changed a rule by clicking **Change rule** in an application control log message. This message does not occur when you use the API to replace the allow rules. |
| 7025 | Info | Application Control Ruleset Build Requested | You manually forced application control to delete the current rules and rebuild them based on the currently installed software. This could be normal if you needed to change many rules at the same time. |
| 7026 | Info | Application Control Maintenance Mode Start Requested | An administrator or API sent the command to enable maintenance mode. |
| 7027 | Info | Application Control Maintenance Mode Stop Requested | An administrator or API sent the command to disable maintenance mode. |
| 7028 | Info | Application Control Maintenance Mode Started | Maintenance mode was enabled. While enabled, the agent automatically adds updated or newly installed software to its allow rules, indicating that you know and want to allow the software update. The agent continues to apply block rules during this time. |
| 7029 | Info | Application Control Maintenance Mode | Maintenance mode was disabled. Once |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Stopped | maintenance mode is stopped, all new or changed software will be considered "unrecognized" until you specifically allow or block it. |
| 7030 | Info | Application Control Ruleset Build Cancelled | The agent began to build the initial allow rules, but an administrator canceled the process. |
| 7031 | Error | Sending Application Control Ruleset Failed | An agent could not download a shared ruleset for application control. This can occur if network connectivity is interrupted (such as a firewall or proxy between the agent and relay), or if there isn't enough free disk space on the agent. |
| 7032 | Info | Sending Application Control Ruleset Succeeded | An agent downloaded a shared ruleset for application control. This normally occurs whenever an administrator or API allows or blocks software, or when a different shared ruleset is applied. |
| 7033 | Info | Application Control Ruleset Created | The API was used to create an application control ruleset. This message does not occur when administrators perform the same action in the GUI. |
| 7034 | Info | Application Control Ruleset Updated | The API was used to allow or block software via an application control ruleset. This message does not occur when administrators perform the same action in the GUI. |
| 7035 | Info | Application Control Ruleset Deleted | The API was used to delete an application control ruleset. This message does not occur when administrators perform the same action in the GUI. |
| 7036 | Info | Application Control Maintenance Mode Reset Duration Requested | An administrator changed the time period for when maintenance mode is active. |
| 7037 | Error | Newly applied ruleset will block some running processes on restart | An administrator applied a new ruleset, but some of the currently running processes exist in block rules. Application control will not terminate the processes, but the next time you reboot or restart those services, depending on your configuration, it will either alert you or block them. If the processes are not authorized, you should terminate them manually. If they are authorized, but are missing from the ruleset, you should add them to the ruleset. |
| 7038 | Error | Unresolved software change limit reached | Software changes detected on the file system exceeded the maximum amount. Application control will continue to enforce existing rules, but will not record any more changes, and it will stop displaying any of that computer's software changes. You must resolve and prevent excessive software change. |
| 7040 | Error | Incompatible Application Control Ruleset | An application control ruleset could not be assigned to one or more computers because the ruleset is not supported by the installed version of the agent. Typically, the problem is that a hash-based ruleset (which is compatible only with Deep Security Agent |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | | 11.0 or newer) has been assigned to an older Deep Security Agent. Deep Security Agent 10.x supports only file-based rulesets. (For details, see "Differences in how Deep Security Agent 10.x and 11.x compare files" on page 462.) To fix this issue, upgrade the Deep Security Agent to version 11.0 or newer. Alternatively, if you are using local rulesets, reset application control for the agent. Or if you are using a shared ruleset, use a shared ruleset that was created with Deep Security 10.x until all agents using the shared ruleset are upgraded to Deep Security Agent 11.0 or newer. |
| 7041 | Info | Application Control Ruleset Upgraded | An application control ruleset was upgraded from a file-based ruleset to a hash-based ruleset. (For details, see "Differences in how Deep Security Agent 10.x and 11.x compare files" on page 462.) |

## Anti-malware events

For general best practices related to events, see "Event collection in Deep Security" on page 795.

To see the anti-malware events captured by Deep Security, go to **Events & Reports** > **Events** > **Anti-Malware Events**.

### What information is displayed for anti-malware events?

These columns can be displayed on the Anti-Malware Events page. You can click **Columns** to select which columns are displayed in the table.

- **Time:** Time the event took place on the computer.
- **Computer:** The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)
- **Infected File(s):** The location and name of the infected file.
- **Tag(s):** Event tags associated with this event.
- **Malware:** The name of the malware that was found.
- **Action Taken:** Displays the results of the actions specified in the malware scan configuration associated with the event.

  - **Cleaned:**Deep Security successfully terminated processes or deleted registries, files, cookies, or shortcuts, depending on the type of malware.
  - **Clean Failed:** Malware could not be cleaned for a variety of possible reasons.
  - **Deleted:** An infected file was deleted.
  - **Delete Failed:** An infected file could not be deleted for a variety of possible reasons. For example, the file may be locked by another application, is on a CD, or is in use. If possible, Deep Security will delete the infected file once it is released.
  - **Quarantined:** An infected file was moved to the identified files folder.
  - **Quarantine Failed:** An infected file could not be quarantined for a variety of possible reasons. For example, the file may be locked by another application, is on a CD, or is in use. If possible, Deep Security will quarantine the infected file once it is released. It is also possible that the "Maximum disk space used to store identified files" (specified on the **Policy/Computer Editor > Anti-Malware > Advanced** tab) has been exceeded.
  - **Access Denied:** Deep Security has prevented the infected file from being accessed without removing the file from the system.
  - **Passed:** Deep Security did not take any action but logged the detection of the malware.
- **Scan Type:** The type of scan that found the malware (Real-Time, Scheduled, or Manual).
- **Event Origin:** Indicates from which part of the Deep Security system the event originated.
- **Reason:** The malware scan configuration that was in effect when the malware was detected.
- **Major Virus Type:** The type of malware detected. Possible values are: Joke, Trojan, Virus, Test, Spyware, Packer, Generic, or Other. For information on these types of malware, see the anti-malware event details or see "Protect against malware" on page 486
- **Target(s):** The file, process, or registry key (if any) that the malware was trying to affect. If the malware was trying to affect more than one, this field will contain the value "Multiple."
- **Target Type:** The type of system resource that this malware was trying to affect, such as the file system, a process, or Windows registry.
- **Container ID:** ID of the Docker container where the malware was found.

- **Container Image Name:** Image name of the Docker container where the malware was found.
- **Container Name:** Name of the Docker container where the malware was found.
- **File MD5:** The MD5 hash of the file.

### List of all anti-malware events

| ID | Severity | Event |
|---|---|---|
| 9001 | Info | Anti-Malware Scan Started |
| 9002 | Info | Anti-Malware Scan Completed |
| 9003 | Info | Anti-Malware Scan Terminated Abnormally |
| 9004 | Info | Anti-Malware Scan Paused |
| 9005 | Info | Anti-Malware Scan Resumed |
| 9006 | Info | Anti-Malware Scan Cancelled |
| 9007 | Warning | Anti-Malware Scan Cancel Failed |
| 9008 | Warning | Anti-Malware Scan Start Failed |
| 9009 | Warning | Anti-Malware Scan Stalled |
| 9010 | Error | File cannot be analyzed or quarantined (VM maximum disk space used to store identified files exceeded) |
| 9011 | Error | File cannot be analyzed or quarantined (maximum disk space used to store identified files exceeded) |
| 9012 | Warning | Smart Protection Server Disconnected for Smart Scan |
| 9013 | Info | Smart Protection Server Connected for Smart Scan |
| 9014 | Warning | Computer reboot is required for Anti-Malware protection |
| 9016 | Info | Anti-Malware Component Update Successful |
| 9017 | Error | Anti-Malware Component Update Failed |
| 9018 | Error | Files could not be scanned for malware |
| 9019 | Error | Directory could not be scanned for malware |

## Firewall events

For general best practices related to events, see "Event collection in Deep Security" on page 795.

To see the firewall events captured by Deep Security, go to **Events & Reports** > **Events** > **Firewall Events**.

Firewall event icons:

Single event

Single event with data

Folded event

Folded event with data

**Note:** Event folding occurs when multiple events of the same type occur in succession. This saves disk space and protects against DoS attacks that may attempt to overload the logging mechanism.

## What information is displayed for firewall events?

These columns can be displayed on the firewall events page. You can click **Columns** to select which columns are displayed in the table.

- **Time:** Time the event took place on the computer.
- **Computer:** The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)
- **Reason:** Log entries on this page are generated either by firewall rules or by firewall stateful configuration settings. If an entry is generated by a firewall rule, the column entry will be prefaced by "Firewall Rule:" followed by the name of the firewall rule. Otherwise the column entry will display the firewall stateful configuration setting that generated the log entry.
- **Tag(s):** Event tags that are applied to this event.
- **Action:** The action taken by the firewall rule or firewall stateful configuration. Possible actions are: Allow, Deny, Force Allow, and Log Only.
- **Rank:** The ranking system provides a way to quantify the importance of intrusion prevention and firewall events. By assigning "asset values" to computers, and assigning "severity values" to intrusion prevention rules and firewall rules, the importance ("rank") of an event is calculated by multiplying the two values together. This allows you to sort events by rank when viewing intrusion prevention or firewall events.
- **Direction:** The direction of the affected packet (incoming or outgoing).

- **Interface:** The MAC address of the interface through which the packet was traveling.
- **Frame Type:** The frame type of the packet in question. Possible values are "IPV4", "IPV6", "ARP", "REVARP", and "Other: XXXX" where XXXX represents the four digit hex code of the frame type.
- **Protocol:** Possible values are "ICMP", "ICMPV6", "IGMP", "GGP", "TCP", "PUP", "UDP", "IDP", "ND", "RAW", "TCP+UDP", AND "Other: nnn" where nnn represents a three digit decimal value.
- **Flags:** Flags set in the packet.
- **Source IP:** The packet's source IP.
- **Source MAC:** The packet's source MAC address.
- **Source Port:** The packet's source port.
- **Destination IP:** The packet's destination IP address.
- **Destination MAC:** The packet's destination MAC address.
- **Destination Port:** The packet's destination port.
- **Packet Size:** The size of the packet in bytes.
- **Repeat Count:** The number of times the event was sequentially repeated.
- **Time (microseconds):** Microsecond resolution for the time the event took place on the computer.
- **Event Origin:** The Deep Security component from which the event originated.

Note: **Log-only** rules will only generate a log entry if the packet in question is not subsequently stopped either by a **deny** rule, or an **allow** rule that excludes it. If the packet is stopped by one of those two rules, *those* rules will generate a log entry and *not* the **log-only** rule. If no subsequent rules stop the packet, the log-only rule will generate an entry.

## List of all firewall events

| ID | Event | Notes |
|---|---|---|
| 100 | Out Of Connection | A packet was received that was not associated with an existing connection. |
| 101 | Invalid Flags | Flag(s) set in a packet were invalid. This event can indicate that a flag does not make sense within the context of a current connection (if any), or that a nonsensical combination of flags. |

| ID | Event | Notes |
|---|---|---|
| | | "Firewall Stateful Configuration" must be On for connection context to be assessed. |
| 102 | Invalid Sequence | A packet with an invalid sequence number or out-of-window data size was encountered. |
| 103 | Invalid ACK | A packet with an invalid acknowledgment number was encountered. |
| 104 | Internal Error | |
| 105 | CE Flags | A packet has congestion flags set and the policy's Anti Evasion settings use a custom configuration where the TCP Congestion Flags property is set to Log or Deny. (See "Configure anti-evasion settings" on page 578.) |
| 106 | Invalid IP | Packet's source IP was not valid. |
| 107 | Invalid IP Datagram Length | The length of the IP datagram is less than the length specified in the IP header. |
| 108 | Fragmented | A fragmented packet was encountered and fragmented packets are not allowed. |
| 109 | Invalid Fragment Offset | |
| 110 | First Fragment Too Small | A fragmented packet was encountered, and the size of the first fragment is less than the size of a TCP packet (no data).<br><br>A packet is dropped with this event when the packet header has the following configuration:<br><br>• Fragment Offset = 0 (The fragment is the first in the packet)<br>• Total length (maximum combined header length) < 120 bytes (the default allowed minimum fragment size)<br><br>To prevent this event from occurring, configure the policy's Advanced Network Engine settings to use a lower value for the Minimum Fragment Size property, or set it to 0 to turn off this inspection. (See "Advanced Network Engine Options" in "Network engine settings" on page 378.) |
| 111 | Fragment Out Of Bounds | The offsets(s) specified in a fragmented packet sequence is outside the range of the maximum size of a datagram. |
| 112 | Fragment Offset Too Small | A fragmented packet was encountered, the size of the fragment was less than the size of a TCP packet (no data). |
| 113 | IPv6 Packet | An IPv6 Packet was encountered, and IPv6 blocking is enabled. See the "Block IPv6 on Agents and Appliances verions 9 and later" property in the Advanced Network Engine Options (see "Network engine settings" on page 378.) |
| 114 | Max Incoming Connections | The number of incoming connections has exceeded the maximum number of connections allowed. See the "Enable TCP stateful inspection" property in "TCP packet inspection" on |

| ID | Event | Notes |
|---|---|---|
| | | page 627. |
| 115 | Max Outgoing Connections | The number of outgoing connections has exceeded the maximum number of connections allowed. See the "Enable TCP stateful inspection" property in "TCP packet inspection" on page 627. |
| 116 | Max SYN Sent | The number of half open connections from a single computer exceeds that specified in the firewall stateful configuration. See the "Limit the number of half-open connections from a single computer to" property in "TCP packet inspection" on page 627. |
| 117 | License Expired | |
| 118 | IP Version Unknown | An IP packet other than IPv4 or IPv6 was encountered. |
| 119 | Invalid Packet Info | |
| 120 | Internal Engine Error | Insufficient system memory. Add more system resources to fix this issue. |
| 121 | Unsolicited UDP | Incoming UDP packets that were not solicited by the computer are rejected. |
| 122 | Unsolicited ICMP | ICMP stateful has been enabled (in firewall stateful configuration) and an unsolicited packet that does not match any Force Allow rules was received. |
| 123 | Out Of Allowed Policy | The packet does not meet any of the Allow or Force Allow rules and so is implicitly denied. |
| 124 | Invalid Port Command | An invalid FTP port command was encountered in the FTP control channel data stream. |
| 125 | SYN Cookie Error | The SYN cookies protection mechanism encountered an error. |
| 126 | Invalid Data Offset | Invalid data offset parameter. |
| 127 | No IP Header | The packet IP header is invalid or incomplete. |
| 128 | Unreadable Ethernet Header | Data contained in this Ethernet frame is smaller than the Ethernet header. |
| 129 | Undefined | |
| 130 | Same Source and Destination IP | Source and destination IPs were identical. |
| 131 | Invalid TCP Header Length | |
| 132 | Unreadable Protocol Header | The packet contains an unreadable TCP, UDP or ICMP header. |
| 133 | Unreadable IPv4 Header | The packet contains an unreadable IPv4 header. |
| 134 | Unknown IP Version | Unrecognized IP version. |
| 135 | Invalid Adapter Configuration | An invalid adapter configuration has been received. |

| ID | Event | Notes |
|---|---|---|
| 136 | Overlapping Fragment | This packet fragment overlaps a previously sent fragment. |
| 138 | Packet on Closed Connection | A packet was received belonging to a connection already closed. |
| 139 | Dropped Retransmit | The network engine detected a TCP Packet that overlaps with data already received on the same TCP connection but does not match the already-received data. (The network engine compares the packet data that was queued in the engine's connection buffer to the data in the packet that was re-transmitted.)<br><br>The network engine reconstructs the sequenced data stream of each TCP connection it processes. The sequence number and length in the received packet specify a specific region in this data stream. The note field in the log indicates the location of the changed content in the TCP stream: prev-full, prev-part, next-full and next-part:<br><br>• "prev-full" and "prev-part": The changed area is in the packet that immediately precedes the retransmitted packet in the sequenced data stream. "prev-full" indicates that the changed area is completely contained in the packet which immediately precedes the retransmitted packet in the sequenced data stream. Otherwise, the note is "prev-part".<br>• "next-full" and "next-part": The changed area is in the packet that immediately follows the retransmitted packet in the sequenced data stream. "next-full" indicates that the changed area is completely contained in the packet that immediately follows the retransmitted packet in the sequenced data stream. Otherwise, the note is "next-part". |
| 140 | Undefined | |
| 141 | Out of Allowed Policy (Open Port) | |
| 142 | New Connection Initiated | |
| 143 | Invalid Checksum | |
| 144 | Invalid Hook Used | |

| ID | Event | Notes |
|---|---|---|
| 145 | IP Zero Payload | |
| 146 | IPv6 Source Is Multicast | |
| 147 | Invalid IPv6 Address | |
| 148 | IPv6 Fragment Too Small | |
| 149 | Invalid Transport Header Length | |
| 150 | Out of Memory | |
| 151 | Max TCP Connections | The maximum number of TCP connections has been exceeded. See "Event: Max TCP connections" on page 984. |
| 152 | Max UDP Connections | |
| 200 | Region Too Big | A region (edit region, uri etc) exceeded the maximum allowed buffering size (7570 bytes) without being closed. This is usually because the data does not conform to the protocol. |
| 201 | Insufficient Memory | The packet could not be processed properly because resources were exhausted. This can be because too many concurrent connections require buffering (max 2048) or matching resources (max 128) at the same time or because of excessive matches in a single IP packet (max 2048) or simply because the system is out of memory. |
| 202 | Maximum Edits Exceeded | The maximum number of edits (32) in a single region of a packet was exceeded. |
| 203 | Edit Too Large | Editing attempted to increase the size of the region above the maximum allowed size (8188 bytes). |
| 204 | Max Matches in Packet Exceeded | There are more than 2048 positions in the packet with pattern match occurrences. An error is returned at this limit and the connection is dropped because this usually indicates a garbage or evasive packet. |
| 205 | Engine Call Stack Too Deep | |
| 206 | Runtime Error | Runtime error. |
| 207 | Packet Read Error | Low level problem reading packet data. |
| 257 | Fail Open: Deny | Log the packet that should be dropped but not when Fail-Open feature is on and in Inline mode. |
| 300 | Unsupported Cipher | An unknown or unsupported cipher suite has been requested. |
| 301 | Error Generating Master Key(s) | Unable to derive the cryptographic keys, Mac secrets, and initialization vectors from the master secret. |
| 302 | Record Layer Message (not ready) | The SSL state engine has encountered an SSL record before initialization of the session. |

| ID | Event | Notes |
|---|---|---|
| 303 | Handshake Message (not ready) | The SSL state engine has encountered a handshake message after the handshake has been negotiated. |
| 304 | Out Of Order Handshake Message | A well formatted handshake message has been encountered out of sequence. |
| 305 | Memory Allocation Error | The packet could not be processed properly because resources were exhausted. This can be because too many concurrent connections require buffering (max 2048) or matching resources (max 128) at the same time or because of excessive matches in a single IP packet (max 2048) or simply because the system is out of memory. |
| 306 | Unsupported SSL Version | A client attempted to negotiate an SSL V2 session. |
| 307 | Error Decrypting Pre-master Key | Unable to un-wrap the pre-master secret from the ClientKeyExchange message. |
| 308 | Client Attempted to Rollback | A client attempted to rollback to an earlier version of the SSL protocol than that which was specified in the ClientHello message. |
| 309 | Renewal Error | An SSL session was being requested with a cached session key that could not be located. |
| 310 | Key Exchange Error | The server is attempting to establish an SSL session with temporarily generated key. |
| 311 | Maximum SSL Key Exchanges Exceeded | The maximum number of concurrent key exchange requests was exceeded. |
| 312 | Key Too Large | The master secret keys are larger than specified by the protocol identifier. |
| 313 | Invalid Parameters In Handshake | An invalid or unreasonable value was encountered while trying to decode the handshake protocol. |
| 314 | No Sessions Available | |
| 315 | Compression Method Unsupported | |
| 316 | Unsupported Application-Layer Protocol | An unknown or unsupported SSL Application-Layer Protocol has been requested. |
| 385 | Fail Open: Deny | Log the packet that should be dropped but not when Fail-Open feature is on and in Tap mode. |
| 500 | URI Path Depth Exceeded | Too many "/" separators. Max 100 path depth. |
| 501 | Invalid Traversal | Tried to use "../" above root. |
| 502 | Illegal | Illegal character used in uri. |

| ID | Event | Notes |
|---|---|---|
| | Character in URI | |
| 503 | Incomplete UTF8 Sequence | URI ended in middle of utf8 sequence. |
| 504 | Invalid UTF8 encoding | Invalid or non-canonical encoding attempt. |
| 505 | Invalid Hex Encoding | %nn where nn are not hex digits. |
| 506 | URI Path Length Too Long | Path length is greater than 512 characters. |
| 507 | Invalid Use of Character | Use of disabled characters |
| 508 | Double Decoding Exploit | Double decoding exploit attempt (%25xx, %25%xxd, etc). |
| 700 | Invalid Base64 Content | Packet content that was expected to be encoded in Base64 format was not encoded correctly. |
| 710 | Corrupted Deflate/GZIP Content | Packet content that was expected to be encoded in Base64 format was not encoded correctly. |
| 711 | Incomplete Deflate/GZIP Content | Incomplete Deflate/GZIP content |
| 712 | Deflate/GZIP Checksum Error | Deflate/GZIP checksum error. |
| 713 | Unsupported Deflate/GZIP Dictionary | Unsupported Deflate/GZIP dictionary. |
| 714 | Unsupported GZIP Header Format/Method | Unsupported GZIP header format or method. |
| 801 | Protocol Decoding Search Limit Exceeded | A protocol decoding rule defined a limit for a search or pdu object but the object was not found before the limit was reached. |
| 802 | Protocol Decoding Constraint Error | A protocol decoding rule decoded data that did not meet the protocol content constraints. |
| 803 | Protocol Decoding Engine Internal Error | |

| ID | Event | Notes |
|---|---|---|
| 804 | Protocol Decoding Structure Too Deep | A protocol decoding rule encountered a type definition and packet content that caused the maximum type nesting depth (16) to be exceeded. |
| 805 | Protocol Decoding Stack Error | A rule programming error attempted to cause recursion or use to many nested procedure calls. |
| 806 | Infinite Data Loop Error | |

## Intrusion prevention events

For general best practices related to events, see "Event collection in Deep Security" on page 795.

To see the intrusion prevention events captured by Deep Security, go to **Events & Reports** > **Events** > **Intrusion Prevention Events**.

### What information is displayed for intrusion prevention events?

These columns can be displayed on the Intrusion Prevention Events page. You can click **Columns** to select which columns are displayed in the table.

- **Time:** Time the event took place on the computer.
- **Computer:** The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)
- **Reason:** The intrusion prevention rule associated with this event.
- **Tag(s):** Any tags attached with the event.
- **Application Type:** The application type associated with the intrusion prevention rule which caused this event.
- **Action:** What action the intrusion prevention rule took (Block or Reset). If the rule is in **Detect Only** mode, the action is prefaced with "Detect Only:").

  **Note:** Intrusion prevention rules created before Deep Security 7.5 SP1 could also perform Insert, Replace, and Delete actions. These actions are no longer performed. If an

older rule is triggered and attempts to perform those actions, the event will indicate that the rule was applied in detect-only mode.

- **Rank:** The ranking system provides a way to quantify the importance of intrusion prevention and firewall events. By assigning "asset values" to computers, and assigning "severity values" to intrusion prevention rules and firewall rules, the importance ("rank") of an event is calculated by multiplying the two values together. This allows you to sort events by rank when viewing intrusion prevention or firewall events.
- **Severity:** The intrusion prevention rule's severity value.
- **Direction:** The direction of the packet (incoming or outgoing)
- **Flow:** whether the packets(s) that triggered this event was travelling with ("Connection Flow") or against ("Reverse Flow") the direction of traffic being monitored by the intrusion prevention rule.
- **Interface:** The MAC address of the interface through which the packet was passing.
- **Frame Type:** The frame type of the packet in question. Possible values are "IPV4", "IPV6", "ARP", "REVARP", and "Other: XXXX" where XXXX represents the four digit hex code of the frame type.
- **Protocol:** Possible values are "ICMP", "ICMPV6", "IGMP", "GGP", "TCP", "PUP", "UDP", "IDP", "ND", "RAW", "TCP+UDP", AND "Other: nnn" where nnn represents a three digit decimal value.
- **Flags:** Flags set in the packet.
- **Source IP:** The packet's source IP.
- **Source MAC:** The packet's source MAC address.
- **Source Port:** The packet's source port.
- **Destination IP:** The packet's destination IP address.
- **Destination MAC:** The packet's destination MAC address.
- **Destination Port:** The packet's destination port.
- **Packet Size:** The size of the packet in bytes.
- **Repeat Count:** The number of times the event was sequentially repeated.

- **Time (microseconds):** Microsecond resolution for the time the event took place on the computer.
- **Event Origin:** The Deep Security component from which the event originated.

## List of all intrusion prevention events

| ID | Event | Notes |
|---|---|---|
| 200 | Region Too Big | A region (edit region, uri etc) exceeded the maximum allowed buffering size (7570 bytes) without being closed. This is usually because the data does not conform to the protocol. |
| 201 | Insufficient Memory | The packet could not be processed properly because resources were exhausted. This can be because there are too many concurrent connections at the same time or simply because the system is out of memory. |
| 202 | Maximum Edits Exceeded | The maximum number of edits (32) in a single region of a packet was exceeded. |
| 203 | Edit Too Large | Editing attempted to increase the size of the region above the maximum allowed size (8188 bytes). |
| 204 | Max Matches in Packet Exceeded | There are more than 2048 positions in the packet with pattern match occurrences. An error is returned at this limit and the connection is dropped because this usually indicates a garbage or evasive packet. |
| 205 | Engine Call Stack Too Deep | |
| 206 | Runtime Error | Runtime error. |
| 207 | Packet Read Error | Low level problem reading packet data. |
| 258 | Fail Open: Reset | Log the connection that should be reset but not when Fail-Open feature is on and in Inline mode |
| 300 | Unsupported Cipher | An unknown or unsupported Cipher Suite has been requested. |
| 301 | Error Generating Master Key(s) | Unable to derive the cryptographic keys, Mac secrets, and initialization vectors from the master secret. |
| 302 | Record Layer Message (not ready) | The SSL state engine has encountered an SSL record before initialization of the session. |
| 303 | Handshake Message (not ready) | The SSL state engine has encountered a handshake message after the handshake has been negotiated. |
| 304 | Out Of Order Handshake Message | A well formatted handshake message has been encountered out of sequence. |
| 305 | Memory Allocation Error | The packet could not be processed properly because resources were exhausted. This can be because there are too many concurrent connections at the same time or simply because the system is out of memory. |
| 306 | Unsupported SSL Version | A client attempted to negotiate an SSL V2 session. |
| 307 | Error Decrypting Pre-master Key | Unable to un-wrap the pre-master secret from the ClientKeyExchange message. |
| 308 | Client Attempted | A client attempted to rollback to an earlier version of the SSL protocol than that which was |

| ID | Event | Notes |
|---|---|---|
| | to Rollback | specified in the ClientHello message. |
| 309 | Renewal Error | An SSL session was being requested with a cached session key that could not be located. |
| 310 | Key Exchange Error | The server is attempting to establish an SSL session with temporarily generated key. |
| 311 | Maximum SSL Key Exchanges Exceeded | The maximum number of concurrent key exchange requests was exceeded. |
| 312 | Key Too Large | The master secret keys are larger than specified by the protocol identifier. |
| 313 | Invalid Parameters In Handshake | An invalid or unreasonable value was encountered while trying to decode the handshake protocol. |
| 314 | No Sessions Available | |
| 315 | Compression Method Unsupported | |
| 316 | Unsupported Application-Layer Protocol | An unknown or unsupported SSL Application-Layer Protocol has been requested. |
| 386 | Fail Open: Reset | Log the connection that should be reset but not when Fail-Open feature is on and in Tap mode. |
| 500 | URI Path Depth Exceeded | Too many "/" separators. Max 100 path depth. |
| 501 | Invalid Traversal | Tried to use "../" above root. |
| 502 | Illegal Character in URI | Illegal character used in uri. |
| 503 | Incomplete UTF8 Sequence | URI ended in middle of utf8 sequence. |
| 504 | Invalid UTF8 encoding | Invalid or non-canonical encoding attempt. |
| 505 | Invalid Hex Encoding | %nn where nn are not hex digits. |
| 506 | URI Path Length Too Long | Path length is greater than 512 characters. |
| 507 | Invalid Use of Character | Use of disabled characters |
| 508 | Double Decoding Exploit | Double decoding exploit attempt (%25xx, %25%xxd, etc). |
| 700 | Invalid Base64 Content | Packet content that was expected to be encoded in Base64 format was not encoded correctly. |
| 710 | Corrupted Deflate/GZIP Content | Packet content that was expected to be encoded in Base64 format was not encoded correctly. |
| 711 | Incomplete Deflate/GZIP Content | Incomplete Deflate/GZIP content |

| ID | Event | Notes |
|---|---|---|
| 712 | Deflate/GZIP Checksum Error | Deflate/GZIP checksum error. |
| 713 | Unsupported Deflate/GZIP Dictionary | Unsupported Deflate/GZIP dictionary. |
| 714 | Unsupported GZIP Header Format/Method | Unsupported GZIP header format or method. |
| 801 | Protocol Decoding Search Limit Exceeded | A protocol decoding rule defined a limit for a search or pdu object but the object was not found before the limit was reached. |
| 802 | Protocol Decoding Constraint Error | A protocol decoding rule decoded data that did not meet the protocol content constraints. |
| 803 | Protocol Decoding Engine Internal Error | |
| 804 | Protocol Decoding Structure Too Deep | A protocol decoding rule encountered a type definition and packet content that caused the maximum type nesting depth (16) to be exceeded. |
| 805 | Protocol Decoding Stack Error | A rule programming error attempted to cause recursion or use to many nested procedure calls. |
| 806 | Infinite Data Loop Error | |

## Integrity monitoring events

For general best practices related to events, see "Event collection in Deep Security" on page 795.

To see the integrity monitoring events captured by Deep Security, go to **Events & Reports** > **Events** > **Integrity Monitoring Events**.

### What information is displayed for integrity monitoring events?

These columns can be displayed on the Integrity Monitoring Events page. You can click **Columns** to select which columns are displayed in the table.

- **Time:** Time the event took place on the computer.
- **Computer:** The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)

- **Reason:** The integrity monitoring rule associated with this event.
- **Tag(s):** Event tags that are applied to this event.
- **Change:** The change detected by the integrity rule. Can be: Created, Updated, Deleted, or Renamed.
- **Rank:** The ranking system provides a way to quantify the importance of events. By assigning "asset values" to computers, and assigning "severity values" to rules, the importance ("rank") of an event is calculated by multiplying the two values together. This allows you to sort events by rank.
- **Severity:** The integrity monitoring rule's severity value
- **Type:** Type of entity from which the event originated
- **Key:** Path and file name or registry key from which the event originated
- **User:** User ID of the file owner
- **Process:** Process from which the event originated
- **Event Origin:** The Deep Security component from which the event originated

## List of all integrity monitoring events

| ID | Severity | Event | Notes |
|---|---|---|---|
| 8000 | Info | Full Baseline Created | Created when the agent has been requested to build a baseline or went from 0 integrity monitoring rules to n (causing the baseline to be built). This event includes information on the time taken to scan (ms), and number of entities cataloged. |
| 8001 | Info | Partial Baseline Created | Created when the agent had a security configuration where one or more integrity monitoring rules changed. This event includes information on the time taken to scan (ms), and number of entities catalogued. |
| 8002 | Info | Scan for Change Completed | Created when the agent is requested to do a full or partial on-demand scan. This event includes information on the time taken to scan (ms), and number of CHANGES catalogued. (Ongoing scans for changes based on the FileSystem Driver or the notify do not generate an 8002 event.) |
| 8003 | Error | Unknown Environment Variable in Integrity Monitoring Rule | Created when a rule uses a ${env.EnvironmentVar} and "EnvironmentVar" is not a known environment variable. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, and the name of the unknown environment variable. |
| 8004 | Error | Bad Base in Integrity Monitoring Rule | Created when a rule contains an invalid base directory or key. For example, specifying a FileSet with a base of "c:\foo\d:\bar" would generate this event, or the invalid value could be the result of environment variable substitution the yields a bad value. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, and the bad base value. |

| ID | Severity | Event | Notes |
|---|---|---|---|
| 8005 | Error | Unknown Entity in Integrity Monitoring Rule | Created when an unknown EntitySet is encountered in an integrity monitoring rule. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, and a comma-separated list of the unknown EntitySet names encountered. |
| 8006 | Error | Unsupported Entity in Integrity Monitoring Rule | Created when a known but unsupported EntitySet is encountered in an integrity monitoring rule. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, and a comma-separated list of the unsupported EntitySet names encountered. Some EntitySet types such as RegistryKeySet are platform-specific. |
| 8007 | Error | Unknown Feature in Integrity Monitoring Rule | Created when an unknown feature is encountered in an integrity monitoring rule. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, the type of entity set (for example, FileSet), and a comma-separated list of the unknown feature names encountered. Examples of valid feature values are "whereBaseInOtherSet", "status", and "executable". |
| 8008 | Error | Unsupported Feature in Integrity Monitoring Rule | Created when a known but unsupported feature is encountered in an integrity monitoring rule. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, the type of entity set (for example, FileSet), and a comma-separated list of the unsupported feature names encountered. Some feature values such as "status" (used for Windows service states) are platform-specific. |
| 8009 | Error | Unknown Attribute in Integrity Monitoring Rule | Created when an unknown attribute is encountered in an integrity monitoring rule. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, the type of entity set (for example, FileSet), and a comma-separated list of the unknown attribute names encountered. Examples of valid attribute values are "created", "lastModified" and "inodeNumber". |
| 8010 | Error | Unsupported Attribute in Integrity Monitoring Rule | Created when a known but unsupported attribute is encountered in an integrity monitoring rule. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, the type of entity set (for example, FileSet), and a comma-separated list of the unsupported attribute names encountered. Some attribute values such as "inodeNumber" are platform-specific. |
| 8011 | Error | Unknown Attribute in Entity Set in Integrity Monitoring Rule | Created when an unknown EntitySet XML attribute is encountered in an integrity monitoring rule. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, the type of entity set (for example,FileSet), and a comma-separated list of the unknown EntitySet attribute names encountered. You would get this event if you wrote <FileSet dir="c:\foo"> instead of <FileSet base="c:\foo"> |
| 8012 | Error | Unknown Registry String in Integrity Monitoring Rule | Created when a rule references a registry key that doesn't exist. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, and the name of the unknown registry string. |
| 8013 | Error | Invalid WQLSet was used. Namespace | Indicates that the namespace is missing from a WQL query because an integrity rule XML is incorrectly formatted. This can occur only in an advanced case, with custom integrity rules that use and monitor WQL queries. |

| ID | Severity | Event | Notes |
|---|---|---|---|
| | | or WQL query was missing. | |
| 8014 | Error | Invalid WQLSet was used. An unknown provider value was used. | |
| 8015 | Warning | Inapplicable Integrity Monitoring Rule | Can be caused by a number of reasons, such as platform mismatch, nonexistent target directories or files, or unsupported functionality. |
| 8016 | Warning | Suboptimal Integrity Rule Detected | |
| 8050 | Error | Regular expression could not be compiled. Invalid wildcard was used. | |

## Log inspection events

For general best practices related to events, see "Event collection in Deep Security" on page 795.

To see the log inspection events captured by Deep Security, go to **Events & Reports > Events > Log Inspection Events**.

### What information is displayed for log inspection events?

These columns can be displayed on the log inspection events page. You can click **Columns** to select which columns are displayed in the table.

- **Time:** Time the event took place on the computer.
- **Computer:** The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)

- **Reason:** The log inspection rule associated with this event.
- **Tag(s):** Any tags attached with the event.
- **Description:** Description of the rule.
- **Rank:** The ranking system provides a way to quantify the importance of events. By assigning "asset values" to computers, and assigning "severity values" to log inspection rules, the importance ("rank") of an event is calculated by multiplying the two values together. This allows you to sort events by rank.
- **Severity:** The log inspection rule's severity value.
- **Groups:** Group that the rule belongs to.
- **Program Name:** Program name. This is obtained from the syslog header of the event.
- **Event:** The name of the event.
- **Location:** Where the log came from.
- **Source IP:** The packet's source IP.
- **Source Port:** The packet's source port.
- **Destination IP:** The packet's destination IP address.
- **Destination Port:** The packet's destination port.
- **Protocol:** Possible values are "ICMP", "ICMPV6", "IGMP", "GGP", "TCP", "PUP", "UDP", "IDP", "ND", "RAW", "TCP+UDP", AND "Other: nnn" where nnn represents a three digit decimal value.
- **Action:** The action taken within the event
- **Source User:** Originating user within the event.
- **Destination User:** Destination user within the event.
- **Event HostName:** Hostname of the event source.
- **ID:** Any ID decoded as the ID from the event.
- **Status:** The decoded status within the event.
- **Command:** The command being called within the event.
- **URL:** The URL within the event.
- **Data:** Any additional data extracted from the event.

- **System Name:** The system name within the event.
- **Rule Matched:** Rule number that was matched.
- **Event Origin:** The Deep Security component from which the event originated.

### List of log inspection security events

**Note:** For system events related to log inspection, see "System events" on page 918.

| ID | Severity | Event |
|---|---|---|
| 8100 | Error | Log Inspection Engine Error |
| 8101 | Warning | Log Inspection Engine Warning |
| 8102 | Info | Log Inspection Engine Initialized |

## Web reputation events

For general best practices related to events, see "Event collection in Deep Security" on page 795.

To see the web reputation events captured by Deep Security, go to **Events & Reports** > **Events** > **Web Reputation Events**.

### What information is displayed for web reputation events?

These columns can be displayed on the web reputation events page. You can click **Columns** to select which columns are displayed in the table.

- **Time:** Time the event took place on the computer.
- **Computer:** The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)
- **URL:** The URL that triggered this event.
- **Tag(s):** Event tags associated with this event.
- **Risk:** What was the risk level of the URL that triggered the event ("Suspicious", "Highly Suspicious", "Dangerous", "Untested", or "Blocked by Administrator").
- **Rank:** Rank provides a way to quantify the importance of events. It is calculated by multiplying the asset value of the computer by the severity of the rule. (See "Rank events to

quantify their importance" on page 813.)

- **Event Origin:** Indicates from which part of the Deep Security system the event originated.

### Add a URL to the list of allowed URLs

If you want to add the URL that triggered an event to the list of allowed URLs, right-click the event and select **Add to Allow List**. (To view or edit the **Allowed** and **Blocked** lists, go to the **Exceptions** tab on the main **Web Reputation** page.)

## Troubleshoot common events, alerts, and errors

This section provides troubleshooting tips for some common events, alerts, and errors.

- "Why am I seeing firewall events when the firewall module is off?" on the next page
- "Why am I getting "Unrecognized Client" events?" on the next page
- Event: Configuration package too large (See "Maximum size for configuration packages " on page 582.)
- "Troubleshoot "Smart Protection Server disconnected" errors" on page 965
- "Error: Activation Failed" on page 965
- "Error: Agent version not supported" on page 967
- "Error: Installation of Feature 'dpi' failed: Not available: Filter" on page 967
- "Error: AWS Marketplace billing usage data has not been successfully submitted in over 48 hours" on page 968
- "Error: Interface out of sync" on page 969
- "Error: Integrity Monitoring Engine Offline and other errors occur after activating a virtual machine" on page 973
- "Error: Module installation failed (Linux)" on page 974
- "Error: There are one or more application type conflicts on this computer" on page 974
- "Error: Unable to connect to the cloud account" on page 976
- "Error: Unable to resolve instance hostname" on page 978
- "Error: Anti-malware engine offline" on page 978

- "Error: Check Status Failed" on page 981
- "Error: Log Inspection Rules Require Log Files" on page 981
- "Alert: Integrity Monitoring information collection has been delayed" on page 983
- "Alert: The memory warning threshold of Manager Node has been exceeded" on page 983
- "Alert: Manager Time Out of Sync" on page 984
- "Warning: Reconnaissance Detected" on page 986
- "Warning: Insufficient disk space" on page 988


## Why am I seeing firewall events when the firewall module is off?

If you have the intrusion prevention module enabled, you may see some firewall events because the intrusion prevention module leverages the firewall's stateful configuration mechanism to perform inspections.

## Why am I getting "Unrecognized Client" events?

The **Unrecognized Client** event message appears when the Deep Security Manager is contacted by a Deep Security Agent that it doesn't recognize.

The most common reason is that an instance has been manually deleted from the **Computers** page in Deep Security Manager *before* deactivating the agent on that instance.

The Deep Security Agent on the instance will continue to try to connect to the Deep Security Manager periodically, generating the **Contact by Unrecognized Client** event message.

In order to bring the deleted computer back into the list of computers in Deep Security Manager, you need to do the following:

1. Go to **Administration** > **System Settings** > **Agents** > **Agent-Initiated Activation** and select **Allow reactivation of unknown VMs**. With this setting enabled, instances will be re-added on their next heartbeat.
2. If you no longer want to protect this computer, use the **Computer** > **Actions** menu to deactivate the agent.

**Note:** After the agent has been deactivated, then you can manually delete the computer from the **Computers** list in the Deep Security Manager.

## Troubleshoot "Smart Protection Server disconnected" errors

If you are using the anti-malware or web reputation modules, you may see either a "Smart Protection Server Disconnected for Smart Scan" or "Smart Protection Server Disconnected for Web Reputation" error in the Deep Security Manager console. To fix the error, try the following troubleshooting tips.

### Check the error details

Double-click the error message to display more detailed information, including the URL that the server is trying to contact. The error may include:

- Timeout was reached
- Couldn't resolve hostname

From a command prompt, use nslookup to check whether the DNS name resolves to an IP address. If the URL doesn't resolve, then there is a DNS issue on the local server.

Use a telnet client to test connectivity to the URL on ports 80 and 443. If you can't connect, check that all of your firewalls, security groups, etc. are allowing outbound communication to the URL on those ports.

## Error: Activation Failed

Several events can trigger an "Activation Failed" alert:

- "Activation Failed - Protocol Error" on the next page
- "Activation Failed - Unable to resolve hostname" on the next page
- "Activation Failed - No Agent/Appliance" on page 967
- "Activation Failed - AWS Marketplace billing usage data has not been submitted in 48 hours" on page 967

## Activation Failed - Protocol Error

This error typically occurs when you use Deep Security Manager to attempt to activate an agent and the manager is unable to communicate with the agent. The communication directionality that the agent uses determines the method that you should use to troubleshoot this error. (See "Agent-manager communication" on page 196.)

### Agent-initiated communication

When the agent uses agent-initiated communication, you need to activate the agent from the agent computer. (See "Activate an agent" on page 256.)

*When using Deep Security as a Service, agent-initiated communication is the recommended communication directionality.*

### Bidirectional communication

Use the following troubleshooting steps when the error occurs and the agent uses bidirectional communication:

1. Ensure that the agent is installed on the computer and that the agent is running.
2. Ensure that the ports are open between the manager and the agent. (See "Port numbers" on page 96 and "Create a firewall rule" on page 597.)

## Activation Failed - Unable to resolve hostname

The error: Activation Failed (Unable to resolve hostname) could be the result of an unresolvable hostname in DNS or of activating the agent from Deep Security Manager when you are not using agent-initiated activation.

If your agent is in bidirectional or manager-initiated mode, your hostname must be resolvable in DNS. Check the DNS on your Deep Security Manager to ensure it can resolve your hosts.

If you are a Deep Security as a Service user or your computers are in cloud accounts, we recommend that you always use agent-initiated activation. Learn how to configure policy rules for agent-initiated communication and deploy agents using deployment scripts, see "Use agent-initiated communication with cloud accounts" on page 202.

### Activation Failed - No Agent/Appliance

This error message indicates that the agent software has not been installed on the computer that you would like to protect.

Review "Deploy the Deep Security AMI from AWS Marketplace" on page 128.

### Activation Failed - AWS Marketplace billing usage data has not been submitted in 48 hours

The error: Unable to activate the Agent because AWS Marketplace billing usage data has not been submitted in 48 hours. Ensure your Deep Security Manager instance is assigned an IAM role with permission 'aws-marketplace:MeterUsage' and can reach the AWS Marketplace Billing end point.

For troubleshooting information, see "Error: AWS Marketplace billing usage data has not been successfully submitted in over 48 hours" on the next page.

## Error: Agent version not supported

The error message "Agent version not supported" indicates that the agent version currently installed on the computer is not supported by the Deep Security Manager.

Although the unsupported agent will still protect the computer based on the last policy settings it received from the Deep Security Manager, we recommend that you upgrade the agent so that you can react quickly to the latest threats. For more information, see "Update the Deep Security Agent" on page 738.

## Error: Installation of Feature 'dpi' failed: Not available: Filter

The error message "Installation of Feature 'dpi' failed: Not available: Filter" indicates that your operating system kernel version is not supported yet by the network driver. You will get this message typically when applying intrusion prevention, web reputation, or firewall because the Deep Security Agent will install a network driver at the same time in order to examine traffic. The same circumstances can cause **engine offline** alerts.

An update may be on its way. Trend Micro actively monitors a variety of operating system vendors for new kernel releases. After completing quality assurance tests, we will release an update with support for these kernels.

Your system will install the required support automatically when an update for your operating system kernel version becomes available.

Contact technical support (sign in Deep Security, and click **Support** in the top right-hand corner) to find out when support for your operating system kernel version will be released.

### Additional information

This only affects intrusion prevention, web reputation, and firewall. All other protection (anti-malware, file integrity monitoring, and log inspection) will operate correctly.

To review supported operating system kernel versions, visit the Deep Security 9.6 Supported Linux Kernels page and look for your operating system distribution.

## Error: AWS Marketplace billing usage data has not been successfully submitted in over 48 hours

If you are subscribed to Deep Security for AWS Marketplace with AWS Marketplace billing you might experience the following error:

"Unable to activate the Agent because AWS Marketplace billing usage data has not been submitted in 48 hours. Ensure your Deep Security Manager instance is assigned an IAM role with permission 'aws-marketplace:MeterUsage' and can reach the AWS Marketplace Billing end point."

Several causes can produce this error:

| Cause | Description |
|---|---|
| The IAM role for the Deep Security Manager is configured incorrectly. | See "Configure the IAM role for the Deep Security AMI from AWS Marketplace" on page 127 |

| Cause | Description |
| --- | --- |
| The Deep Security Manager cannot reach the AWS billing service. | The Deep Security Manager communicates with the AWS billing service over port 443 at a URL corresponding with the AWS region that your Deep Security Manager runs in (for example: https://metering.marketplace.*us-east-1*.amazonaws.com).<br><br>To test if connectivity with the AWS billing service is the cause of the error, check if<br><br>• Communications over port 443 or to the AWS billing service URL are restricted by either Deep Security or a third-party firewall.<br>• The server on which the Deep Security Manager is running connects directly to the Internet. The Deep Security Manager cannot connect to the AWS billing service through a proxy or VPN. |
| The Deep Security Manager cannot reach the AWS metadata server. | To test if connectivity with the AWS metadata server is causing the error, log in to the Deep Security Manager over SSH and run the following curl command:<br><br>`curl http://169.254.169.254/latest/meta-data/` |

## Error: Interface out of sync

This error occurs when the interface information that the Deep Security Manager has stored in its database for the guest virtual machine is not the same as the interface information being reported by the Deep Security Virtual Appliance (for example, different MAC addresses).

To determine the root cause of this issue, you need to find out where the information has become out of sync.

The first step is to check the error message from Deep Security Manager to determine which virtual computer and which interface has the issue.

## Check the specific virtual computer interfaces

1. Log on to the virtual computer.
2. Open a command prompt and type the following: `ipconfig /all`
3. Verify all of the NICs and MAC addresses and make sure that the NICs have the correct driver and that they are working properly.

## Check the virtual computer interface information in vCenter

1. Check the VM interface information from the Managed Object Reference (MoRef) in the vCenter Server by accessing the virtual computer MOB from the web browser and going to: **https://<VC_SERVER>/mob/?moid=<OBJECT_ID>**

   For example: https://192.168.100.100/mob/?moid=vm-1136&doPath=config

   Where:

   <VC_SERVER> is the FQDN or IP of the vCenter Server

   =<OBJECT_ID> is the ID of the object you are looking up

   For more information on accessing the VC MOB see Looking up Managed Object Reference (MoRef) in vCenter Server.

2. Go to **Config > extraConfig["ethernet0.filter0....."] > hardware** to check all the NICs and MAC address.
3. Compare the MAC addresses with step 3 from above.

## Check the vmx file and the virtual computer interface information in Deep Security Manager

1. Use the vCenter Server datastore browser to download the specific vmx file of the virtual computer.
2. Open the vmx file using Notepad and check the IPs, uuid.bios, and MAC addresses. For example:

```
Check virtual computer UUID
- uuid.bios = "42 23 d6 5d f2 d5 22 41-87 41 86 83 ea 2f 23 ac"
Check EPSec Settings
- VFILE.globaloptions = "svmip=169.254.50.39 svmport=8888"
- scsi0:0.filters = "VFILE"
```

```
Check DvFilter Settings
- ethernet0.filter0.name = "dvfilter-dsa"
- ethernet0.filter0.onFailure = "failOpen"
- ethernet0.filter0.param0 = "4223d65d-f2d5-2241-8741-8683ea2f23ac"
- ethernet0.filter0.param2 = "1"
- ethernet0.filter0.param1 = "00:50:56:A3:02:D8"
```

3. Go to the Deep Security Manager dashboard, double-click the specific **VM > Interfaces**, and verify the IPs and MAC addresses.
4. Compare the IP and MAC address with the results from above.

## Check the virtual computer interface information in the Deep Security Virtual Appliance

1. Use the vCenter Server datastore browser to download the specific vmx file of the virtual computer.
2. Open the vmx file using Notepad and check the uuid.bios value.
3. Log on to the Deep Security Virtual Appliance console and press **Alt + F2** to switch to command mode and then enter the Deep Security Virtual Appliance user name and password.
4. Run the following command to verify if the interface of the virtual computer was recognized by Deep Security Virtual Appliance. (Note: Replace $uuid with your actual bios uuid.)

   ```
   cd /var/opt/ds_agent/guests/$uuid
   >/opt/ds_guest_agent/ratt if
   ```

5. Execute the **ifconfig -a** command to verify if the Deep Security Virtual Appliance NIC settings and IP are configured correctly.
6. Compare the IP and MAC address with the results from above.

## Workaround Options

If any of the above items are out of sync then you need to fix this issue.

### Option 1

When cloning an activated virtual computer in Deep Security, you might receive the interface out of sync alert if you power on and activate a virtual computer. As a work around, clean the dvfilter settings before powering on the cloned virtual computer.

- ethernet0.filter0.name = "dvfilter-dsa"
- ethernet0.filter0.onFailure = "failOpen"
- ethernet0.filter0.param0 = "4223d65d-f2d5-2241-8741-8683ea2f23ac"
- ethernet0.filter0.param2 = "1"
- ethernet0.filter0.param1 = "00:50:56:A3:02:D8"

### Option 2

1. Suspend the specific virtual computer and power it on again.
2. Restart the Deep Security Virtual Appliance.
3. Deactivate the virtual computer and then activate it again.

### Option 3

vMotion the specific VM to a protected host and then clean the warning message.

**Note:** The vCenter must be connected to the Deep Security Manager all the time. Otherwise, the interface out of sync issue will happen often.

## Further Troubleshooting

1. Provide the results of the step from above where you verified the IP and MAC Addresses in "Check the virtual computer interface information in the Deep Security Virtual Appliance " on the previous page
2. Get the rattif.txt file from the step from above where you verified that the interface of the virtual computer was recognized by Deep Security Virtual Appliance.
3. Get the output from the following commands:
   ```
   $ ls -alR > /home/dsva/ls.txt
   $ netstat -an > /home/dsva/netstat.txt
   $ ps auxww > /home/dsva/ps.txt
   $ lsof > /home/dsva/lsof.txt
   $ ifconfig -a > /home/dsva/ifconfig.txt
   $ cp /var/log/syslog /home/dsva/syslog.txt
   ```
4. Get the diagnostic packages for the Deep Security Manager, Deep Security Agent, and the Deep Security Virtual Appliance.
5. Collect the following files and send them to Trend Micro Technical Support.

- rattif.txt
- ls.txt
- netstat.txt
- ps.txt
- lsof.txt
- ifconfig.txt
- syslog.txt

If you cannot find the MAC address of the virtual computer from the output of the `ratt if` command, then use the following workaround:

1. Deploy a virtual computer from a template in vCenter.
2. Delete the existing NIC.
3. Power on this virtual computer but there is no need to log on.
4. Power off this virtual computer.
5. Add a new NIC.
6. Power on the virtual computer.

## Error: Integrity Monitoring Engine Offline and other errors occur after activating a virtual machine

The following errors are displayed in Deep Security Manager when activating a virtual machine protected by Deep Security Virtual Appliance (DSVA). These errors appears even when the activation is successful:

- Anti-Malware Engine Offline
- Rebuild Baseline Failure (Agent or Appliance error)
- Integrity Monitoring Engine Offline

The issue remains unresolved even when the following troubleshooting tasks are performed:

- Confirm that vSphere Endpoint is already installed.
- Confirm that VMware tools are installed and up to date.
- Confirm that VMCI and VSEPFLT drivers are installed and running on the VM.

- Synchronize vCenter on the DSM console.
- Deactivate and reactivate the DSVA.
- Deactivate and reactivate the particular VM with issue.
- Reinstall VMware tools.

These errors appear because the virtual machine is not running VMversion 7 or above. To resolve the issue, you need to upgrade the VM to the latest hardware version.

## Error: Module installation failed (Linux)

The error message "Module Installation Failed" indicates that your operating system's kernel version is not supported by the Deep Security network driver, or file system hook. These circumstances can cause **engine offline** alerts. Lack of a compatible network driver is the most common cause of this message.

When you apply intrusion prevention, web reputation, or firewall, the Deep Security Agent installs a network driver so it can examine traffic. Anti-malware and integrity monitoring install a file system hook module. This is required to monitor file system changes in real time. (Scheduled scans do not require the same file system hook.)

An update may be in progress. Trend Micro monitors many vendors for new kernel releases. After completing quality assurance tests, we release an update with support for these kernels. To ask when support for your kernel version will be supported, contact technical support. (When logged in, you can click **Support** in the top right corner.)

Your system will install the module support update automatically when it becomes available.

To view supported operating system kernel versions, see "Deep Security Agent Linux kernel support" on page 76.

## Error: There are one or more application type conflicts on this computer

This error message appears in the DPI Events tab in Deep Security Manager when updating the Deep Security Agents:

*There are one or more application type conflicts on this computer. One or more DPI rules associated with one application type are dependent on one or more DPI rules associated with*

*another application type. The conflict exists because the two application types use different ports.*

The conflicting application types are:

```
[A] "Web Application Tomcat" Ports: [80,8080,4119]
```

```
[B] "Web Server Common" Ports: [80,631,8080,7001,7777,7778,7779,7200,7501,8007,
8004,4000,32000,5357,5358,9000]
```

```
[A] "Web Server Miscellaneous" Ports:
[80,4000,7100,7101,7510,8043,8080,8081,8088,8300,8500,
8800,9000,9060,19300,32000,3612,10001,8093,8094]
```

```
[B] "Web Server Common" Ports: [80,631,8080,7001,7777,7778,7779,7200,7501,8007,
8004,4000,32000,5357,5358,9000]"
```

## Resolution

To resolve the conflict, edit the port numbers used by application types B so that they include the port numbers used by application types A. The two application types (Web Application Tomcat and Web Server Miscellaneous) are both dependent on the application type Web Server Common. This is why the ports listed in the first two application types should also appear in the Web Server Common ports.

If you consolidate the port numbers for these three application types, the result is as follows:
`80,631,3612,4000,4119,5357,5358,7001,7100,7101,7200,7501,7510,7777,7778,7779,`
`8004,8007,8043,8080,8081,8088,8093,8094,8300,8500,8800,9000,9060,10001,19300,32000`

After adding this to the Web Server Common port list, you will see the following message in the Events tab: *The Application Type Port List Misconfiguration has been resolved.*

## Consolidate ports

1. Log on to Deep Security Manager and go to **Policies > Rules > Intrusion Prevention Rules**.
2. Search for **Web Server Common** in the search box in the and double-click the Web Server Common application type.
3. Go to **General > Details > Application type > Edit > Web server common**.
4. Go to **General > Connection > Port** and click **Edit** to replace all of the ports with this consolidated entry: `80,631,3612,4000,4119,5357,5358,7001,7100,7101,7200,`

```
7501,7510,7777,7778,7779,8004,8007,8043,8080,8081,8088,8093,
8094,8300,8500,8800,9000,9060,10001,19300,32000
```

5. Click **OK**.

### Disable the inherit option

It is also recommended that administrators disable the inherit option for DPI for a security profile. Any change you make to the application type will only affect this particular security profile.

1. Log on to Deep Security Manager and go to **Security Profiles**.
2. Double-click a security profile in the right pane.
3. Go to the **DPI** section and click to clear **Inherit** .
4. Click **OK**.

Check the IPS rule 1000128.

1. Right-click **Application Type Properties**.
2. Click to clear **Inherit**.
3. Verify that the current inherited port list contains the listening port number for the Deep Security Manager's GUI. If not, add this port to the Web Server Common port group.
4. Click **Inherit**.

## Error: Unable to connect to the cloud account

When adding an Amazon Cloud account, the error "Unable to connect to the cloud account" can occur. The cause can be:

- invalid key ID or secret
- incorrect permissions
- failed network connectivity

### Your AWS account access key ID or secret access key is invalid

**To resolve this:**

Verify the security credentials that you entered.

## The incorrect AWS IAM policy has been applied to the account being used by Deep Security

**To resolve this:**

Go you your AWS account and review the IAM policy for that account.

The AWS IAM policy must have these permissions:

- Effect: Allow
- AWS Service: Amazon EC2
- Select the following Actions:
  - DescribeImages
  - DescribeInstances
  - DescribeTags
- Amazon Resource Name (ARN) to: *

## NAT, proxy, or firewall ports are not open, or settings are incorrect

This can occur in a few cases, including if you are deploying a new Deep Security Manager installation using the AMI on AWS Marketplace.

Your Deep Security Manager must be able to connect to the Internet, specifically to Amazon Cloud, on the required port numbers.

To resolve this:

You may need to:

- configure NAT or port forwarding on a firewall or router between your AMI and the Internet
- get an external IP address for your AMI

The network connection must also be reliable. If it is intermittent, this error message may occur sometimes (but not every time).

## Error: Unable to resolve instance hostname

The error message "Unable to Resolve Instance Hostname" may occur as a result of activating the Agent from Deep Security Manager when you are not using agent-initiated activation.

We recommend that you always use **Agent-Initiated Activation**. Learn how to configure policy rules for agent-initiated communication and deploy agents using deployment scripts, see "Use agent-initiated communication with cloud accounts" on page 202.

## Error: Anti-malware engine offline

This error can occur for a variety of reasons. To resolve the issue, follow the instructions below for the mode of protection that is being used:

- "Agent-based protection" below
- "Agentless protection" on page 980

For an overview of the anti-malware module, see "Protect against malware" on page 486.

### Agent-based protection

1. In the Deep Security Manager, check for other errors on the same machine. If errors exist, there could be other issues that are causing your anti-malware engine to be offline, such as communications or agent installation failure.
2. Check communications from the agent to the relay and the Deep Security Manager.
3. In the Deep Security Manager, view the details for the agent with the issue. Verify that the policy or setting for anti-malware is turned on, and that the configuration for each scan (real-time, manual, scheduled) is in place and active. (See "Enable and configure anti-malware" on page 494.)
4. Deactivate and uninstall the agent before reinstalling and re-activating it. See "Uninstall Deep Security" on page 1081 and "Activate the agent" on page 219 for more information.
5. In the Deep Security Manager, go to the **Updates** section for that computer. Verify that the Security Updates are present and current. If not, click **Download Security Updates** to initiate an update.
6. Check if there are conflicts with another anti-virus product, such as OfficeScan. If conflicts exist, uninstall the other agent and Deep Security Agent, reboot, and reinstall the Deep

Security Agent. To remove OfficeScan, see Uninstalling clients or agents in OfficeScan (OSCE).

If your agent is Windows:

1. Make sure the following services are running:
   - Trend Micro Deep Security Agent
   - Trend Micro Solution Platform
2. Check that all the anti-malware related drivers are running properly by running the following commands:
   - `# sc query AMSP`
   - `# sc query tmcomm`
   - `# sc query tmactmon`
   - `# sc query tmevtmgr`

   If a driver is not running, restart the Trend Micro services. If it is still not running, continue with the following steps below.

3. Verify the installation method. Only install the MSI, not the zip file.
4. The agent might need to be manually removed and reinstalled. For more information, see Manually uninstalling Deep Security Agent, Relay, and Notifier from Windows
5. The installed Comodo certificate could be the cause of the issue. To resolve the issue, see "Anti-Malware Driver offline" status occurs due to Comodo certificate issue.
6. All instances and virtual machines deployed from a catalog or vApp template from vCloud Director are given the same BIOS UUID. Deep Security distinguishes different VMs by there BIOS UUID, so a duplicate value in the vCenter causes an Anti-Malware Engine Offline error. To resolve the issue, see VM BIOS UUIDs are not unique when virtual machines are deployed from vApp templates (2002506).

If your agent is Linux:

1. To check that the agent is running, enter the following command in the command line:
   - `service ds_agent status`
2. If you're using a Linux server, your kernel might not be supported. For more information, see "Error: Module installation failed (Linux)" on page 974.

If the problem is still unresolved after following these instructions, create a diagnostic package and contact support. For more information, see "Create a diagnostic package and logs" on page 1105.

## Agentless protection

1. In the Deep Security Manager, verify synchronization to vcenter and nsx. Under the **Computers** section, right click on your Vcenter and go to **Properties**. Click **Test Connection**. Then click on the NSX tab and test the connection. Click **Add/Update Certificate** in case the certificate has changed.
2. Log into the NSX manager and verify that it is synching to Vcenter properly.
3. Log into your Vsphere client and go to **Network & Security > Installation > Service Deployments**. Check for errors with Trend Micro Deep Security and Guest Introspection, and resolve any that are found.
4. In Vsphere client, go to **Network & Security > Service Composer**. Verify that the security policy is assigned to the appropriate security group.
5. Verify that your vmware tools are compatible with Deep Security. For more information, see VMware Tools 10.x Interoperability Issues with Deep Security.
6. Verify that the File Introspection Driver (vsepflt) is installed and running on the target VM. As an admin, run `sc query vsepflt` at the command prompt.
7. All instances and virtual machines deployed from a catalog or vApp template from vCloud Director are given the same BIOS UUID. Deep Security distinguishes different VMs by there BIOS UUID, so a duplicate value in the vCenter causes an Anti-Malware Engine Offline error. To resolve the issue, see VM BIOS UUIDs are not unique when virtual machines are deployed from vApp templates (2002506).
8. If the problem is still unresolved, open a case with support with the following information:
   - Diagnostic package from each Deep Security Manager. For more information, see "Create a diagnostic package and logs" on page 1105.
   - Diagnostic package from the Deep Security Virtual Appliance.
   - Vcenter support bundle for the effected hosts.

## Error: Check Status Failed

You can check the status of the agent / appliance on a computer from the Deep Security Manager console. On the Computers page, right-click the computer and click **Actions > Check Status**.

If you get a "Check Status Failed" error, open the error message to see a more detailed description.

If description indicates a protocol error, it's usually caused by a communication issue. There are a few possible causes:

- Check whether the computer (or the policy assigned to the computer) is configured for agent-initiated communication or bidirectional communication. Unless you are using Deep Security as a Service, the "Check Status" operation will fail if you are using agent-initiated communication.
- Check that the Deep Security Manager can communicate with the agent. The manager should be able to reach the agent. See "Port numbers" on page 96.
- Check the resources on the agent computer. Lack of memory, CPU, or disk space can cause this error.

If the description indicates a SQLITE_IOERR_WRITE[778]: disk I/O error, there is likely a problem with the agent computer. The most common problem is that the disk is full or write-protected.

## Error: Log Inspection Rules Require Log Files

If a log inspection rule requires you to add the location of the files to be monitored, of if you add an unnecessary log inspection rule and the files do not exist on your machine, the following error will occur in the **Computer**[1] or **Policy editor**[2]:

To resolve the error:

---

[1]To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2]To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

1. Click on the **Log Inspection Rules Require Log Files** error. A window will open with more information about the error. Under **Description**, the name of the rule causing the error will be listed.
2. In the Deep Security Manager, go to **Policies > Common Objects > Rules > Log Inspection Rules** and locate the rule that is causing the error.
3. Double-click the rule. The rule's properties window will appear.
4. Go to the **Configuration** tab.

If the file's location is required:

1. Enter the location under **Log Files to monitor** and click **Add**.
2. Click **OK**. Once the agent receives the policy, the error will clear.

If the files listed do not exist on the protected machine:

1. Go to the **Computer**[1] **or Policy editor**[2] **> Log Inspection**.
2. Click **Assign/Unassign**.
3. Locate the unnecessary rule and uncheck the checkbox.
4. Click **OK**. Once the agent receives the policy, the error will clear.

To prevent this error, run a recommendation scan for suggested rules:

1. On the Deep Security Manager, go to **Computers**.
2. Right-click the computer you'd like to scan and click **Actions > Scan for Recommendations**.
3. View the results on the **General** tab of the protection module in the **Computer**[3] or **Policy editor**[4].

---

[1]To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2]To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

[3]To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[4]To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

## Alert: Integrity Monitoring information collection has been delayed

This alert indicates that the rate at which integrity monitoring information is collected has been temporarily delayed. The delay is due to an increase in the volume of integrity monitoring data that is being transmitted from agents to Deep Security Manager. During this time the baseline and integrity monitoring event views may not be current for some computers.

This alert is automatically dismissed when the collection of integrity monitoring data is no longer delayed.

For more information about integrity monitoring, see "Set up integrity monitoring" on page 632.

## Alert: The memory warning threshold of Manager Node has been exceeded

The **Memory Warning Threshold Exceeded** or **Memory Critical Threshold Exceeded** alerts appear in Deep Security when the maximum memory that has been allotted for Deep Security Manager has been exceeded.

The following Deep Security Manager message is also logged:

```
The DSM has reached the maximum memory that's been allocated for the application.
(default = 4GB) <InformationItem> <Name>usedMemory</Name> <Value>3.98 GB
(4,269,473,792 bytes)</Value> </InformationItem> <InformationItem>
<Name>maxMemory</Name> <Value>3.98 GB (4,269,473,792 bytes)</Value>
```

To resolve the issue, increase the RAM available to the Deep Security Manager to a minimum of 8 GB.

### Increase the allocated memory on a Windows server

1. Go to the Deep Security Manager folder and create a new file called `Deep Security Manager.vmoptions`.
   This is the same folder where Deep Security Manager.exe is located. For example: `C:\Program Files\Trend Micro\Deep Security Manager`
2. Add the following line to the file: `-Xmx8g`
3. Save the file and "Restart the Deep Security Manager" on page 734.

### Increase the allocated memory on a Linux server

1. Go to `/opt/dsm`and create a new file called `dsm_s.vmoptions`.
2. Add the following line to the file: `-Xmx8g`
3. Save the file and "Restart the Deep Security Manager" on page 734.

### Verify the memory allocation change

You can confirm that the memory allocation change has taken effect by going to **Administration > System Information** Deep Security Manager and viewing the memory information under **System Details > Manager Node**.

## Alert: Manager Time Out of Sync

The system time on the Deep Security Manager operating system must be synchronized with the time on the database computer. This alert appears in the Alert Status widget of the manager console when the computer times are more than 30 seconds out of sync.

To synchronize the times, apply the following configurations:

- Configure the database and all manager nodes to use the same time zone.
- Ensure that the database and all manager nodes are synchronizing time to the same time source.
- If the manager runs on a Linux operating system, ensure the ntpd daemon is running.

## Event: Max TCP connections

Deep Security is configured to allow a maximum number of TCP connections to protected computers. When the number of connections exceeds the maximum, network traffic is dropped and Max TCP Connections firewall events occur. To prevent dropped connections, increase the maximum allowed TCP connections on the computer where the Max TCP Connection event occurs.

> **Note:** The intrusion protection module enables the network engine which enforces the allowed number of TCP connections.

1. In Deep Security Manager, click **Policies**.
2. Determine which policy to configure to affect the computer in question. See "Policies, inheritance, and overrides" on page 354.
3. To open the policy that you want to configure, double-click the policy.
4. In the left-hand pane, click **Settings** and then click the **Advanced** tab.
5. In the **Advanced Network Engine Settings** area, if Inherit is selected clear the checkbox to enable changes.
6. Increase the value of the **Maximum TCP Connections** property to 10000 or more, according to your needs.
7. Click **Save**.

## Warning: Census, Good File Reputation, and Predictive Machine Learning Service Disconnected

The Census, Good File Reputation, and Predictive Machine Learning Services are security services hosted by Trend Micro in its Smart Protection Network. They are necessary for the full and successful operation of the Deep Security behavior monitoring, predictive machine learning, and process memory scan features.

The following table maps the services to features.

| Service name | Required for these features |
|---|---|
| Global Census Service | behavior monitoring, predictive machine learning |
| Good File Reputation Service | behavior monitoring, predictive machine learning, process memory scans |
| Predictive Machine Learning Service | predictive machine learning |

If you see the alert...

*Census, Good File Reputation, and Predictive Machine Learning Service Disconnected*

...there are a few causes:

- "Cause 1: The agent or relay-enabled agent doesn't have Internet access" on the next page

- "Cause 2: A proxy was enabled but not configured properly" on the next page

### Cause 1: The agent or relay-enabled agent doesn't have Internet access

If your agent or relay-enabled agent doesn't have access to the Internet, then it can't reach these services.

Solutions:

- Check your firewall policies and ensure that the outbound HTTP and HTTPS ports (by default, 80 or 443) are open.
- If you are unable to open those ports, see "Configure agents that have no Internet access" on page 207 for other solutions.

### Cause 2: A proxy was enabled but not configured properly

The Census, Good File Reputation and Predictive Machine Learning Services can be accessed using a proxy.

To check whether a proxy was enabled and make sure it was configured properly:

1. Open the **Computer or Policy editor**[1].
2. On the left, click Settings.
3. In the main pane, click the General tab.
4. Find the heading titled, **Network Setting for Census, Good File Reputation Service, and Predictive Machine Learning**.
5. If a proxy was specified, click **Edit** and make sure its **Proxy Protocol**, **Address**, **Port** and optional **User Name** and **Password** are accurate.

## Warning: Reconnaissance Detected

The reconnaissance scan detection feature serves as an early warning of a potential attack or intelligence gathering effort against a network.

---

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

## Types of reconnaissance scans

Deep Security can detect several types of reconnaissance scans:

- **Computer OS Fingerprint Probe:** The agent or appliance detects an attempt to discover the computer's OS.
- **Network or Port Scan:** The agent or appliance reports a network or port scan if it detects that a remote IP is visiting an abnormal ratio of IPs to ports. Normally, an agent or appliance computer will only see traffic destined for itself, so a port scan is the most common type of probe that will be detected. The statistical analysis method used in computer or port scan detection is derived from the "TAPS" algorithm proposed in the paper "Connectionless Port Scan Detection on the Backbone" presented at IPCCC in 2006.
- **TCP Null Scan:** The agent or appliance detects packages with no flags set.
- **TCP SYNFIN Scan:** The agent or appliance detects packets with only the SYN and FIN flags set.
- **TCP Xmas Scan:** The agent or appliance detects packets with only the FIN, URG, and PSH flags set or a value of 0xFF (every possible flag set).

## Suggested actions

When you receive a Reconnaissance Detected alert, double-click it to display more detailed information, including the IP address that is performing the scan. Then, you can try one of these suggested actions:

- The alert may be caused by a scan that is not malicious. If the IP address listed in the alert is known to you and the traffic is okay, you can add the IP address to the reconnaissance allow list:

a. In the **Computer or Policy editor**[1], go to **Firewall > Reconnaissance**.
b. The **Do not perform detection on traffic coming from** list should contain a list name. If a list name hasn't already been specified, select one.
c. You can edit the list by going to **Policies > Common Objects > Lists > IP Lists**. Double-click the list you want to edit and add the IP address.

- You can instruct the agents and appliances to block traffic from the source IP for a period of time. To set the number of minutes, open the **Computer or Policy editor**[2], go to **Firewall > Reconnaissance** and change the **Block Traffic** value for the appropriate scan type.
- You can use a firewall or Security Group to block the incoming IP address.

**Note:** Deep Security Manager does not automatically clear the "Reconnaissance Detected" alerts, but you can manually clear the issue from Deep Security Manager.

For more information on reconnaissance scans, see "Firewall settings" on page 612.

## Warning: Insufficient disk space

An "Insufficient Disk Space" warning indicates that the computer where the Deep Security Agent or Appliance is running is low on disk space and may not be able to store more events. If you open the warning to display its details, it will show you the location of the agent or appliance, how much free space is left, and how much is required by the agent or appliance.

To fix this issue, check the drive or file system that's affected and clear anything you can.

**Note:** The agent or appliance will continue to protect your instance even if the drive is out of space; however, it will stop recording events.

---

[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

### Tips

- Even though the warning is generated by the Deep Security Agent or Appliance, another program that shares the same file system could be causing the space issue.
- Deep Security Agent automatically truncates and rotates its log files.
- Deep Security Agent will clean up its own log files, but not those of other applications.
- Deep Security Manager does not automatically clear the "Insufficient Disk Space" warnings, but you can manually clear them from Deep Security Manager.

# Create and manage users

Deep Security has users, roles, and contacts that can be created and managed under **Administration > User Management**.

- **Users** are Deep Security account holders who can sign in to the Deep Security Manager with a unique user name and password. You can "Synchronize with an Active Directory" below or "Add or edit an individual user" on page 991
- **Roles** are a collection of permissions to view data and perform operations within Deep Security Manager. Each user is assigned a role. See "Define roles for users" on page 995.
- **Contacts** do not have a user account and cannot sign in to Deep Security Manager but they can be designated as the recipients of email notifications and scheduled reports. See "Add users who can only receive reports" on page 1010.

## Synchronize with an Active Directory

If you use Active Directory to manage users, you can synchronize Deep Security with the Active Directory to populate the user list. Users can then sign into Deep Security Manager using the password stored in the directory.

**Note:** To successfully import an Active Directory user account into Deep Security as a Deep Security user or contact, the Active Directory user account must have a **userPrincipalName** attribute value. The **userPrincipalName** attribute corresponds to an Active Directory account holder's "User logon name".

**Note:** If you are using Deep Security in FIPS mode, you must import the Active Directory's SSL certificate before synchronizing with the Directory. See "Manage trusted certificates" on page 216.

1. In Deep Security Manager go to **Administration > User Management > Users**.
2. Click **Synchronize with Directory** to display the **Synchronize with Directory** wizard.
3. Type the address of the directory server and your access credentials and click **Next**. The wizard attempts to connect to the Active Directory.

   **Note:** If you are using Deep Security in FIPS mode, click **Test Connection** in the Trusted Certificate section to check whether the Active Directory's SSL certificate has been imported successfully into Deep Security Manager.

4. You will then be prompted to select which Active Directory group of users to import and whether they will be users or contacts. Once they have been imported, you are given the option to create a scheduled task to periodically synchronize with the directory to keep your list up to date.

The imported list of users are locked out of the Deep Security Manager by default. You will have to modify their properties to allow them to sign in to the Deep Security Manager.

**Note:** If you delete a user from Deep Security Manager who was added as a result of synchronizing with an Active Directory and then resynchronize with the directory, the user will reappear in your user list if they are still in the Active Directory.

## Filtering the Active Directory

The **Synchronize with Directory** wizard has an area called Search Options where you can write filters to specify a subset of users to import into the Deep Security Manager. The filter language follows the Internet Engineering Task Force "Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters RFC 4515".

The default filter (objectClass=group) imports all users.

The RFC 4515 filter syntax can be used to filter for specific users or groups in a directory. For example, the following filter would import only users who are members of an Active Directory group called "DeepSecurityUsers": "(&(objectClass=group)(cn=DeepSecurityUsers))".

The RFC 4515 definition is available at https://datatracker.ietf.org/doc/rfc4515/.

**Note:** The new users, although being in the "locked out" state, are given the Full Access user role.

## Add or edit an individual user

1. In Deep Security Manager go to **Administration > User Management > Users**.
2. Click **New** to add a new user or double-click an existing user account to edit its settings.
3. Specify the general properties for the user, including:
   - **Username:** The username that the user will enter on the Deep Security Manager login screen.
   - **Password** and **Confirm Password:** Note the password requirements listed in the dialog box. You can password requirements in the user security settings (see "Enforce user password rules" on page 773
   - **Name:** (Optional) The name of the account holder.
   - **Description:** (Optional) A description of the account.
   - **Role:** Use the list to assign a predefined role to this user. You can also assign a role to a user from the Users list, by right-clicking a user and then clicking **Assign roles**.

     **Note:** The Deep Security Manager comes preconfigured with two roles: Full Access and Auditor. The Full Access role grants users all possible privileges for managing the Deep Security system, such as creating, editing, and deleting computers, computer groups, policies, rules, and so on. The auditor role gives users the ability to view all of the information in the Deep Security system but not the ability to make any modifications except to their personal settings (password, contact information, view preferences, and so on). Roles with various levels of system access rights can be created and modified on the Roles page or by selecting **New** in the **Role** list.

   - **Language:** The language that will be used in the interface when this user logs in.
   - **Time zone:** Time zone where the user is located. This time zone is used when displaying dates and times in the Deep Security Manager.

- **Time format:** Time format used to display time in the Deep Security Manager. You can use 12-hour or 24-hour format.
- **Password never expires:** When this option is selected, the user's password will never expire. Otherwise, it will expire as specified in the user security settings (see "Enforce user password rules" on page 773

4. If you want to enable multi-factor authentication (MFA), click **Enable MFA**. If MFA is already enabled for this user, you can select **Disable MFA** to disable it. For details, see "Set up multi-factor authentication" on page 775.
5. Click the **Contact information** tab and enter any contact information that you have for the user and also indicate if they are your primary contact or not. You can also check the **Receive Alert Emails** check box to include this user in the list of users who receive email notifications when alerts are triggered.
6. You can also edit the settings on the **Settings** tab. However, increasing some of these values will affect Deep Security Manager performance. If you make changes and aren't happy with the results, you can click **Reset to Default Settings** (at the bottom of the tab) to reset all settings on this page to their default values:

   Module

   - **Hide Unlicensed Modules:** This setting determines whether unlicensed modules will be hidden rather than simply grayed out for this User. This option can be set globally on the **Administration > System Settings > Advanced** tab.

   Refresh Rate

   - **Status Bar:** This setting determines how often the status bar of the Deep Security Manager refreshes during various operations such as discovering or scanning computers.
   - **Alerts List/Summary:** How often to refresh the data on the Alerts page in List view or Summary view.
   - **Computers List:** How often to refresh the data on the Computers page.

     Note: The **Last Successful Update** column value will not be recalculated unless the page is manually reloaded.

- **Computer Details:** The frequency with which an individual computer's property page refreshes itself with the latest information (if required).

### List Views

- **Remember last Tag filter on each page:** Events pages let you filter displayed events by Tag(s). This List Views setting determines if the "Tag" filter setting is retained when you navigate away from and return to an Events page.
- **Remember last Time filter on each page:** Events pages let you filter displayed events by Time period and computer(s). These List Views settings determine if the "Period" and "Computer" filter settings are retained when you navigate away from and return to an Events page.
- **Remember last Computer filter on each page:** Events pages let you filter displayed events by Time period and computer(s). These List Views settings determine if the "Period" and "Computer" filter settings are retained when you navigate away from and return to an Events page.
- **Remember last Advanced Search on each page:** If you have performed an "Advanced Search" on an Events page, this setting will determine if the search results are kept if you navigate away from and return to the page.
- **Number of items to show on a single page:** Screens that display lists of items will display a certain number of items per "Page". To view the next page, you must use the pagination controls. Use this setting to change the number of list-items displayed per page.
- **Maximum number of items to retrieve from database:** This setting limits the number of items that can retrieved from the database for display. This prevents the possibility of the Deep Security Manager getting bogged down trying to display an excessive number of results from a database query. If a query produces more than this many results, a message will appear at the top of the display informing you that only a portion of the results are being displayed.

**Note:** Increasing these values will affect Deep Security Manager performance.

### Reports

- **Enable PDF Encryption:** When this option is selected, reports exported in PDF format will be password protected with the **Report Password**.

## Change a user's password

To change a user's password, click **Administration > User Management > Users**, right-click the user, and click **Set Password**. You will be prompted for the old password as well as the new password.

## Lock out a user or reset a lockout

If a user enters the wrong password too many times when trying to sign in, they will be locked out automatically. If you have resolved the situation and want to allow the user the log in, see "Unlock a locked out user name" on page 1012.

## View system events associated with a user

To see any system events associated with a user, click **Administration > User Management > Users**, right-click the user, and click **View System Events**.

## Delete a user

To remove a user account from Deep Security Manager, click **Administration > User Management > Users**, click the user, and then click **Delete**.

> **Note:** If you delete a user from Deep Security Manager who was added as a result of synchronizing with an Active Directory and then resynchronize with the directory, the user will reappear in your user list if they are still in the Active Directory.

## Define roles for users

Deep Security uses role-based access control (RBAC) to restrict user permissions to parts of Deep Security. Access rights and editing privileges are attached to roles and not to users. Once you have installed Deep Security Manager, you should create individual accounts for each user

and assign each user a role that will restrict their activities to all but those necessary for the completion of their duties. To change the access rights and editing privileges of an individual user, you must assign a different role to the user or edit the role.

The access that roles have to computers and policies can be restricted to subsets of computers and policies. For example, users can be permitted to view all existing computers, but only permitted to modify those in a particular group.

Deep Security comes preconfigured with two roles:

- **Full Access:** The full access role grants the user all possible privileges in terms of managing the Deep Security system including creating, editing, and deleting computers, computer groups, policies, rules, malware scan configurations, and others.
- **Auditor:** The auditor role gives the user the ability to view all the information in the Deep Security system but without the ability to make any modifications except to their own personal settings, such as password, contact information, dashboard layout preferences, and others.

**Note:** Depending on the level of access granted, controls in Deep Security Manager will be either visible and changeable, visible but disabled, or hidden. For a list of the rights granted in the preconfigured roles, as well as the default rights settings when creating a new role, see "Default settings for full access, auditor, and new roles" on page 1002.

You can create new roles that can restrict users from editing or even seeing Deep Security objects such as specific computers, the properties of security rules, or the system settings.

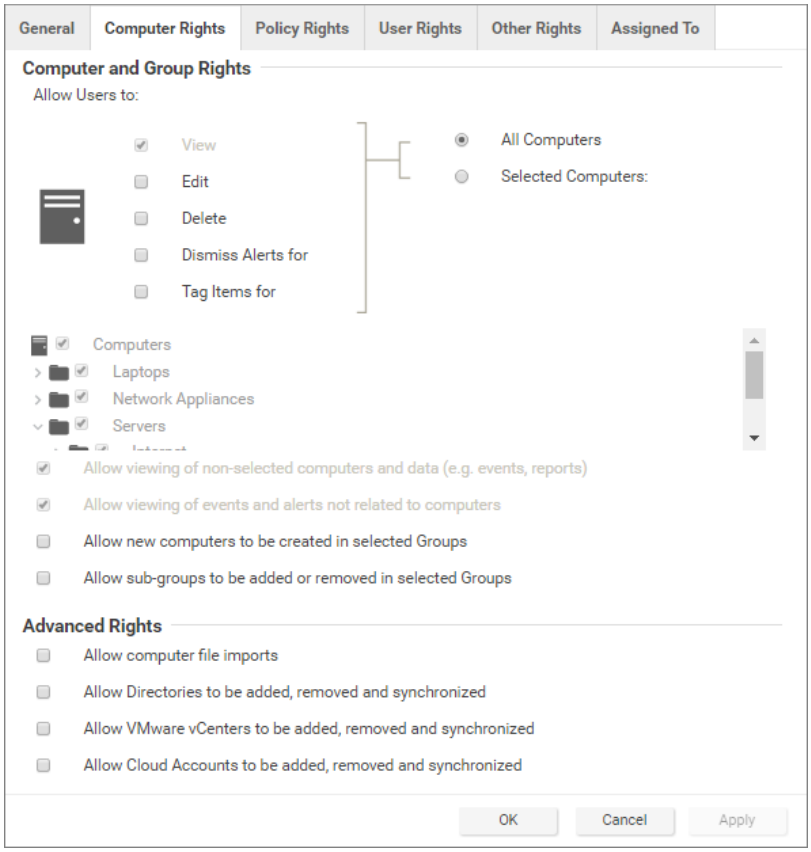
Before creating user accounts, identify the roles that your users will take and itemize what Deep Security objects those roles will require access to and what the nature of that access will be (viewing, editing, creating, and so on). Once you have created your roles, you can then begin creating user accounts and assigning them specific roles.

**Note:** Do not create a new role by duplicating and then modifying the full access role. To ensure that a new role only grants the rights you intend, create the new role by clicking **New** in the toolbar. The rights for a new role are set at the most restrictive settings by default. You can then proceed to grant only the rights that are required. If you duplicate the full access role and then apply restrictions, you risk granting some rights that you did not intend.

Clicking **New** ( ) or **Properties** ( ) displays the **Role properties window** with six tabs (**General, Computer Rights, Policy Rights, User Rights, Other Rights,** and **Assigned To**).

## Add or edit a role

1. In Deep Security Manager go to **Administration > User Management > Roles**.
2. Click **New** to add a new role or double-click an existing role to edits its settings.
3. Specify the general properties for the role, including:
   - **Name:** The name of the role, which will appear on the Roles page and in the list of available roles when adding a user.
   - **Description:** (Optional) A description of the role.
   - **Access Type:** Select whether users with this role will have access to Deep Security Manager, the Deep Security Manager Web service API, or both.
   - **Note:** To enable the Web service API, go to **Administration > System Settings > Advanced > SOAP Web Service API**.
4. Use the **Computer Rights** pane to confer viewing, editing, deleting, alert-dismissal, and event tagging rights to users in a role. These rights can apply to all computers and computer groups or they can be restricted to only certain computers. If you wish to restrict access, select the **Selected Computers** radio button and put a check next to the computer groups and computers that users in this role will have access to.
5. **Note:** These rights restrictions will affect not only the user's access to computers in Deep Security Manager, but also what information is visible, including events and alerts. As well, email notifications will only be sent if they relate to data that the user has access rights to.




Four basic options are available:

- **Allow viewing of non-selected computers and data:** If users in this role have restricted edit, delete, or dismiss-alerts rights, you can still allow them to view but not change information about other computers by checking this box.
- **Allow viewing of events and alerts not related to computers:** Set this option to allow users in this role to view non-computer-related information (for example, system events, like users being locked out, new firewall rules being created, IP Lists being deleted, and so on)

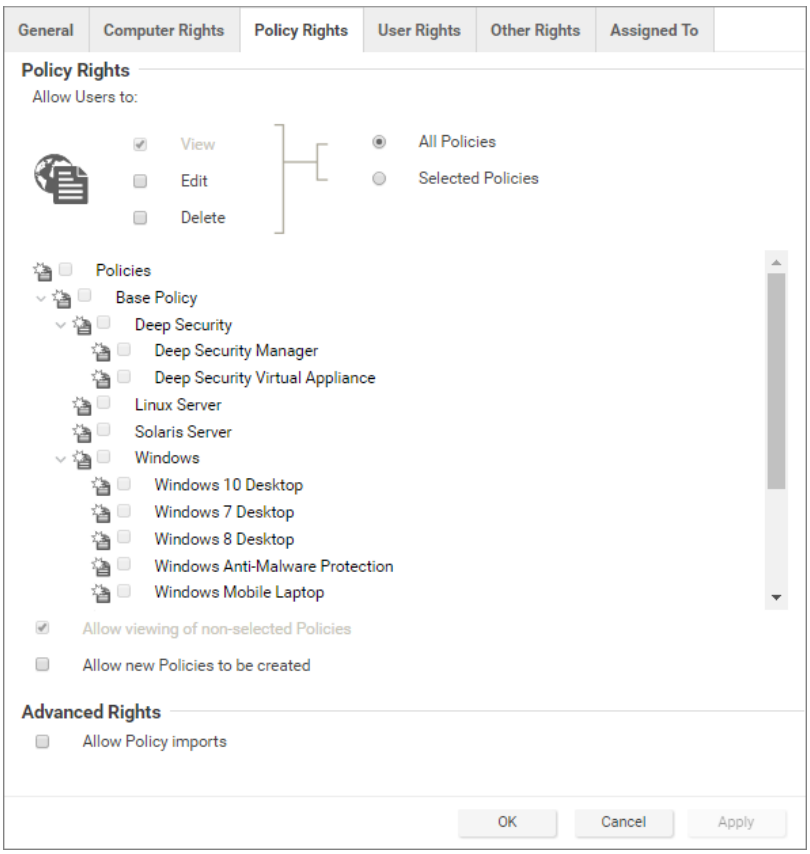
  **Note:** The previous two settings affect the data that users have access to. Although the ability of a user to make changes to computers have been restricted, these two settings control whether they can see information relating to computers they don't otherwise have access to. This includes receiving email notifications related to those computers.

- **Allow new computers to be created in selected Groups:** Set this option to allow users in this role to create new computers in the computer groups they have access to.
- **Allow sub-groups to be added/removed in selected Groups:** Set this option to allow users in this role to create and delete subgroups within the computer groups they have access to.

You can also enabled these in the Advanced Rights section:

- **Allow computer file imports:** Allow Users in this Role to import computers using files created using the Deep Security Manager's **Computer Export** option.
- **Allow Directories to be added, removed and synchronized:** Allow Users in this Role to add, remove, and synchronize computers that are being managed using an LDAP-based directory like MS Active Directory.
- **Allow VMware vCenters to be added, removed and synchronized:** Allow Users in this Role to add, remove and synchronize VMware vCenters. (Not available with Deep Security as a Service)
- **Allow Cloud Providers to be added, removed, and sychronized:** Allow Users in this Role to add, remove, and synchronize Cloud Providers. (Not available with Deep Security as a Service)

6. Use the **Policy Rights** tab to confer viewing, editing, and deleting rights to users in a role. These rights can apply to all policies or they can be restricted to only certain policies. If you wish to restrict access, click **Selected Policies** and put a check mark next to the policies that users in this role will have access to.




When you allow rights to a policy that has "child" policies, users automatically get rights to the child policies as well.

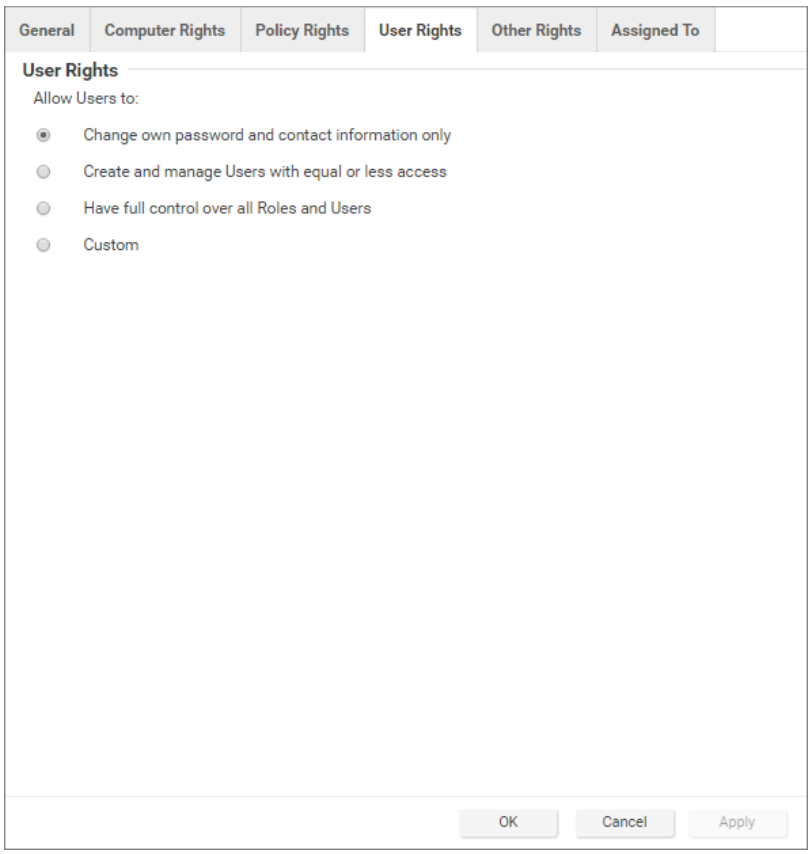
Two basic options are available:

- **Allow viewing of non-selected Policies:** If users in this role have restricted edit or delete rights, you can still allow them to view but not change information about other policies by checking this box.
- **Allow new Policies to be created:** Set this option to allow users in this role to create new policies.

You can also enabled this in the Advanced Rights section:

- **Allow Policy imports:** Allow users in this role to import policies using files created with the Deep Security Manager **Export** option on the **Policies** tab.

7. The options on the **User Rights** tab allow you to define permissions for administrator accounts.




- **Change own password and contact information only:** Users in this role can change their own password and contact information only.
- **Create and manage Users with equal or less access:** Users in this role can create and manage any users who do not have any privileges greater than theirs. If there is even a single privilege that exceeds those of the users with this role, the users with this role will not be able to create or manage them.
- **Have full control over all Roles and Users:** Gives users in this role the ability to create and edit and users or roles without restrictions. Be careful when using this option. If you assign it to a role, you may give a user with otherwise restricted privileges the ability to create and then sign in as a user with full unrestricted access to all aspects of the Deep Security Manager.
- **Custom:** You can further restrict the ability of a user to view, create, edit, or delete users and roles by selecting **Custom** and using the options in the **Custom Rights** section. Some options may be restricted for certain users if the **Can only manipulate**

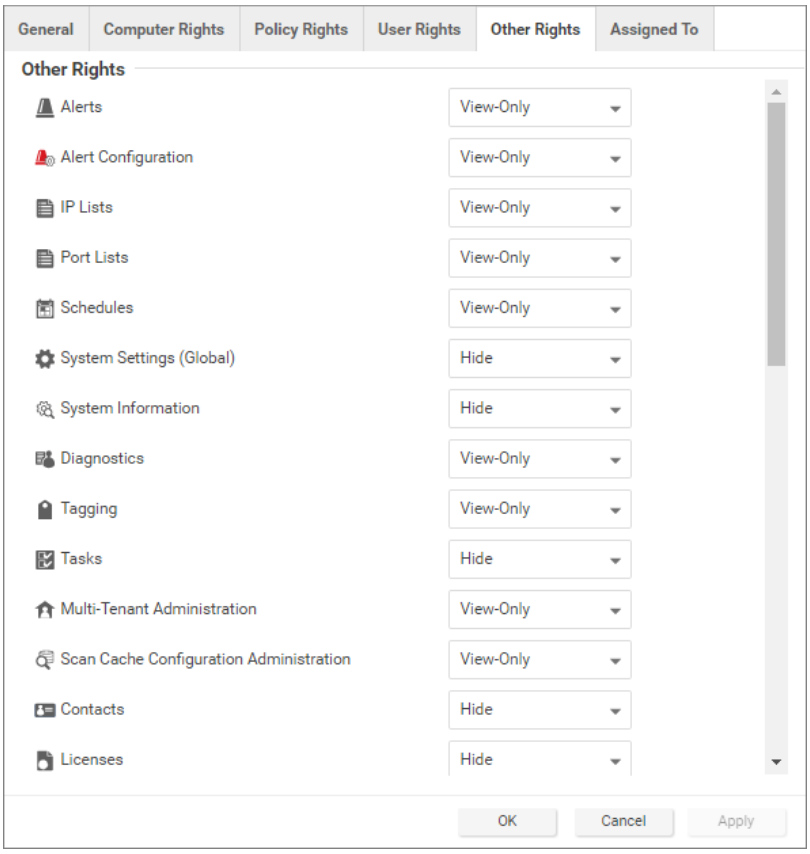
**Users with equal or lesser rights** option is selected.

The **Can only manipulate Users with equal or lesser rights** option limits the authority of users in this role. They will only be able to effect changes to users that have equal or lesser rights than themselves. Users in this Role will not be able to create, edit, or delete roles. Selecting this option also places restrictions on some of the options in the **Custom Rights** section:

- **Can Create New Users:** Can only create users with equal or lesser rights.
- **Can Edit User Properties:** Can only edit a user (or set or reset password) with equal or lesser rights.
- **Can Delete Users:** Can only delete users with equal or lesser rights.

8. The **Other Rights** tab enables you to restrict roles' permissions so that they can only access specific Deep Security features, and sometimes specific actions with those features. This can be useful if, for example, you have a team of administrators, and you want to make sure that they don't accidentally impact each others' work. By default, roles are View Only or Hide for each feature. To allow to full control or customized access, select

**Custom** from the list.




9. The **Assigned To** tab displays a list of the users who have been assigned this role.

## Default settings for full access, auditor, and new roles

The following table identifies the default rights settings for the full access role and the auditor role. Also listed are the rights settings that are in place when creating a new role by clicking New in the toolbar on the Roles page.

| RIGHTS | SETTINGS BY ROLE | | |
|---|---|---|---|
| **General** | **Full Access Role** | **Auditor Role** | **New Role Defaults** |
| **Access to DSM User Interface** | Allowed | Allowed | Allowed |
| **Access to Web Service API** | Allowed | Allowed | Not allowed |

| RIGHTS | SETTINGS BY ROLE | | |
|---|---|---|---|
| **Computer Rights** | Full Access Role | Auditor Role | New Role Defaults |
| **View** | Allowed, All Computers | Allowed, All Computers | Allowed, All Computers |
| **Edit** | Allowed, All Computers | Not allowed, All Computers | Not allowed, All Computers |
| **Delete** | Allowed, All Computers | Not allowed, All Computers | Not allowed, All Computers |
| **Dismiss Alerts for** | Allowed, All Computers | Not allowed, All Computers | Not allowed, All Computers |
| **Tag Items for** | Allowed, All Computers | Not allowed, All Computers | Not allowed, All Computers |
| **Allow viewing of non-selected computers and data (e.g. events, reports)** | Allowed | Allowed | Allowed, All Computers |
| **Allow viewing of events and alerts not related to computers** | Allowed | Allowed | Allowed, All Computers |
| **Allow new computers to be created in selected Groups** | Allowed | Not allowed | Not allowed |
| **Allow sub-groups to be added or removed in selected Groups** | Allowed | Not allowed | Not allowed |

| RIGHTS | SETTINGS BY ROLE | | |
|---|---|---|---|
| **Allow computer file imports** | Allowed | Not allowed | Not allowed |
| **Allow Cloud Accounts to be added, removed and synchronized** | Allowed | Not allowed | Not allowed |
| **Policy Rights** | Full Access Role | Auditor Role | New Role Defaults |
| **View** | Allowed, All Policies | Allowed, All Policies | Allowed, All Policies |
| **Edit** | Allowed, All Policies | Not allowed, All Policies | Not allowed, All Policies |
| **Delete** | Allowed, All Policies | Not allowed, All Policies | Not allowed, All Policies |
| **View non-selected Policies** | Allowed | Allowed | Allowed |
| **Create new Policies** | Allowed | Not allowed | Not allowed |
| **Import Policies** | Allowed | Not allowed | Not allowed |
| **User Rights (See note on User rights below)** | Full Access Role | Auditor Role | New Role Defaults |
| **View Users** | Allowed | Allowed | Not allowed |
| **Create Users** | Allowed | Not allowed | Not allowed |
| **Edit User Properties** | Allowed | Not | Not |

| RIGHTS | SETTINGS BY ROLE | | |
|---|---|---|---|
| | | allowed | allowed |
| **Delete Users** | Allowed | Not allowed | Not allowed |
| **View Roles** | Allowed | Allowed | Not allowed |
| **Create Roles** | Allowed | Not allowed | Not allowed |
| **Edit Role Properties** | Allowed | Not allowed | Not allowed |
| **Delete Roles** | Allowed | Not allowed | Not allowed |
| **Delegate Authority** | Allowed | Not allowed | Not allowed |
| **Other Rights** | Full Access Role | Auditor Role | New Role Defaults |
| **Alerts** | Full (Can Dismiss Global Alerts) | View-Only | View-Only |
| **Alert Configuration** | Full (Can Edit Alert Configurations) | View-Only | View-Only |
| **IP Lists** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **Port Lists** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **Schedules** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **System Settings (Global)** | Full (Can View, Edit System Settings (Global)) | View-Only | Hide |
| **Diagnostics** | Full (Can Create Diagnostic Packages) | View-Only | View-Only |
| **Tagging** | Full (Can Tag (Items not belonging to Computers), Can Delete Tags, Can Update Non-Owned Auto-Tag Rules, Can Run Non-Owned Auto-Tag Rules, Can Delete Non- | View-Only | View-Only |

| RIGHTS | SETTINGS BY ROLE | | |
|---|---|---|---|
| | Owned Auto-Tag Rules) | | |
| **Tasks** | Full (Can View, Add, Edit, Delete Tasks, Execute Tasks) | View-Only | Hide |
| **Multi-Tenant Administration** | Full | Hide | View-Only |
| **Scan Cache Configuration Administration** | Full | View-Only | View-Only |
| **Contacts** | Full (Can View, Create, Edit, Delete Contacts) | View-Only | Hide |
| **Licenses** | Full (Can View, Change License) | View-Only | Hide |
| **Updates** | Full (Can Add, Edit, Delete Software; Can View Update For Components; Can Download, Import, Apply Update Components; Can Delete Deep Security Rule Updates) | View-Only | Hide |
| **Asset Values** | Full (Can Create, Edit, Delete Asset Values) | View-Only | View-Only |
| **Certificates** | Full (Can Create, Delete SSL Certificates) | View-Only | View-Only |
| **Relay Groups** | Full | View-Only | View-Only |
| **Proxy** | Full | View-Only | View-Only |
| **SAML Identity Providers** | Full | Hide | Hide |
| **Malware Scan Configuration** | Full (Can Create, Edit, Delete Malware Scan Configuration) | View-Only | View-Only |
| **Quarantined File** | Full (Can Delete, Download Quarantined File) | View-Only | View-Only |
| **Web Reputation Configuration** | Full | View-Only | View-Only |
| **Directory Lists** | Full (Can Create, Edit, Delete) | View-Only | View-Only |

| RIGHTS | SETTINGS BY ROLE | | |
|---|---|---|---|
| **File Lists** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **File Extension Lists** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **Firewall Rules** | Full (Can Create, Edit, Delete Firewall Rules) | View-Only | View-Only |
| **Firewall Stateful Configurations** | Full (Can Create, Edit, Delete Firewall Stateful Configurations) | View-Only | View-Only |
| **Intrusion Prevention Rules** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **Application Types** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **MAC Lists** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **Contexts** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **Integrity Monitoring Rules** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **Log Inspection Rules** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **Log Inspection Decoders** | Full (Can Create, Edit, Delete) | View-Only | View-Only |

The custom settings corresponding to the **Change own password and contact information only** option are listed in the following table:

| **Custom settings corresponding to "Change own password and contact information only" option** | |
|---|---|
| Users | |
| **Can View Users** | Not allowed |
| **Can Create New Users** | Not allowed |
| **Can Edit User Properties (User can always edit select properties of own account)** | Not allowed |

| Custom settings corresponding to "Change own password and contact information only" option | |
|---|---|
| **Can Delete Users** | Not allowed |
| Roles | |
| **Can View Roles** | Not allowed |
| **Can Create New Roles** | Not allowed |
| **Can Edit Role Properties (Warning: conferring this right will let Users with this Role edit their own rights)** | Not allowed |
| **Can Delete Roles** | Not allowed |
| Delegate Authority | |
| **Can only manipulate Users with equal or lesser rights** | Not allowed |

The custom settings corresponding to the **Create and manage Users with equal or less access** option are listed in the following table:

| Custom settings corresponding to "Create and manage Users with equal or less access" option | |
|---|---|
| Users | |
| **Can View Users** | Allowed |
| **Can Create New Users** | Allowed |
| **Can Edit User Properties (User can always edit select properties of own account)** | Allowed |
| **Can Delete Users** | Allowed |
| Roles | |
| **Can View Roles** | Not allowed |

| Custom settings corresponding to "Create and manage Users with equal or less access" option | |
|---|---|
| **Can Create New Roles** | Not allowed |
| **Can Edit Role Properties (Warning: conferring this right will let Users with this Role edit their own rights)** | Not allowed |
| **Can Delete Roles** | Not allowed |
| Delegate Authority | |
| **Can only manipulate Users with equal or lesser rights** | Allowed |

The custom settings corresponding to the **Have full control over all Roles and Users** option are listed in the following table:

| Custom settings corresponding to "Have full control over all Roles and Users" option | |
|---|---|
| Users | |
| **Can View Users** | Allowed |
| **Can Create New Users** | Allowed |
| **Can Edit User Properties (User can always edit select properties of own account)** | Allowed |
| **Can Delete Users** | Allowed |
| Roles | |
| **Can View Roles** | Allowed |
| **Can Create New Roles** | Allowed |
| **Can Edit Role Properties (Warning: conferring this right will let Users with this Role edit their own rights)** | Allowed |
| **Can Delete Roles** | Allowed |

| Custom settings corresponding to "Have full control over all Roles and Users" option | |
|---|---|
| Delegate Authority | |
| **Can only manipulate Users with equal or lesser rights** | Not applicable |

# Add users who can only receive reports

"Contacts" are users who cannot sign in to the Deep Security Manager but can periodically be sent reports (using scheduled tasks). Contacts can be assigned a "clearance" level that maps to existing roles. When a contact is sent a report, the report will not contain any information not accessible to a user of the same level. For example, three contacts may each be listed as the recipients of a weekly summary report but the contents of the three reports could be entirely different for each contact depending on their computer rights.

## Add or edit a contact

1. In Deep Security Manager go to **Administration > User Management > Contacts**.
2. Click **New** to add a new contact or double-click an existing contact to edit its settings.
3. In the **General Information** section, specify the name, description, and preferred language of this contact.
4. In the **Contact Information** section, enter the email address to which reports will be sent if this contact is included in a report distribution list. (See the **Reports** page for more information.)
5. In the **Clearance** section, specify the role that determines the information this contact will be allowed to see. For example, if a computer report has been scheduled to be sent to this contact, only information on the computers that his role permits him access to will be included in the report.
6. In the **Password Protected Reports** section, select **Reports generated by this user are password protected** to password-protect exported PDF reports with the **Report Password**.

## Delete a contact

To remove a contact from Deep Security Manager, click **Administration > User Management > Contacts**, click the contact, and then click **Delete**.

## Create an API key for a user

To use the Deep Security Manager API, you will need an API key.

**Note:** API keys can only be used with the new"Use the Deep Security API to automate tasks" on page 261 available in Deep Security Manager 11.1 and later.

**Note:** Trend Micro recommends creating one API key for every user needing API access to the Deep Security Manager.

**Tip:** You can automate API key creation using the Deep Security API. For examples, see the Create and Manage API Keys guide.

To create a new API key:

1. Go to **Administration > User Management > API Keys**.
2. Click **New**.
3. In the Properties window, enter a **Name** and **Description** for the API key.
4. Click on the **Role** list and select a role. **Auditor** grants read-only access to the Deep Security Manager through the API, while **Full Access** grants both read and write access. If you need more specific roles for API key users, you can select **New** and define one. See "Define roles for users" on page 995 for more information on doing so.
5. Select a **Language**.
6. Select a **Time Zone**.
7. Optionally select **Expires on** and select an expiry date for the API key.
8. Click **OK**.
9. Copy the **Secret key value**.

   **Note:** Make sure to copy the secret key value now, this is the only time it will be shown.

## Lock out an existing API key

If an existing API key has been compromised you can lock it out:

1. Double click on the API key you want to lock out.
2. Optionally select **Locked Out (Denied permission to authenticate)** to block usage of the API key.
3. Click **OK**.

# Unlock a locked out user name

If you have attempted to sign in multiple times to Deep Security Manager with an incorrect password, your user account will be locked out. The number of sign-in attempts allowed before lock out is configured in **Administration > System Settings > Security > Number of incorrect sign-in attempts allowed (before lock out)**.

You can unlock users in different ways, depending on the following situations:

- If an administrator user is available, see "Unlock users as an administrator" below.
- If all the administrative users are locked out, see "Unlock administrative users from a command line" below.

## Unlock users as an administrator

1. Log in to Deep Security Manager with a working administrator user name and password.
2. Go to **Administration > User Management > Users**. Select the user you want to unlock, right-click, and click **Properties**.
3. In the wizard, go to **General > Sign-In Credentials**. Deselect the **Locked Out (Denied permission to sign in)** check box.
4. Click **Save**.

## Unlock administrative users from a command line

1. Go to your local command line interface.

   If your Deep Security Manager is Windows, go to the `..\Program Files\Trend Micro\Deep security Manager` directory.

   If your Deep Security Manager is Linux, go to the `/opt/dsm` directory.

2. Enter the following command:

```
dsm_c -action unlockout -username <username>
```

# Implement SAML single sign-on

**Note:** SAML single sign-on is not available when FIPS mode is enabled. See "FIPS 140-2 support" on page 1049.

To implement SAML single sign-on, see "Getting started with SAML single sign-on" on page 1015.

## What are SAML and single sign-on?

Security Assertion Markup Language (or **SAML**) is an open authentication standard that allows for the secure exchange of user identity information from one party to another. SAML supports **single sign-on**, a technology that allows for a single user login to work across multiple applications and services. For Deep Security, implementing SAML single sign-on means that users signing in to your organization's portal would be able to seamlessly sign in to Deep Security without an existing Deep Security account.

## How SAML single sign-on works in Deep Security

### Establishing a trust relationship

In SAML single sign-on, a trust relationship is established between two parties: the **identity provider** and the **service provider**. The identity provider has the user identity information stored on a directory server. The service provider (which in this case is Deep Security) uses the identity provider's user identities for its own authentication and account creation.

The identity provider and the service provider establish trust by exchanging a **SAML metadata document** with one another.

**Note:** At this time, Deep Security supports **only** the HTTP POST binding of the SAML 2.0 identity provider (IdP)-initiated login flow, and not the service provider (SP)-initiated login flow

## Creating Deep Security accounts from user identities

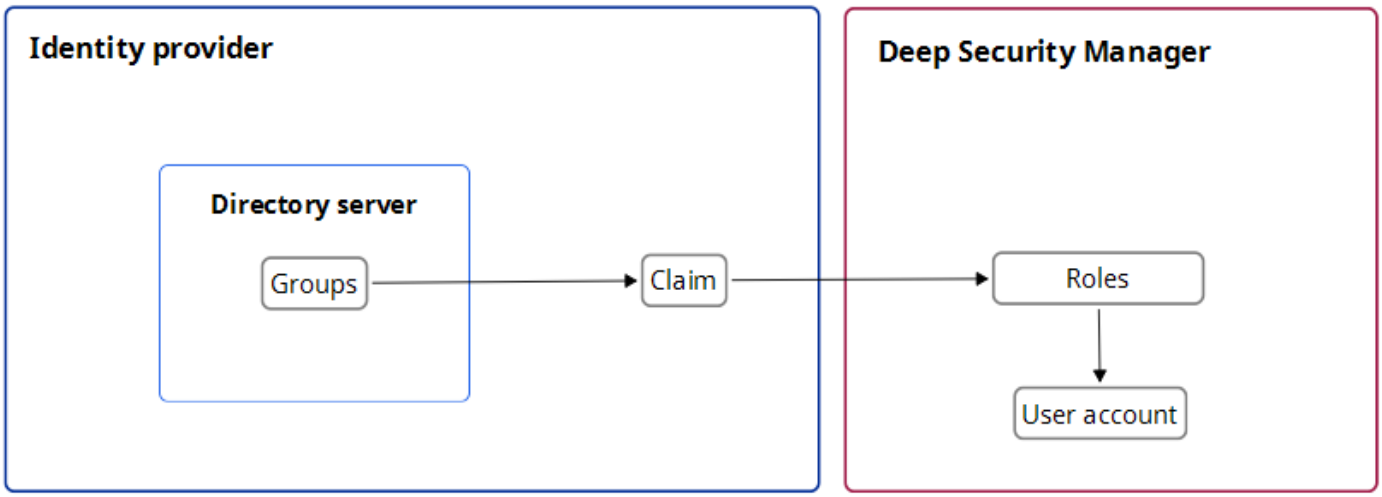
Once Deep Security and the identity provider have exchanged SAML metadata documents and established a trust relationship, Deep Security can access the user identities on the identity provider's directory server. However, before Deep Security can actually create accounts from the user identities, account types need to be defined and instructions for transforming the data format need to be put in place. This is done using **groups**, **roles** and **claims**.

Groups and roles specify the tenant and access permissions that a Deep Security user account will have. Groups are created on the identity provider's directory server. The identity provider assigns user identities to one or more of the groups. Roles are created in the Deep Security Manager. There must be both a group and a role for each Deep Security account type, and their access permissions and tenant assignment must match.

Once there are matching groups and roles for each user type, the group data format needs to be transformed into a format Deep Security can understand. This is done by the identity provider with a claim. The claim contains instructions for transforming the group data format into the matching Deep Security role.

> **Tip:** Learn more about the "SAML claims structure" on page 1019 required by Deep Security.

Below is a representation of this process:



### Implement SAML single sign-on in Deep Security

Once trust has been established between Deep Security and an identity provider with a SAML metadata document exchange, matching groups and roles have been created, and a claim put in place to translate the group data into roles, Deep Security can use SAML single sign-on to automatically make Deep Security accounts for users signing in through your organization's portal.

For more information on implementing SAML single sign-on, see "Getting started with SAML single sign-on" below.

## Getting started with SAML single sign-on

**Note:** SAML single sign-on is not available when FIPS mode is enabled. See "FIPS 140-2 support" on page 1049.

When you configure Deep Security to use SAML single sign-on, users signing in to your organization's portal can seamlessly sign in to Deep Security without an existing Deep Security account. SAML single sign-on also makes it possible to implement user authentication access control features such as:

- Password strength or change enforcement.
- One-Time Password (OTP).
- Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA).

For a more detailed explanation of Deep Security's implementation of the SAML standard, see "Implement SAML single sign-on" on page 1013.

**Note:** At this time, Deep Security supports **only** the HTTP POST binding of the SAML 2.0 identity provider (IdP)-initiated login flow, and not the service provider (SP)-initiated login flow

To use SAML single sign-on with Deep Security, you will need to do the following:

1. "Configure pre-set up requirements" on the next page
2. "Configure Deep Security as a SAML service provider" on the next page
3. "Configure SAML in Deep Security" on page 1018

4. "Provide information for your identity provider administrator" on page 1018
5. "SAML claims structure" on page 1019
6. "Test SAML single sign-on" on page 1022
7. "Service and identity provider settings" on page 1022

## Configure pre-set up requirements

1. Ensure your Deep Security Manager is functioning properly.
2. Contact the identity provider administrator to:
   - Establish a naming convention for mapping directory server groups to Deep Security roles.
   - Obtain their identity provider SAML metadata document.
   - Ask them to add any required user authentication access control features to their policy.

Support is available to assist with the following identity providers that have been tested in Deep Security with SAML single sign-on:

- Active Directory Federation Services (ADFS)
- Okta
- PingOne
- Shibboleth

## Configure Deep Security as a SAML service provider

As the first step in the SAML single sign-on configuration, you will need to set up Deep Security as a service provider.

For a more detailed explanation of Deep Security's implementation of the SAML standard, see "Implement SAML single sign-on" on page 1013.

**Note:** In multi-tenant Deep Security installations, only the primary tenant administrator can configure Deep Security as a SAML service provider.

1. On the **Administration** page, go to **User Management > Identity Providers > SAML**.
2. Click **Get Started**.

3. Enter an **Entity ID** and a **Service Name**, and then click **Next**.

   **Note:** The **Entity ID** is a unique identifier for the SAML service provider. The SAML specification recommends that the entity ID is a URL that contains the domain name of the entity, and industry practices use the SAML metadata URL as the entity ID. The SAML metadata is served from the */saml* endpoint on the Deep Security Manager, so an example value might be *https://<DSMServerIP:4119>/saml*.

4. Select a certificate option, and click **Next**. The service provider certificate is not used at this time, but would be used in the future to support service-provider-initiated login or single sign-out features. When creating the service provider, you can import a certificate and private key or create a new self-signed certificate and private key.

### Import a Certificate and Private Key

1. Click **Choose File** and open the PKCS #12 keystore file containing your certificate.
2. Enter the password for the keystore.
3. Click **Next**.

   You will be shown a summary of your certificate details.

4. Click **Finish**.

### Generate a new self-signed server certificate

1. Enter the following details for your certificate:
   - Common Name (CN)
   - Organization (O)
   - Organizational Unit (OU)
   - Email Address (E)

2. Click **Next**.

   You will be shown a summary of your certificate details.

3. Click **Finish**.

### Keep the current Server Certificate

1. Click **Next**, and then click **Finish**.

Deep Security is now set up as a SAML service provider.

## Configure SAML in Deep Security

### Import your identity provider's SAML metadata document

**Note:** Your Deep Security account must have both administrator and "Create SAML identity provider" permissions.

1. On the Administration page, go to **User Management > Identity Providers > SAML**.
2. Click **Get Started**.
3. Click **Choose File**, select the SAML metadata document provided by your identity provider, and click **Next**.
4. Enter a **Name** for the identity provider, and then click **Finish**.

   You will be brought to the Roles page.

### Create Deep Security roles for SAML users

You need to create a role for each of your expected user types. Each role must have a corresponding group in your identity provider's directory server, and match the group's access permissions and tenant assignment.

Your identity provider's SAML integration will have a mechanism to transform group membership into SAML claims. Consult the documentation that came with your identity provider to learn more about claim rules.

For information on how to create roles, see "Define roles for users" on page 995.

## Provide information for your identity provider administrator

### Download the Deep Security Manager service provider SAML metadata document

1. On the Administration page, go to **User Management > Identity Providers > SAML**.
2. Under SAML Service Provider, click **Download**.
   Your browser will download the Deep Security service provider SAML metadata document (`ServiceProviderMetadata.xml`).

### Send URNs and the Deep Security SAML metadata document to the identity provider administrator

You need to give the identity provider administrator Deep Security's service provider SAML metadata document, the identity provider URN and the URN of each Deep Security role you created.

> **Tip:**
> To view role URNs, go to **Administration > User Management > Roles** and look under the URN column.
>
> To view identity provider URNs, go to **Administration > User Management > Identity Providers > SAML > Identity Providers** and look under the URN column.

Once the identity provider administrator confirms they have created groups corresponding to the Deep Security roles and any required rules for transforming group membership into SAML claims, you are done with configuring SAML single sign-on.

> **Note:** If necessary, you can inform the identity provider administrator about the "SAML claims structure" below required by Deep Security.

### SAML claims structure

The following SAML claims are supported by Deep Security :

- "Deep Security user name (required)" below
- "Deep Security user role (required)" on the next page
- "Maximum session duration (optional)" on page 1021
- "Preferred language (optional)" on page 1021

### Deep Security user name (required)

The claim must have a SAML assertion that contains an `Attribute` element with a `Name` attribute of `https://deepsecurity.trendmicro.com/SAML/Attributes/RoleSessionName` and a single `AttributeValue` element. The Deep Security Manager will use the `AttributeValue` as the Deep Security user name.

## Sample SAML data (abbreviated)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
      <Attribute
Name="https://deepsecurity.trendmicro.com/SAML/Attributes/RoleSessionName">
        <AttributeValue>alice</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

### Deep Security user role (required)

The claim must have a SAML assertion that contains an `Attribute` element with a `Name` attribute of `https://deepsecurity.trendmicro.com/SAML/Attributes/Role` and between one and ten `AttributeValue` elements. The Deep Security Manager uses the attribute value(s) to determine the tenant, identity provider, and role of the user. A single assertion may contain roles from multiple tenants.

## Sample SAML data (abbreviated)

**Note:** The line break in the `AttributeValue` element is present for readability; in the claim it must be on a single line.

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
      <Attribute Name="https://deepsecurity.trendmicro.com/SAML/Attributes/Role">
        <AttributeValue>urn:tmds:identity:[pod ID]:[tenant ID]:saml-provider/[IDP
name],
            urn:tmds:identity:[pod ID]:[tenant ID]:role/[role name]</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

### Maximum session duration (optional)

If the claim has a SAML assertion that contains an `Attribute` element with a `Name` attribute of `https://deepsecurity.trendmicro.com/SAML/Attributes/SessionDuration` and an integer-valued `AttributeValue` element, the session will automatically terminate when that amount of time (in seconds) has elapsed.

## Sample SAML data (abbreviated)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
      <Attribute
Name="https://deepsecurity.trendmicro.com/SAML/Attributes/SessionDuration">
        <AttributeValue>28800</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

### Preferred language (optional)

If the claim has a SAML assertion that contains an `Attribute` element with the `Name` attribute of `https://deepsecurity.trendmicro.com/SAML/attributes/PreferredLanguage` and a string-valued `AttributeValue` element that is equal to one of the supported languages, the Deep Security Manager will use the value to set the user's preferred language.

The following languages are supported:

- `en-US` (US English)
- `ja-JP` (Japanese)
- `zh-CN` (Simplified Chinese)

## Sample SAML data (abbreviated)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
```

```
      <Attribute
Name="https://deepsecurity.trendmicro.com/SAML/Attributes/PreferredLanguage">
        <AttributeValue>en-US</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

## Test SAML single sign-on

Navigate to the single sign-on login page on the identity provider server, and log in to the Deep Security Manager from there. You should be redirected to the Deep Security Manager console. If SAML single sign-on is not functioning, follow the steps below:

### Review the set-up

1. Review the "Configure pre-set up requirements" on page 1016 section.
2. Ensure that the user is in the correct directory group.
3. Ensure that the identity provider and role URNs are properly configured in the identity provider federation service.

### Create a Diagnostic Package

1. Go to **Administration > System Information** and click **Diagnostic Logging**.
2. Select **SAML integration Issues** and click **Save**.
3. Generate logs. Replicate the issue by logging in to the Deep Security Manager through your identity provider.
4. After the login fails, generate a diagnostic package by navigating to **Administration > System Information** and clicking on **Create Diagnostic Package**.
5. Once the diagnostic package has been created, navigate to *https://success.trendmicro.com* to open a Technical Support Case, and upload the diagnostic package during the case creation.

## Service and identity provider settings

You can set how far in advance Deep Security will alert you to the expiry date of the server and identity provider certificates, as well as how much time must pass before inactive user accounts added through SAML single sign-on are automatically deleted.

To change these settings, go to **Administration > System Settings > Security > Identity Providers**.

# Navigate and customize Deep Security Manager

You can customize the Deep Security Manager console to suit your needs and to display useful information about your deployment.


- "Group computers dynamically with smart folders" below
- "Customize the dashboard" on page 790
- "View active Deep Security Manager nodes" on page 1036
- "Check your license information" on page 730


## Group computers dynamically with smart folders

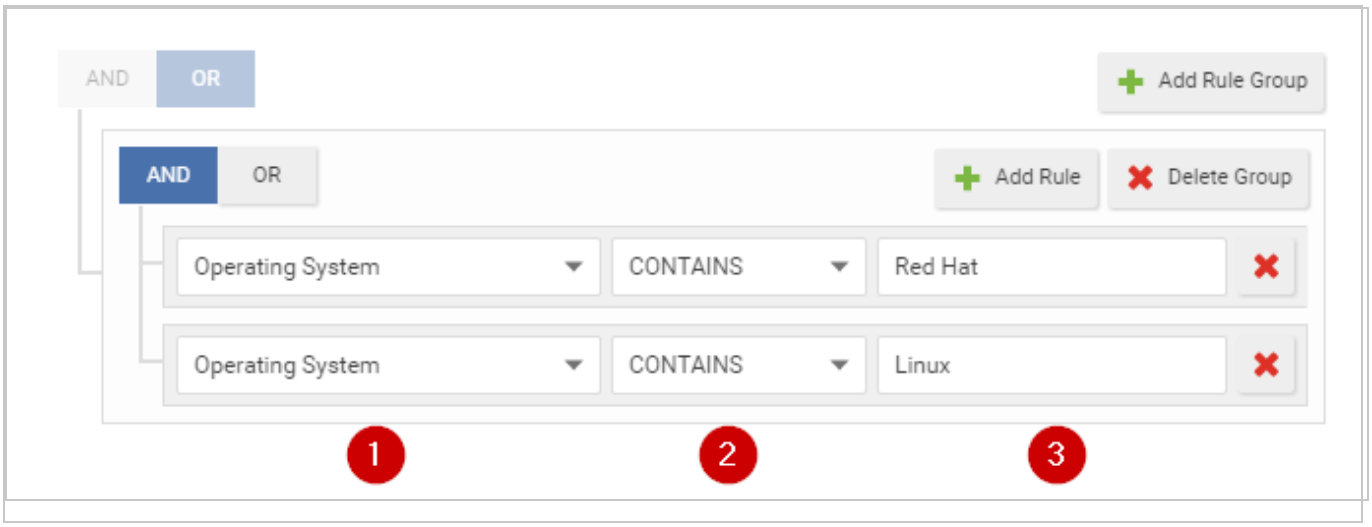
A smart folder is a dynamic group of computers that you define with a saved search query. It finds matching computers each time you click the group. For example, if you want to view your computers grouped by attributes such as operating system or AWS project tags, you can do this using smart folders.

> **Tip:** If you prefer to search for resources programmatically, you can automate resource searches using the Deep Security API. For examples, see the Search for Resources guide.

You create smart folders by defining:

1. What to search (1 - computer properties)
2. How to determine a match (2 - operator)

3. What to search for (3 - value)




## Create a smart folder

1. Go to **Computers > Smart Folders**.
2. Click **Create a Smart Folder**.

   A default, empty search criteria group ("rule group") appears. You must configure this first. If you need to define more or alternative possible matches, you can add more rule groups later.

3. Type a name for your smart folder.
4. In the first dropdown, select a property that all matching computers have, such as **Operating System**. (See "Searchable Properties" on page 1028.)

   If you selected AWS Tag, also type the tag's name.

5. Select the operator: whether to match identical, similar, or opposite computers, such as **CONTAINS**.

   **Note:** Some operators are not available for all properties.

6. Type all or part of the search term.

   **Note:** Wild card characters are not supported.

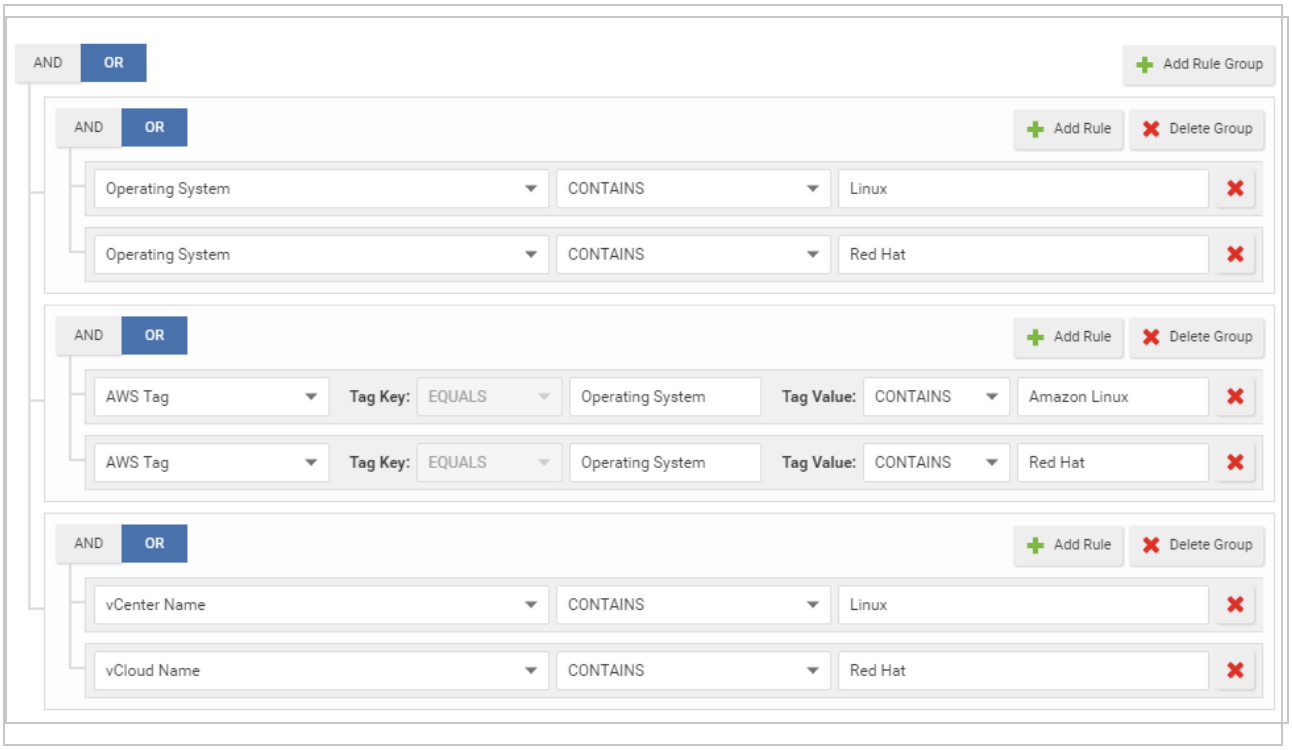
> **Tip:** If you enter multiple words, it compares the *entire phrase* - not each word separately. No match occurs if the property's value has words in a different order, or only some of the words.
> To match *any* of the words, instead click **Add Rule** and **OR**, and then add another value: one word per rule.

7. If computers must match multiple properties, click **Add Rule** and **AND**. Repeat steps 4-6.

   For more complex smart folders, you can chain multiple search criteria. Click **Add Group**, then click **AND** or **OR**. Repeat steps 4-7.

   For example, you might have Linux computers deployed both on-premises and in clouds such as AWS, Azure, or vCloud. You could create a smart folder that contains all of them by using 3 rule groups based on:

   a. local physical computers' operating system
   b. AWS tag
   c. vCenter or vCloud name



> **Tip:** To test the results of your query before saving your smart folder, click **Preview**.

8. Click **Save**.
9. To verify, click your new smart folder. Verify that it contains all expected computers.

   > **Tip:** For faster smart folders, remove unnecessary AND operations, and reduce sub-folder depths. They increase query complexity, which reduces performance.

   Also verify that it omits computers that shouldn't match the query. If you need to edit your smart folder's query, double-click the smart folder.

   > **Note:** If your account's role doesn't have the permissions, some computers won't appear, or you won't be able to edit their properties. For more information, see "Define roles for users" on page 995.

## Edit a smart folder

If you need to edit your smart folder's query, double-click the smart folder.

To reorder search criteria rules or rule groups, move your cursor onto a rule or group until it changes to a ✥, then drag it to its destination.

## Clone a smart folder

To duplicate and modify an existing smart folder as a template for a new smart folder, right-click the original smart folder, then select **Copy Smart Folder**.

## Focus your search using sub-folders

You can use sub-folders to filter a smart folder's search results.

Smart folders can be nested up to 10 levels deep.

- Smart folder 1
  - Sub-folder 2
    - Sub-folder 3 ...

For example, you might have a smart folder for all your Windows computers, but want to focus on computers that are specifically Windows 7, and maybe specifically either 32-bit or 64-bit. To do this, under the "Windows" parent folder, you could create a child smart folder for Windows 7. Then, under the "Windows 7" folder, you would create two child smart folders: 32-bit and 64-bit.

1. Right-click a smart folder and select **Create Child Smart Folder**.
2. Edit your child smart folder's query groups or rules. Click **Save**.
3. Click your new smart folder. Verify that it contains all expected computers. Also verify that it omits computers that shouldn't match the query.

## Automatically create sub-folders

**Note:** Applies to AWS computers only.

Instead of manually creating child folders, if you use Amazon's cloud, you can automatically create sub-folders for each value of an AWS tag. For information on how to apply AWS tags to your computers, see Amazon's guide on Tagging Your Amazon EC2 Resources.

**Note:** AWS tag-based sub-folders replace any existing manually created child folders under the parent folder.

1. Select the **Automatically create sub-folders for each value of a specific AWS tag key:** check box located below the smart folder groups.
2. Type name of the AWS tag. Sub-folders are automatically created for each of this tag's values.
3. Click **Save**.

**Tip:** Empty sub-folders can appear if an AWS tag value is not being used anymore. To remove them, right-click the smart folder and select **Synchronize Smart Folder**.

## Searchable Properties

Properties are an attribute that some or all computers you want to find have. Smart folders show computers that have the selected property, and its value matches.

**Note:** Type your search *exactly as that property appears in Deep Security Manager*- not, for example, vCenter/AWS/Azure. Otherwise your smart folder query won't match.
To find the exact matching text, (unless otherwise noted) go to **Computers** and look in the navigation pane on the left.

### General

| Property | Description | Data type | Examples |
|---|---|---|---|
| Hostname | The computer's host name, as seen on **Computers > Details** in Hostname. | string | ca-staging-web1 |
| Computer Display Name | The computer's display name in Deep Security (if any), as seen on **Computers > Details** in Display Name. | string | nginxTest |
| Folder Name | The computer's assigned group. | string | US-East |
| Operating System | The computer's operating system, as seen on **Computers > Details** in Platform. | string | Microsoft Windows 7 (64 bit) Service Pack 1 Build 7601 |
| IP Address | The computer's IP address.<br><br>You can find the IP address in Deep Security Manager. To find the IP of:<br><br>• an AWS instance or Azure VM that was added to Deep Security through **Add > Add AWS Account** or **Add > Add Azure Account**, go the AWS or | IPv4 or IPv6 address, or an IPv4 range | 172.20.1.5-172.20.1.55<br><br>2001:db8:face::5 |

| Property | Description | Data type | Examples |
|---|---|---|---|
| | Azure computer's details page, and under the **General** tab, scroll to the **Virtual machine Summary** section. The AWS IP addresses are listed in these fields:<br>• **Private IP Address**<br>• **Public IP (PIP) Address**<br><br>**Note:** If you added the AWS or Azure computer through **Add > Add Computers**, its IP is located in the same place as a physical computer's.<br><br>• a physical computer (not AWS, Azure, vCenter, or vCloud), go to the computer's details page and on the left, click **Interfaces**<br><br>**Note:** If "DHCP" is displayed instead of a static IP address, it won't match the smart folder query.<br><br>• a vCenter or vCloud VM, go to the vCenter computer's details page, and under the **General** tab, scroll to the **Virtual machine Summary** section. The vCenter or vCloud IP address is listed in the **IP Address** field. | | |
| Policy | The computer's assigned Deep Security policy, as seen on **Computers > Details**. | string | Base Policy |

| Property | Description | Data type | Examples |
|---|---|---|---|
| | | (option in drop-down list) | |
| Activated | Whether or not the computer has been activated with Deep Security Manager, as seen on **Computers > Details**. | Boolean | Yes |
| Docker Host | Whether or not Docker is installed on the computer, as seen on **Computers > Details**. | Boolean | No |
| Computer Type | The type of computer. Options are: Physical Computer, Amazon EC2 Instance, Amazon WorkSpace, vCenter VM, Azure Instance, Azure ARM Instance. | string (option in drop-down list) | Examples: Physical Computer, Amazon EC2 Instance |
| Last Successful Recommendation Scan | Whether or not the computer has had a successful recommendation scan within a specified time period. The last recommendation scan date and results can be seen on **Computers > Details > General > Intrusion Prevention** or **Integrity Monitoring** or **Log Inspection > Recommendations**. | Date operator drop-down list, String, Date unit drop-down list | **OLDER THAN**, 7, **DAYS** |

## AWS

| Property | Description | Data type | Examples |
|---|---|---|---|
| Tag | The computer's AWS tag key:value pair, as seen on **Computers > Details > Overview > General** under Virtual machine Summary, in Cloud Instance Metadata. | string | Tag Key: env<br>Tag Value: staging |

| Property | Description | Data type | Examples |
|---|---|---|---|
| | Type the tag name, then its value. Case-sensitive. | | |
| Security Group Name | The computer's associated AWS security group name, as seen on **Computers > Details > Overview > General** under Virtual machine Summary, in Security Group(s). | string | SecGrp1 |
| Security Group ID | The computer's AWS security group ID, as seen on **Computers > Details > Overview > General** under Virtual machine Summary, in Security Group(s). | string | sg-12345678 |
| AMI ID | The computer's Amazon Machine AMI ID, as seen on **Computers > Details > Overview > General** under Virtual machine Summary, in AMI ID. | string | ami-23c44a56 |
| Account ID | The computer's associated 12-digit AWS Account ID, as seen on **Computers** when you right-click **Amazon Account** and select **Properties**.<br><br>Results include computers in sub-folders. | string | 123456789012 |
| Account Name | The computer's associated AWS Account Alias, as seen on **Computers** when you right-click the AWS Cloud Connector and select **Properties**.<br><br>Results include computers in sub-folders. | string | MyAccount-123 |
| Region ID | The computer's AWS region suffix.<br><br>Results include computers in sub-folders. | string | us-east-1 |
| Region Name | The computer's associated AWS region name.<br><br>Results include computers in sub-folders. | string | US East (Ohio) |
| VPC ID | The computer's Virtual Private Cloud (VPC) ID.<br><br>If an alias exists, the folder name is the alias, followed | string | vpc-3005e48a |

| Property | Description | Data type | Examples |
|---|---|---|---|
| | by the VPC ID in parentheses. Otherwise the folder's name is the VPC ID.<br><br>Results include computers in sub-folders. | | |
| Subnet ID | The computer's associated Virtual Private Cloud (VPC) subnet ID.<br><br>If an alias exists, the folder name is the alias, followed by the VPC subnet ID in parentheses. Otherwise the folder's name is the VPC subnet ID.<br><br>Results include computers in sub-folders. | string | subnet-b1c2e468 |
| Directory ID | The ID of the AWS directory where the user entry associated with an Amazon WorkSpace resides. The directory ID is seen on the **Computers > Details > Virtual machine Summary**, in the **WorkSpace Directory** field. That field takes the format <directory_alias>(<directory_ID>), for example, myworkspacedir(d-9367232d89). | string | d-9367232d89 |

## Azure

| Property | Description | Data type | Examples |
|---|---|---|---|
| Subscription Name | The computer's associated Azure subscription account ID, as seen on **Computers** when you right-click **Azure** and select **Properties**.<br><br>Results include computers in sub-folders. | string | MyAzureAccount |
| Resource Group | The computer's associated resource group. | string | MyResourceGroup |

## vCenter

| Property | Description | Data type | Examples |
|---|---|---|---|
| Name | The computer's associated vCenter.<br>Results include computers in sub-folders. | string | vCenter - lab13-vc.example.com |
| Datacenter | The computer's associated vCenter data center.<br>Results include computers in sub-folders. | string | lab13-datacenter |
| Folder | The computer's vCenter folder.<br>Results include computers in sub-folders. | string | db_dev |
| Parent ESX Hostname | The host name of the ESX or ESXi hypervisor where the computer's guest VM is running, as seen on **Computers**. | string | lab13-esx2.example.com |
| Custom Attribute | The computer's assigned vCenter custom attribute, as seen on **Computers > Details** in Virtual machine Summary. | string<br>(comma-separated attribute name and value) | env, production |

## vCloud

| Property | Description | Data type | Examples |
|---|---|---|---|
| Name | The computer's associated vCloud.<br>Results include computers in sub-folders. | string | vCloud-lab23 |
| Datacenter | The computer's associated vCloud data center.<br>Results include computers in sub-folders. | string | lab13-datacenter |

| Property | Description | Data type | Examples |
|---|---|---|---|
| vApp | The computer's associated vCloud data center folder.<br>Results include computers in sub-folders. | string | db_dev |

Folder

| Property | Description | Data type | Examples |
|---|---|---|---|
| Name | The host name of the Microsoft Active Directory or LDAP directory.<br>Results include computers in sub-folders. | string | ad01.example.com |
| Folder | The computer's Microsoft Active Directory or LDAP folder name.<br>Results include computers in sub-folders. | string | Computers |

## Operators

Smart folder operators indicate whether matching computers should have a property value that is identical, similar, or dissimilar to your search term. Not all operators are available for every property.

| Operator | Description | Example usage |
|---|---|---|
| EQUALS | The search query only finds computers that are an exact match. | A search query for 'Windows' in the Operating System property does not find computers with 'Windows 7' or 'Microsoft Windows'. |
| DOES NOT EQUAL | The search query finds any computers that are not an exact match. | A search query for 'Amazon Linux (64 bit)' in the Operating System property finds all computers other than Amazon Linux 64-bit machines. |
| CONTAINS | The search query finds any computers that contain the search term. | A search query for '203.0.113.' in the IP Address property finds any computers on the 203.0.113.xxx subnet. |

| Operator | Description | Example usage |
|---|---|---|
| DOES NOT CONTAIN | The search query finds any computers that do not contain the search term. | A search query for 'Windows' in the Operating System property finds any computers that do not have 'Windows' in their operating system name. |
| ANY VALUE | The search query finds all computers with the selected property. | A search query in the Group Name property finds all computers in that group. |
| IN RANGE | The search query finds all computers between the specified start and end range. | A search query in the IP Address property with Start Range 10.0.0.0 and End Range 10.255.255.255 would find all computers with IP addresses between 10.0.0.0 and 10.255.255.255. |
| NOT IN RANGE | The search query finds all computers that are not between the specified start and end range. | A search query in the IP Address property with Start Range 10.0.0.0 and End Range 10.255.255.255 finds all computers that have IP addresses outside the range of 10.0.0.0 and 10.255.255.255. |
| Yes | The search query finds all computers with the selected property. | A search query with 'Yes' selected for the Docker property finds any computers with the Docker service running. |
| No | The search query finds all computers that do not have the selected property. | A search query with 'No' selected for the Docker property would find any computers that do not have the Docker service running. |
| OLDER THAN | The search query finds all computers prior to the specified date for the property.<br>Used with an accompanying DAYS, WEEKS, HOURS, or MINUTES operator. | A search query with 'OLDER THAN', '7', 'DAYS' for the 'Last Successful Recommendation Scan' property finds computers that have had a successful recommendation scan 8 days or longer ago. |
| MORE RECENTLY THAN | The search query finds all computers more recent than the | A search query with 'MORE RECENTLY THAN', '1', 'MONTH' for the 'Last Successful Recommendation Scan' property finds computers that have had a successful recommendation scan earlier than 1 month ago. |

| Operator | Description | Example usage |
|---|---|---|
| | specified date for the property.<br><br>Used with an accompanying DAYS, WEEKS, HOURS, or MINUTES operator. | |
| NEVER | The search query finds all computers that do not match the property. | A search query with 'NEVER' for the 'Last Successful Recommendation Scan' property finds computers that have never had a successful recommendation scan. |

## View active Deep Security Manager nodes

To display a list of all active Deep Security Manager nodes, go to **Administration > Manager Nodes** . (See also "Run Deep Security Manager on multiple nodes" on page 130. )

To display details about one of the manager nodes, double-click its row in the list. The Properties window will display:

- **Hostname:** The hostname of the computer where Deep Security Manager is installed.
- **Description:** A description of the manager node.
- **Performance Profile:** Deep Security Manager's performance can be affected by several factors including number of CPUs, available bandwidth, and database responsiveness. The manager's default performance settings are designed to be suited for most installation environments. However, if you experience performance issues your support provider may suggest that you change the performance profile assigned to one or more of your Deep Security Manager nodes. (You should not change these settings without first consulting your support provider.)

**Note:** The "Simultaneous Endpoint Disk and Network Jobs" referred to in the tables below include anti-malware scans, integrity monitoring scans, reconnaissance scans, sending policy updates to computers, and distributing security updates.

- **Aggressive:** This performance profile is optimized for installations where the Deep Security Manager is installed on a dedicated server. For example, this is how some common concurrent operations could be distributed per manager node using the **Aggressive** performance profile:

| Operation | 2-core system | 8-core system |
|---|---|---|
| Activations | 10 | 20 |
| Updates | 25 | 50 |
| Recommendation Scans | 5 | 12 |
| Check Status | 100 | Same (100) |
| Agent- or Appliance-Initiated Heartbeats | 20 Active<br>40 Queued | 50 Active<br>40 Queued |
| Simultaneous Endpoint Disk and Network Jobs | 50 | 50 |
| Simultaneous Endpoint Disk and Network Jobs per ESXi | 3 | 3 |

- **Standard:** This Performance Profile is optimized for installations where the Deep Security Manager and the database share the same host. For example, this is how some common concurrent operations could be distributed per manager node using the **Standard** performance profile:

| Operation | 2-core system | 8-core system |
|---|---|---|
| Activations | 5 | 10 |
| Updates | 16 | 46 |
| Recommendation Scans | 3 | 9 |
| Check Status | 65 | 100 |
| Agent- or Appliance-Initiated Heartbeats | 20 Active<br>40 Queued | 50 Active<br>40 Queued |
| Simultaneous Endpoint Disk and Network Jobs | 50 | 50 |
| Simultaneous Endpoint Disk and Network Jobs per ESXi | 3 | 3 |

- **Unlimited Agent Disk and Network Usage:** This setting is identical to **Aggressive** but has no limit on computer disk and network usage operations.

| Operation | 2-core system | 8-core system |
|---|---|---|
| Activations | 10 | 20 |
| Updates | 25 | 25 |
| Recommendation Scans | 5 | 12 |

| Operation | 2-core system | 8-core system |
|---|---|---|
| Check Status | 100 | Same (100) |
| Agent- or Appliance-Initiated Heartbeats | 20 Active<br>40 Queued | 50 Active<br>40 Queued |
| Simultaneous Endpoint Disk and Network Jobs | Unlimited | Unlimited |
| Simultaneous Endpoint Disk and Network Jobs per ESXi | Unlimited | Unlimited |

**Note:** All performance profiles limit the number of concurrent component updates to 100 per relay group.

- **Status:** Indicates the node's online and active status from the perspective of the Deep Security Manager node you are currently logged into.
- **Options:** You can choose to decommission a manager node. The node must be offline (uninstalled or service halted) to be decommissioned.

# Customize advanced system settings

Several features for advanced users are located on **Administration > System Settings > Advanced**.

**Tip:** You can automate system setting changes using the Deep Security API. For examples, see the Configure Policy, Computer, and System Settings guide.

## Primary Tenant Access

By default, the primary tenant can access your Deep Security environment.

If the primary tenant enabled the "Primary Tenant Access" settings in your environment, however, you can prevent the primary tenant from accessing your Deep Security environment, or grant access for a limited amount of time.

## Load Balancers

**Note:** The load balancer settings are not available when FIPS mode is enabled. See "FIPS 140-2 support" on page 1049.

Agents are configured with a list of Deep Security Manager and Deep Security Relays. When multiple managers and relays are deployed *without* a load balancer, agents will automatically contact the managers and relays using a round robin sequence.

To better scale your network, you can put a load balancer in front of the managers or relays. When you configure the load balancer hostname and port numbers, it will override the IP address or hostname and port numbers currently used by the agents.

The script generator uses the address of the Deep Security Manager that you are connected to. This ensures that the scripts continue to function even if one of the Deep Security Manager nodes fails or is down for maintenance or upgrades.

**Note:** The load balancer must be non-terminating for the SSL or TLS session with the agent's heartbeat port number because its uses mutual authentication. SSL inspection that terminates (for example, if you try to use SSL offloading) will break the session.

## Multi-tenant Mode

1. Select **Enable Multi-Tenant Mode**.
2. In the wizard that appears, enter your **Multi-Tenant Activation Code** and click **Next**.
3. Select the license mode, either:
   - **Inherit Licensing from Primary Tenant:** All tenants use the same licenses as the primary tenant.
   - **Per Tenant Licensing:** Tenants themselves enter a license when they log in for the first time.
4. Click **Next**.

## Deep Security Manager Plug-ins

Plug-ins are modules, reports and other add-ons for the Deep Security Manager. Trend Micro occasionally produces new or additional versions of these which are distributed as self-installing packages.

## SOAP Web Service API

Much of the Deep Security Manager's functionality can be controlled via SOAP-invoked Web services. The WSDL (Web Services Description Language) can be found at the URL displayed in the panel on the page. For assistance with Deep Security Manager's Web services API contact your support provider.

**Note:** A User's ability to access Web Services in the Deep Security Manager will depend on that User being granted the appropriate privileges. These privileges are associated with the Role the User has been assigned. The setting is found on the **General** tab of the **Role properties window** found at **Administration > User Management > Roles**.

## Status Monitoring API

The REST Status Monitoring API lets you query the Deep Security Manager (including individual Manager Nodes) for status information such as CPU and memory usage, number of queued jobs, total and Tenant-specific database size. For assistance with Deep Security Manager's REST Status Monitoring API contact your support provider.

## Export

**Export file character encoding:** The character encoding used when you export data files from the Deep Security Manager. The encoding must support characters in your chosen language.

**Exported Diagnostics Package Language:** Your support provider may ask you generate and send them a Deep Security diagnostics package. This setting specifies the language the package will be in. The diagnostic package is generated on **Administration > System Information**.

## Whois

Whois can be used to look up which domain name is associated with an IP address when you review logged intrusion prevention and firewall events. Enter the search URL using "[IP]" as a placeholder for the IP address to look up.
(For example, "http://reports.internic.net/cgi/whois?whois_nic=[IP]&type=nameserver".)

## Licenses

**Hide unlicensed Protection Modules for new Users** determines whether unlicensed modules are hidden rather than simply grayed out for subsequently created Users. (This setting can be overridden on a per-user basis on **Administration > User Management > Users > Properties**).

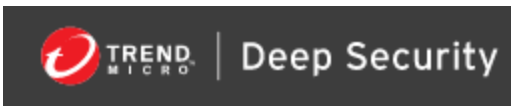
## Scan Cache Configurations

## CPU Usage During Recommendation Scans

This setting controls the amount of CPU resources dedicated to performing Recommendation Scans. If you notice that CPU usage is reaching unreasonably high levels, try changing to a lower setting to remedy the situation. For other performance controls, see **Administration > Manager Nodes > Properties > Performance Profiles**.

## Logo

You can replace the Deep Security logo that appears on the login page, at the top right of the Deep Security Manager GUI, and at the top of reports. Your replacement image must be in PNG format, be 320 px wide and 35 px high, and have a file size smaller than 1 MB. A template is available in the `installfiles` directory of the Deep Security Manager.




Click **Import Logo** to import your own logo, or click **Reset Logo** to reset the logo to its default image.

## Manager AWS Identity

You can configure cross-account access. Select either:

- **Use Manager Instance Role:** The more secure option to configure cross-account access. Attach a policy with the sts:AssumeRole permission to the Deep Security Manager's instance role, then select this option. Does not appear if the Deep Security Manager does not have an instance role, or if you're using an Azure Marketplace or on-premise

installation of Deep Security Manager.

- **Use AWS Access Keys:** Create the keys and attach a policy with the sts:AssumeRole permission before you select this option, and then type the **Access Key** and **Secret Key**. Does not appear if you're using an Azure Marketplace or on-premise installation of Deep Security Manager.

## Application control

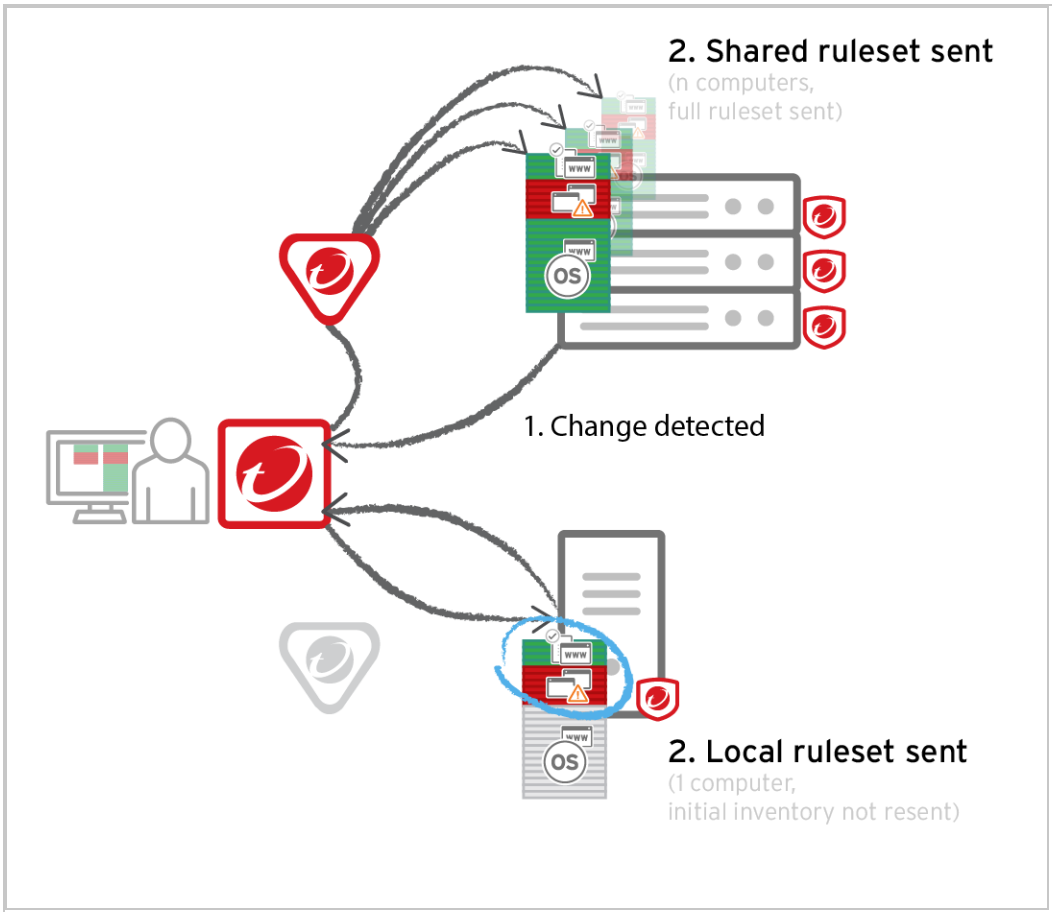
Each time you create an application control ruleset or change it, it must be distributed to all computers that use it. Shared rulesets are bigger than local rulesets. Shared rulesets are also often applied to many servers. If they all downloaded the ruleset directly from the manager at the same time, high load could cause slower performance. Global rulesets have the same considerations.

Using Deep Security Relays can solve this problem. (For information on configuring relays, see "Distribute security and software updates with relays" on page 234.)

Steps vary by whether or not you have a multi-tenant deployment.

**Single tenant deployments**

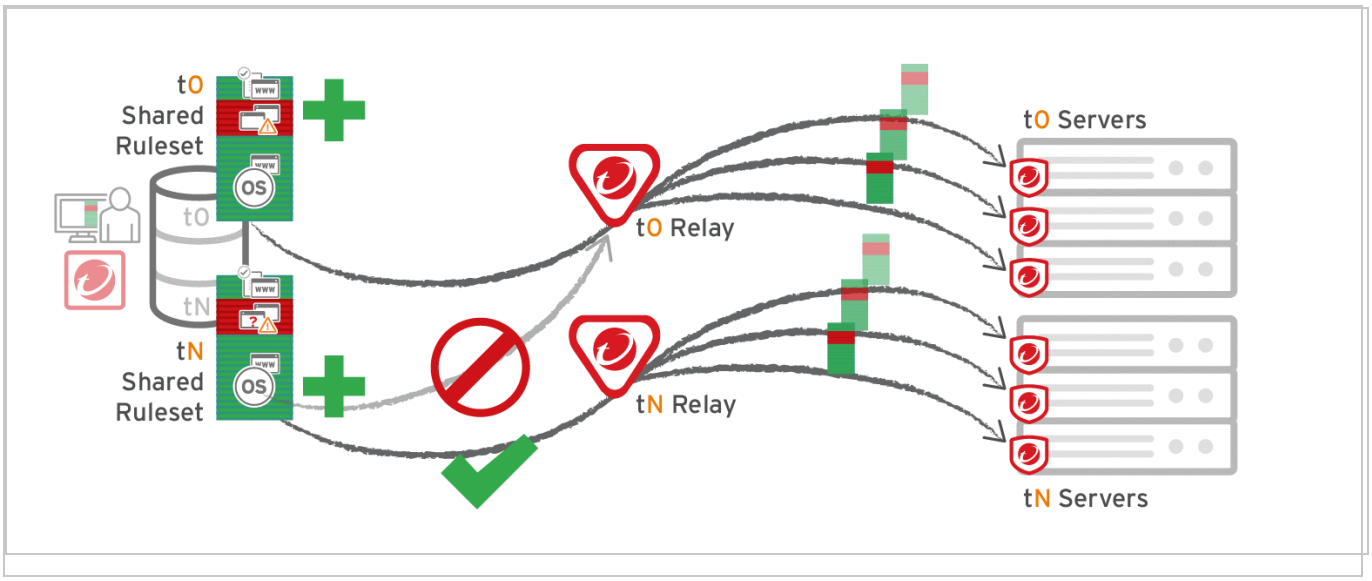
Go to **Administration > System Settings > Advanced** and then select **Serve application control rulesets from relays**.




### Multi-tenant deployments

The primary tenant (t0) can't access other tenants' (tN) configurations, so t0 relays don't have tN application control rulesets. (Other features like IPS don't have this consideration, because their rules come from Trend Micro, not a tenant.)

Other tenants (Tn) must create their own relay group, then select **Serve application control rulesets from relays**.




**Warning:**

Verify compatibility with your deployment before using relays. If the agent doesn't have any previously downloaded ruleset currently in effect, and **if it doesn't receive new application control rules, then the computer won't be protected by application control.** If application control ruleset download fails, a ruleset download failure event will be recorded on the manager and on the agent.

Relays might either change performance, break application control ruleset downloads, or be required; it varies by proxy location, multi-tenancy, and global/shared vs. local rulesets.

| Required for... | Faster performance for... | Slower performance for... | Don't enable for... |
|---|---|---|---|
| Agent > Proxy > Manager<br><br>**Note:** In Deep Security | Shared rulesets<br><br>Global ruleset | Local rulesets | Multi-tenant configurations when non-primary tenants (tN) use the default, primary (t0) relay group:<br><br>• Agent (tN) > DSR (t0) > DSM (tN)<br>• Agent (tN) > Proxy > DSR (t0) > DSM (tN) |

| Required for... | Faster performance for... | Slower performance for... | Don't enable for... |
| --- | --- | --- | --- |
| Agent 10.0 GM and earlier, agents didn't have support for connections through a proxy to relays. If a ruleset download fails due to a proxy, and if your agents require a proxy to access the relay or manager (including Deep | | | |

| Required for... | Faster performance for... | Slower performance for... | Don't enable for... |
|---|---|---|---|
| Security as a Service), then you must either:<br>• update agents' software, then configure the proxy<br>• bypass the proxy<br>• add a rela | | | |

| Required for... | Faster performance for... | Slower performance for... | Don't enable for... |
|---|---|---|---|
| y and then select **Serve application control rule sets from relays** | | | |

# Accelerate compliance

Trend Micro helps to accelerate compliance by consolidating multiple security controls into one product, while also delivering comprehensive auditing and reporting. For more information, see Regulatory Compliance on the Trend Micro website.

Depending on your requirements, see:

- "Meet PCI DSS requirements with Deep Security" on the next page
- "FIPS 140-2 support" on page 1049

- "Set up AWS Config Rules" on page 1059
- "Bypass vulnerability management scan traffic in Deep Security" on page 1060


## Meet PCI DSS requirements with Deep Security

Coalfire (a PCI auditor) has written a commissioned white paper that examines how Trend Micro Deep Security can be used to help secure Payment Card Industry (PCI) data in accordance with the PCI Data Security Standard (PCI DSS).

For more information, see the white paper Using Trend Micro's Hybrid Cloud Security Solution to Meet PCI DSS 3.2 Compliance.

> **Tip:** For tips on how to:
> - accelerate PCI DSS compliance in AWS, see Accelerating PCI Compliance in AWS using Deep Security.
> - enable TLS 1.2 for PCI compliance, see "Use TLS 1.2 with Deep Security" on page 1062.

Trend Micro Deep Security as a Service is now a PCI DSS Level 1 Service Provider! This means you can further streamline your PCI DSS certification process and take more items off of your to do list. For more information, see Trend Micro Deep Security as a Service Achieves PCI DSS Level 1 Certification.

## GDPR

The European Union's (EU) General Data Protection Regulation (GDPR) mandates that organizations anywhere in the world processing EU citizen data reassess their data processing controls and put a plan in place to better protect it. For information about GDPR and Trend Micro, see the Trend Micro GDPR Compliance site.

For information about personal data collection in Deep Security, see "Privacy and personal data collection disclosure" on page 56.

# FIPS 140-2 support

Federal Information Processing Standard (FIPS) is a set of standards for cryptographic modules. For in-depth information about FIPS, see the National Institute of Standards and Technology (NIST) website. Deep Security provides settings that enable cryptographic modules to run in a mode that is compliant with FIPS 140-2 standards. We have obtained certification for our Java crypto module and Native crypto module (OpenSSL).

There are some differences between a Deep Security deployment running in FIPS mode instead of non-FIPS mode (see "Differences when operating Deep Security in FIPS mode" on the next page).

**Tip:** If you intend to replace the Deep Security Manager SSL certificate, do so before enabling FIPS mode. If you need to replace the certificate after enabling FIPS mode, you will need to disable FIPS mode, follow the instructions in "Replace the Deep Security Manager SSL certificate" on page 756, and then re-enable FIPS mode.

To operate Deep Security in a FIPS 140-2 mode, you will need to:

1. Review "Differences when operating Deep Security in FIPS mode" on the next page to make sure the Deep Security features you require are available when operating in FIPS 140-2 mode.
2. Ensure that your Deep Security Manager and Deep Security Agents meet the "System requirements for FIPS mode" on page 1051.
3. "Enable FIPS mode for your Deep Security Manager" on page 1052.
4. If your Deep Security Manager needs to connect to an external service (such as an Active Directory, vCenter, or NSX Manager) using SSL, see "Connect to external services when in FIPS mode" on page 1053.
5. "Enable FIPS mode for the operating system of the computers you are protecting" on page 1053.
6. "Enable FIPS mode for the Deep Security Agent on the computers you are protecting" on page 1054
7. With some versions of the Linux kernel, you must enable Secure Boot to enable FIPS mode. See "Linux Secure Boot support for agents" on page 225 for instructions.

| Release | Kernel Version | Secure Boot Required |
|---|---|---|
| RHEL 7.4 | 3.10.0-693 | No |
| RHEL 7.3 | 3.10.0-514 | No |
| RHEL 7.2 | 3.10.0-327 | No |
| RHEL 7.1 | 3.10.0-229 | No |
| RHEL 7.0 GA | 3.10.0-123 | Yes |

This section also includes instructions on how to "Disable FIPS mode" on page 1059.

## Differences when operating Deep Security in FIPS mode

These Deep Security features are **not available** when operating in FIPS mode:

- Agentless protection, including connecting to an NSX Manager and settings related to the Deep Security Virtual Appliance
- Connecting to a Microsoft Azure account using the methods described in "Add a Microsoft Azure account to Deep Security" on page 311. Key Pair Generation for use with Azure is also not available with FIPS mode.
- Connecting to virtual machines hosted on VMware vCloud, as described in "Add virtual machines hosted on VMware vCloud" on page 318. The **Administration > System Settings > Agents > Agentless vCloud Protection** settings are also unavailable.
- Multi-tenant environment
- Load balancer settings (**Administration > System Settings > Advanced > Load Balancers**)
- Deep Security Scanner (integration with SAP Netweaver)
- The Connected Threat Defense feature
- Identity provider support via SAML 2.0
- When configuring SMTP settings, the STARTTLS option is not available.

# System requirements for FIPS mode

## Deep Security Manager requirements

The Deep Security Manager requirements with FIPS mode enabled are the same as those described in "System requirements" on page 69, with the following exceptions.

Only these operating systems are supported:

- Red Hat Enterprise Linux 7 (64bit)
- Windows Server 2016 (64-bit)
- Windows Server 2012 or 2012 R2 (64-bit)
- Windows Server 2008 or 2008 R2 (64-bit)

Only these databases are supported:

- PostgreSQL 9.6 (see "Using FIPS mode with a PostgreSQL database" on page 1054)
- Microsoft SQL Server 2016 Enterprise Edition (See "Using FIPS mode with a Microsoft SQL Server database" on page 1057)
- Microsoft SQL Server 2014 Enterprise Edition (See "Using FIPS mode with a Microsoft SQL Server database" on page 1057)
- Microsoft SQL Server 2012 Enterprise Edition (See "Using FIPS mode with a Microsoft SQL Server database" on page 1057)
- Microsoft SQL Server 2008 R2 Enterprise Edition (See "Using FIPS mode with a Microsoft SQL Server database" on page 1057)
- Microsoft SQL Server 2008 Enterprise Edition (See "Using FIPS mode with a Microsoft SQL Server database" on page 1057)

**Note:** Oracle Database is not supported, even if it has enabled FIPS mode for SSL connections.

**Note:** Microsoft SQL Server named pipes are not supported.

### Deep Security Agent requirements

The Deep Security Agent requirements with FIPS mode enabled are the same as those described in "System requirements" on page 69, except that only these operating systems are supported:

- Windows Server 2016 (64-bit)
- Windows Server 2012 or 2012 R2 (64-bit)
- Windows Server 2008 or 2008 R2 (64-bit)
- Windows 10 (64-bit)
- Windows 8 (64-bit)
- Windows 7 (64-bit)
- Red Hat Enterprise Linux 7 (64bit)
- CentOS 7 (64-bit)

## Enable FIPS mode for your Deep Security Manager

### Enable FIPS mode for a Deep Security Manager on Windows

1. Use the Services window of the Microsoft Management Console to stop the "Trend Micro Deep Security Manager" service.
2. In the Windows command line, go to the Deep Security Manager's working folder, for example, `C:\Program Files\Trend Micro\Deep Security Manager`.
3. Enter this command to enable FIPS mode:

   ```
   dsm_c -action enablefipsmode
   ```

4. Restart the Deep Security Manager service.

### Enable FIPS mode for a Deep Security Manager on Linux

1. On the Deep Security Manager computer, open a command line and go to the Deep Security Manager's working folder, for example, `/opt/dsm`.
2. Enter this command to stop the Deep Security Manager service:

   ```
   service dsm_s stop
   ```

3. Enter this command to enable FIPS mode:

   ```
   dsm_c -action enablefipsmode
   ```

4. Enter this command to restart the Deep Security Manager service:

   ```
   service dsm_s start
   ```

## Connect to external services when in FIPS mode

When Deep Security Manager is operating in FIPS mode and you want to connect to an external service (such as an Active Directory, vCenter, or NSX Manager) with an SSL connection, you must import the SSL certificate for that external service into the manager before connecting to it. For instructions on how to import the certificate, see "Manage trusted certificates" on page 216.

For instructions on importing computers from an Active Directory, see "Add computer groups from Microsoft Active Directory" on page 321.

For instructions on synchronizing user information with an Active Directory, see "Create and manage users" on page 989.

For instructions on adding a VMware vCenter to Deep Security Manager, see Add a vCenter when Deep Security Manager is in FIPS mode.

## Enable FIPS mode for the operating system of the computers you are protecting

For instructions on enabling FIPS mode on Windows 7, please refer to the Microsoft Support site: System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" security setting effects in Windows XP and in later versions of Windows.

For instructions on enabling FIPS mode on RHEL 7 or CentOS 7, please refer to Red Hat documentation: Federal Standards and Regulations and How can I make RHEL 6 or RHEL 7 FIPS 140-2 compliant.

## Enable FIPS mode for the Deep Security Agent on the computers you are protecting

**Note:** This step is not required for new Deep Security 11.0 or higher agents that you install after enabling FIPS mode in Deep Security Manager. In that situation, FIPS mode is already enabled for the agent.

### Enable FIPS mode for a Windows 7 agent

1. In the Windows system root folder (for example, `C:\Windows`), look for a file named `ds_agent.ini`. Open the file in a text editor or create a new file if you don't have one already.
2. Add this line to the file:

   ```
   FIPSMode=1
   ```

3. Restart the Deep Security Agent service.

### Enable FIPS mode for an RHEL 7 or CentOS 7 agent

1. In the `/etc/`), look for a file named `ds_agent.conf`. Open the file in a text editor or create a new file if you don't have one already.
2. Add this line to the file:

   ```
   FIPSMode=1
   ```

3. Restart the Deep Security Agent:

   ```
   /etc/init.d/ds_agent restart
   ```

## Using FIPS mode with a PostgreSQL database

If you are using PostgreSQL as your Deep Security Manager database, there are some extra requirements in addition to those outlined in "Prepare a database for Deep Security Manager on AWS" on page 114.

In FIPS mode, the keystore must be the BCFKS type. Instead of converting the java default keystore (`C:\Program Files\Trend Micro\Deep Security Manager\jre\lib\security\cacerts` or `/opt/dsm/jre/lib/security/cacerts`) directly, copy the default keystore to another location and use it as the default keystore for SSL connection.

1. Create the PostgreSQL environment
2. Copy the "`server.crt`" file from the PostgreSQL server and paste them into `<Deep Security Manager install folder>`.
3. Install Deep Security Manager.
4. "Enable FIPS mode for your Deep Security Manager" on page 1052.
5. Copy the default Java cacerts file into the Deep Security Manager root installation folder.

   On Windows:

   ```
   copy "C:\Program Files\Trend Micro\Deep Security Manager\jre\lib\security\cacerts" "C:\Program Files\Trend Micro\Deep Security Manager\cacerts"
   ```

   On Linux:

   ```
   cp "/opt/dsm/jre/lib/security/cacerts" "/opt/dsm/cacerts"
   ```

6. Convert the keystore file from JKS to BCFKS. The following command will create a cacerts.bcfks file in the Deep Security Manager installation folder:

   On Windows:

   ```
   cd C:\Program Files\Trend Micro\Deep Security Manager\jre\bin
   ```

   ```
   keytool -importkeystore -srckeystore "C:\Program Files\Trend Micro\Deep Security Manager\cacerts" -srcstoretype JKS -deststoretype BCFKS -destkeystore "C:\Program Files\Trend Micro\Deep Security Manager\cacerts.bcfks" -srcstorepass <changeit> -deststorepass <changeit> -providerpath "C:\Program Files\Trend Micro\Deep Security Manager\jre\lib\ext\ccj-3.0.0.jar" -providerclass com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider
   ```

   On Linux:

   ```
   cd /opt/dsm/jre/bin
   ```

   ```
   keytool -importkeystore -srckeystore "/opt/dsm/cacerts" -srcstoretype JKS -deststoretype BCFKS -destkeystore "/opt/dsm/cacerts.bcfks" -srcstorepass <changeit> -deststorepass <changeit> -providerpath "/opt/dsm/jre/lib/ext/ccj-3.0.0.jar" -providerclass com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider
   ```

7. Import the certificate ("`Deep Security Manager root folder/server.crt`"):

   On Windows:

   ```
   cd C:\Program Files\Trend Micro\Deep Security Manager\jre\bin
   ```

   ```
   keytool -import -alias psql -file "C:\Program Files\Trend Micro\Deep Security Manager\server.crt" -keystore "C:\Program Files\Trend Micro\Deep Security Manager\cacerts.bcfks" -storepass <changeit> -provider com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider -providerpath "C:\Program Files\Trend Micro\Deep Security Manager\jre\lib\ext\ccj-3.0.0.jar" -storetype BCFKS
   ```

   On Linux:

   ```
   cd /opt/dsm/jre/bin
   ```

   ```
   keytool -import -alias psql -file "/opt/dsm/server.crt" -keystore "/opt/dsm/cacerts.bcfks" -storepass <changeit> -provider com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider -providerpath "/opt/dsm/jre/lib/ext/ccj-3.0.0.jar" -storetype BCFKS
   ```

8. The Deep Security installer can use a `.vmoptions` file to assign the JVM parameter:

   On Windows, create a file named `Deep Security Manager.vmoptions` in the installation folder and add the following text in the file:-Djavax.net.ssl.keyStoreProvider=CCJ

   ```
   -Djavax.net.ssl.trustStore=C:\Program Files\Trend Micro\Deep Security Manager\cacerts.bcfks
   ```

   ```
   -Djavax.net.ssl.trustStorePassword=<changeit>
   ```

   ```
   -Djavax.net.ssl.keyStoreType=BCFKS
   ```

   ```
   -Djavax.net.ssl.trustStoreType=BCFKS
   ```

   On Linux, create a file named `dsm_s.vmoptions` in the installation folder and add the following text in the file:

   ```
   -Djavax.net.ssl.keyStoreProvider=CCJ
   ```

   ```
   -Djavax.net.ssl.trustStore=/opt/dsm/cacerts.bcfks
   ```

   ```
   -Djavax.net.ssl.trustStorePassword=<changeit>
   ```

```
-Djavax.net.ssl.keyStoreType=BCFKS
```

```
-Djavax.net.ssl.trustStoreType=BCFKS
```

9. Open the `<Deep Security Manager directory>\webclient\webapps\ROOT\WEB-INF\dsm.properties` file in a text editor and add:

```
database.PostgreSQL.connectionParameters=ssl=true
```

10. Open the `/opt/postgresql/data/postgresql.conf` file in a text editor and add:

```
ssl= on
```

```
ssl_cert_file= 'server.crt'
```

```
ssl_ksy_file= 'server.key'
```

11. Restart PostgreSQL and then restart the Deep Security Manager service.
12. Check the connection:

```
cd /opt/postgresql/bin
```

```
./psql -h 127.0.0.1 -Udsm dsm
```

Enter the password when prompted. You should see:

```
dsm=> select a.client_addr, a.application_name, a.usename, s.* from pg_stat_
ssl s join pg_stat_activity a using (pid) where a.datname='dsm';
```

## Using FIPS mode with a Microsoft SQL Server database

If you are using Microsoft SQL Server as your Deep Security Manager database, you must set up the database SSL encryption using the instructions below **before** enabling FIPS mode.

1. Stop the Deep Security Manager service.
2. Create a BCFKS keystore file with the SQL server certificate. You can use the keytool in `C:\Program Files\Trend Micro\Deep Security Manager\jre\bin`.
3. Use the following command to import the SQL server certificate (`C:\sqlserver_cert.cer`) to a new keystore file (`C:\Program Files\Trend Micro\Deep Security Manager\mssql_keystore.bcfks`):

> **Note:** If the Deep Security Manager package doesn't contain a `ccj-3.0.0.jar` file, get the jar file from the FIPS page.

```
keytool -import -alias mssql -file "C:\sqlserver_cert.cer" -keystore "C:\Program Files\Trend Micro\Deep Security Manager\mssql_keystore.bcfks" -storepass <changeit> -provider com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider -providerpath "C:\Program Files\Trend Micro\Deep Security Manager\jre\lib\ext\ccj-3.0.0.jar" -storetype BCFKS
```

During the import process, answer "YES" to trust this certificate.

4. If the keystore file is created successfully, you will be able to use the following command to list see the certificate listed in the keystore:

```
keytool -list -v -keystore "C:\Program Files\Trend Micro\Deep Security Manager\mssql_keystore.bcfks" -provider com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider -providerpath "C:\Program Files\Trend Micro\Deep Security Manager\jre\lib\ext\ccj-3.0.0.jar" -storetype BCFKS -storepass <changeit>
```

5. Open the `C:\Program Files\Trend Micro\Deep Security Manager\webclient\webapps\ROOT\WEB-INF\dsm.properties` file in a text editor and add the following lines enable SSL/TLS and FIPS settings:

```
database.SqlServer.encrypt=true
```

```
database.SqlServer.trustServerCertificate=false
```

```
database.SqlServer.fips=true
```

```
database.SqlServer.trustStorePassword=<changeit>
```

```
database.SqlServer.fipsProvider=CCJ
```

```
database.SqlServer.trustStoreType=BCFKS
```

```
database.SqlServer.trustStore=C\:\\Program Files\\Trend Micro\\Deep Security Manager\\mssql_keystore.bcfks
```

6. Optionally, you can also change the SQL server/client connection protocols from Named Pipes to TCP/IP. This will allow for FIPS support after upgrading to Deep Security 10.2:
   a. In the SQL Server Configuration Manager, go to **SQL Network Configuration > Protocols for MSSQLSERVER** and enable **TCP/IP**.
   b. Go to **SQL Native Client 11.0 Configuration > Client Protocols** and enable **TCP/IP**.

c. Follow the instruction provided by Microsoft to enable encrypted connections for an instance of the SQL Server database. See Enable Encrypted Connections to the Database Engine.
d. Edit the `dsm.properties` file to change `database.sqldserver. driver=MSJDBC` and `database.SqlServer.namedPipe=false`.

7. Restart the Deep Security Manager service.
8. "Enable FIPS mode for your Deep Security Manager" on page 1052.

## Disable FIPS mode

1. To disable FIPS mode for the Deep Security Manager, follow the instructions that you used to enable it (see "Enable FIPS mode for your Deep Security Manager" on page 1052), but use this command in place of step 3:

   ```
   dsm_c -action disablefipsmode
   ```

2. To disable FIPS mode for the Deep Security Agent, follow the instructions that you used to enable it (see "Enable FIPS mode for the Deep Security Agent on the computers you are protecting" on page 1054), but instead of `FIPSMode=1`, use `FIPSMode=0`.

# Set up AWS Config Rules

Deep Security supports the use of AWS Config Rules to query the status of your AWS instances. This can be especially useful if you want to have a centralized view into whether your instances meet certain compliance requirements.

There are four Lambda functions available from the Deep Security AWS Config Rules Repository on GitHub:

- **ds-IsInstanceProtectedByAntiMalware** checks whether the current instance is protected by the Deep Security anti-malware module.
- **ds-IsInstanceProtectedBy** checks whether the current instance is protected by any of the Deep Security protection modules. This is a generic version of ds-IsInstanceProtectedByAntiMalware.
- **ds-DoesInstanceHavePolicy** checks whether the current instance is protected by a specific Deep Security policy.

- **ds-IsInstanceClear** checks whether the current instance has any warnings, alerts, or errors in Deep Security.

For more information about using AWS Config Rules with Deep Security, including a helpful video that walks you through the process of setting up a rule, see Deploying AWS Config Rules for Deep Security. For more information about AWS Config, see the AWS Config section of the Amazon AWS website.

## Bypass vulnerability management scan traffic in Deep Security

If you are using a vulnerability management provider such as Qualys or Nessus (for PCI compliance, for example), you need to set up Deep Security to bypass or allow this provider's scan traffic through untouched.


- "Create a new IP list from the vulnerability scan provider IP range or addresses" below
- "Create firewall rules for incoming and outbound scan traffic" on the next page
- "Assign the new firewall rules to a policy to bypass vulnerability scans" on page 1062


After these firewall rules have been assigned to the new policy, the Deep Security Manager will ignore ANY traffic from the IPs you have added in your IP List.

Deep Security will not scan the vulnerability management provider traffic for stateful issues or vulnerabilities - it will be allowed through untouched.

### Create a new IP list from the vulnerability scan provider IP range or addresses

Have handy the IP addresses that the vulnerability scan provider has given you.

1. In the Deep Security Manager, go to **Policies**.
2. In the left pane, expand **Lists** > **IP Lists**.
3. Click **New** > **New IP List**.
4. Type a **Name** for the new IP List, for example "Qualys IP list".
5. Paste the IP addresses that the vulnerability management provider has given you into the **IP(s)** box, one per line.
6. Click **OK**.

## Create firewall rules for incoming and outbound scan traffic

After you've created the IP list, you need to create two firewall rules: one for incoming and one for outgoing traffic.

Name them as suggested, below:

```
<name of provider> Vulnerability Traffic - Incoming

<name of provider> Vulnerability Traffic - Outgoing
```

1. In the main menu, click **Policies**.
2. In the left pane, expand **Rules**.
3. Click **Firewall Rules** > **New** > **New Firewall Rule**.
4. Create the first rule to bypass Inbound AND Outbound for TCP and UDP connections that are incoming to and outgoing from vulnerability management provider.

   *Tip: For settings not specified, you can leave them as the default.*

   **Name**: (suggested) <name of provider> Vulnerability Traffic - Incoming

   **Action**: Bypass

   **Protocol**: Any

   **Packet Source**: IP List and then select the new IP list created above.

5. Create a second rule:

   **Name:** <name of provider> Vulnerability Traffic - Outgoing

   **Action:** Bypass

   **Protocol:** Any

   **Packet Destination**: IP List and then select the new IP list created above.

## Assign the new firewall rules to a policy to bypass vulnerability scans

Identify which policies are already used by computers that will be scanned by the vulnerability management provider.

Edit the policies individually to assign the rules in the firewall module.

1. Click **Policies** on the main menu.
2. Click **Policies** in the left pane.
3. In the right pane, for each policy, double-click to open the policy details.
4. In the pop-up, in the left pane, click **Firewall**.
5. Under **Assigned Firewall Rules**, click **Assign/Unassign**.
6. Ensure your view at the top-left shows **All** firewall rules in the .
7. Use the search window to find the rules you created and select them.
8. Click **OK**.

# Use TLS 1.2 with Deep Security

In Deep Security Manager 11.1 and higher, TLS 1.2 is enforced by default for new installations.

Review the table below to determine whether you need to take action.

| If you are doing... | And your deployment includes... | Do this... |
|---|---|---|
| A new installation of Deep Security Manager 11.1+ | Only 10.0+ Deep Security Agents, Relays, and Virtual Appliances | Nothing.<br><br>By default, TLS 1.2 is used between all components and enforced on the manager and relays. |
| | Pre-10.0 Deep Security Agents, Relays, or | (Recommended.) Upgrade all of your components to 10.0+ versions which support TLS 1.2. See "Upgrade components to use TLS 1.2" on page 1069. This is the best option to increase |

| If you are doing... | And your deployment includes... | Do this... |
|---|---|---|
| | Virtual Appliances | the security of your deployment.<br><br>Alternatively, you can re-enable TLS 1.0 to ensure backward compatibility with older components. See "Re-enable early TLS (1.0)" on page 1075. |
| An upgrade to Deep Security Manager 11.1+ | Only 10.0+ Deep Security Agents, Relays, or Virtual Appliances | (Recommended.) Enable TLS 1.2 enforcement to increase the security of your deployment. See "Enforce TLS 1.2" on page 1071.<br><br>Alternatively, you can do nothing. Whatever your TLS settings were in your previous deployment are preserved. If you had enforced TLS 1.2 before, then your enforcement settings are preserved after the upgrade. Conversely, if you had disabled enforcement, then those settings are preserved as well. |
| | Pre-10.0 Deep Security Agents, Relays, or Virtual Appliances | (Recommended.) Although no immediate action is required, you should plan to upgrade older components to 10.0+ which support TLS 1.2, and then enforce TLS 1.2. See "Upgrade components to use TLS 1.2" on page 1069 and "Enforce TLS 1.2" on page 1071. This is the best option to increase the security of your deployment.<br><br>Alternatively, you can do nothing. Whatever your TLS settings were in your previous deployment are preserved. If TLS 1.0 was allowed before, then it will also be allowed after the upgrade. |

Topics on this page:


- "Benefits of TLS 1.2" below
- "TLS 1.2 architectures" below

- "Upgrade components to use TLS 1.2" on page 1069
- "Enforce TLS 1.2" on page 1071
- "Re-enable early TLS (1.0)" on page 1075
- "Determine whether TLS 1.2 is enforced" on page 1076
- "Guidelines for deploying agents, and relays after TLS 1.2 is enforced" on page 1077


## Benefits of TLS 1.2

Transport Layer Security (TLS), and the earlier Secure Sockets Layer (SSL), are encryption protocols that enable secure connections between different endpoints. When Deep Security components need to communicate, they determine the latest mutually-supported version of the encryption protocol and then use that version to secure all communication for the duration of their session. The latest version of TLS is 1.2. SSL has been discontinued due to security issues.

Trend Micro strongly recommends that you use TLS 1.2 communication between all its components. This page describes the benefits of TLS 1.2, and how to use and enforce it in your Deep Security environment.

The main benefits of TLS 1.2 are:

- **additional security**. TLS 1.2 has been enhanced to safeguard against the latest exploits.
- **PCI compliance**. The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard that promotes the safety of cardholder data. To be PCI-compliant, organizations must disable Secure Sockets Layer (SSL) and early TLS on applicable connections. For more information on PCI compliance, see "Meet PCI DSS requirements with Deep Security" on page 1048.

## TLS 1.2 architectures

The diagrams below show the TLS communication in the Deep Security architecture.

Figure 1 shows the TLS communication when TLS 1.2 *is* enforced (This is the default for new 11.1+ Deep Security Manager installations.) You can see that the 9.6 agents can no longer communicate with Deep Security Manager, and neither can older third-party applications.

Figure 2 shows the TLS communication when TLS 1.2 is *not* enforced. You can see that 10.0 or higher agents communicate with Deep Security Manager over TLS 1.2, while 9.6 versions communicate over early TLS. Similarly, newer third-party applications use TLS 1.2, while older ones use early TLS.

**Figure 1: TLS 1.2 is enforced**

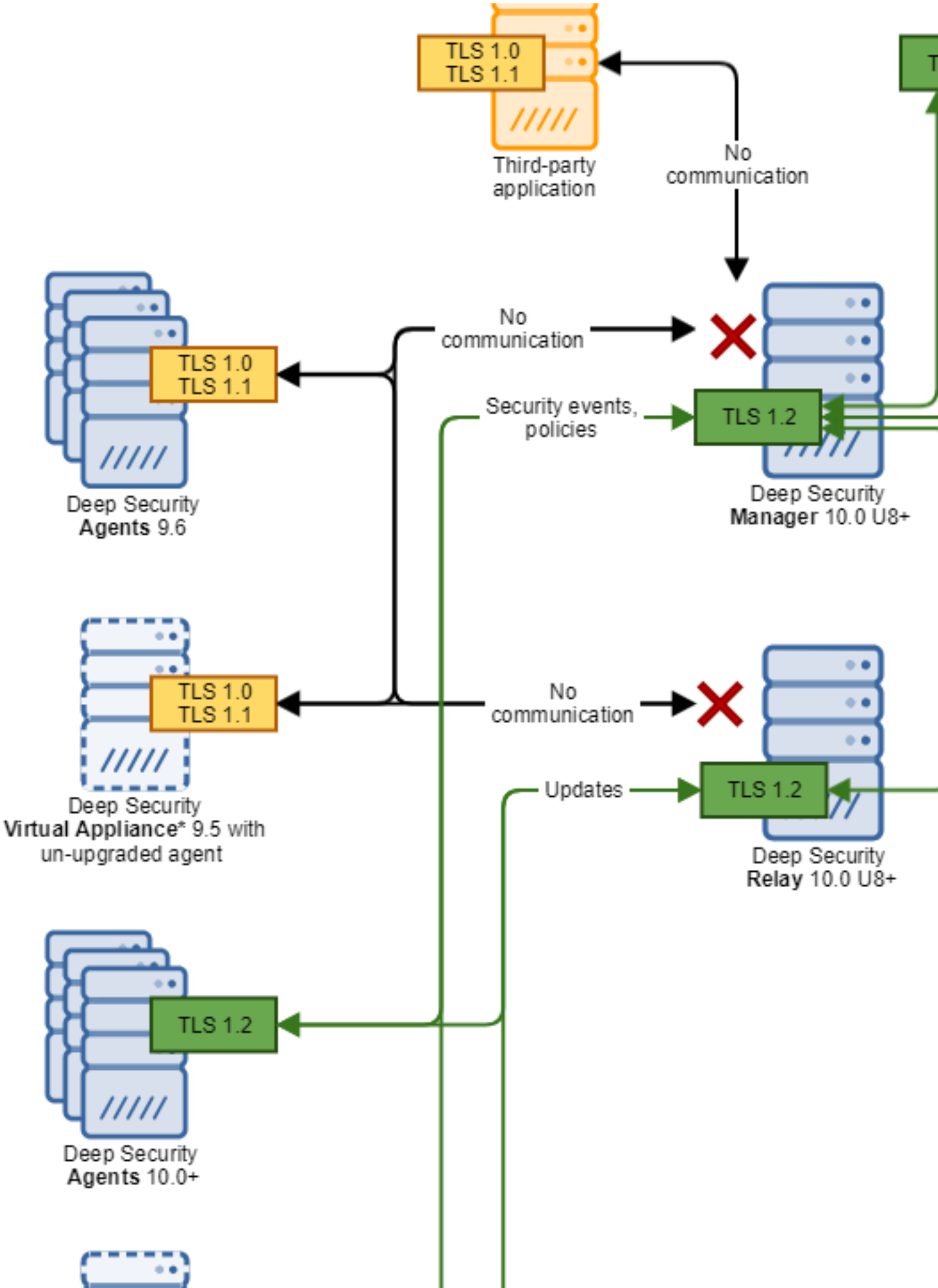
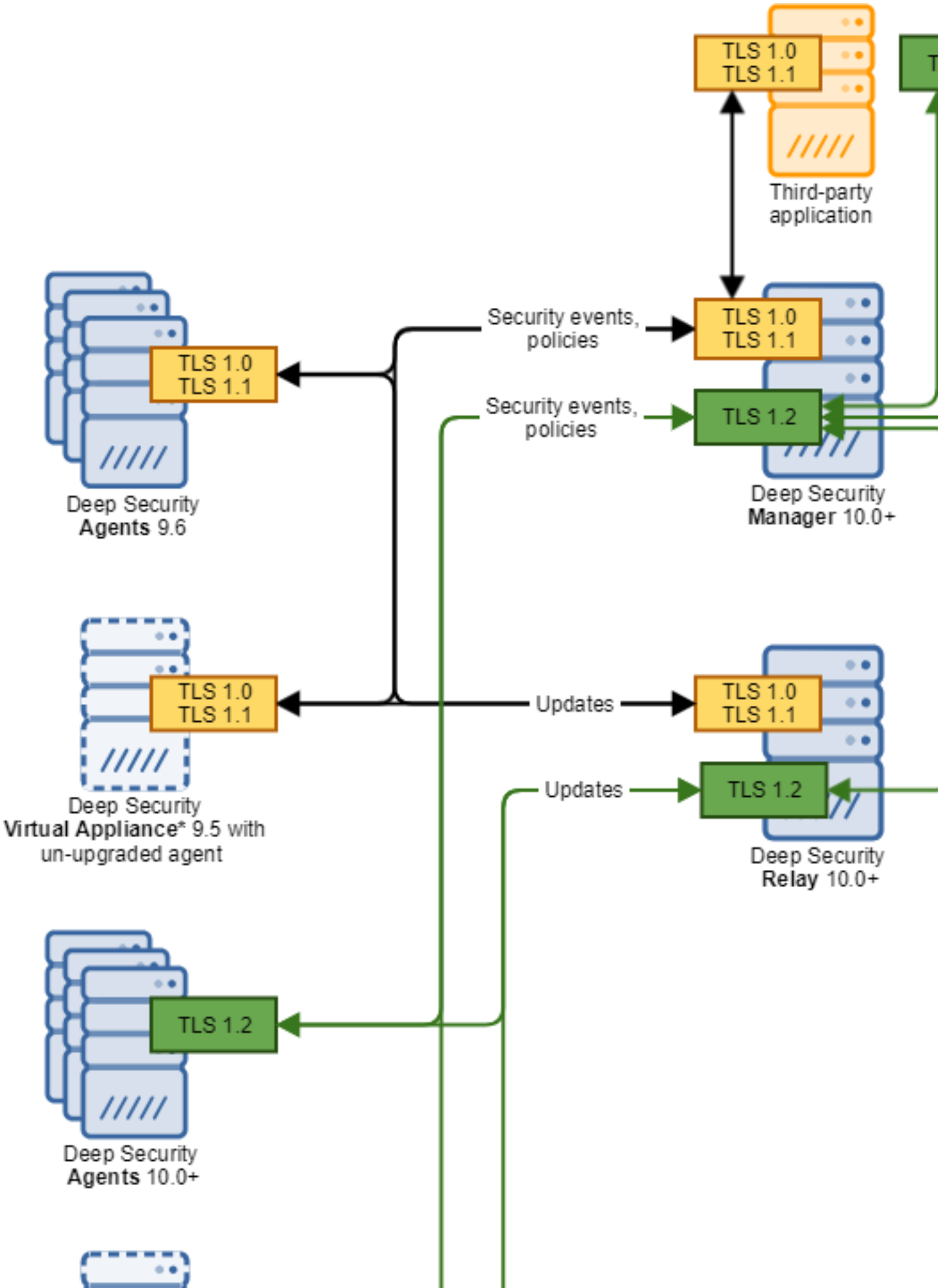

TLS 1.0
TLS 1.1
Third-party application
No communication
No communication
Security events, policies
TLS 1.2
Deep Security Manager 10.0 U8+
TLS 1.0
TLS 1.1
Deep Security Agents 9.6
TLS 1.0
TLS 1.1
Deep Security Virtual Appliance* 9.5 with un-upgraded agent
No communication
Updates
TLS 1.2
Deep Security Relay 10.0 U8+
TLS 1.2
Deep Security Agents 10.0+

Figure 2: TLS 1.2 is *not* enforced


TLS 1.0
TLS 1.1
Third-party application
Security events, policies
TLS 1.0
TLS 1.1
Security events, policies
TLS 1.2
Deep Security Manager 10.0+
TLS 1.0
TLS 1.1
Deep Security Agents 9.6
TLS 1.0
TLS 1.1
Updates
TLS 1.0
TLS 1.1
Updates
TLS 1.2
Deep Security Virtual Appliance* 9.5 with un-upgraded agent
Deep Security Relay 10.0+
TLS 1.2
Deep Security Agents 10.0+

# Upgrade components to use TLS 1.2

If you want your Deep Security components to use TLS 1.2, but do not necessarily want to enforce TLS 1.2, all you need to do is make sure that each component supports TLS 1.2. When two components support TLS 1.2, they automatically use TLS 1.2 to communicate. If one component does not support TLS 1.2 and another does, then they negotiate an earlier version of TLS.

Follow the instructions below to verify that your Deep Security components support TLS 1.2 and upgrade them if needed.

**Note:** If you want to *enforce* TLS 1.2 and prevent the use of early TLS, see instead "Enforce TLS 1.2" on page 1071.

## Verify and upgrade your Deep Security Manager

- Make sure you're using one of the following versions of Deep Security Manager, and if not, upgrade it:
  - Use Deep Security Manager 10.0 *update 8* or later if you're planning to "Enforce TLS 1.2" on page 1071 on the manager. Only 10.0 update 8 and later managers support TLS 1.2 enforcement.
  - Using Deep Security Manager 10.0 or later if you're *not* planning to "Enforce TLS 1.2" on page 1071 on the manager. Only 10.0 and later managers support TLS 1.2 communication.
- For upgrade instructions, see "Upgrade the Deep Security Manager AMI" on page 740.

## Verify your Deep Security Manager database

- If you're using Microsoft SQL Server as your Deep Security Manager database, make sure the database supports TLS 1.2, and if not, upgrade it. See this Microsoft article for guidance.
- If you're using a PostgrSQL database, it supports TLS 1.2 so no action is necessary.
- If you're using an Oracle database, only Oracle's native encryption is supported for database-manager communication, not TLS, so no action is necessary.

- By default, there is no encryption between the database (SQL Server, PostgreSQL, or Oracle) and Deep Security Manager. You can enable it manually.

## Verify your Deep Security Agents

- If you have existing Deep Security Agents, make sure they're at version 10.0 or higher. Only 10.0 or higher agents support TLS 1.2.

**Note:** If some agents are left un-upgraded (that is, they are pre-10.0), those agents communicate over early TLS, and you may need to re-enable early TLS. For details, see "Re-enable early TLS (1.0)" on page 1075.

To upgrade your agents:

1. Import the latest Deep Security Agent software into Deep Security Manager, either manually or automatically. See "Update the Deep Security Agent" on page 738 for details.
2. Upgrade your Deep Security Agents:
   - To automatically upgrade an agent, see "Initiate an agent update" on page 739.

## Verify your Deep Security Relays

- Make sure you're using one of the following versions of Deep Security Relay, and if not, upgrade it:
  - Use Deep Security Relay 10.0 *update 8* or later if you're planning to "Enforce TLS 1.2" on the next page on the relay. Only 10.0 update 8 and higher relays support TLS 1.2 enforcement.
  - Use Deep Security Relay 10.0 or later if you're *not* planning to "Enforce TLS 1.2" on the next page on the relay. Only 10.0 and higher relays support TLS 1.2 communication.

To upgrade a relay, follow the same process as upgrading an agent:

1. Import the latest Deep Security Relay software into Deep Security Manager, either manually or automatically. See "Update the Deep Security Agent" on

page 738 for details.

2. Upgrade the relay:

   - To automatically upgrade a relay, see "Initiate an agent update" on page 739.

## Enforce TLS 1.2

Topics in this section:


- "Where can TLS 1.2 be enforced?" below
- "What happens when TLS 1.2 enforced?" below
- "Is TLS 1.2 enforced by default?" on the next page
- "Under what circumstances is TLS 1.2 enforcement possible? " on the next page
- "Enforce TLS 1.2 on Deep Security Manager" on the next page
- "Enforce TLS 1.2 on the Deep Security Relay" on page 1073
- "Enforce TLS 1.2 on just the manager's GUI port (4119)" on page 1073
- "Test that TLS 1.2 is enforced" on page 1074


### Where can TLS 1.2 be enforced?

There are two enforcement points:

- on the Deep Security Manager
- on the Deep Security Relays

### What happens when TLS 1.2 enforced?

When TLS 1.2 is enforced, the manager and relays stop accepting early TLS connections, and any applications that try to use early TLS are denied access and cease to function properly.

If you choose *not* to enforce TLS 1.2, the manager and relays still accept early TLS as well as TLS 1.2 connections. This means that both older and newer applications are able to connect.

## Is TLS 1.2 enforced by default?

- If you have a new installation of Deep Security Manager 11.1+ (not an upgrade), TLS 1.2 is enforced by default.
- If you are upgrading an existing Deep Security Manager to 11.1 or higher, then your existing TLS settings are preserved, so if TLS was not enforced previously, it will continue to not be enforced after the upgrade. Conversely, if it was enforced, it will continue to be enforced.

## Under what circumstances is TLS 1.2 enforcement possible?

You can only enforce TLS 1.2 if *all* Deep Security Agents have been upgraded to 10.0+, which is the version at which TLS 1.2 is supported.

## Enforce TLS 1.2 on Deep Security Manager

1. Before you begin:
   - Make sure that Deep Security Manager is at version *10.0 Update 8* or higher. You need this version to enforce TLS 1.2.
   - Make sure that all other components support TLS 1.2. See "Upgrade components to use TLS 1.2" on page 1069.
2. On the Deep Security Manager computer, run this dsm_c command:

   ```
   dsm_c -action settlsprotocol -MinimumTLSProtocol ShowValue
   ```

   A TLS version appears. This is the minimum TLS version that Deep Security Manager currently accepts.

3. Run this `dsm_c` command:

   ```
   dsm_c -action settlsprotocol -MinimumTLSProtocol TLSv1.2
   ```

   This command sets the minimum TLS version to 1.2. Deep Security Manager now accepts TLS 1.2 connections and disallows TLS 1.0 connections.

   The Deep Security Manager service is restarted automatically.

## Enforce TLS 1.2 on the Deep Security Relay

1. Before you begin:
   - Make sure that Deep Security Relay is at version *10.0 Update 8* or higher. You need this version to enforce TLS 1.2.
   - Make sure that all your components support TLS 1.2. See "Upgrade components to use TLS 1.2" on page 1069.
   - Make sure that you have enforced TLS 1.2 on Deep Security Manager.
2. Resend the policies associated with your relays:
   a. In Deep Security Manager, click **Computers** and find one of your relays in the list of computers. If you're not sure which ones are your relays, at the top, click **Administration**. On the left, expand **Updates** and then click **Relay Management**. In the main pane, expand a relay group to see your relays.
   b. Double-click the relay in the list of computers.
   c. In the main pane, click the **Actions** tab.
   d. Click **Send Policy** to resend the policy.
   e. Resend the policy to each of your relays.

## Enforce TLS 1.2 on just the manager's GUI port (4119)

Only read this section if you were unable to do a full enforcement on the Deep Security Manager and Relays as described previously in "Enforce TLS 1.2 on Deep Security Manager" on the previous page and "Enforce TLS 1.2 on the Deep Security Relay" above.

This section describes how to set the minimum TLS version to TLS 1.2 on port 4119. Applications that connect on port 4119 are typically web browsers and REST or SOAP API clients. Older Deep Security components that do not support TLS 1.2 can continue to connect to the manager (on port 4120, by default) using TLS 1.0.

1. On Deep Security Manager, enable TLS 1.0 by running this dsm_c command:

   ```
   dsm_c -action settlsprotocol -MinimumTLSProtocol TLSv1
   ```

   Deep Security Manager now accepts TLS 1.0 connections from older agents and applications.

2. Disable early TLS on the manager's GUI port (4119) (it is possible that it's already disabled):
   a. Open the `configuration.properties` file in the root of the Deep Security Manager installation directory.
   b. Under `serviceName=`, look for the `protocols=` setting.

      This setting defines the protocols that can be used to connect to Deep Security Manager when it is acting as a server to web browsers and REST or SOAP API clients.

   c. If the `protocols=` setting is present, remove it so that only TLS 1.2 is allowed on port 4119.
   d. Save the file.
3. Restart the Deep Security Manager service.

## Test that TLS 1.2 is enforced

1. On a Deep Security component where early TLS 1.2 is enforced, run the following nmap command:

   ```
   nmap --script ssl-enum-ciphers <ds_host> -p <ds_port> -Pn
   ```

   where:
   - `<ds_host>` is replaced with the IP address or hostname of the manager or relay
   - `<ds_port>` is replaced with the listening port where TLS is being used (4119 for manager, 4122 for the relay, and 4118 for the agent–if manager-initiated activation is used)

   The response should only list TLS 1.2. Example response:

   ```
   PORT STATE SERVICE
   443/tcp open https
   | ssl-enum-ciphers:
   | | TLSv1.2:
   | ciphers:
   | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
   ```

```
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
| TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
| TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
| TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
| TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
| TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
| compressors:
```

## Re-enable early TLS (1.0)

You'll need to re-enable early TLS (1.0) if you have a *new* installation of Deep Security Manager 11.1+ (not an upgrade) and:

- you are using pre-10.0 agents. These only support early TLS. Go here to see if a 10.0+ agent is available for your OSs.
- you are using third-party components that are older and need to use early TLS to communicate with Deep Security Manager.
- you are using a 9.5 version of the Deep Security Virtual Appliance with an un-upgraded embedded agent.

To re-enable early TLS (1.0), follow the instructions below.

### Re-enable TLS 1.0 on Deep Security Manager and the Deep Security Relay

1. On the Deep Security Manager computer, run this dsm_c command:

   ```
   dsm_c -action settlsprotocol -MinimumTLSProtocol ShowValue
   ```

A TLS version appears. This is the minimum TLS version that Deep Security Manager currently accepts.

2. Run this `dsm_c` command:

   ```
   dsm_c -action settlsprotocol -MinimumTLSProtocol TLSv1
   ```

   This command sets the minimum TLS version to 1.0.

   TLS 1.0 is now re-enabled on your Deep Security Manager.

   The Deep Security Manager service is restarted automatically.

3. Resend the policies associated with your relays:
   a. In Deep Security Manager, click **Computers** and find one of your relays in the list of computers. If you're not sure which ones are your relays, at the top, click **Administration**On the left, expand **Updates** and then click **Relay Management**. In the main pane, expand a relay group to see your relays.
   b. Double-click the relay in the list of computers.
   c. In the main pane, click the **Actions** tab.
   d. Click **Send Policy** to resend the policy.
   e. Resend the policy to each of your relays.

   TLS 1.0 is now re-enabled on your relays.

### Re-enable TLS 1.0 on the manager's GUI port (4119)

Read this section if you previously enforced TLS 1.2 only on the manager's GUI port (4119) and now want to re-enable TLS 1.0 on this port.

1. Follow the instructions in Re-enabled TLS 1.0 on Deep Security Manager. This re-enables TLS 1.0 on the GUI port (4119).

## Determine whether TLS 1.2 is enforced

If you're not sure whether TLS 1.2 is enforced on Deep Security Manager, follow the instructions below to find out.

1. On the Deep Security Manager computer, open a command prompt and run the following dsm_c command:

```
dsm_c -action settlsprotocol -MinimumTLSProtocol ShowValue
```

The minimum TLS protocol accepted by the manager is displayed. If it shows TLS 1.2, then TLS 1.2 is enforced. If it shows TLS 1.0, then early TLS is allowed and TLS 1.2 is not enforced.

Determining whether TLS 1.2 is enforced on the relay is harder. If you pushed out your TLS settings to the relay through policy according to "Enforce TLS 1.2 on the Deep Security Relay" on page 1073 or "Re-enable TLS 1.0 on Deep Security Manager and the Deep Security Relay" on page 1075, then those TLS settings apply to the relay. If you did not push out TLS settings through policy, then the relay's default TLS settings apply. The relay's default settings depend on its version: if you're using an 11.1+ relay, then TLS 1.2 is enforced by default. For pre-11.1 relays, TLS 1.2 is not enforced by default.

## Guidelines for deploying agents, and relays after TLS 1.2 is enforced

This section discusses special considerations when deploying agents and relays when TLS 1.2 is enforced. If you re-enabled early TLS (1.0), then there are no special considerations, and you do not need to read this section.

Topics in this section:

- "Guidelines for deploying agents, and relays when TLS 1.2 is enforced" below
- "Guidelines for using deployment scripts when TLS 1.2 is enforced" below

### Guidelines for deploying agents, and relays when TLS 1.2 is enforced

- You must deploy 10.0+ agents, and relays. Only 10.0+ agents and relays support TLS 1.2.
- If you need to deploy a 9.6 or earlier agent or relay you must re-enable early TLS (1.0) wherever it was enforced (either on the manager, on the relay, or on the manager's GUI port 4119).

### Guidelines for using deployment scripts when TLS 1.2 is enforced

If TLS 1.2 is enforced, you can install 10.0+ agents and relays using deployment scripts. Below are some guidelines to ensure the deployment scripts work:

1. If you are deploying an agent or relay onto Windows computers, use PowerShell 4.0 or higher, which supports TLS 1.2.
2. If you are deploying onto Windows XP, 2003, or 2008, where PowerShell 4.0 is not supported, see the "Workaround" below below.
3. If you are deploying an agent or relay onto Linux, use curl 7.34.0 or higher, which supports TLS 1.2.
4. If you are deploying onto Red Hat Enterprise Linux 6, which uses curl 7.19 by default, do one of the following:
   - upgrade to curl 7.34.0 or later

     OR

   - See the "Workaround" below below

## Workaround

If TLS 1.2 is enforced, and...

- you are deploying onto Windows XP, 2003, or 2008, where PowerShell 4.0 is not supported...

  OR

- you are deploying onto a Red Hat Enterprise Linux 6 computer with curl 7.19 that cannot be upgraded...

  Do this:
  1. From Deep Security Manager, download the agent installation package for your operating system. See "Get Deep Security Agent software" on page 177 for details.
  2. Copy the installation package to your web server.
  3. Follow the instructions in "Use deployment scripts to add and protect computers" on page 281 to add and protect computers, but instead of using Deep Security Manager to generate the script, use the Windows script or Linux script that is provided below.

  Windows script:

**Note:** You must set the `baseUrl` variable to the URL of your agent package on your web server.

```
$env:LogPath = "$env:appdata\Trend Micro\Deep Security Agent\installer"
New-Item -path $env:LogPath -type directory
Start-Transcript -path "$env:LogPath\dsa_deploy.log" -append
echo "$(Get-Date -format T) - DSA download started"
$baseUrl=<server/package>
echo "$(Get-Date -format T) - Download Deep Security Agent Package" $sourceUrl
(New-Object System.Net.WebClient).DownloadFile($sourceUrl,
"$env:temp\agent.msi")
if ( (Get-Item "$env:temp\agent.msi").length -eq 0 ) {
echo "Failed to download the Deep Security Agent. Please check if the package
is on the server. "
exit 1 }
echo "$(Get-Date -format T) - Downloaded File Size:" (Get-Item
"$env:temp\agent.msi").length
echo "$(Get-Date -format T) - DSA install started"
echo "$(Get-Date -format T) - Installer Exit Code:" (Start-Process -FilePath
msiexec -ArgumentList "/i $env:temp\agent.msi /qn ADDLOCAL=ALL /l*v
`"$env:LogPath\dsa_install.log`"" -Wait -PassThru).ExitCode
Stop-Transcript
echo "$(Get-Date -format T) - DSA Deployment Finished"
```

Linux script:

Use the script that is appropriate for your Linux distribution.

**Note:** Replace `<server/package>` with the URL of the agent package on your web server.

For Linux distributions that use the RPM Package Manager:

```
#!/usr/bin/env bash
```

```
curl <server/package> -o /tmp/agent.rpm -silent
```

```
rpm -ihv /tmp/agent.rpm
```

For Debian-based Linux distributions:

```
#!/usr/bin/env bash
```

```
curl <server/package> -o /tmp/agent.deb -silent
```

```
dpkg -i /tmp/agent.deb
```

# Migrate a Microsoft SQL Server Express database to Enterprise

Microsoft SQL Server Express is supported in very limited deployments (see "Microsoft SQL Server Express considerations" on page 126 for details). If you are using a Microsoft SQL Server Express database but find its limitations too constricting, you can migrate it to a supported database.

1. Stop the Deep Security Manager service so that it stops writing to the database.

   Deep Security Agents will continue to apply their current protection policies while the manager is stopped. Events will be kept and transmitted when Deep Security Manager returns online.

2. Back up the database(s).

3. Back up the database connection settings file:

   ```
   [Deep Security install directory]/webclient/webapps/ROOT/WEB-INF/dsm.properties
   ```

4. Move the database to the new database engine. Restore the backup.

5. Edit dsm.properties to connect to the migrated database:

   ```
   database.SqlServer.user
   ```

   ```
   database.name
   ```

```
database.SqlServer.instance
```

```
database.SqlServer.password
```

```
database.type
```

```
database.SqlServer.server
```

If using the default instance, you can delete the `database.SqlServer.instance` setting.

You can enter a plain text password for `database.SqlServer.password`; Deep Security Manager will encrypt it when the service starts, like this:

```
database.SqlServer.password=!CRYPT!20DE3D96312D6803A53C0D1C691FE6DEB7476104C0A
```

6. Restart the Deep Security Manager service.
7. To verify that it has successfully reconnected to the database, log in to Deep Security Manager.

   Existing protected computers and event logs should appear. As new events such as administrator logins or policy changes occur, they should be added. If not, verify that you have granted permissions to the database user account on the new database server.

# Uninstall Deep Security

When you manually uninstall an activated agent or relay from a computer, the computer doesn't notify Deep Security Manager that the software has been uninstalled. On the Computers page in Deep Security Manager, the computer's status will be "Managed (Offline)" or similar, depending on the context. To avoid this, on Deep Security Manager, either:

- Deactivate the agent or relay *before* you uninstall it, or
- Delete the computer from the list *after* you uninstall

## Uninstall Deep Security Relay

A Deep Security Relay is an agent where you have enabled the relay feature, so in order to remove the relay, you must uninstall the agent software.

## Uninstall a relay (Windows)

**Note:** Before updating or uninstalling a Deep Security agent or relay on Windows, you must disable agent self-protection. To do this, on the Deep Security Manager, go to **Computer editor**[1] > **Settings** > **General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override.

From the Windows Control Panel, select **Add/Remove Programs**. Double-click **Trend Micro Deep Security Agent**, and click **Remove**.

Alternatively, you can uninstall from the command line:

```
msiexec /x <package name including extension>
```

For a silent uninstall, add `/quiet`.

## Uninstall a relay (Linux)

To completely remove the relay and any configuration files it created on a platform that uses the Red Hat package manager (rpm), such as CentOS, Amazon Linux, Oracle Linux, SUSE, or Cloud Linux, enter the command:

```
# sudo rpm -ev ds_agent
 Stopping ds_agent: [ OK ]
 Unloading dsa_filter module [ OK ]
```

If iptables was enabled prior to the installation of the relay-enabled agent, it will be re-enabled when the relay-enabled agent is uninstalled.

**Note:** Remember to remove the relay-enabled agent from Deep Security Manager's list of managed computers, and to remove it from the relay group.

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

# Uninstall Deep Security Agent

## Uninstall an agent (Windows)

**Note:** Before updating or uninstalling a Deep Security Agent or Relay on Windows, you must disable agent self-protection. To do this, on the Deep Security Manager, go to **Computer editor**[1] > **Settings** > **General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override.

1. Deactivate the agent using the Deep Security Manager by going to the **Computers** page, right-clicking the computer and selecting **Actions** > **Deactivate**.
   If you are unable to deactivate the agent because the Deep Security Manager is unable to communicate with the agent, you will need to do the following before continuing to the next step:
   ```
   C:\Program Files\Trend Micro\Deep Security Agent>dsa_control --selfprotect 0
   ```
2. Go to the Control Panel and select **Uninstall a program**. Look for the Trend Micro Deep Security Agent and then select **Uninstall**.

Alternatively, you can uninstall from the command line:

```
msiexec /x <package name including extension>
```

For a silent uninstall, add `/quiet`.

## Uninstall an agent (Linux)

If your version of Linux provides a graphical package management tool, you can search for the `ds_agent` package and use the tool remove the package. Otherwise, use the command line instructions below.

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

To completely remove the agent and any configuration files it created on a platform that uses the Red Hat package manager (rpm), such as CentOS, Amazon Linux, Oracle Linux, SUSE, or Cloud Linux, enter the command:

```
# sudo rpm -ev ds_agent
 Stopping ds_agent: [ OK ]
 Unloading dsa_filter module [ OK ]
```

If iptables was enabled prior to installing Deep Security Agent, it will be re-enabled when the agent is uninstalled.

If the platform uses Debian package manager (dpkg), such as Debian and Ubuntu, enter the command:

```
$ sudo dpkg -r ds-agent
 Removing ds-agent...
 Stopping ds_agent: .[OK]
```

## Uninstall an agent (Solaris 9 or 10)

Enter the command:

```
pkgrm ds-agent
```

(Note that uninstall may require a reboot.)

## Uninstall an agent (Solaris 11)

Enter the command:

```
pkg uninstall ds-agent
```

Uninstall may require a reboot.

## Uninstall an agent (AIX)

Enter the command:

```
installp -u ds_agent
```

### Uninstall an agent (HP-UX)

Enter the command:

```
swremove ds_agent
```

## Uninstall Deep Security Notifier

From the Windows Control Panel, select **Add/Remove Programs**. Double-click **Trend Micro Deep Security Notifier**, and click **Remove**.

To uninstall from the command line:

```
msiexec /x <package name including extension>
```

For a silent uninstall, add `/quiet`.

## Uninstall Deep Security Manager

### Uninstall the manager (Windows)

From the Windows Start Menu, go to **Trend Micro > Trend Micro Deep Security Manager Uninstaller**, and follow the wizard steps to complete the uninstallation.

To initiate the same Windows GUI uninstall procedure from the command line, go to the installation folder and enter:

```
<installation folder>\Uninstall.exe
```

For a silent uninstall from the command line (without the Windows GUI prompts), add `-q`.

```
<installation folder>\Uninstall.exe -q
```

During a silent uninstall via command line, the configuration files are kept so that if you re-install in future, the installer repairs or upgrades using existing settings, without asking you to input them again.

### Uninstall the manager (Linux)

To uninstall via command line, go to the installation folder and enter:

```
sudo ./uninstall
```

For a silent uninstall, add `-q` .

During a silent uninstall via command line, by default, the configuration files are kept so that if you re-install in future, the installer repairs upgrades using existing settings, without asking you to input them again.

If you selected not to keep the configuration files during the uninstallation, and you later want to reinstall Deep Security Manager, you should perform a manual clean-up before reinstalling. To remove the Deep Security Manager installation directory enter the command:

```
sudo rm -rf <installation location>
```

The default installation location is `/opt/dsm`.

# FAQs

## Deep Security release life cycle and support policy

Trend Micro provides two types of Deep Security releases:

- Major releases: Released annually, major releases provide new features, bug fixes, and feature enhancements, and include long-term support.
- Feature releases: Released between major releases, feature releases provide early access to new features. (For more information, see "Feature releases" on page 66.) Feature releases include shorter support periods. Feature release functionality is cumulative and is ultimately rolled into the next major release.

You might choose to obtain major releases because they are more compatible with longer adoption cycles, and you value sustainability over early adoption of new features. However, if

new features are more critical to your immediate requirements, you can obtain feature releases before the next major release becomes available.

Additionally, you should understand the release life cycle and corresponding support that is provided for major releases:

- "Support milestones for major releases" below
- "Major release support services" below

## Support milestones for major releases

The following table lists the life cycle milestones for major releases and indicates their timing relative to the initial availability of the release.

| Life cycle milestone | Timing (Global) |
|---|---|
| General Availability (GA) | GA (Annually) |
| End of standard support (Only extended support is subsequently available.) | GA + 3 years |
| End of life (End of extended support.) | GA + 4 years |

Trend Micro publishes a list of end-of-life products.

## Major release support services

The following table indicates which support items are available during the life cycle of Deep Security major releases.

| Support item | Standard support | Extended support |
|---|---|---|
| Small enhancements (no change to core functionality) | ✔ | |
| Linux kernel updates | ✔ | On request |
| General bug fixes | ✔ | |
| Critical bug fixes (system crash or hang, or loss of major functionality) | ✔ | ✔ |

| Support item | Standard support | Extended support |
|---|---|---|
| Critical and high vulnerability fixes | ✔ | ✔ |
| Medium and low vulnerability fixes | ✔ | |
| Anti-Malware pattern updates | ✔ | ✔ |
| Intrusion prevention system, integrity monitoring, and log inspection rules updates | ✔ | ✔ |
| Support for Agents and Deep Security Manager on new versions of supported operating systems | ✔ | |

For a list of support items that are provided for feature releases, see "Feature releases" on page 66.

# Why does my Windows machine lose network connectivity when I turn on protection?

A Windows machine will lose connectivity for a brief period of time during the network driver installation while the Deep Security Agent installs a network driver to examine traffic. This only happens the *first* time a policy is applied that includes one of the following:

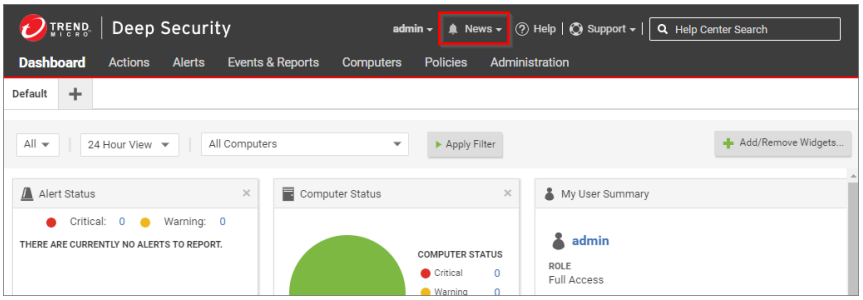
- Web reputation
- Firewall
- Intrusion prevention

A Windows machine uses the same driver is used for all three protection modules listed above. Turning on web reputation, firewall or intrusion prevention after one of those features already turned on will not cause another network blip. You may see a similar interruption in network connectivity when the agent is upgraded (as the driver may also need to be upgraded).

# How do I get news about Deep Security?

Deep Security publishes a news feed to inform you of upcoming events, emerging threat trends, product updates, and tips to improve your Deep Security deployment.

You can access the news feed by clicking **News** at the top of the Deep Security Manager:




You can also access the news feed in an RSS and Atom feed reader by subscribing to:

https://news.deepsecurity.trendmicro.com/news.atom

# How do I migrate to a larger RDS database instance?

If you are using an Amazon RDS database instance as your Deep Security database and you want to move to an RDS instance that includes more storage, follow these steps:

1. Back up your current database. Follow the instructions provided by AWS for backing up your database to an S3 bucket. For example, see Amazon RDS for SQL Server - Support for Native Backup/Restore to Amazon S3.

   **Note:** RDS SQL Server Express is supported in very limited deployments. See "Microsoft SQL Server Express considerations" on page 126 for important details. In addition, migrating from RDS SQL Server Express to SQL Server Enterprise is not supported with Deep Security.

   **Note:** For general database requirements, see "Prepare a database for Deep Security Manager on AWS" on page 114.

2. Stop the Deep Security Manager service. In a Windows environment, you can use the Windows Services UI. In a Linux environment, use the `service dsm_s stop` command.

3. Restore the database in your new database instance.
4. If your database IP address or login information has changed, update the Deep Security Manager properties file. On Windows, the file is `[Deep Security install directory]\webclient\webapps\ROOT\WEB-INF\dsm.properties`. On Linux, it's `/opt/dsm/webclient/webapps/ROOT/WEB-INF/dsm.properties`. Here is an example of the contents:

```
#Wed Jun 11 16:19:19 EDT 2017 database.SqlServer.user=sa database.name=IDF
database.directory=null
database.SqlServer.password=$1$87251922972564e6bb3e2da917463fb1de
4a5fcea848e688cd4ceb42b9bfb17a942c3c8ad99ff05938c81a60a2a11f4c3c6
c1af5c9d01f3c8bfa60e634502aba112b9394ee4f73c970a6970fc9db6f96ba0cc
80600ad4e36869881bddc3bdfc1abf8a7b2be459ff92c5dfeabbd8e7fd8
database.SqlServer.instance=DSM mode.demo=false
database.SqlServer.namedPipe=true database.type=SqlServer
database.SqlServer.server=. manager.node=1
```

5. Start the Deep Security Manager service.

# AWS GovCloud (US) support

There are two ways that Deep Security provides AWS GovCloud (US) support:

- You can use the Trend Micro Deep Security AMI (Per Protected Instance Hour or BYOL license type) that is available from the AWS GovCloud Marketplace. The deployment instructions for the AWS GovCloud (US) region are the same as any other region. See Getting started with Deep Security AMI from AWS Marketplace.
- You can install the enterprise version of the Deep Security software on an AWS instance running in the AWS GovCloud (US) region.

**Note:** Deep Security as a Service does not support GovCloud. Computers on the AWS GovCloud must comply with user and data transmission restrictions as specified by United States of America International Traffic in Arms Regulations (ITAR). Because the Deep Security as a Service operating model requires the transmission of data outside of the AWS GovCloud, using it to manage computers in the GovCloud would break this compliance.

## Protecting GovCloud instances using a manager in a commercial AWS instance

**Warning:** Be aware that if your Deep Security Manager is outside of the AWS GovCloud, using it to manage computers in the GovCloud would break ITAR compliance.

If your Deep Security Manager is in a commercial AWS instance and you want to use it to protect GovCloud instances, you cannot use the cloud connector provided in the Deep Security Manager console to add the instances. If Deep Security Manager is running in a special region (like GovCloud), it can connect to that region and also connect to instances in commercial AWS regions. But if Deep Security Manager is in a commercial region, it can connect to all commercial AWS regions but not special regions like GovCloud.

If you want to add a special region connector (like GovCloud) into a Deep Security Manager running in commercial AWS, you will need to use the Deep Security API to do so and supply the `seedRegion` argument to tell the Deep Security Manager that it's connecting outside of commercial AWS. For information on using the API, see "Use the Deep Security API to automate tasks" on page 261.

## How can I minimize heartbeat alerts for offline environments in an AWS Elastic Beanstalk environment?

AWS Elastic Beanstalk allows you to create multiple environments so that you can run different versions of an application at the same time. These environments usually include a production and development environment and often the development environment is powered down at night. When the development environment is brought back online in the morning, Deep Security will generate alerts related to communication problems for the period of time that it was offline. Although these alerts are actually false from your perspective, they are legitimate alerts from the perspective of Deep Security because an alert is generated whenever a specified number of heartbeats is missed.

You can minimize these heartbeat-related alerts or even prevent them from being generated for environments that you know will be offline for a period of time every day by creating a policy with

specific heartbeat settings and applying that policy to the servers in those partially offline environments.

1. Go to the **Policies** tab in the main Deep Security Manager window.
2. Create a new policy or edit an existing one.
3. Click the **Settings** tab in the **Policy editor**[1] and go to the **Computer** tab.
4. Change one or both of the **Heartbeat Interval** and **Number of Heartbeats that can be missed before an alert is raised** setting to numbers that take into account the number of hours your Elastic Beanstalk environment will be offline.
   *For example, if you know that a server will be offline for 12 hours a day and the Heartbeat Interval is set at 10 minutes, you could change the Number of Heartbeats that can be missed before an alert is raised setting to unlimited to never get an alert or you could increase the Heartbeat Interval to something greater than 10 to get fewer alerts.*
5. Click **Save** and apply the policy to all relevant servers.

For more information on using Deep Security in an AWS Elastic Beanstalk environment, you can watch the Trend Micro webinar Deploying Scalable and Secure Web Apps with AWS Elastic Beanstalk and Deep Security.

# Why can't I add my Azure server using the Azure cloud connector?

If an Azure server loses connectivity to the Azure metadata service, the Deep Security Manager will no longer be able to identify it as an Azure server and you will be unable to add it using the Azure cloud connector.

This situation can happen if the server's public or private IP address is changed outside of the Azure console. The Azure server relies on DHCP to communicate with the metadata service and changing the IP outside of the console disables DHCP.

[1] To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

Microsoft recommends against changing the Azure VM's IP address from within its operating system, unless necessary, such as when assigning multiple IP addresses to a Windows VM. For details, see this Azure article.

To check if your Azure server is able to connect to the Azure metadata service, run the Detect Windows Azure Virtual Machine PowerShell script from the Microsoft Script Center.

## Why can't I view all of the VMs in an Azure subscription in Deep Security?

If not all of the virtual machine resources in an Azure subscription are being displayed on the Computers page of Deep Security Manager, this could be because they were deployed using the Azure deployment model Resource Manager. All resources are deployed using this model unless you select **Classic** from the **Select a deployment model** list.

Not all VMs are displayed because older versions of the Deep Security Manager use the Service Management API provided by the classic Azure deployment model (the Service Management model) to connect to Azure virtual machines so it can only enumerate VMs deployed with the Classic model.

To see both Classic or Resource Manager VMs, upgrade your cloud connector. For more information, see "Why should I upgrade to the new Azure Resource Manager connection functionality?" on page 317.

**Note:** If you are unable to upgrade your Resource Manager servers as per the article above, you can still protect them by using the deployment script on the VM and letting the activation create a new computer object outside of the connector.

# Troubleshooting

## AWS Marketplace Quick Start

If you are experiencing issues with the CloudFormation template during Quick Start deployment, you can check the stack events of the template to help you diagnose them. If your issue isn't covered here, you can also" Gather stack information and contact Trend Micro support" on page 1096.

### Check CloudFormation template stack events

The CloudFormation template uses multiple stacks to deploy Deep Security. You can check the event history of each stack for status messages that may help you diagnose issues.

> **Note:** It may take 50 or more minutes for all stacks in the template to finish.

Issues often occur because:

- "AWS Marketplace terms were not accepted" on the next page.
- "A stack could not create the IAM role" on the next page.
- "A stack could not create the Deep Security Manager database" on page 1096.

To check the event history of each stack and see if these or other issues have occurred:

1. In the AWS console, go to the **CloudFormation** page.
   The CloudFormation template page will appear with the Quick Start deployment CloudFormation template stacks displayed.
2. Select a stack from the list.

   > **Note:** By default the template page only shows active stacks. If there has been an issue in a stack, it may no longer be active. To see event logs for stacks in other states, click on the **Filter** dropdown list and select each of the filter options.

3. Check the event log of the stack for messages caused by the frequently occurring issues described below or for any other unusual status messages.
4. Repeat the above for each stack in the template.

For more general troubleshooting information on CloudFormation templates see the AWS troubleshooting guide on CloudFormation. You can also learn more about stack information and status from the AWS guide on Viewing Stack Information.

## AWS Marketplace terms were not accepted

If you don't accept the terms in the AWS Marketplace page before subscribing, you will see the following error for one of the stacks:

| Status | Status Description |
|---|---|
| `CREATE_FAILED` | `In order to use this AWS Marketplace product you need to accept terms and subscribe. To do so please visit <link to Deep Security marketplace product page>` |

The error message will include a link to the product page. Go to the product page, select **Continue** and agree to the licensing terms, and then run the CloudFormation template again.

**Note:** If you are using single sign on (SSO) and have a parent account, that account may also need to accept the subscription.

## A stack could not create the IAM role

If you don't acknowledge that CloudFormation may create IAM resources during stack creation, you will see the following error for one of the stacks:

| Status | Status Description |
|---|---|
| `CREATE_FAILED` | `Requires capabilities : [CAPABILITY_IAM]` |

If this happens, you will need to run the CloudFormation template again. During stack creation, on the bottom of the confirmation page, make sure that you've selected **I acknowledge that AWS CloudFormation might create IAM resources with custom names** before continuing.

## A stack could not create the Deep Security Manager database

You may see the following error for one of the stacks:

| Status | Status Description |
| --- | --- |
| `CREATE_FAILED` | `The following resource(s) failed to create: [DSDatabaseAbstract]` |

This error will occur if the private subnets for the database in your Multi-AZ deployment are in the same availability zone. For the CloudFormation template to run correctly, each private subnet must be in a different availability zone.

## Gather stack information and contact Trend Micro support

If you are still unable to diagnose your issue you can open a ticket with Trend Micro support. Before you do so build the stack with the 'Rollback on failure' setting disabled. This will help support better diagnose your issue. To do so:

1. On the Option page, open the Advanced section and select **No** for **Rollback on Failure**.
2. Record your AWS region and the URL of your Quick Start template.
3. Open a support ticket with Trend Micro, and provide them with the AWS region and the Quick Start template URL you recorded. If this is your first time contacting support, you can provide the same to Trend Micro Support at aws@trendmicro.com.

# "Activation Failed" agent status

When activating or re-activating a Deep Security Agent, if you receive an "Activation Failed" error message, see:

- Deep Security Manager (DSM) imported via vCenter shows "Activation Failed (Duplicate Computer)".
- Event ID 705: Activation Failed appears when activating the Deep Security Agent (DSA).

# "Offline" agent

A computer status of "Offline" or "Managed (Offline)" means that the Deep Security Manager hasn't communicated with the agent's instance for some time and has exceeded the missed heartbeat threshold. (See "Configure the heartbeat" on page 196.) The status change can also appear in alerts and events.

## Causes

Heartbeat connections can fail because:

- The agent is installed on a workstation or other computer that has been shut down. If you are using Deep Security to protect computers that sometimes get shut down, make sure the policy assigned to those computers does not raise an alert when there is a missed heartbeat. In the policy editor, go to **Settings > General > Number of Heartbeats that can be missed before an alert is raised** and change the setting to "Unlimited".
- Firewall, IPS rule, or security groups block the heartbeat port number
- Bi-directional communication is enabled, but only one direction is allowed or reliable (see "Configure communication directionality" on page 198)
- Computer is powered off
- Computer has left the context of the private network
  This can occur if roaming endpoints (such as a laptop) cannot connect to Deep Security Manager at their current location. Guest Wi-Fi, for example, often restricts open ports, and has NAT when traffic goes across the Internet.
- Amazon WorkSpace computer is being powered off, and the heartbeat interval is fast, for example, one minute; in this case, wait until the WorkSpace is fully powered off, and at that point, the status should change from 'Offine' to 'VM Stopped'
- DNS was down, or could not resolve the Deep Security Manager's host name
- Deep Security Manager, the agent, or both are under very high system resource load
- Deep Security Agent process might not be running
- Certificates for mutual authentication in the SSL or TLS connection have become invalid or revoked (see "Replace the Deep Security Manager SSL certificate" on page 756)

- Deep Security Agent's or Deep Security Manager's system time is incorrect (required by SSL/TLS connections)
- Deep Securityrule update is not yet complete, temporarily interrupting connectivity
- On AWS EC2, ICMP traffic is required, but is blocked

**Tip:** If you are using manager-initiated or bi-directional communication, and are having communication issues, we strongly recommend that you change to agent-initiated activation (see "Use agent-initiated communication with cloud accounts" on page 202).

To troubleshoot the error, verify that the Deep Security Agent is running, and then that it can communicate with Deep Security Manager.

## Verify that the agent is running

On the computer with Deep Security Agent, verify that the Trend Micro Deep Security Agent service is running. Method varies by operating system.

- On Windows, open the Microsoft Windows Services Console (services.msc) or Task Manager. Look for the service named ds_agent.

- On Linux, open a terminal and enter the command for a process listing. Look for the service named ds_agent or ds-agent, such as:

  ```
  sudo ps -aux | grep ds_agent
  ```

  ```
  sudo service ds_agent status
  ```

## Verify DNS

If agents connect to the Deep Security Manager via its domain name or hostname, not its IP address, test the DNS resolution:

```
nslookup [manager domain name]
```

**DNS service must be reliable.**

If the test fails, verify that the agent is using the correct DNS proxy or server (internal domain names can't be resolved by a public DNS server such as Google or your ISP). If a name such as dsm.example.com cannot be resolved into its IP address, communication will fail, even though correct routes and firewall policies exist for the IP address.

If the computer uses DHCP, in the computer or policy settings, in the **Advanced Network Engine** area, you might need to enable **Force Allow DHCP DNS**(see "Network engine settings" on page 378).

## Allow outbound ports (agent-initiated heartbeat)

Telnet to required port numbers on Deep Security Manager to verify that a route exists, and the port is open:

```
telnet [manager IP]:4120
```

**Tip:**
Telnet success proves most of the same things as a ping: that a route and correct firewall policy exist, and that Ethernet frame sizes are correct. (Ping is disabled on computers that use the default security policy for Deep Security Manager. Networks sometimes block ICMP ping and traceroute to block attackers' reconnaissance scans. So usually, you can't ping the Manager to test.)

If telnet fails, trace the route to discover which point on the network is interrupting connectivity. Methods vary by operating system.

- On Linux, enter the command:

  ```
  traceroute [agent IP]
  ```

- On Windows, enter the command:

  ```
  tracert [agent IP]
  ```

Adjust firewall policies, routes, NAT port forwarding, or all three to correct the problem. Verify both network and host-based firewalls, such as Windows Firewall and Linux iptables. For an AWS EC2 instance, see Amazon's documentation on Amazon EC2 Security Groups for Linux

Instances or Amazon EC2 Security Groups for Windows Instances. For an Azure VM instance, see Microsoft's Azure documentation on modifying a Network Security Group.

If connectivity tests from the agent to the manager succeed, then next you must test connectivity in the other direction. (Firewalls and routers often require policy-route pairs to allow connectivity. If only 1 of the 2 required policies or routes exist, then packets will be allowed in one direction, but not the other.)

## Allow inbound ports (manager-initiated heartbeat)

On the Deep Security Manager, ping the Deep Security Agent and telnet to the heartbeat port number to verify that heartbeat and configuration traffic can reach the agent:

```
ping [agent IP]
```

```
telnet [agent IP]:4118
```

If the ping and telnet fail, use:

```
traceroute [agent IP]
```

to discover which point on the network is interrupting connectivity. Adjust firewall policies, routes, NAT port forwarding, or all three to correct the problem.

If IPS or firewall rules are blocking the connection between the Deep Security Agent and the Deep Security Manager, then the manager cannot connect in order to unassign the policy that is causing the problem. To solve this, enter the command on the computer to reset policies on the agent:

```
dsa_control -r
```

**Note:** You must re-activate the agent after running this command.

## Allow ICMP on Amazon AWS EC2 instances

In the AWS cloud, routers require ICMP type 3 code 4. If this traffic is blocked, connectivity between agents and the manager may be interrupted.

You can force allow this traffic in Deep Security. Either create a firewall policy with a force allow, or in the computer or policy settings, in the **Advanced Network Engine** area, enable **Force Allow ICMP type3 code4** (see "Network engine settings" on page 378).

# High CPU usage

On a computer protected by Deep Security Agent, you can use these steps to determine and resolve the cause of high CPU usage.

1. Verify that the Trend Micro Deep Security Agent process (ds_agent.exe on Windows) has unusually high CPU usage. Method varies by operating system.

   Windows: Task Manager

   Linux: `top`

2. Verify that the agent is updated to the latest version.
3. Apply the best practices on "Performance tips for anti-malware" on page 510 and "Performance tips for intrusion prevention" on page 581.
4. If you have just enabled application control, wait until the initial baseline ruleset is complete. Time required varies by the number of files on the file system. The CPU usage should decrease.
5. If a recommendation scan is being performed, try running scans during a time when the computer is less busy, or (if the computer is a VM) allocating more vCPUs.
6. Temporarily disable each protection feature (anti-malware etc.), one at a time. Check CPU usage each time to determine if a specific module is the cause.
7. If high CPU usage still continues, try temporarily stopping the agent. Verify that the issue stops when the agent is stopped. If it does, collect diagnostic information and give it to your support provider.

# Security update connectivity

Verify the connectivity between the relay server and its Active Update source or proxy server.

1. To verify that both a route exists and that the relay port number is open, enter the command:

   ```
   telnet [relay IP] [port number]
   ```

   If the telnet fails, verify that a route exists and that firewall policies (if any) allow the traffic by pinging or using traceroute. Also verify that the port number is open, and doesn't have a port conflict.

2. To verify that the DNS server can resolve the domain name of the relay, enter the command:

   ```
   nslookup [relay domain name]
   ```

   If the test fails, verify that the agent is using the correct DNS proxy or server (internal domain names can't be resolved by a public DNS server such as Google or your ISP).

   If you are using Deep Security as a Service, you might not be using your own relays; instead, you will be using the relays that are built into the service: relay.deepsecurity.trendmicro.com.

3. If you use a proxy server, on Deep Security, confirm that the proxy settings are correct.
4. To determine if your Deep Security settings are blocking connectivity, unassign the current policy.

# Purple screen of death

If you encounter a Purple Screen of Death issue, collect the necessary files and submit them to Trend Micro Technical Support to determine if the issue is coming from the VMware side or Trend Micro side.

1. Capture a screen shot of the Purple Diagnostic Screen via remote KVM or take a picture of the physical console's Purple Diagnostic Screen prior to reboot.
2. Get the core dump from the VMkernel sent to the ESXi Dump Collector Network Service.
   a. Log in to the vSphere client and navigate to the Home page.
   b. Click **Hosts and Clusters** and select the host.

   c. Click **Export > Export System Logs**.
   d. Click **Select all** and choose the log store location to complete the process.
3. Extract the log from the dump using the procedure in this VMware article: Extracting the log file after an ESX or ESXi host fails with a purple screen error (1006796).
4. Gather a vm-support log bundle from the host by typing "vm-support" in ESXi command line.

# Prevent MTU-related agent communication issues across Amazon Virtual Private Clouds (VPC)

Agents in different VPCs might experience problems when trying to communicate with Deep Security Manager. This could be because the network maximum transmission unit (MTU) supported by Amazon Web Services is 1500 and Deep Security Agent communication traffic can exceed this, which results in fragmented and dropped packets.

You can prevent this MTU-related communication issue from happening by adding a new firewall rule to all firewall policies. The key settings for this new firewall rule are shown in the image below.

General | Options | Assigned To

**General Information**

Name: New Firewall Rule

Description:

Action: Force Allow

Priority: 0 - Lowest

Packet direction: Incoming

Frame Type: IP — Not

Protocol: ICMP — Not

**Packet Source**

IP: Any — Not

MAC: Any — Not

Port: Any — Not

**Packet Destination**

IP: Any — Not

MAC: Any — Not

Port: Any — Not

**Specific Flags**

Any Flags

Type: 3 Destination Unreacha — Code: 4 Fragmentation Neede — Not

OK | Cancel

# Create a diagnostic package and logs

To diagnose an issue, your support provider may ask you to send a diagnostic package containing debug information for either or both:

- Deep Security Manager
- Deep Security Agent

## Deep Security Manager diagnostics

### Create a diagnostic package for Deep Security Manager

1. Go to **Administration > System Information**.
2. Click **Create Diagnostic Package**.

   The package will take several minutes to create. After the package has been generated, a summary will be displayed and your browser will download a ZIP file containing the diagnostic package.

### Enable debug logs for Deep Security Manager

In addition to a diagnostic package, your support provider may ask you to enable diagnostic logging.

**Warning:** Don't enable diagnostic logging unless recommended by your support provider. Diagnostic logging can consume large amounts of disk space and increase CPU usage.

1. Go to **Administration** > **System Information.**
2. Click **Diagnostic Logging**.
3. In the wizard that appears, select the options requested by your support provider.

   While diagnostic logging is running, Deep Security Manager will display the message "Diagnostic Logging enabled" on the status bar. If you changed the default options, the

status bar will display the message "Non default logging enabled" upon diagnostic logging completion.

4. To find diagnostic logging files, go to the root directory of the Deep Security Manager, and look for file names with the pattern `server#.log`.

# Deep Security Agent diagnostics

For an agent, you can create a diagnostic package either:

- via the Deep Security Manager
- using the CLI on a protected computer (if the Deep Security Manager cannot reach the agent remotely)

For Linux-specific information on increasing or decreasing the anti-malware debug logging for the diagnostic package, see "Increase debug logging for anti-malware in protected Linux instances" on page 536.

Your support provider may also ask you collect:

- a screenshot of Task Manager (Windows) or output from `top`(Linux)
- debug logs
- Perfmon log (Windows) or Syslog
- memory dumps (Windows) or core dumps (Linux)

## Create an agent diagnostic package via Deep Security Manager

**Note:** Deep Security Manager must be able to connect to an agent remotely to create a diagnostic package for it. If the Deep Security Manager cannot reach the agent remotely, or if the agent is using agent-initiated activation, you must create the diagnostic package directly from the agent.

1. Go to **Computers** .
2. Double-click the name of the computer you want to generate the diagnostic package for.
3. Select the **Actions** tab.
4. Under **Support**, click **Create Diagnostics Package**.

5. Click **Next**.

   The package will take several minutes to create. After the package has been generated, a summary will be displayed and your browser will download a ZIP file containing the diagnostic package.

## Create an agent diagnostic package via CLI on a protected computer

Linux

1. Connect to the server that you want to generate the diagnostic package for.
2. Enter the command:

   ```
   sudo /opt/ds_agent/dsa_control -d
   ```

   The output shows the name and location of the diagnostic package: `/var/opt/ds_agent/diag`

Windows

1. Connect to the computer that you want to generate the diagnostic package for.
2. Open a command prompt as an administrator.
3. Enter these commands:

   ```
   cd C:\Program Files\Trend Micro\Deep Security Agent
   ```

   ```
   dsa_control.cmd -d
   ```

   The output shows the name and location of the diagnostic package: `C:\ProgramData\Trend Micro\Deep Security Agent\diag`

## Collect debug logs with DebugView

On Windows computers, you can collect debug logs using DebugView software.

**Warning:** Only collect debug logs if your support provider asks for them. During debug logging, CPU usage will increase, which will make high CPU usage issues worse.

1. Download the DebugView utility.
2. If self-protection is enabled, disable it.
3. Stop the Trend Micro Deep Security Agent service.

4. In the C:\Windows directory, create a plain text file named ds_agent.ini.
5. In the ds_agent.ini file, add this line:

   ```
   trace=*
   ```

6. Launch DebugView.exe.
7. Go to **Menu > Capture**.
8. Enable these settings:
   - **Capture Win32**
   - **Capture Kernel**
   - **Capture Events**
9. Start the Trend Micro Deep Security Agent service.
10. Export the information in DebugView to a CSV file.
11. Re-enable self-protection if you disabled it at the beginning of this procedure.