TREND MICRO™

9.6 Deep Security

Service Pack 1

Deep Security Manager UI Guide

Advanced Protection for Physical, Virtual, and Cloud Servers

Cloud & Data Center

Complete End User

Cyber Threats

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 readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

http://www.trendmicro.com/download

Document version: 1.3
Document number: APEM97216_150921
Release date: November 2015
Document last updated: April 17, 2017

Table of Contents

The Deep Security Manager Console 7

- Alerts 8
- Events and Reports 9
  - System Events 10
  - Anti-Malware Events 13
    - Quarantined Files 16
  - Web Reputation Events 19
  - Firewall Events 21
  - Intrusion Prevention Events 24
  - Integrity Monitoring Events 27
  - Log Inspection Events 29
  - Generate Reports 32
- Computers 35
- Policies 45
  - Policies 46
  - Common Objects 48
    - Directory Lists 49
    - File Extension Lists 52
    - File Lists 53
    - IP Lists 56
    - MAC Lists 57
    - Port Lists 58
    - Schedules 59
    - Tags 60
    - Contexts 61
    - Firewall Stateful Configurations 63
    - Malware Scan Configurations 67
    - Firewall Rules 74
    - Intrusion Prevention Rules 78
      - Application Types 82
    - Integrity Monitoring Rules 84
    - Log Inspection Rules 88
- Computer and Policy Editors 91

Overview (Policy Editor) 92

General 93

Computer(s) Using This Policy 94

Events 95

Overview (Computer Editor) 97

General 98

Actions 101

TPM 103

Events 104

Anti-Malware 106

General 107

Smart Protection 109

Advanced 110

Quarantined Files 113

Events 114

Web Reputation 115

General 116

Smart Protection 117

Advanced 118

Exceptions 119

Events 120

Firewall 121

General 122

Interface Isolation 123

Reconnaissance 124

Advanced 126

Events 127

Intrusion Prevention 128

General 129

Advanced 131

Events 134

Integrity Monitoring 135

General 136

Advanced 137

Events 138

Log Inspection 139

General 140

Advanced ... 141

Events ... 142

SAP ... 143

Interfaces/Interface Types ... 144

Settings ... 145

Computer ... 146

Network Engine ... 150

Scanning ... 157

SIEM ... 158

Updates (Computer Editor only) ... 159

Overrides ... 160

Administration ... 161

System Settings ... 162

Tenants ... 163

Agents ... 166

Alerts ... 169

Contexts ... 170

SIEM ... 171

SNMP ... 172

Ranking ... 173

System Events ... 175

Security ... 176

Updates ... 178

Smart Feedback ... 181

SMTP ... 182

Storage ... 183

Proxies ... 184

Advanced ... 185

Scheduled Tasks ... 188

Event-Based Tasks ... 190

Manager Nodes ... 194

Tenants ... 196

Licenses ... 197

Users ... 198

Roles ... 202

Contacts ... 206

System Information ... 208

Updates ... 210

Security Updates 211

- Rules 213
- Patterns 215

Software Updates Overview 216

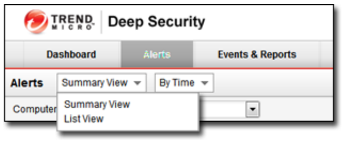
- Download Center 217
- Local Software 218

Relay Groups 221

The Deep Security Manager Console

Alerts

The **Alerts** page displays all active Alerts. Alerts can be displayed in a Summary View which will group similar Alerts together, or in List View which lists all Alerts individually. To switch between the two views, use the drop-down menu next to "Alerts" in the page's title.



In Summary View, expanding an Alert panel (by clicking **Show Details**) displays all the computers (and/or Users) that have generated that particular Alert. (Clicking the computer will display the computer's **Details** window.)

In Summary View, if the list of computers is longer than five, an ellipsis ("...") appears after the fifth computer. Clicking the ellipsis displays the full list. Once you have taken the appropriate action to deal with the Alert, you can dismiss the Alert by selecting the checkbox next to the target of the Alert and clicking the **Dismiss** link. (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.

In cases where an Alert condition occurs multiple times 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 reoccurrence will be displayed.

Alerts can be of two types: system and security. System Alerts are triggered by System Events (Agent Offline, Clock Change on Computer, etc.) Security Alerts are triggered by Intrusion Prevention, Firewall, Integrity Monitoring, Log Inspection, and Anti-Malware Rules. Alerts can be configured by clicking **Configure Alerts...** ().

Note: *Use the computers filtering bar to view only Alerts for computers in a particular computer group, with a particular Policy, etc.*

Events and Reports

The following pages are available in the Events and Reports section:

- *System Events (page 10)*
- *Anti-Malware Events (page 13)*
  - *Quarantined Files (page 16)*
- *Web Reputation Events (page 19)*
- *Firewall Events (page 21)*
- *Intrusion Prevention Events (page 24)*
- *Integrity Monitoring Events (page 27)*
- *Log Inspection Events (page 29)*
- *Generate Reports (page 32)*

System Events

The System Event log is a record of system-related events (as opposed to security-related events).

Once collected by the Deep Security Manager, Event logs are kept for a period of time which can be set **Administration > System Settings > Storage**. The default setting is one week.

From the main page you can:

- **View** () the details (properties) of a system event
- **Search** () for a particular system event
- **Export** () currently displayed system events to a CSV file
- View existing **Auto-Tagging** () Rules.

Additionally, right-clicking an Event gives you the option to:

- **Add Tag(s):** Add an Event Tag to this event (See **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help.)
- **Remove Tag(s):** Remove exiting Event Tags

View

Selecting an event and clicking **View** () displays the **Event Viewer Properties** window.

General

General Information

- **Time:** The time according to the system clock on the computer hosting the Deep Security Manager.
- **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.)
- **Tag(s):** Any tags attached with the Event.
- **Event Origin:** The Deep Security component from which the event originated.
- **Target:** The system object associated with the event will be identified here. Clicking the object's identification will display the object's properties sheet.
- **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 entry in the system event log will be displayed here.

Tags

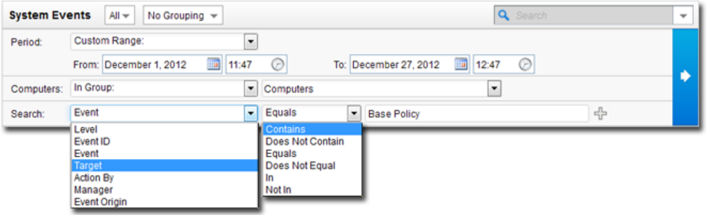
The **Tags** tab displays tags that have been attached to this Event. For More information on Event tagging, see **Policies > Common Objects > Other > Tags**, and **More About Event Tagging** in the Deep Security Manager Administrator's Guide or the online help in the **Reference** section.

Filter the List and/or 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 **Advanced Search** toggles the display of the search bar.



Period: Custom Range:
From: December 1, 2012 11:47 To: December 27, 2012 12:47
Computers: In Group: Computers
Search: Event Equals Base Policy

Pressing 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).

Advanced Search functions (searches are not case sensitive):

- **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

Export

You can export displayed events to a CSV file. (Paging is ignored, all pages will be exported.) You have the option of displaying the displayed list or the selected items.

Auto-Tagging

Clicking **Auto-Tagging...** displays a list of existing System Event Auto-Tagging Rules.

Anti-Malware Events

By default, the Deep Security Manager collects Anti-Malware Event logs from the Agents/Appliances at every heartbeat. The Event data is used to populate the various reports, graphs, and charts in the Deep Security Manager.

Once collected by the Deep Security Manager, Events are kept for a period of time which can be set from **Storage** tab in the **Administration > System Settings** page. The default setting is one week.

From the main page you can:

- **View** () the properties of an individual event.
- **Filter the list.** Use the **Period** and **Computer** toolbars to filter the list of events.
- **Export** () the event list data to a CSV file.
- View existing **Auto-Tagging** () Rules.
- **Search** (🔍) for a particular event.

Additionally, right-clicking an Event gives you the option to:

- **Add Tag(s)** to this event (See **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help.)
- **Remove Tag(s)** from this event.
- View the **Computer Details window** of the computer that generated the log entry.
- View **Quarantined File Details** of the file associated with this event. (Only available if the action associated with this event was quarantined.)

Columns for the Anti-Malware Events display:

- **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.
- **Scan Type:** The type of scan that found the malware (Real-Time, Scheduled, or Manual).
- **Action Taken:** Displays the results of the actions specified in the Malware Scan Configuration associated with 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 quarantine 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 quarantined 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.
- **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 Anit-Malware event details or see **Anti-Malware** in the Deep Security Manager Administrator's Guide or the online help.

View Event Properties

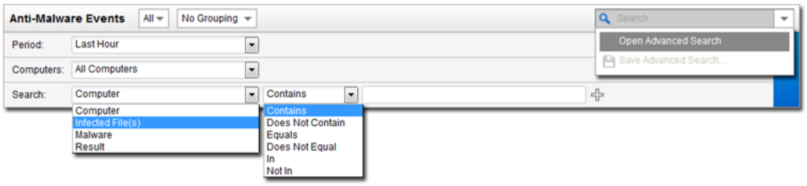
Double-clicking an event (or selecting **View** from the context menu) displays the **Properties** window for that entry which displays all the information about the event on one page. The **Tags** tab displays tags that have been attached to this Event. For More information on Event tagging, see **Policies > Common Objects > Other > Tags**, and **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help in the **Reference** section.

Filter the List and/or Search for an Event

Selecting "Open Advanced Search" from the "Search" drop-down menu toggles the display of the advanced search options.

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.



Anti-Malware Events

Period: Last Hour

Computers: All Computers

Search: Computer Contains

Advanced Search functions (searches are not case sensitive):

- **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

Pressing the "plus" 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 button (at the right of the toolbars with the right-arrow on it).

Export

Clicking **Export...** exports all or selected events to a CSV file.

Auto-Tagging...

Clicking **Auto-Tagging...** displays a list of existing Anti-Malware Auto-Tagging Rules.

Quarantined Files

A Quarantined 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. ("Quarantine" is a scan action that you can specify when creating a Malware Scan Configuration.) Once the file has been identified and quarantined, you can choose to download it to your computer in an encrypted and compressed format. Whether or not an infected file is quarantined depends on the Anti-Malware Configuration that was in effect when the file was scanned.

Note: *After the quarantined file has been downloaded to your computer, the **Quarantined File** wizard will display a link to an **Administration Utility** which you can use to decrypt, examine, and restore the file.*

A limited amount of disk space is set aside for storing quarantined files. The amount of space can be configured in **Policy/ Computer Editor > Anti-Malware > Advanced > Quarantined Files**. Alerts are raised when there is not enough disk space to quarantine a suspicious file.

If you are using a Deep Security Virtual Appliance to provide protection to virtual machines, all quarantined files from the Agentless VMs will be stored on the Virtual Appliance. As a result, you should increase the amount of disk space for quarantined files on the Virtual Appliance.

Quarantined files will be automatically deleted from a Virtual Appliance under the following circumstances:

- If a VM is moved to another ESXi host by vMotion, quarantined files associated with that VM will be deleted from the Virtual Appliance.
- If a VM is deactivated from the Deep Security Manager, quarantined files associated with that VM will be deleted from the Virtual Appliance.
- If a Virtual Appliance is deactivated from the Deep Security Manager, all the quarantined files stored on that Virtual Appliance will be deleted.
- If a Virtual Appliance is deleted from the vCenter, all the quarantined files stored on that Virtual Appliance will also be deleted.

The **Anti-Malware Quarantined Files** page allows you to manage quarantine tasks. Using the menu bar or the right-click context menu, you can:

- **Restore...** () Restore quarantined files back to their original location and condition.
- **Download...** () Move quarantined files from the computer or Virtual Appliance to a location of your choice.
- **Delete...** ( ) Delete one or more quarantined files from the computer or Virtual Appliance.
- **Export** () information about the quarantined file(s) (not the file itself) to a CSV file.
- **View** the details () of a quarantined file.
- View the **Computer Details** () screen of the computer on which the malware was detected.
- **View Anti-Malware Event...**() displays the Anti-Malware event associated with this quarantined file.
- **Add or Remove Columns** () columns can be added or removed by clicking **Add/Remove.**
- **Search** ( ) for a particular quarantined file.

Details

The Quarantined File **Details window** displays more information about the file and lets you download the quarantined file to your computer or delete it where it is.

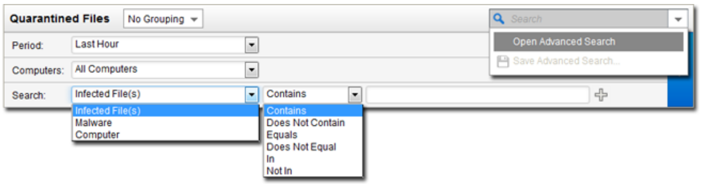
- **Detection Time:** Date/Time (on the infected computer) that the infection was detected.
- **Infected File(s):** The name of the infected file.
- **Malware:** The name of the malware that was found.
- **Scan Type:** Indicates whether the malware was detected by a Real-time, Scheduled, or Manual scan.
- **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".)

Filter the List and/or Search for a Quarantined File

The **Period** tool bar allows you to filter the list to display only those files quarantined within a specific time frame.

The **Computers** tool bar allows you to organize the display of quarantined file entries by Computer Groups or Computer Policies.

Selecting "Open Advanced Search" from the "Search" drop-down menu toggles the display of the advanced search options:



Quarantined Files: No Grouping
Period: Last Hour
Computers: All Computers
Search: Infected File(s) Contains

Advanced Search functions (searches are not case sensitive):

- **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.

Pressing the "plus" 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 button (at the right of the tool bars with the right-arrow on it).

- **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.

Manually Restoring Quarantined Files

To manually restore a quarantined file, you must 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.*

Web Reputation Events

By default, the Deep Security Manager collects Web Reputation Event logs from the Deep Security Agents/Appliances at every heartbeat. The data from the logs is used to populate the various reports, graphs, and charts in the Deep Security Manager.

Once collected by the Deep Security Manager, Event logs are kept for a period of time which can be set **Administration > System Settings > Storage**. The default setting is one week.

From the main page you can:

- **View** (▤) the properties of an individual event
- **Filter the list:** Use the **Period** and **Computer** toolbars to filter the list of events
- **Export** (⇨) the event list data to a CSV file
- View existing **Auto-Tagging** (🏷) Rules.
- **Search** (🔍) for a particular event

Additionally, right-clicking an Event gives you the option to:

- **Add Tag(s):** Add an Event Tag to this event (See **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help.)
- **Remove Tag(s):** Remove exiting event Tags
- **Add to Allow List (✓):** Add the URL that triggered this Event to the list of Allowed URLs. (To view or Edit the **Allowed** and **Blocked** lists, go to the **Exceptions** tab on the main **Web Reputation** page.)
- **Computer Details:** View the Details window of the computer that generated the log entry

Columns for the Web Reputation Events display:

- **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 ***Ranking (page 173)***.)
- **Event Origin:** Indicates from which part of the Deep Security System the event originated.

View Event Properties

Double-clicking an event displays the **Properties** window for that entry which displays all the information about the event on one page.

Reclassify: If you feel that site safety ratings or the classification of a particular site is incorrect, please send feedback to Trend Micro through the Site Safety Center at http://sitesafety.trendmicro.com.

Add to Allow List...: Use the **Add to Allow List...** button to add this URL to the Allowed URLs list. (To view or Edit the **Allowed** and **Blocked** lists, go to the **Exceptions** tab on the main **Web Reputation** page.)

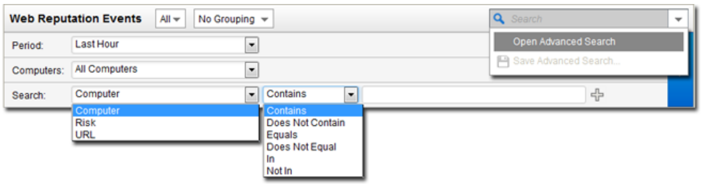
The **Tags** tab displays tags that have been attached to this Event. For More information on Event tagging, see **Policies > Common Objects > Other > Tags**, and **More About Event Tagging** in the Deep Security Manager Administrator's Guide or the online help in the **Reference** section.

Filter the List and/or Search for an Event

Selecting "Open Advanced Search" from the "Search" drop-down menu toggles the display of the advanced search options.

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.



Web Reputation Events All No Grouping

Period: Last Hour

Computers: All Computers

Search: Computer Contains

Advanced Search functions (searches are not case sensitive):

- **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

Pressing the "plus" 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 button (at the right of the toolbars with the right-arrow on it).

Export

Clicking the **Export...** button exports all or selected events to a CSV file.

Auto-Tagging

Clicking **Auto-Tagging...** displays a list of existing Web Reputation Auto-Tagging Rules.

Firewall Events

By default, the Deep Security Manager collects Firewall and Intrusion Prevention Event logs from the Deep Security Agents/Appliances at every heartbeat. The data from the logs is used to populate the various reports, graphs, and charts in the Deep Security Manager.

Once collected by the Deep Security Manager, Event logs are kept for a period of time which can be set in **Administration > System Settings > Storage**. The default setting is one week.

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.*

From the main page you can:

- **View** () the properties of an individual event
- **Filter the list:** Use the **Period** and **Computer** toolbars to filter the list of events
- **Export** () the event list data to a CSV file
- View existing **Auto-Tagging** () Rules.
- Add or remove **Columns** () from the Events list view.
- **Search** () for a particular event

Additionally, right-clicking an Event gives you the option to:

- **Add Tag(s):** Add an Event Tag to this event (See **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help.)
- **Remove Tag(s):** Remove exiting event Tags
- **Computer Details:** View the Details window of the computer that generated the log entry

Columns for the Firewall Events display:

- **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. (For a listing of possible packet rejection reasons, see "Packet Rejection Reasons" in the **Reference** section.)

- **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.*

View Event Properties

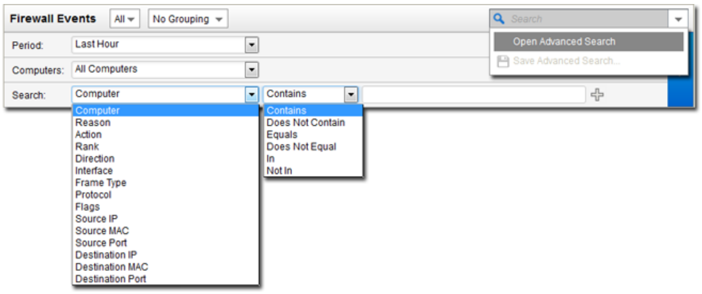
Double-clicking an event displays the **Properties** window for that entry which displays all the information about the event on one page. The **Tags** tab displays tags that have been attached to this Event. For More information on Event tagging, see **Policies > Common Objects > Other > Tags**, and **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help in the **Reference** section.

Filter the List and/or Search for an Event

Selecting "Open Advanced Search" from the "Search" drop-down menu toggles the display of the advanced search options.

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.



Advanced Search functions (searches are not case sensitive):

- **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

Pressing the "plus" 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 button (at the right of the toolbars with the right-arrow on it).

Export

Clicking the **Export...** button exports all or selected events to a CSV file.

Auto-Tagging

Clicking **Auto-Tagging...** displays a list of existing Firewall Auto-Tagging Rules.

Intrusion Prevention Events

By default, the Deep Security Manager collects Firewall and Intrusion Prevention Event logs from the Deep Security Agents/Appliances at every heartbeat.

Once collected by the Deep Security Manager, Event logs are kept for a period of time which can be set **Administration > System Settings > Storage**. The default setting is one week.

From the main page you can:

- **View** () the properties of an individual event
- **Filter the list:** Use the **Period** and **Computer** toolbars to filter the list of events
- **Export** () the event log data to a CSV file
- View existing **Auto-Tagging** () Rules.
- Add or remove **Columns** () from the Events list view.
- **Search** () for a particular event

Additionally, right-clicking an Event gives you the option to:

- **Select All:** Select all of the displayed events, up to a maximum of 100 events
- **Exported Selected to CSV:** Create a comma-separated file that lists details for the selected events. You can then open the CSV file in a spreadsheet.
- **View:** Display details about the event
- **Add Tag(s):** Add an Event Tag to this event (See **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help.)
- **Remove Tag(s):** Remove exiting event Tags
- **Computer Details:** View the Details window of the computer that generated the log entry

Columns for the Intrusion Prevention Events display:

- **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.

View Event Properties

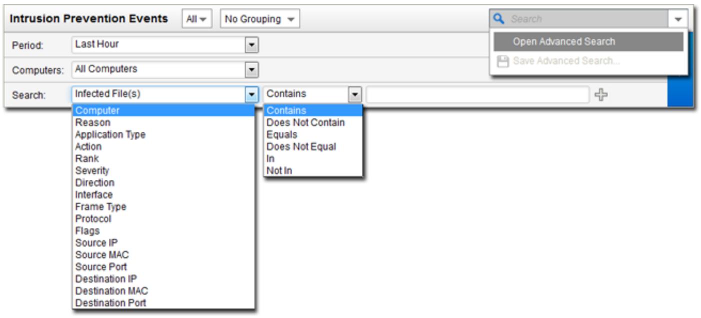
Double-clicking an event displays the **Properties** window for that entry. The **Tags** tab displays tags that have been attached to this Event. For More information on Event tagging, see **Policies > Common Objects > Other > Tags**, and **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help in the **Reference** section.

Filter the List and/or Search for an Event

Selecting "Open Advanced Search" from the "Search" drop-down menu toggles the display of the advanced search options.

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.



Period: Last Hour

Computers: All Computers

Search: Infected File(s) Contains

Advanced Search functions (searches are not case sensitive):

- **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

Pressing the "plus" 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 button (at the right of the toolbars with the right-arrow on it).

Export

Clicking the **Export...** button exports all event log entries to a CSV file.

Auto-Tagging

Clicking **Auto-Tagging...** displays a list of existing Intrusion Prevention Auto-Tagging Rules.

Integrity Monitoring Events

Deep Security Manager collects Integrity Monitoring Events from the Deep Security Agents at every heartbeat. The data from the logs is used to populate the various reports, graphs, and charts in the Deep Security Manager.

Once collected by the Deep Security Manager, Event logs are kept for a period of time which can be set **Administration > System Settings > Storage**. The default setting is one week.

From the main page you can:

- **View** () the properties of an individual event
- **Filter the list:** Use the **Period** and **Computer** toolbars to filter the list of events
- **Export** () the event list data to a CSV file
- Add an Auto-Tagging Rule
- Add or remove **Columns** () from the Events list view.
- **Search** (🔍) for a particular event

Additionally, right-clicking an Event gives you the option to:

- **Add Tag(s):** Add an Event Tag to this event (See **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help.)
- **Remove Tag(s):** Remove exiting event Tags
- **Computer Details:** View the Details window of the computer that generated the log entry
- **Integrity Monitoring Rule Properties:** View the properties of the Integrity Monitoring Rule associated with this event

Columns for the Integrity Monitoring Events display:

- **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

View Event Properties

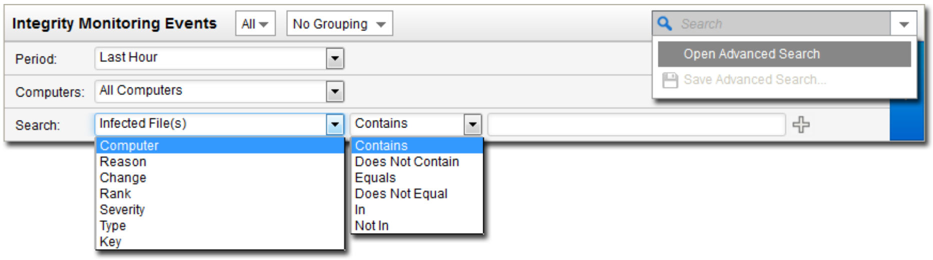
Double-clicking an event displays the **Properties** window for that entry which displays all the information about the event on one page. The **Tags** tab displays tags that have been attached to this Event. For More information on Event tagging, see **Policies > Common Objects > Other > Tags**, and **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help in the **Reference** section.

Filter the List and/or 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.

Use the "Search" or "Advanced Search" options to search, sort, or filter displayed events.



Integrity Monitoring Events All No Grouping

Period: Last Hour

Computers: All Computers

Search: Infected File(s) Contains

Advanced Search functions (searches are not case sensitive):

- **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

Export

Clicking the **Export...** button exports all or selected events to a CSV file.

Auto-Tagging

Clicking **Auto-Tagging...** displays a list of existing Integrity Monitoring Auto-Tagging Rules.

Log Inspection Events

Deep Security Manager collects Log Inspection Events from the Deep Security Agents at every heartbeat. The data from the logs is used to populate the various reports, graphs, and charts in the Deep Security Manager.

Once collected by the Deep Security Manager, Event logs are kept for a period of time which can be set **in Administration > System Settings > Storage**. The default setting is one week.

From the main page you can:

- **View** () the properties of an individual event
- **Search** () for a particular event
- **Filter the list:** Use the **Period** and **Computer** toolbars to filter the list of events
- View existing **Auto-Tagging** () Rules.
- Add or remove **Columns** () from the Events list view.
- **Export** () the event list data to a CSV file

Additionally, right-clicking an Event gives you the option to:

- **Add Tag(s):** Add an Event Tag to this event (See **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help.)
- **Remove Tag(s):** Remove exiting event Tags
- **Computer Details:** View the Details window of the computer that generated the log entry
- **Log Inspection Rule Properties:** View the properties of the Log Inspection Rule associated with this event

Columns for the Log Inspection Events display:

- **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.

View Event Properties

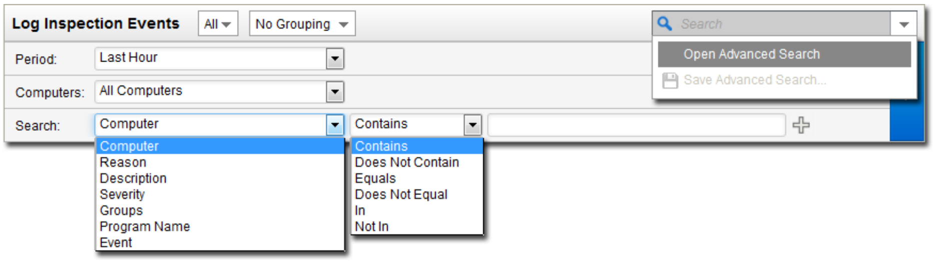
Double-clicking an event displays the **Properties** window for that entry which displays all the information about the event on one page. The **Tags** tab displays tags that have been attached to this Event. For More information on Event tagging, see **Policies > Common Objects > Other > Tags**, and **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help in the **Reference** section.

Filter the List and/or 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.

Use the "Search" or "Advanced Search" options to search, sort, or filter displayed events.



Log Inspection Events

Period: Last Hour

Computers: All Computers

Search: Computer Contains

Advanced Search functions (searches are not case sensitive):

- **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

Export

Clicking the **Export...** button exports all event log entries to a CSV file.

Auto-Tagging

Clicking **Auto-Tagging...** displays a list of existing Log Inspection Auto-Tagging Rules.

You can use Auto-tagging to automatically apply tags for the Log Inspection groups. LI 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.

Generate Reports

Deep Security Manager produces reports in PDF, or RTF formats. Most of the reports generated by the **Generate Reports** page 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.

Single Report

Report

The various reports can be output to PDF or RTF format, with the exception of the "Security Module Usage Report" and "Security Module Usage Cumulative Report", which are output as CSV files.

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
- **Computer Report:** Summary of each computer listed on the Computers tab
- **DPI Rule Recommendation Report:** Intrusion Prevention rule recommentations. 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

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.

Tag Filter

When you select a report that contains event data, you have the option to filter the report data using Event Tags. 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).

Time Filter

You can set the 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 occured between December 4th at 10:00am and December 5th at 10:00am.
- **Last 7 Days:** Includes events from the past week, ending at midnight of the current day. For example if you generate a report on December 5th at 10:14am, you will get a report for events that occured 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 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.*

Computer Filter

Set the computers whose data will be included in the report. You can include any computer for which you have viewing rights. Viewing rights are specified on the Computer Rights tab for a Role. (see ***Roles (page 202)*** for more information.)

Computer filter options:

- **All Computers:** If your viewing rights allow you to see all computers managed by Deep Security, you can select this option to include all computers in the report.
- **My Computers:** If your viewing rights allow you to see only certain computers, you can select this option to include all of the computers that you can view.
- **In Group:** Enables you to limit the report to computers that belong to a selected Group (and optionally, its sub-Groups).
- **Using Policy:** Enables you to limit the report to computers that are using a selected Policy (and optionally, its sub-Policies).

- **Computer:** Enables you to limit the report to just one selected 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.*

Encryption

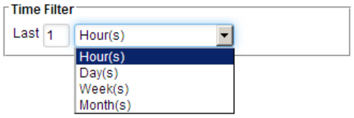
You can protect the report with a password.

Encryption options:

- Disable Report Password: The report will not be password-protected.
- Use Current User's Report Password: The report will be protected with the password of the currently signed in User. This option is not available if your role is Full Access.
- Use custom Report Password: The report will be protected with the password that you enter in the **Use custom Report Password** and **Confirm Password** boxes. The password does not have any complexity requirements.

Recurring Reports

Recurring Reports are simply Scheduled Tasks that periodically generate and distribute Reports to any number of Users and Contacts. Most of the options are identical to those for single reports, with the exception of Time Filter, which looks like this:



Time Filter

Last 1 Hour(s)

- **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, go to **Administration > Scheduled Tasks**.

Computers

The **Computers** section of the Deep Security Manager is where you to manage and monitor the computers on your network. 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 double-click on a User to open the User **Properties** window. The **Computer List** refresh rate can be set in the **Refresh Rate** area on the **Settings** tab.)

Computer icons:

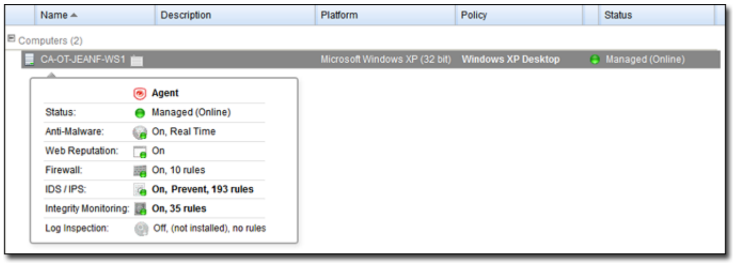
- Ordinary Computer
- Deep Security Relay (a computer with a Relay-enabled Agent)
- ESXi server
- Virtual computer (a virtual machine managed by VMware vCenter)
- Virtual computer (started)
- Virtual computer (stopped)
- Virtual computer (suspended)
- Virtual Appliance
- Virtual Appliance (started)
- Virtual Appliance (stopped)
- Virtual Appliance (suspended)

Preview Panes

Clicking the **Preview** icon () next to a listed computer expands a display area beneath it. The information displayed in the preview depends on the type of computer.

Ordinary Computer

The preview pane for an ordinary computer displays the presence of an Agent, its status, and the status of the Protection Modules. (Note that the Log Inspection module is off and the plug-in is not installed.)



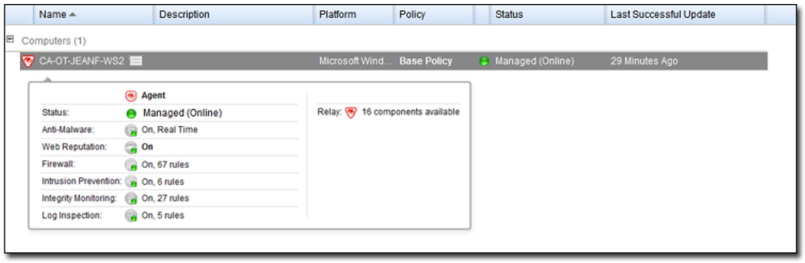
Name ▲	Description	Platform	Policy	Status
⊟ Computers (2)				
CA-OT-JEANF-WS1		Microsoft Windows XP (32 bit)	Windows XP Desktop	● Managed (Online)

	Agent
Status:	● Managed (Online)
Anti-Malware:	On, Real Time
Web Reputation:	On
Firewall:	On, 10 rules
IDS / IPS:	**On, Prevent, 193 rules**
Integrity Monitoring:	**On, 35 rules**
Log Inspection:	Off, (not installed), no rules

Protection Module Status

Relay

The preview pane for a Deep Security Relay 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.



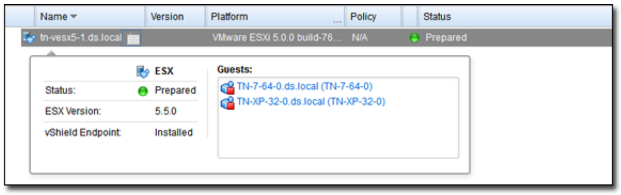
Name ▲	Description	Platform	Policy		Status	Last Successful Update
Computers (1)						
CA-OT-JEANF-WS2		Microsoft Wind...	Base Policy	●	Managed (Online)	29 Minutes Ago

	Agent
Status:	● Managed (Online)
Anti-Malware:	On, Real Time
Web Reputation:	On
Firewall:	On, 67 rules
Intrusion Prevention:	On, 6 rules
Integrity Monitoring:	On, 27 rules
Log Inspection:	On, 5 rules

Relay: 16 components available

ESXi server

The preview pane for an ESXi server displays its status and the version number of the ESXi software. It also displays the status of vShield Endpoint on this server (vShield Endpoint must be Installed to provide Anti-Malware protection). In the **Guests** area are displayed the presence of a Deep Security Virtual Appliance, and the virtual machines running on this host.



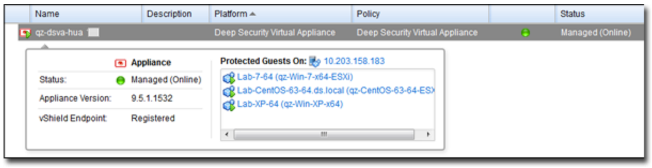
Name ▼	Version	Platform	Policy		Status
tn-vesx5-1.ds.local		VMware ESXi 5.0.0 build-76...	N/A	●	Prepared

	ESX
Status:	● Prepared
ESX Version:	5.5.0
vShield Endpoint:	Installed

Guests:
TN-7-64-0.ds.local (TN-7-64-0)
TN-XP-32-0.ds.local (TN-XP-32-0)

Virtual Appliance

The preview pane for a Virtual Appliance displays its status, the version number of the Appliance and the status of the vShield Endpoint on this Appliance (vShield Endpoint must be Registered to provide Anti-Malware protection). In the **Protected Guests On** area the protected virtual machines are displayed.



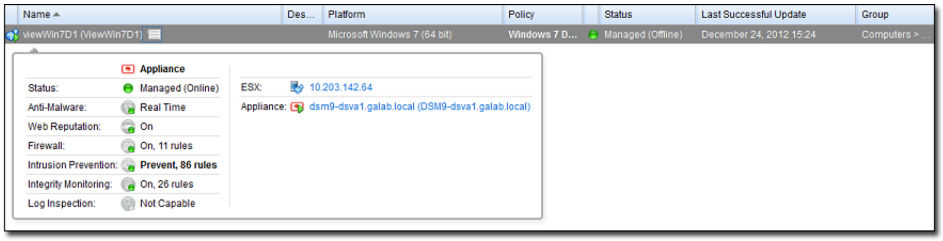
Name	Description	Platform ▲	Policy		Status
qz-dsva-hua		Deep Security Virtual Appliance	Deep Security Virtual Appliance	●	Managed (Online)

	Appliance
Status:	● Managed (Online)
Appliance Version:	9.5.1.1532
vShield Endpoint:	Registered

Protected Guests On: 10.203.158.183
Lab-7-64 (qz-Win-7-x64-ESXi)
Lab-CentOS-63-64.ds.local (qz-CentOS-63-64-ESX
Lab-XP-64 (qz-Win-XP-x64)

Virtual Machine with Agentless Protection

The preview pane for a virtual machine displays whether it is being protected by a Virtual Appliance, an in-guest Agent, or both. It displays details about the components running on the virtual machine.



Name ▲	Des...	Platform	Policy	Status	Last Successful Update	Group
viewWin7D1 (ViewWin7D1)		Microsoft Windows 7 (64 bit)	Windows 7 D...	Managed (Offline)	December 24, 2012 15:24	Computers > ...

	Appliance
Status:	Managed (Online)
Anti-Malware:	Real Time
Web Reputation:	On
Firewall:	On, 11 rules
Intrusion Prevention:	**Prevent, 86 rules**
Integrity Monitoring:	On, 26 rules
Log Inspection:	Not Capable

ESX: 10.203.142.64
Appliance: dsm9-dsva1.galab.local (DSM9-dsva1.galab.local)

Adding Computers to the Manager

For more detailed instructions on adding computers to the Deep Security Manager see **Adding Computers** in the Deep Security Manager Administrator's Guide or the online help.

Note: *After being installed on a computer, an Agent must be "activated" by the Deep Security Manager. During this process, the Deep Security Manager sends a "fingerprint" to the Agent. From that point on, the Agent will only accept instructions from a Manager with that unique fingerprint.*

Note: *If you install an Agent on a virtual machine that was previously being protected agentlessly by a Deep Security Virtual Appliance, the virtual machine will have to be activated again from the Manager to register the presence of the Agent on the computer.*

Define a New Computer

Clicking **New** in the toolbar displays a computer creation wizard. Type the hostname or IP address of the new computer and optionally select a Policy to be applied to the new computer from the drop-down list. Clicking **Next** will tell the Manager to find the computer on the network.

- **If the computer you specified is not found,** the Manager will still create an entry for it in the **Computers** page, but you will have to ensure that the Manager can reach this computer and that the Agent is installed and activated. Then you can apply the appropriate Policy to it.
- **If the computer is found but no Agent is identified,** the Manager will create an entry for the computer on the **Computers** page. You will have to install an Agent on the computer and activate it.
- **If the computer is found and an Agent is detected,** the Manager will create an entry in the **Computers** page. As soon as you exit the wizard (by clicking **Finish**), the Manager will activate the Agent on the computer and apply the Policy you selected.

Discover Computers

Clicking **Discover...** in the toolbar displays the **Discover Computers** dialog. During discovery, the Manager searches the network for any visible computers that are not already listed. When a new 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. After discovery operations, a computer can be in one of the following states:

- **Discovered (No Agent/Appliance):** The computer has been detected but no Agent/Appliance is present. The computer may also be in this state if an Agent/Appliance is installed but has been previously activated and is configured for Agent/Appliance initiated communications. Because of the one-way communication from the

Agent/Appliance, the Manager will not know the status of the Agent/Appliance. In this case, you will have to deactivate the Agent/Appliance on the computer and reactivate it from the Manager.

- **Discovered (Activation Required):** The Agent is installed and listening for communication from the Manager, but has not been activated. This status may also indicate that the Agent/Appliance is installed and listening, and has been activated, but is not yet being managed by the Manager. This could occur if this Manager was at one point managing the Agent/Appliance, but the Agent/Appliance'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/Appliance on this computer, right-click the computer and select "Activate/Reactivate". Once reactivated, the status will change to "Online".
- **Discovered (Deactivation Required):** The Agent/Appliance is installed and listening, but it has already been activated by another Manager. In this case the Agent/Appliance must be deactivated prior to activation by this Manager.
- **Discovered (Unknown):** The computer has been detected but the presence or absence of an Agent/Appliance cannot be ascertained.

Note: *The Discovery operation will only check the status of newly discovered computers. To update the status of already listed computers, right-click the selected computer(s) and select **Actions > Check Status**.*

Note: *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.*

Note: *When running a Discovery operation with the **Automatically Resolve IPs to hostnames** option enabled, it is possible that the discovery operation will find hostnames where Deep Security Manager can not. Discovery is able to fall back to using a WINS query or NetBIOS broadcast to resolve the hostname in addition to DNS. Deep Security Manager only supports hostname lookup via DNS.*

Note: *The Discovery operation will not discover computers running as virtual machines in a vCenter. The Discovery operation will not discover computers in a Microsoft Active Directory.*

Add Directory

Deep Security Manager can connect to and synchronize with a Microsoft Active Directory. For detailed instructions on importing a list of computers from an Active Directory, see **Active Directory** in the Deep Security Manager Administrator's Guide or the online help.

Add VMware vCenter

Deep Security Manager supports a tight integration with VMware vCenter and ESXi server. You can import the organizational and operational information from vCenter and ESXi nodes and allow detailed application of security to an enterprise's VMware infrastructure. For detailed instructions on importing virtual computers from a VMware system, see **VMware vCenter** in the Deep Security Manager Administrator's Guide or the online help.

Add Cloud Account

Deep Security can connect to and manage computers (virtual or physical) provided by Amazon EC2, VMware vCloud, and Microsoft Azure services. For detailed instructions on adding computers from a Cloud Provider, see **Cloud Account** in the Deep Security Manager Administrator's Guide or the online help.

Search for a Computer

Use the **Search** textbox to search for a particular computer among already discovered (i.e. listed) computers. For more sophisticated search options, use the "Advanced Search" option below it.

Advanced Search functions (searches are not case sensitive):

- **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

Export Selected Computers

Export your computers list to an XML or CSV file. You may wish to do this to backup your computer information, integrate it with other reporting systems, or if you are migrating computers to another Deep Security Manager. (This will save you the trouble of re-discovering and scanning 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. In order to export this configuration information use the Policy export option in the **Policies** page.*

Activate/Reactivate the Agent/Appliance on a Computer

When a computer is unmanaged the Agent/Appliance must be activated to move the computer into a managed state. Prior to activation the Agent/Appliance will be one of the following states: On the **Computers** page, right-click the computer whose Agent/Appliance you wish to Activate/Reactivate and select "Activate/Reactivate" from the **Actions** menu. (Alternatively, you can click the **Activate** or **Reactivate** button in the computer's **Details** window.)

- **No Agent/Appliance:** Indicates there is no Agent/Appliance running or listening on the default port. The "No Agent/Appliance" status can also mean that an Agent/Appliance is installed and running but is working with another Manager and communications are configured as "Agent/Appliance Initiated", and so the Agent/Appliance is not listening for this Manager. (If you wish to correct the latter situation, you will have to deactivate the Agent from the computer).
- **Activation Required:** The Agent/Appliance is installed and listening, and is ready to be activated by the Manager.
- **Reactivation Required:** The Agent/Appliance is installed and listening and is waiting to be reactivated by the Manager.
- **Deactivation Required:** The Agent/Appliance is installed and listening, but has already been activated by another Manager.

- **Unknown:** The computer has been imported (as part of an imported computer list) without state information, or has been added by way of an LDAP directory discovery process.

After a successful activation the Agent/Appliance state will change to "Online". If the activation failed the computer status will display "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 and Appliances, it is blocked by default. To allow IPv6 traffic on Deep Security 8.0 Agents and Appliances, go to the* ***Advanced Network Engine Settings*** *area of the* ***Settings > Network Engine*** *tab in a Policy or Computer editor and set the* ***Block IPv6 for 8.0 and Above Agents and Appliances*** *option to* ***No****.*

Check the Status of a Computer

This command checks the status of a computer without performing a scan or activation attempt.

Deactivate the Agent/Appliance on a Computer

You may want to transfer control of a computer from one Deep Security Manager installation to another. If so, the Agent/Appliance has to be deactivated and then activated again by the new Manager. Deactivating the Agent/Appliance can be done from the Manager currently managing the Agent. *Deactivating an Agent may also be done directly on the computer from the command line. Deactivating an Appliance may also be done directly on the vSphere client by connecting to the Deep Security Virtual Appliance console and then selecting* ***Reset Appliance****.*

Send an Updated Policy to a Computer

When you use Deep Security Manager to change the configuration of an Agent/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/Appliance. This is a "Send Policy" instruction. Policy updates usually happen immediately but you can force an update by clicking **Send Policy**.

Download a Security Update

This command downloads the latest Security Update from the configured Relay to the Agent/Appliance.

Roll back Security Update

This command rolls back the latest Security Update for the Agent/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:

- If the Agent for the computer has been reset locally
- If the computer has been removed from the network before you had a chance to deactivate or delete it from the list of computers

Upgrade the Agent/Appliance Software on a Computer

To upgrade an Agent or Appliance, you first need to import a newer version of the Agent or Appliance software package into the Deep Security Manager. You can import an Agent or Appliance software package from the Trend Micro Download Center (as described below) or you can manually import the software to the Manager from a local directory (see ***Local Software (page 218)***).

To import a software package to Deep Security from the Download Center:

1. Go to **Administration > Updates > Software** > **Download Center**. This page lists all of the software packages available on the Trend Micro Download Center. Packages that you have already imported into Deep Security Manager have a green checkmark (✓) in the **Imported** column. They are also listed on the **Administration > Updates > Software** > **Local** tab. Packages that are out-of-date have ⚠ in the **Imported** column.
2. To update a package that is out of date, right-click the package name and click **Import**.

Once a package has been imported, you can use it to upgrade one or more Agents or Appliances.

To upgrade the Agent/Appliance:

1. On the **Computers** page, right-click the computers whose Agents or Appliances you wish to upgrade and select **Actions** > **Upgrade Agent/Appliance Software**.
2. If there are no installers of an appropriate platform and version (the version must be higher than the Agent/Appliance's) the following message will be displayed: "There are no authenticated Agent/Appliance Software Install Programs available for the selected computer(s) platform or version. Please add an appropriate Agent/Appliance Software Install Program using the **Download Center** or **Local** panel in **Administration** > **Updates** > **Software** before upgrading the Deep Security Agents/Appliances." Otherwise, the Upgrade Agent/Appliance Software dialog appears. In that dialog box, select the version of the Agent/Appliance that you want to install and specify when the upgrade will occur. You can choose to upgrade the Agent/Appliance now, or select **Use a Schedule for Upgrade** and specify how often you want Deep Security to check for and install upgraded Agent/Appliance software.

Note: *In rare circumstances, the computer may require a reboot to complete the upgrade. If this is the case, an Alert will be triggered. To find out right away whether a reboot is required, check the text of the "Agent Software Upgraded" or "Virtual Appliance Upgraded" event to see if the platform installer indicated that a reboot is required.*

Note: *The "Reboot Required" Alert must be dismissed manually, it will not be dismissed automatically.*

Note: *The Deep Security Virtual Appliance uses the Red Hat Enterprise Linux 6 (64 bit) Agent package. When you import the Virtual Appliance into Deep Security Manager, the Red Hat Agent will be imported as well. When you activate a Virtual Appliance on a computer, Deep Security upgrades the Red Hat Agent to the latest version available in Deep Security Manager. You cannot delete the latest Red Hat Agent unless you first remove all Virtual Appliance software packages. You can delete older versions of the Red Hat Agent only if they are not in use.*

Scan for Recommendations

Deep Security Manager can scan computers and then make recommendations for Security Rules. The results of a Recommendation Scan can be seen in the computer's **Details** window in the various **Rules** pages. See the documentation for the **Computer Details window** for more information.

Clear Recommendations

Clear Rule recommendations resulting from a Recommendation Scan on this computer. This will also remove the computer from those listed in an Alert produced as a result of a Recommendation Scan.

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 ***Malware Scan Configurations (page 67)*** for more information.

Quick Scan for Malware

Scans critical system areas for currently active threats. Quick Scan will look for currently active malware but it will not perform deep file scans to look for dormant or stored infected files. On larger drives it is significantly faster than a Full Scan.

Note: *Quick Scan is only available on-demand. You cannot schedule a Quick Scan as part of a Scheduled Task.*

Scan Computers for Open Ports

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 **Policy/Computer Editor > Settings > Scanning**.)

Note: *Port 4118 is always scanned regardless of port range settings. It is the port on the computer to which Manager initiated communications are sent. If communication direction is set to "Agent/Appliance Initiated" for a computer (**Policy/Computer Editor > Settings > Computer > Communication Direction**), port 4118 is closed.*

Note: *New computers on the network will not be detected. To find new computers you must use the **Discover** tool.*

Cancel any Currently Executing Port Scans

If you have initiated a set of port scans to a large number of computers and/or over a large range of ports and the scan is taking too long, use this 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 the documentation for the **Integrity Monitoring** page.

Rebuild Integrity Baseline

Rebuild a baseline for Integrity Monitoring on this computer.

Move a Computer to a Computer Group

To move a computer to new computer group, right-click the computer and choose **Actions > Move to Group...**

Assign a Policy to a Computer

This opens a window with a drop-down list allowing 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.

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.*

Assign an 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. For more information see **Administration > System Settings > Ranking**.

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...**.

Delete a Computer

If you delete a computer, 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.

Examine Events Associated with a Computer

Examine system and security-related Events associated with the computer.

Add a New Computer Group

Creating computer groups is useful from an organizational point of view and it speeds up the process of applying and managing Policies. Right-click the computer group under which you want to create the new computer group and select **Add Group**.

Add Computers and Computer Groups Imported from a Microsoft Active Directory structure

Discover computers by importing from an LDAP-based directory (such as Microsoft Active Directory). Computers are imported, and synchronized according to the structure in the directory. For more information, see **Adding Computers** in the Deep Security Manager Administrator's Guide or the online help.

Remove a Group

You can only remove a computer group if it contains no computers and has no sub-groups.

Move Computers from the Current Group to Another

You can move a computer from one computer group to another but 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.

View or Edit the Properties of a Computer Group

The properties of groups include their name and description.

Note: *Some of the features described on this page will appear only after the corresponding modules are enabled. For example, when you click **Actions** on the **Computers** page, **Full Scan for Malware** and **Scan for Integrity Changes** are displayed only if the Anti-Malware and Integrity Monitoring modules are enabled.*

Policies

Policies

The Policies page displays your existing Policies showing their parent/child relationship in a hierarchical tree structure.

- ***Policies (page 46)***

Common Objects

The Common Objects pages list objects that can be shared by many constructs like Policies and Rules throughout Deep Security. This can be considered the root repository for shared objects. The Policy and Computer editor windows display the same list of objects but the properties of these common objects can be overridden for the Policy or the specific 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** in the Deep Security Manager Administrator's Guide or the online help.

Rules

The Rules pages list existing protection module Rules (for those modules that make use of Rules).

- ***Firewall Rules (page 74)***
- ***Intrusion Prevention Rules (page 78)***
- ***Integrity Monitoring Rules (page 84)***
- ***Log Inspection Rules (page 88)***

Lists

- ***Directory Lists (page 49)***
- ***File Extension Lists (page 52)***
- ***File Lists (page 53)***
- ***IP Lists (page 56)***
- ***MAC Lists (page 57)***
- ***Port Lists (page 58)***

Other

- ***Contexts (page 61)***
- ***Firewall Stateful Configurations (page 63)***
- ***Malware Scan Configurations (page 67)***
- ***Schedules (page 59)***
- ***Tags (page 60)***

Policies

Policies allow collections of Rules and configuration settings to be saved for easier assignment to multiple computers.

The **Policies** page shows your existing Policies in their hierarchical tree structure. From the Policies page you can:

- Create **New** Policies from scratch ( )
- **Import** Policies from an XML file ( ) (located under the **New** menu.)

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.*

- Examine or modify the **Details** of an existing Policy ( )
- **Duplicate** (and then modify and rename) an existing Policy ( )
- **Delete** a Policy ( )
- **Export** a Policy to an XML file ( )

  Note: *When you export a selected Policy to XML, any child Policies 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.*

Clicking **New** ( ) opens the **Policies** wizard which will prompt you for the name of the new Policy and then give you the option of opening the **Policy Details window**. Clicking **Details** ( ) displays the **Policy Details** window.

Note: *You can create a new Policy based on a Recommendation Scan of a computer. To do so, select a computer and run a Recommendation Scan. (Right-click the computer on the **Computers** page 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.*

To assign a Policy to a computer:

1. In the Deep Security Manager, 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**.

For more information on how to use Policies to protect your computers, see **Quick Start: Protecting a Server** in the Deep Security Manager Administrator's Guide or the online help.

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** in the Deep Security Manager Administrator's Guide or the online help.

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 **Recommendation Scans** in the Deep Security Manager Administrator's Guide or the online help for more information.

Common Objects

Common Objects include:

- ***Directory Lists (page 49)***
- ***File Lists (page 53)***
- ***File Extension Lists (page 52)***
- ***IP Lists (page 56)***
- ***MAC Lists (page 57)***
- ***Port Lists (page 58)***
- ***Contexts (page 61)***
- ***Firewall Stateful Configurations (page 63)***
- ***Schedules (page 59)***
- ***Tags (page 60)***
- ***Firewall Rules (page 74)***
- ***Intrusions Prevention Rules (page 78)***

Directory Lists

Directory Lists are reusable lists of directories.

From the main page you can:

- Create a **New Directory List** ( ) from scratch
- **Import from File** ( ) imports scan directory lists from an XML file
- Examine or modify the **Properties** of an existing directory list ( )
- **Duplicate** (and then modify) existing directory lists ( )
- **Delete** a directory list ( )
- **Export** ( ) one or more directory list(s) to an XML or CSV file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)
- **Add/Remove Columns** ( ) columns can be added or removed by clicking **Add/Remove Columns**. The order in which the columns are displayed can be controlled by dragging them into their new position. Listed items can be sorted and searched by the contents of any column.

Clicking **New** ( ) or **Properties** ( ) displays the Directory List **Properties** window.

Directory List Properties

General Information

The name and description of the directory list.

Directory(s)

Type the directory(s) that are going to be on your list. Only put one directory per line.

Supported Formats

Note: *The inclusion directory settings accept either forward slash "/" or backslash "\" to support both Windows and Linux conventions.*

The following table describes the syntax available for defining Directory Lists:

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\***

Directory	Format	Description	Examples
			Includes all files on a network resource identified using an IP or a hostname. ***\\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. ***C:\abc\wx*z*** *Matches:* C:\abc\wxz\ C:\abc\wx123z\ *Does not match:* C:\abc\wxz C:\abc\wx123z ***C:\abc\*wx*** *Matches:* C:\abc\wx\ C:\abc\123wx\ *Does not match:* C:\abc\wx 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\**** *Matches:* C:\abc\ C:\abc\1 C:\abc\123 *Does not match:* C:\abc C:\abc\123\ C:\abc\123\456 C:\abx\ C:\xyz\ ***C:\abc\*wx*** *Matches:* C:\abc\wx C:\abc\123wx *Does not match:* C:\abc\wx\ C:\abc\123wx\ ***C:\abc\wx*z*** *Matches:* C:\abc\wxz C:\abc\wx123z *Does not match:*

Directory	Format	Description	Examples
			C:\abc\wxz\ C:\abc\wx123z\ ***C:\abc\wx**** *Matches:* C:\abc\wx C:\abc\wx\ C:\abc\wx12 C:\abc\wx12\345\ C:\abc\wxz\ *Does not match:* C:\abc\wx123z\
Environment variable	${ENV VAR}	Includes all files and subdirectories defined by an environment variable with the format ${ENV VAR}. For a Virtual Appliance, the value pairs for the environment variable must be defined in **System Setting > Computers Tab > Environment Variable Overrides.**	***${windir}*** 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***

Assigned To

The **Assigned To** tab lists the rules making use of this directory list. Clicking the names of the rules displays their **Properties** window.

File Extension Lists

The **File Extension Lists** page contains a list of file extensions that are used by **Malware Scan Configurations**. 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.

From the main page you can:

- Create a **New File Extension List** ( ) from scratch
- **Import from File** () imports scan file extensions from an XML file
- Examine or modify the **Properties** of an existing file extension list ()
- **Duplicate** (and then modify) existing file extension lists ()
- **Delete** a file extension list ( )
- **Export** () one or more file extension list(s) to an XML or CSV file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)
- **Add/Remove Columns** () columns can be added or removed by clicking **Add/Remove Columns**. The order in which the columns are displayed can be controlled by dragging them into their new position. Listed items can be sorted and searched by the contents of any column.

Clicking **New** ( ) or **Properties** () displays the File Extension Lists **Properties** window.

File Extension List Properties

General Information

The name and description of the file extension list.

File Extensions(s)

Type the file extension(s) that are going to be on your list. Only put one extension per line.

Assigned To

The **Assigned To** tab lists the rules making use of this file extension list. Clicking the names of the rules displays their **Properties** window.

File Lists

File Lists are reusable lists of files.

General

Use the **File Lists** section to create a reusable list of valid files. From the main page you can:

- Create a **New File List** ( ) from scratch
- **Import from File** ( ) imports scan files from an XML file
- Examine or modify the **Properties** of an existing file list ( )
- **Duplicate** (and then modify) existing file lists ( )
- **Delete** a file list ( )
- **Export** ( ) one or more file list(s) to an XML or CSV file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)
- **Add/Remove Columns** ( ) columns can be added or removed by clicking **Add/Remove Columns**. The order in which the columns are displayed can be controlled by dragging them into their new position. Listed items can be sorted and searched by the contents of any column.

Clicking **New** ( ) or **Properties** ( ) displays the File List **Properties** window.

File List Properties

General Information

The name and description of the file list.

File(s)

Type the file(s) that are going to be on your list. Only put one filename per line.

Supported Formats

Note: *The inclusion settings accept either forward slash "/" or backslash "\" to support both Windows and Linux conventions.*

The following table describes the syntax available for defining File List inclusions:

Inclusion	Format	Description	Example
File	FILE	Includes all files with the specified file name regardless of its location or directory.	**_abc.doc_** Includes all files named "abc.doc" in all directories. Does not include "abc.exe".
File path	FILEPATH	Includes the specific file specified by the file path.	**_C:\Documents\abc.doc_** 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_** Includes any file that has prefix of "abc" and extension of ".exe". **_*.db_** _Matches:_ 123.db abc.db _Does not match:_ 123db 123.abd cbc.dba **_*db_** _Matches:_ 123.db 123db ac.db acdb db _Does not match:_ db123 **_wxy*.db_** _Matches:_ wxy.db wxy123.db _Does not match:_ wxydb
File with wildcard (*)	FILE.EXT*	Includes all files with a matching pattern in the file extension.	**_abc.v*_** Includes any file that has file name of "abc" and extension beginning with ".v". **_abc.*pp_** _Matches:_ abc.pp abc.app _Does not match:_ wxy.app **_abc.a*p_** _Matches:_ abc.ap abc.a123p _Does not match:_

Inclusion	Format	Description	Example
			abc.pp ***abc.**** *Matches:* abc.123 abc.xyz *Does not match:* 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*** *Matches:* ac.ap a123c.ap ac.a456p a123c.a456p *Does not match:* ad.aa
Environment variable	${ENV VAR}	Includes files specified by an environment variable with the format ${ENV VAR}. These can be defined or overridden using **System Setting > Computers Tab > Environment Variable Overrides.**	***${myDBFile}*** Includes the file "myDBFile".
Comments	FILEPATH #Comment	Allows you to add comments to your inclusion definitions.	***C:\Documents\abc.doc #This a comment***

Assigned To

The **Assigned To** tab lists the names of the files making use of this file list. Clicking the names of the file lists displays their **Properties** windows.

IP Lists

Use the **IP Lists** page to create reusable lists of IP addresses for use by multiple Firewall Rules.
From the main page you can:

- Create **New** IP Lists from scratch ( )
- **Import** ( ) IP Lists from an XML file
- Examine or modify the **Properties** of an existing IP List ( )
- **Duplicate** (and then modify) existing IP Lists ( )
- **Delete** an IP List ( )
- **Export** ( ) one or more IP lists to an XML or CSV file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking **New** ( ) or Properties ( ) displays the IP List **Properties** window.

IP List Properties

General Information

The name and description of the IP list.

IPs

Type the IP addresses, masked IP addresses, and IP address ranges that are going to be on your list. Only put one of these per line.

Supported Formats

As well as individual addresses, you can enter IP ranges and masked IPs. Use these examples to properly format your entries. (You can insert comments into your IP list by preceding the text with a hash sign ("#").)

Assigned To

The **Assigned To** tab lists the rules making use of this IP List. Clicking the names of the rules displays their **Properties** window.

MAC Lists

Use the **MAC Lists** section to create reusable lists of MAC addresses.
From the main page you can:

- Create **New** ( ) MAC lists from scratch
- **Import** ( ) MAC lists from an XML file
- Examine or modify the **Properties** of an existing MAC list ( )
- **Duplicate** (and then modify) existing MAC lists ( )
- **Delete** a MAC list ( )
- **Export** ( ) one or more MAC lists to an XML or CSV file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking **New** ( ) or Properties ( ) displays the MAC List **Properties** window.

MAC List Properties

General Information

The name and description of the list.

MAC(s)

Type the MAC addresses that are going to be on your list. Only put one of these per line.

Supported Formats

The MAC(s) list supports MAC addresses in both hyphen- and colon-separated formats. Use these examples to properly format your entries. (You can insert comments into your MAC list by preceding the text with a pound sign ("#").)

Assigned To

The **Assigned To** tab lists the rules making use of this MAC list. Clicking the names of the rules displays their **Properties** window.

Port Lists

Use the **Port Lists** page to create reusable lists of ports.
From the main page you can:

- Create **New** port lists from scratch ( )
- **Import** ( ) port lists from an XML file
- Examine or modify the **Properties** of an existing port list ( )
- **Duplicate** (and then modify) existing port lists ( )
- **Delete** a port list ( )
- **Export** ( ) one or more port lists to an XML or CSV file. (Either export them all using the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking **New** ( ) or **Properties** ( ) displays the Port List **properties window.**

Port List Properties

General Information

The name and description of the list.

Port(s)

Enter the ports that are going to be on your list. Only put one of these per line.

Note: *For a listing commonly accepted port assignments, see the [Internet Assigned Numbers Authority (IANA)]*

Supported Formats

Individual ports and port ranges can be included on the list. Use these examples to properly format your entries. (You can insert comments into your port list by preceding the text with a pound sign ("#").)

Assigned To

The **Assigned To** tab lists the rules making use of this port list. Clicking the names of the rules displays their **Properties** window.

Schedules

Schedules are reusable timetables.

From the toolbar or the right-click shortcut menu you can:

- Create **New** schedules from scratch ( )
- **Import** ( ) schedules from an XML file
- Examine or modify the **Properties** of an existing schedule ( )
- **Duplicate** (and then modify) existing schedules ( )
- **Delete** a schedule ( )
- **Export** ( ) one or more schedules to an XML or CSV file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking New ( ) or Properties ( ) displays the Schedule properties window.

Schedule Properties

Schedule periods are defined by hour-long time blocks. Clicking a time block selects it, and shift-clicking de-selects it.

Assigned To

The **Assigned To** tab displays a list of the rules making use of this schedule.

Tags

Event Tagging allows administrators to manually tag events with predefined labels ("attack", "suspicious", "patch", "acceptable change", "false positive", "high priority", etc.) and the ability to define custom labels ("Assigned to Tom for review", etc.).

In addition to the manual tagging of events, automated event tagging can be accomplished via the use of a "Trusted Computer" which is particularly useful for managing Integrity Monitoring events. 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 automatically be tagged as "acceptable changes" thereby reducing the number of events that need to be analyzed by an administrator.

Event tagging enables specialized views of events, dashboards, and reports and can be applied to a single event, similar events, or even to all future similar events.

Tags

All currently defined tags are displayed in the **Policies > Common Objects > Other > Tags** page. This includes predefined as well as custom tags. (Only tags that are currently in use are displayed.)

Delete Tags: Deleting a tag removes the tag from all events to which it is attached.

Auto-Tag Rules

Auto-Tag Rules are created by selecting events and choosing to tag similar items.

For information on Event Tagging procedures, see **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help.

Contexts

Contexts are a powerful way of implementing different security policies depending on the 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. (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" drop-down menu.)

Contexts can be used to provide Agents with "location awareness". To determine a computer's location, Contexts examine the nature of the computer's connection to its domain controller and connectivity to the Internet. Select the **Context applies when Domain Controller connection is** option and choose from the following:

- **Locally Connected to Domain:** true only if the computer can connect to its domain controller directly
- **Remotely Connected to Domain:** true if the computer can only connect to its domain controller via VPN
- **Not Connected to Domain:** true if the computer cannot connect to its domain controller
- **Not Connected to Domain, No Internet Connectivity:** true if the computer cannot connect to its domain controller by any means and the host has no Internet connectivity. (The test for Internet connectivity can be configured in **Administration > System Settings > Contexts**.)

By assessing the ability of the computer to connect with its domain controller or the Internet, the Agent can then implement rules such as restricting HTTP traffic to non-routable ("private") IP addresses only.

Note: *For an example of a Policy that implements Firewall Rules using Contexts, examine the properties of the "Location Aware - High" Policy.*

From the toolbar or the right-click shortcut menu on the **Contexts** page, you can:

- Create **New** () Contexts from scratch
- **Import** () Contexts from an XML file (located under the **New** menu.)
- Examine or modify the **Properties** of an existing Context ()
- **Duplicate** (and then modify) existing Contexts ()
- **Delete** a Context ( )
- **Export** () one or more Contexts to an XML or CSV file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)
- **Add/Remove Columns** () columns can be added or removed by clicking **Add/Remove Columns**. The order in which the columns are displayed can be controlled by dragging them into their new position. Listed items can be sorted and searched by the contents of any column.

Clicking **New** () or Properties () displays the Context **Properties** window.

Context Properties

General Information

The name and description of the Context Rule as well as the earliest version of the Deep Security Agent the rule is compatible with.

Options

Context applies when Domain Controller connection is

Specifying an option here will determine whether or not 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 (VPN) ".

The time interval between Domain Controller connectivity tests is the same as the Internet Connectivity Test interval which is also configurable in **Administration > System Settings > Contexts**.

Note: *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. (Primarily used for Allow or Force Allow Firewall Rules.)

Assigned To

The **Assigned To** tab displays a list of the rules making use of this Context.

Firewall Stateful Configurations

Deep Security's Firewall Stateful 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.).

Note: *ICMP stateful filtering is only available in Deep Security Agent versions 8.0 or earlier.*

The **Firewall Stateful Configurations** page lets you define multiple stateful inspection configurations which you can then include in your Policies. From the toolbar or shortcut menu you can:

- Create **New** () Firewall Stateful Configurations from scratch
- **Import** () Firewall Configuration from an XML file (located under the **New** menu.)
- Examine or modify the **Properties** () of an existing Firewall Stateful Configuration
- **Duplicate** () (and then modify) existing Firewall Stateful Configurations
- **Delete** a Firewall Stateful Configuration ()
- **Export** () one or more Firewall Stateful Configurations to an XML or CSV file. (Either export them all using the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)
- **Add/Remove Columns** () columns can be added or removed by clicking **Add/Remove Columns**. The order in which the columns are displayed can be controlled by dragging them into their new position. Listed items can be sorted and searched by the contents of any column.

Clicking **New** () or **Properties** () displays the **Firewall Stateful Configuration properties window.**

Firewall Stateful Configuration Properties

General Information

- **Name:** The name of the Firewall Stateful Configuration.
- **Description:** Type a description of the Firewall Stateful Configuration. This description will only appear here.

IP Packet Inspection

- **Deny all incoming fragmented packets:** If this option is enabled, all fragmented packets are dropped with the following log entry: "IP fragmented packet". The one exception to this rule is the presence of packets with a total length smaller than the IP header length. Such packets are dropped silently.
  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

TCP Packet Inspection

- **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]*

  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.

    Note: *Incoming connection limits are only available on Deep Security Agent 8.0 and earlier.*

  - **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.

    Note: *Outgoing connection limits are only available on Deep Security Agent 8.0 and earlier.*

  - **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:* *Half-open connection limits are only available on Deep Security Agent 8.0 and earlier.*

> *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

The following FTP options are only available on Deep Security Agent 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

- **Enable UDP stateful inspection:** Check 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.*

Without stateful inspection of UDP traffic, an attacker could masquerade as a DNS server and send unsolicited UDP "replies" from source port 53 to computers behind a firewall.

- **Enable UDP stateful logging:** Checking this option will enable the logging of UDP stateful inspection events.

ICMP

Note: ICMP stateful inspection is only available on Deep Security Agent versions 8.0 or earlier.

- **Enable ICMP stateful inspection:** Check 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.)

  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:** Checking this option will enable the logging of ICMP stateful inspection events.

Assigned To

The **Assigned To** tab lists the Policies and computers that are making use of this stateful inspection configuration.

Malware Scan Configurations

Deep Security allows you to create a variety of Malware Scan Configurations to automatically handle the way the detection of malware is processed. Configuration options include what files to scan, whether the scanning is done in real time or on a scheduled basis, and what actions to carry out if malware is detected. This page lets you define global Malware Scan Configurations. How, in what combination, and when these configurations are in effect on a computer is set at the Policy and at the computer levels. Also, as with most elements in Deep Security, many global settings can be overridden at the Policy and computer levels. (See **Policies, Inheritance and Overrides** in the Deep Security Manager Administrator's Guide or the online help for more information.)

There are two kinds of Malware Scan Configurations: **Real-time Scan** and **Manual/Scheduled Scan**. While most actions are available to both types of scans, some actions, like **Deny Access** are available to Real-time Scans only, and other options, like **CPU Usage** are available to Manual/Scheduled Scans only.

From the global **Malware Scan Configuration** page you can:

- Create **New** ( ) Real-time or Manual/Scheduled Scan configurations
- **Import** () an existing Scan Configuration from an XML file. (located under the **New** menu.)
- View the **Properties** () of a Malware Scan Configuration.
- **Duplicate** () (and then modify) existing file configurations.
- **Delete** ( ) the highlighted configuration file from the configuration list.
- **Export** () the displayed or selected configuration to a XML or CSV file.
- **Add or Remove Columns** () from the display**.**
- **Search** ( ) for a particular configuration file.

Properties

General

General Information

- Name and description of the Malware Scan Configuration, and whether this is a Real-Time or a Manual/Scheduled scan type.

Scan Settings

- **Directories to scan:** Specify which directories to scan for malware. You can scan **All directories** or select from a defined **Directory List**.
- **Files to scan:** Specify which files to scan for malware. Choose between **All files**, **File types scanned by IntelliScan**, or choose from a defined **File Extension List** (which will scan all files with the extensions defined in the list).

Note: ***IntelliScan*** *only scans file types that are vulnerable to infection (for example, .zip or .exe). IntelliScan does not rely on file extensions to determine file type but instead reads the header and/or content of a file to determine whether it should be scanned. Compared to scanning all files, using IntelliScan provides a performance boost by reducing the total number of files to scan.*

Exclusions

Allows you to exclude specific directories, files, and file extensions 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: *The scan exclusion directory settings accept either forward slash "/" or backslash "\" to support both Windows and Linux conventions.*

The following table describes the syntax available for defining Directory List exclusions:

Exclusion	Format	Description	Examples
Directory	DIRECTORY	Excludes all files in the specified directory and all files in all subdirectories.	***C:\Program Files\*** Excludes all files in the "Program Files" directory and all subdirectories.
Directory with wildcard (*)	DIRECTORY*\	Excludes any subdirectories with any subdirectory name, but does not exclude the files in the specified directory.	***C:\abc\*\\*** Excludes all files in all subdirectories of "abc" but does not exclude the files in the "abc" directory. ***C:\abc\wx*z\*** *Matches:* C:\abc\wxz\ C:\abc\wx123z\ *Does not match:* C:\abc\wxz C:\abc\wx123z ***C:\abc\*wx\*** *Matches:* C:\abc\wx\ C:\abc\123wx\ *Does not match:* C:\abc\wx 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\\**** *Matches:* C:\abc\ C:\abc\1 C:\abc\123 *Does not match:* C:\abc C:\abc\123\ C:\abc\123\456

Exclusion	Format	Description	Examples
			C:\abx\ C:\xyz\ ***C:\abc\*wx*** *Matches:* C:\abc\wx C:\abc\123wx *Does not match:* C:\abc\wx\ C:\abc\123wx\ ***C:\abc\wx*z*** *Matches:* C:\abc\wxz C:\abc\wx123z *Does not match:* C:\abc\wxz\ C:\abc\wx123z\ ***C:\abc\wx**** *Matches:* C:\abc\wx C:\abc\wx\ C:\abc\wx12 C:\abc\wx12\345\ C:\abc\wxz\ *Does not match:* C:\abc\wx123z\
Environment variable	${ENV VAR}	Excludes all files and subdirectories defined by an environment variable with the format ${ENV VAR}. For a Virtual Appliance, the value pairs for the environment variable must be defined in **Policy/Computer Editor > Settings > Computer > Environment Variable Overrides.**	***${windir}*** If the variable resolves to "c:\windows", excludes all the files in "c:\windows" and all its subdirectories.
Comments	DIRECTORY #Comment	Allows you to add comments to your exclusion definitions.	***c:\abc #Exclude the abc directory***

The following table describes the syntax available for defining File List exclusions:

Exclusion	Format	Description	Example
File	FILE	Excludes all files with the specified file name regardless of its location or directory.	***abc.doc*** 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*** Excludes only the file named "abc.doc" in the "Documents" directory.
File with wildcard (*)	FILE*	Excludes all files with a matching pattern in the file name.	***abc*.exe*** Excludes any file that has prefix of "abc" and extension of ".exe". ****.db*** *Matches:* 123.db abc.db

Exclusion	Format	Description	Example
			Does not match: 123db 123.abd cbc.dba **_*db_** *Matches:* 123.db 123db ac.db acdb db *Does not match:* db123 **_wxy*.db_** *Matches:* wxy.db wxy123.db *Does not match:* wxydb
File with wildcard (*)	FILE.EXT*	Excludes all files with a matching pattern in the file extension.	**_abc.v*_** Excludes any file that has file name of "abc" and extension beginning with ".v". **_abc.*pp_** *Matches:* abc.pp abc.app *Does not match:* wxy.app **_abc.a*p_** *Matches:* abc.ap abc.a123p *Does not match:* abc.pp **_abc.*_** *Matches:* abc.123 abc.xyz *Does not match:* 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_** *Matches:* ac.ap a123c.ap ac.a456p a123c.a456p

Exclusion	Format	Description	Example
			Does not match: ad.aa
Environment variable	${ENV VAR}	Excludes files specified by an environment variable with the format ${ENV VAR}. These can be defined or overridden using **System Setting > Computers Tab > Environment Variable Overrides.**	***${myDBFile}*** Excludes the file "myDBFile".
Comments	FILEPATH #Comment	Allows you to add comments to your exclusion definitions.	***C:\Documents\abc.doc #This a comment***

The following table describes the syntax available for defining File Extension List exclusions:

Exclusion	Format	Description	Example
File Extension	EXT	Excludes all files with a matching file extension.	***doc*** Excludes all files with a ".doc" extension in all directories.
Comments	EXT #Comment	Allows you to add comments to your exclusion definitions.	***doc #This a comment***

The following table describes the syntax available for defining Process Image File List exclusions (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*** Excludes only the file named "file.exe" in the "abc" directory.

Actions

Recognized Malware

Upon detection

You can instruct Deep Security to automatically decide which actions to take upon detecting malware by selecting the **Use action determined by ActiveAction** option.

> *Note:* ***ActiveAction*** *is a predefined set 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. ActiveAction scan actions are updated along with virus pattern updates.*

The following table lists the actions taken when ActiveAction is selected:

Malware Type	Real-Time Scan	Manual/ Scheduled Scan	Notes
Virus	Clean	Clean	Viruses are able to infect normal files by inserting malicious code. Typically, whenever an infected file is opened, the malicious code automatically runs and delivers a payload in addition to infecting other files. Some of the more common types of viruses include COM and EXE infectors, macro viruses, and boot sector viruses.
Trojan	Quarantine	Quarantine	Trojans are non-infecting executable malware files that do not have file infection capabilities.
Packer	Quarantine	Quarantine	Packers are compressed and/or 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)	Quarantine	Quarantine	Although possibly legitimate, grayware exhibit spyware-like behavior and may be unwanted.
Possible malware	Pass	Pass	Files detected as possible malware are typically unknown malware components. By default, these detections are logged and files are anonymously sent back to Trend Micro for analysis.

Malware Type	Real-Time Scan	Manual/ Scheduled Scan	Notes
Cookies	N/A	Delete	Cookies are text files stored by a Web browser. Cookies contain site-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.
Other Threats	Clean	Clean	The Other Threats category includes joke programs, which display false notifications or manipulate screen behavior, but are generally harmless.

Alternatively, you can manually specify the actions you want Deep Security to take upon detecting malware. There are five possible actions that Deep Security can take when it encounters an infected file:

1. **Pass:** Allows full access to the infected file without doing anything to the file. (An Anti-Malware Event will still be recorded.)
2. **Clean:** Cleans a cleanable file before allowing full access to the file. (Not available for Possible Malware.)
3. **Delete:** Deletes the infected file.
4. **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 or Scheduled scan, a "Pass" action will be applied and an Anti-Malware Event will be recorded.
5. **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 **Anti-Malware > Quarantined Files** for more information.)

Possible malware

Select an action to take if a file is identified as possible malware. Possible malware is a file that appears suspicious but cannot be classified as a specific malware variant. If you leave this option set to "Default", the action will be what was selected in **Upon Detection**, above. When possible malware is detected, Trend Micro recommends that you contact your support provider for assistance in further analysis of the file.

Options

General Options

- **Enable Spyware/Grayware Scan:** The Spyware Scan Engine scans for Spyware/Grayware and performs the actions specified on the **Actions** tab.
- **Scan Compressed Files:** Specify under what conditions to scan a file and whether to scan compressed files.
  - **Maximum levels of compression from which to extract files:** A file or group of files can undergo more than one round of compression. This option lets you specify through how many levels of compression you want Deep Security to scan.
  - **Maximum size of individual extracted files:** The maximum size of the individual files in a compressed archive to scan.

    Note: *Scanning large files with multiple layers of compression can affect performance.*

  - **Maximum number of files to extract:** The maximum number of files to extract from a compressed archive and scan.

- **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. Because embedded objects can contain other objects, there can be multiple layers of embedding within a single Office file. To reduce the impact on performance, you can select to scan only a few layers of embedded objects within each file.
    - **Scan for exploit code in Microsoft Office Objects:** Exploit Detection heuristically identifies malware by checking Microsoft Office files for exploit code.

> Note: *The specified number of layers is applicable to both OLE objects and Scan for exploit options.*

- **Enable IntelliTrap (Real-Time only):** Virus writers often attempt to circumvent virus filtering by using real-time compression algorithms. IntelliTrap helps reduce the risk of such viruses entering your network by blocking real-time compressed executable files and pairing them with other malware characteristics. (IntelliTrap only works in Real-Time mode.)

> 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. If users regularly exchange real-time compressed executable files, disable IntelliTrap. IntelliTrap uses the following Anti-Malware components: Virus Scan Engine, IntelliTrap Pattern, IntelliTrap Exception Pattern.*

- **Enable Network Directory Scan (Real-Time only):** To scan files and folders in network shares and mapped network drives, enable this option.

> Note: *Resources accessed in "**~/.gvfs**" via GVFS, a virtual filesystem available for the GNOME desktop, will be treated as local resources, not network drives.*

- **Scan files when (Real-Time only):** Choose between scanning files only when they are opened for reading, or when they are opened for both reading and writing.
- **CPU Usage (Manual/Scheduled Scan only):** Specifies the CPU resources allocated to scanning.
    - **High:** Scans files one after another without pausing
    - **Medium:** Recommended; pauses when overall CPU usage exceeds 50%
    - **Low:** Pauses when overall CPU usage exceeds 20%

Alert

Select whether an Alert is raised if this Malware Scan Configuration triggers an event.

Assigned To

Indicates which Policy(s) and computer(s) are using this particular Malware Scan Configuration.

Firewall Rules

Firewall Rules examine the control information in individual packets. The Rules either block or allow those packets based on rules that are defined on these pages. Firewall Rules are assigned directly to computers or to Policies which are in turn assigned to a computer or collection of computers.

Note: *Solaris Agents will only examine packets with an IP frame type, and 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.*

Firewall Rule icons:

- Normal Firewall Rules
- Firewall Rules that operate according to a schedule

From the main page you can:

- Create **New** ( ) Firewall Rules from scratch
- **Import** ( ) Firewall Rules from an XML file (located under the **New** menu.)
- Examine or modify the **Properties** of an existing Firewall Rule ( )
- **Duplicate** (and then modify) existing Firewall Rules ( )
- **Delete** a Firewall Rule ( )
- **Export** ( ) one or more Firewall Rules to an XML or CSV file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)
- **Add/Remove Columns** ( ) columns can be added or removed by clicking **Add/Remove Columns**. The order in which the columns are displayed can be controlled by dragging them into their new position. Listed items can be sorted and searched by the contents of any column.

Note: *Firewall Rules that are assigned to one or more computers or that are part of a Policy cannot be deleted.*

Clicking **New** ( ) or Properties ( ) displays the **Firewall Rules Properties** window.

Firewall Rule Properties

General Information

- **Name:** The name of the Firewall Rule.
- **Description:** A detailed description of the Firewall Rule.
- **Action:** Your Firewall Rule can behave in four different ways. These are described here in order of precedence:
  1. The traffic can **bypass** the firewall completely. This is a special rule that can cause the packets to bypass the Firewall and Intrusion Prevention engine entirely. Use this setting for media intensive protocols where

filtering may not be desired. To find out more about the **bypass** rule, see "Bypass Rule" in the **Reference** section.

2. It can **log only**. This means it will only make an entry in the logs and not interfere with the traffic.
3. It can **force allow** defined traffic (it will allow traffic defined by this rule *without* excluding any other traffic.)
4. It can **deny** traffic (it will deny traffic defined by this rule.)
5. It 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.*

> Note: *Only one rule action is applied to any particular packet, and rules (of the same priority) are applied in the order listed above.*

- **Priority:** If you have selected "force allow", "deny", or "log only" as your rule action, you can set a priority here of 0 (low) to 4 (highest). Setting a priority allows you to combine the actions of rules to achieve a cascading rule effect. **Log only** rules can only have a priority of **4**, and **Allow** rules can only have a priority of **0**.

> Note: *The priority determines the order in which rules are applied. 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 ever gets applied to it.*

- **Packet Direction:** Select whether this rule will be applied to **incoming** or **outgoing** traffic.
- **Frame Type:** Select a frame type. Use the **Not** checkbox to specify whether you will be filtering *for* this frame type or *anything but* this frame type.

> Note: *You can exclusively select **IPv4** or **IPv6**. To specify either (both), select **IP**.*

> Note: *For a list of frame types, see the Internet Assigned Numbers Authority (IANA) Web site.*

- **Protocol:** Select or specify the protocol your rule will be looking for. Use the checkbox to specify whether you will be filtering *for* this protocol or *anything but* this protocol.

> Note: *You can choose from the drop down list of predefined common protocols, or you can select "Other" and enter the protocol code yourself (a three digit decimal value from 0 to 255).*

Packet Source

The following options apply to the packet header's source information:

- **IP:** Specify an IP address, a masked IP address, an IP range, or select an IP list from one you defined in the **IP Lists** page.
- **MAC:** Specify a MAC address or select a MAC list from one you defined in the **MAC Lists** page.
- **Port:** You can specify a comma separated list of ports or a dash separated port range in the port(s) option as well as just a single port (e.g., 80, 443, 1-100) or select a Port list from one you defined in the **Port Lists** page.

Packet Destination

The following options apply to the packet header's destination information:

- **IP:** Specify an IP address, a masked IP address, an IP range, or select an IP list from one you defined in the **IP Lists** page.
- **MAC:** Specify a MAC address or select a MAC list from one you defined in the **MAC Lists** page.
- **Port:** You can specify a comma separated list of ports or a dash separated port range in the port(s) option as well as just a single port (e.g., 80, 443, 1-100) or select a Port list from one you defined in the **Port Lists** page.

Specific Flags

If you have selected TCP, ICMP, or TCP+UDP as your protocol in the General Information section above, you can direct your Firewall Rule to watch for specific flags.

Events

Select whether to enable or disable logging Events because of this Rule. If event logging is enabled, you can record the packet data with the Event.

Note: *Note that any form of allow Rule (Allow, Force Allow, Bypass) will not log any events because they would overwhelm the database.*

Options

Alert

Select whether or not this Firewall Rule should trigger an Alert when it is triggered. If you only wish this rule to be active during specific periods, assign a schedule from the drop-down list.

Note: *Only Firewall Rules whose "Action" is set to "Deny" or "Log Only" can be configured to trigger an Alert. (This is because Alerts are triggered by counters which are incremented with data from log files.)*

Schedule

Select whether the Firewall Rule should only be active during a scheduled time.

Note: *Firewall Rules that are active only at scheduled times are displayed in the* ***Firewall Rules*** *page with a small clock over their icon ().*

Context

Rule Contexts are a powerful way of implementing different security policies depending on the computer's network environment. You will most often use Contexts to create Policies which apply different Firewall and Intrusion Prevention Rules to computers (usually mobile laptops) depending on whether that computer is in or away from the office.

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.

To determine a computer's location, Contexts examine the nature of the computer's connection to its domain controller. For more information on Contexts, see **Policies > Common Objects > Other > Contexts**.

Note: *For an example of a Policy that implements Firewall Rules using Contexts, look at the properties of the "Windows Mobile Laptop" Policy.*

Assigned To

This tab displays a list of Policies which include this Firewall Rule as well as any computers to which this Firewall Rule has been assigned directly. Firewall Rules can be assigned to Policies in the **Policies** page and to computers in the **Computers** page.

Intrusion Prevention Rules

Whereas Firewall Rules and Firewall Stateful Configurations examine a packet's control information (data that describes the packet), Intrusion Prevention Rules examine the actual content of the packet (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets: from replacing specifically defined or suspicious byte sequences, to completely dropping packets and resetting the connection.

Intrusion Prevention Rule icons:

- Normal Intrusion Prevention Rules
- Intrusion Prevention Rules that operate according to a schedule
- Intrusion Prevention Rules that have configuration options
- ⚠ Intrusion Prevention Rules must be configured before use

The **Intrusion Prevention Rules** page lets you create and manage Intrusion Prevention Rules. From the toolbar or the right-click shortcut menu you can:

- Create **New** Intrusion Prevention Rules from scratch ( )
- **Import** ( ) Intrusion Prevention Rules from an XML file (located under the **New** menu.)
- Examine or modify the **Properties** of an existing Intrusion Prevention Rule ( )
- **Duplicate** (and then modify) existing Intrusion Prevention Rules ( )
- **Delete** an Intrusion Prevention Rule ( )
- **Export** ( ) one or more Intrusion Prevention Rules to an XML or CSV file. (Either export them all using the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)
- **Add/Remove Columns** ( ) columns can be added or removed by clicking **Add/Remove Columns**. The order in which the columns are displayed can be controlled by dragging them into their new position. Listed items can be sorted and searched by the contents of any column.

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.*

Intrusion Prevention Rule 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/Appliance required to implement this Intrusion Prevention Rule.

Details

- **Application Type:** The Application Type this Intrusion Prevention Rule will be grouped under. You can select an existing type, or create a new one.

Note: *You can also edit existing types from this panel. Remember that if you edit an existing Application Type from here, the changes will be applied to all security elements making use of it.*

- **Priority:** The priority level of the Intrusion Prevention 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.
- **Detect Only:** Use this checkbox when testing new rules. By checking this box, the rule will create a log entry prefaced with the words "detect only:" but will not interfere with traffic. If you set the "disable logging" checkbox in the next panel (below), the rule's activity will not be logged regardless of whether "Detect Only" is checked or not.

Note: *Some Intrusion Prevention Rules are designed to only operate in "Detect Only" mode and cannot be configured to block traffic. For these rules, the "Detect Only" option will be set and locked so it cannot be changed.*

Events

- **Disable Event Logging:** Check to disable Event logging.
  - **Generate Event on Packet Drop:** Log the dropping/blocking of a packet.
  - **Always Include Packet Data:** Includes the packet data in the log entry.
  - **Enable Debug Mode:** Logs multiple packets preceding and following the packet that triggered the rule. Trend Micro recommends only using this option if instructed to do so by your support provider.

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. When X-Forwarded-For header data is available, it is displayed in the Event's Properties window. To enable this feature, the "Always Include Packet Data" option must be selected. In addition, rule 1006540 " Enable X-Forwarded-For HTTP Header Logging" must be enabled.*

Identification (Displayed for 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 (not downloaded).
- **Last Updated:** The last time the Rule was modified either locally or during Security Update download.

- **Identifier:** The rule's unique identifier tag.

Vulnerability (Displayed for Trend Micro rules only)

Displays information about this particular vulnerability. 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.)

Configuration (Displayed for Trend Micro rules only)

- **Configuration Options:** If the downloaded rule has any configurable options, they will be displayed here. Examples of options might be header length, allowed extensions for http, cookie length, etc. If you apply a rule without setting a required option, an Alert will be triggered telling you which rule on which computer(s) requires configuration. (This also applies to any rules that are downloaded and automatically applied by way of a Security Update.)

Note: *Intrusion Prevention Rules that have configuration options are displayed in the **Intrusion Prevention Rules** page with a small gear over their icon ( ).*

View Rules (Available for custom Intrusion Prevention Rules only)

The **View Rules...** button will be available for Intrusion Prevention Rules that have not been marked confidential by Trend Micro. (Contact Trend Micro for information on writing your own Intrusion Prevention Rules.)

Options

Alert

Select whether or not this Intrusion Prevention Rule should trigger an Alert when it is triggered. If you only wish this rule to be active during specific periods, assign a schedule from the drop-down list.

Schedule

Select whether the Intrusion Prevention Rule should only be active during a scheduled time.

Note: *Intrusion Prevention Rules that are active only at scheduled times are displayed in the **Intrusion Prevention Rules** page with a small clock over their icon ( ).*

Context

Contexts are a powerful way of implementing different security policies depending on the computer's network environment. You will most often use Contexts to create Policies which apply different Firewall and Intrusion Prevention Rules to computers (usually mobile laptops) depending on whether that computer is in or away from the office.

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.

To determine a computer's location, Contexts examine the nature of the computer's connection to its domain controller. For more information on Contexts, see **Policies > Common Objects > Other > Contexts**.

Recommendation Options

Use this option to exclude this Intrusion Prevention Rule from Rule recommendations made after Recommendation Scans.

Assigned To

This tab displays the list of computers and Policies to which this Intrusion Prevention Rule is assigned.

Application Types

The applications defined by Application Types are identified by the direction of traffic, the protocol being used, and the port through which the traffic passes. Application Types are a useful way of grouping Intrusion Prevention Rules. They are used to organize Intrusion Prevention Rules with a common purpose into groups. This simplifies the process of selecting a set of Intrusion Prevention Rules to assign to a computer. For example, consider the set of Intrusion Prevention Rules required to protect HTTP traffic to an Oracle Report Server. By grouping Intrusion Prevention Rules into Application Types it is easy to select rules in the "Web Server Common" and "Web Server Oracle Report Server" sets while excluding, for example, the set of rules that are specific to IIS Servers.

Application Type icons:

- Application Types without configuration options
- Application Types that have configuration options

From the main page you can:

1. Define a **New** ( ) Application Type
2. **Import** ( ) Application Types from an XML file (located under the **New** menu.)
3. View or edit the **Properties** ( ) of an existing Application Type
4. **Duplicate** (and then modify) existing Application Types ( )
5. **Export** ( ) one or more Application Types to an XML or CSV file. (Either export them all using the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)
6. **Delete** ( ) an Application Type
7. **Add/Remove Columns** ( ) columns can be added or removed by clicking **Add/Remove Columns**. The order in which the columns are displayed can be controlled by dragging them into their new position. Listed items can be sorted and searched by the contents of any column.

Clicking **New** ( ) or **Properties** ( ) displays the Application Type **Properties** window.

General

General Information

The name and description of the Application Type. "Minimum Agent/Appliance Version" tells you what version of the Deep Security Agent/Appliance 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.)

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 over source port 80.

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.

Integrity Monitoring Rules

Integrity Monitoring Rules allow the Deep Security Agents to 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. These changes are logged as Events in the Manager and can be configured to generate Alerts like any other Events. Integrity Monitoring Rules can be assigned directly to computers or can be made part of a Policy.

Integrity Monitoring Rules specify which Entities (files, registry keys, services, etc) to monitor for changes. Deep Security scans all the Entities specified by the rules assigned to a computer and creates a baseline against which to compare future scans of the computer. If future scans do not match the baseline, the Deep Security Manager will log an Integrity Monitoring Event and trigger an Alert (if so configured).

Integrity Monitoring Rule icons:

- Normal Integrity Monitoring Rules
- Integrity Monitoring Rules that have configuration options

From the main page you can:

- Create **New** Integrity Monitoring Rules from scratch ( )
- **Import** ( ) Integrity Monitoring Rules from an XML file
- Examine or modify the **Properties** of an existing Integrity Monitoring Rule ( )
- **Duplicate** (and then modify) existing Integrity Monitoring Rules ( )
- **Delete** a Integrity Monitoring Rule ( )
- **Export** ( ) one or more Integrity Monitoring Rules to an XML or CSV file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)

Note: *Integrity Monitoring Rules that are assigned to one or more computers or that are part of a Policy cannot be deleted.*

Clicking **New** ( ) or Properties ( ) displays the **Integrity Monitoring Rules Properties** window.

Integrity Monitoring Rule Properties

General Information

The name and description of the Integrity Monitoring Rule, and -- if the rule is issued by Trend Micro -- the minimum versions of the Agent and the Deep Security Manager that are required for the Rule to function.

Details

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**.)

Identification

Date when the rule was first issued and when it was last updated, as well as a unique identifier for the rule.

Content

Note: *The **Content** tab only appears for Integrity Monitoring Rules that you create yourself. Integrity Monitoring Rules issued by Trend Micro have a **Configuration** tab instead that displays the Integrity Monitoring Rule's configuration options (if any). Integrity Monitoring Rules issued by Trend Micro are not editable (although you can duplicate them and then edit the copy.)*

You have the choice between three templates for creating new Integrity Rules: the **Registry Value** template, the **File** template, or the **Custom (XML)** template. Use the **Registry Value** template for creating Integrity Monitoring Rules that monitor changes to registry values. Use the **File** template for creating simple Integrity Monitoring Rules that monitor changes to files only. Use the **Custom (XML)** template to write rules in XML for monitoring directories, registry values, registry keys, services, processes, installed software, ports, (and files).

This section of the help describes the use of the **Registry Value** and **File** templates. For information on writing Integrity Monitoring Rules in XML using the Custom (XML) template, see **Integrity Monitoring Rule Language** in the Deep Security Manager Administrator's Guide or the online help in the **Reference** section.

Registry Value Template

Base Key

Select the base key to monitor and whether or not to monitor contents of sub keys.

Value Names

List value names to be included or excluded. Use "?" and "*" as wildcard characters.

Attributes

Use "Standard" to monitor changes in size or content. For other attributes, see *RegistryValueSet* in the **Reference** section under Integrity Rules Language.

File Template

Base Directory

Specifies the base directory for the rule. Everything else about the rule will be relative to this directory. Select "Include Sub Directories" to include sub directories. For example, a valid entry would be `C:\Program Files\MySQL` and selecting "Include Sub Directories".

File Names

Use the **File Names** fields to include or exclude specific files. Use wildcards (" ? " for a single character and " * " for zero or more characters).

> Note: *These fields can be left blank to monitor all files in the base directory, but this can be very demanding on system resources if there are many and/or large files in the directory.*

Attributes

The following file attributes can be monitored for change:

- **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 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 will prevent the OS from updating the last accessed timestamp and will speed 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.
- **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 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 only): The inode number of the file.
- **DeviceNumber** (Unix only): Device number of the disk on which the inode associated with the file is stored.
- **BlocksAllocated** (Unix only: The number of blocks allocated to store the file.

You can use the shorthand keyword "STANDARD", which will look for changes to:

- **Created**
- **LastModified**
- **Permissions**
- **Owner**
- **Group**

- **Size**
- **Contents**
- **Flags (Windows only)**
- **SymLinkPath (Unix only)**

Options

- **Alert when this rule logs an event:** Triggers an Alert if the rule is triggered.
- **Allow Real Time Monitoring:** This options is selected by default. When it is not selected, the Integrity Monitoring events will be raised only when you perform a scan for changes.

Assigned To

Displays a list of Policies which include this Integrity Monitoring Rule as well as any computers to which this Integrity Monitoring Rule has been assigned directly. Integrity Monitoring Rules can be assigned to Policies in the **Policies** page and to computers in the **Computers** page.

Log Inspection Rules

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. Log Inspection Rules can be assigned directly to computers or can be made part of a Policy. Like Integrity Monitoring Events, Log Inspection events can be configured to generate Alerts in the Deep Security Manager.

Log Inspection icons:

- Normal Log Inspection Rules
- Log Inspection Rules that have configuration options

From the main page you can:

- Create **New** ( ) Log Inspection Rules from scratch
- **Import** ( ) Log Inspection Rules from an XML file
- Examine or modify the **Properties** of an existing Log Inspection Rule ( )
- **Duplicate** (and then modify) existing Log Inspection Rules ( )
- **Delete** a Log Inspection Rule ( )
- **Export** ( ) one or more Log Inspection Rules to an XML or CSV file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)

Note: *Log Inspection Rules that are assigned to one or more computers or that are part of a Policy cannot be deleted.*

Note: *Deep Security Manager ships with a standard set of OSSEC Log Inspection Rules. For more information on Log Inspection, see* **Examining a Log Inspection Rule** in the Deep Security Manager Administrator's Guide or the online help *and* **Log Inspection** in the Deep Security Manager Administrator's Guide or the online help*. For further assistance in writing your own Log Inspection Rules using the XML-based language, consult the OSSEC documentation or contact your support provider.*

Clicking **New** ( ) or Properties ( ) displays the **Log Inspection Rules Properties** window.

General

General Information

The name and description of the Log Inspection Rule, and -- if the rule is issued by Trend Micro -- the minimum versions of the Agent and the Deep Security Manager that are required for the Rule to function.

Identification

Date when the rule was first issued and when it was last updated, as well as a unique identifier for the rule.

Content

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). Log Inspection Rules issued by Trend Micro are not editable (although you can duplicate them and then edit the copy.)*

Template

In the **Content** tab, select the "Basic Rule" template.

General Information

Enter a Rule ID. A 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.)

Give the rule a level. Zero (0) means the rule never logs an event, although other rules that watch for this rule may fire. (See the dependency fields below.)

Optionally assign the rule to one or more comma-separated groups. This can come into play when dependency is used since you can create rules that fire on the firing of a rule, or a rule that belongs to a specific group.

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

Note: *For information on the regular expression syntax used by the Log Inspection module, see http://www.ossec.net/doc/syntax/regex.html*

Composite

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.

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.

Files

Type the full path to the file(s) you want your rule to monitor and specify the type of file it is.

Options

Alert

Select whether this rule triggers an alert in the Deep Security Manager or not.

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 which have different severity levels, you can use the "Alert Minimum Severity Level" drop-down menu to set the minimum severity from the multiple rules which will trigger an Alert.

Assigned To

Lists which Security Profiles or computers are using this Log Inspection Rule.

Recommendations

Deep Security can be configured to perform regular Recommendation Scans which scan a computer and make recommendations about the application of various Security Rules. Selecting this checkbox will automatically assign recommended Log Inspection Rules to the computer and automatically unassign rules that are not required.

To turn the recommendation engine on or off, go to **Policy/Computer Editor > Settings > Scanning**.

Computer and Policy Editors

Whereas the main Deep Security Manager window serves to manage and organize the elements of the whole Deep Security system, the **Policy Editor** and **Computer Editor** windows are used to select Deep Security elements from the Deep Security Manager and apply them to the Policy or specific computer.

The Policy **Details** window is very similar to the main Deep Security Manager window except that all elements in the Policy Details window apply specifically to the Policy. By default, all settings are inherited from the global settings of the main Deep Security Manager window. Changes can be made in the Policy window that will apply only to this Policy. When modifying the properties of an element in the main Deep Security Manager window (Firewall Rule, Intrusion Prevention Rule, etc.), the only option is to modify the "Properties". When modifying the properties of an element in the Policy Details window, an additional option is available: "Properties (For This Policy)".

If you edit the "Properties (For this Policy)", the changes will only affect that element when it is applied to a computer by this Policy.

If you edit the "Properties", the changes will affect the element globally (except where it has been overridden elsewhere).

An element whose properties have been edited "For This Policy" will appear in bold letters in the Task Pane to indicate that it has special properties when applied to a computer as a part of this Policy.

See also:

- **Policies, Inheritance and Overrides** in the Deep Security Manager Administrator's Guide or the online help

Overview (Policy Editor)

The Policy **Overview** page has the following tabbed sections:

- ***General (page 93)***
- ***Computer(s) Using This Policy (page 94)***
- ***Events (page 95)***

General

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:** When Anti-Malware protection is on, the Anti-Malware status light is green. When it is off, the Anti-Malware status light is gray.
- **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.

Computer(s) Using This Policy

Lists computers to which this Policy has been assigned.

Events

Note: *The Events lists in the Policy Editors only display Events that are associated with the current Policy.*

The System Event log is a record of system-related events (as opposed to security-related events). From the main page you can:

- **View** () the details (properties) of a system event
- **Search** () for a particular system event
- **Export** () currently displayed system events to a CSV file
- View existing **Auto-Tagging** () Rules.

Additionally, right-clicking an Event gives you the option to:

- **Add Tag(s):** Add an Event Tag to this event (See **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help.)
- **Remove Tag(s):** Remove exiting Event Tags

View

Selecting an event and clicking **View** () displays the **Event Viewer Properties** window.

General

General Information

- **Time:** The time according to the system clock on the computer hosting the Deep Security Manager.
- **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 entry in the system event log will be displayed here.

Tags

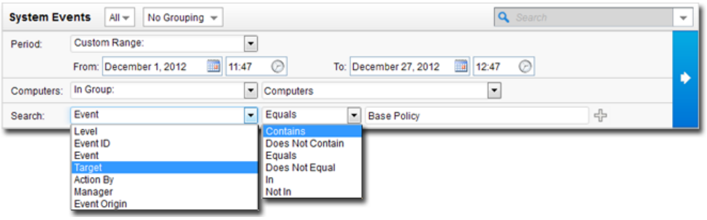
The **Tags** tab displays tags that have been attached to this Event. For More information on Event tagging, see **Policies > Common Objects > Other > Tags**, and **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help in the **Reference** section.

Filter the List and/or 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.



System Events

Period: Custom Range:

From: December 1, 2012 11:47 To: December 27, 2012 12:47

Computers: In Group: Computers

Search: Event Equals Base Policy

Pressing 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

You can export displayed events to a CSV file. (Paging is ignored, all pages will be exported.) You have the option of displaying the displayed list or the selected items.

Auto-Tagging

Clicking **Auto-Tagging...** displays a list of existing System Event Auto-Tagging Rules.

Overview (Computer Editor)

The computer **Overview** page has the following tabbed sections:

- *General (page 98)*
- *Actions (page 101)*
- *TPM (ESXi servers only.) (page 103)*
- *Events (page 104)*

General

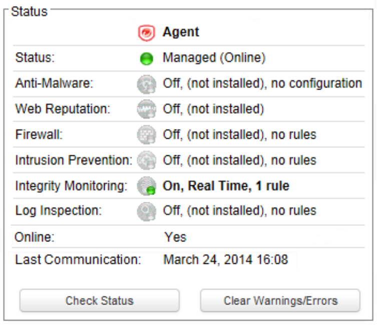
General

- **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 may be used if a hostname is used instead of an IP address.)
- **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 drop-down 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** drop-down 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.)

Status



Status

	Agent
Status:	● Managed (Online)
Anti-Malware:	Off, (not installed), no configuration
Web Reputation:	Off, (not installed)
Firewall:	Off, (not installed), no rules
Intrusion Prevention:	Off, (not installed), no rules
Integrity Monitoring:	**On, Real Time, 1 rule**
Log Inspection:	Off, (not installed), no rules
Online:	Yes
Last Communication:	March 24, 2014 16:08

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/Appliance with respect to activation. The status will display either "Discovered" or "New" followed by the Agent/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/Appliance in brackets ("Online" or "Offline").
  - When the computer is managed and the Agent/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 **Status** area provides information about the install 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. For example, in the image above, the Integrity Monitoring module is on and its light is green because a rule has been assigned to it.

- **Anti-Malware:** When Anti-Malware protection is on, the Anti-Malware status light is green. When it is off, the Anti-Malware status light is gray.
- **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.
- **SAP:** Whether the SAP integration module is on or off.
- **Online:** Indicates whether the Manager can currently communicate with the Agent/Appliance.
- **Last Communication:** The last time the Manager successfully communicated with the Agent/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/Appliance. Check Status will not perform a security update of the Agent/Appliance. (If an update is required click the **Update Now** button on the **Actions** tab.) When Manager to Agent/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.
- **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.
- **Anti-Malware Ready:** If the computer is a virtual machine, Anti-Malware Ready indicates whether or not the VMware vShield Endpoint Thin Client has been installed. If the computer is a Virtual Appliance, Anti-Malware Ready indicates whether or not the VMware vShield Endpoint driver has been installed on the hosting ESXi server.
- **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/Appliance is running (VMware virtual machines only).

Actions

Actions

Activation

A newly installed Deep Security Agent/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/Appliance can be activated by any Deep Security Manager.

Agents/Appliances can only be deactivated locally on the computer or from the Deep Security Manager which activated it. If an Agent/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/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/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/Appliance. This is a "Send Policy" instruction. Policy updates usually happen immediately but you can force an update by clicking the **Send Policy** button.

Software

This displays the version of the Agent/Appliance currently running on the computer. If a newer version of the Agent/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/Appliance software running on any of your computers by going to the **Administration > System Settings > Updates** tab.

Note: *Agent Self-Protection must be disabled on computers that you want to upgrade. To configure Agent Self-Protection, go to the **Computer** tab on the **Policy/Computer Editor > Settings** page. Agent Self-Protection is a Windows-only feature.*

Versions 9.5 and later of the Windows and Linux Agents can be be configured to act as Deep Security Relays. Relays distribute Security and Software Updates throughout your network. Click **Enable Relay** to enable this functionality on the Agent. Once an Agent has Relay functionality enabled, it will retrieve the latest Security and Software Updates and distribute them according to your existing Updates settings. For more information about Relays, see **Relay Groups** in the Deep Security Manager Administrator's Guide or the online help.

Support

The **Create Diagnostic Package...** button creates a snapshot of the state of the Agent/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.

To create a diagnostics package locally on a Windows computer:

1. From a command line, type:
   ```
   C:\Program Files\Trend Micro\Deep Security Agent> dsa_control -d
   ```
   and press **Enter**.
2. A numbered zip file (for example, "341234567.zip") containing the diagnostics information will be created in c:\ProgramData\TrendMicro\Deep Security Agent\diag.

To create a diagnostics package locally on a Linux computer:

1. From a command line, type:
   ```
   $ /opt/ds_agent/dsa_control -d
   ```
   and press **Enter**.
2. A numbered zip file (for example, "341234567.zip") containing the diagnostics information will be created in the same directory.

To create a diagnostics package locally on a Deep Security Virtual Appliance computer:

1. 1.From a command line, type:
   ```
   $ sudo /opt/ds_agent/dsa_control -d
   ```
   and press **Enter**.
2. A numbered zip file (for example, "341234567.zip") containing the diagnostics information will be created in the same directory.

TPM (ESXi hypervisors only)

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 which doesn't support it, the option will be automatically disabled.

Note: *The Deep Security Integrity Monitoring module is a requirement for TPM.*

The minimum requirements for TPM monitoring are:

- Deep Security Manager 9+
- vCenter 5.1+
- ESXi 5.1+
- TPM/TXT installed and enabled on the ESXi (consult your VMware documentation for details)
- the Deep Security Integrity Monitoring Module must be On for this ESXi.

TPM

ESXi Trusted Platform Module

Note: This tab only appears for ESXi servers.

Alert when TPM monitoring detects changes to ESXi hypervisor configuration: The Trusted Platform Module (TPM) is a hardware-based encryption module attached to a VMware ESXi. It monitors the boot sequence of an ESXi and generates an encrypted signature. Changes to the ESXi boot sequence could represent corruption of the stored image, tampering, or unexpected or unauthorized updates or other types of changes.

Events

Note: The Events lists in the Computer Editors only display Events that are associated with the current computer.

The System Event log is a record of system-related events (as opposed to security-related events). From the main page you can:

- **View** () the details (properties) of a system event
- **Search** () for a particular system event
- **Export** () currently displayed system events to a CSV file
- View existing **Auto-Tagging** () Rules.

Additionally, right-clicking an Event gives you the option to:

- **Add Tag(s):** Add an Event Tag to this event (See **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help.)
- **Remove Tag(s):** Remove exiting Event Tags

View

Selecting an event and clicking **View** () displays the **Event Viewer Properties** window.

General

General Information

- **Time:** The time according to the system clock on the computer hosting the Deep Security Manager.
- **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.
- **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 entry in the system event log will be displayed here.

Tags

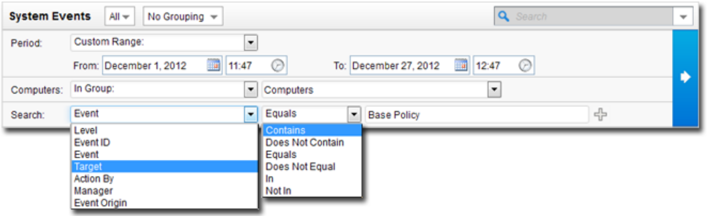
The **Tags** tab displays tags that have been attached to this Event. For More information on Event tagging, see **Policies > Common Objects > Other > Tags**, and **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help in the **Reference** section.

Filter the List and/or 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 **Advanced Search** toggles the display of the search bar.



System Events: All, No Grouping

Period: Custom Range:

From: December 1, 2012 11:47 To: December 27, 2012 12:47

Computers: In Group: Computers

Search: Event Equals Base Policy

Pressing 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

You can export displayed events to a CSV file. (Paging is ignored, all pages will be exported.) You have the option of displaying the displayed list or the selected items.

Auto-Tagging

Clicking **Auto-Tagging...** displays a list of existing System Event Auto-Tagging Rules.

Anti-Malware

The **Anti-Malware** module provides both real-time and on-demand protection against file-based threats, including threats commonly referred to as malware, viruses, Trojans, and spyware. To identify threats, Anti-Malware checks files against a comprehensive threat database, portions of which are hosted on servers or kept locally as updatable patterns. Anti-Malware also checks files for certain characteristics, such as compression and known exploit code.

To address threats, Anti-Malware selectively performs actions that contain and remove the threats while minimizing system impact. Anti-Malware can clean, delete, or quarantine malicious files. It can also terminate processes and delete other system objects that are associated with identified 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 global Trend Micro Update Servers after installation.*

The **Anti-Malware** page has the following tabbed sections:

- ***General (page 107)***
- ***Smart Protection (page 109)***
- ***Advanced (page 110)***
- ***Quarantined Files (page 113)***
- ***Events (page 114)***

General

Anti-Malware State

Turn Anti-malware on or off. You can configure this Policy or computer to inherit its Anti-Malware On/Off state from its parent Policy or you can override the setting locally.

Real-Time Scan

Real-time Scan is a persistent and ongoing scan. Each time a file is received, opened, downloaded, copied, or modified, Real-time Scan 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, showing the name of the infected file and the specific security risk.

To perform Real-Time Malware Scans, you must select a Scan Configuration and a Schedule during which it is in effect.

Note: ***Malware Scan Configurations*** *determine such things as which file types are scanned in which directories, what types of malware to scan for, and what to do with malware when it is detected. You can examine a Scan Configuration's properties by selecting it from the drop-down menu and then clicking* ***Edit****. To manage all your different Malware Scan Configurations, go to* ***Policies > Common Objects > Other > Malware Scan Configurations*** *in the Deep Security Manager.*

Manual Scan

Manual Scan is an on-demand scan and starts immediately after a user runs the scan on the computer. The time it takes to complete scanning depends on the number of files to scan and the computer's hardware resources.

To perform Manual Malware Scans, you must select a Scan Configuration.

Note: ***Malware Scan Configurations*** *determine such things as which file types are scanned in which directories, what types of malware to scan for, and what to do with malware when it is detected. You can examine a Scan Configuration's properties by selecting it from the drop-down menu and then clicking* ***Edit****. To manage all your different Malware Scan Configurations, go to* ***Policies > Common Objects > Other > Malware Scan Configurations*** *in the Deep Security Manager.*

Scheduled Scan

Scheduled Scan runs automatically on the appointed date and time. Use Scheduled Scan to automate routine scans and improve scan management efficiency.

To perform Scheduled Malware Scans, you must select a Scan Configuration.

Note: ***Malware Scan Configurations*** *determine such things as which file types are scanned in which directories, what types of malware to scan for, and what to do with malware when it is detected. You can examine a Scan Configuration's properties by selecting it from the drop-down menu and then clicking* ***Edit****. To manage all your different Malware Scan Configurations, go to* ***Policies > Common Objects > Other > Malware Scan Configurations*** *in the Deep Security Manager.*

Malware Scan (Computer Editor only)

Displays the times and dates of the last Manual and Scheduled Malware Scans and allows you to perform or abort a Quick or Full Malware Scan.

See also:

- **Policies, Inheritance and Overrides** in the Deep Security Manager Administrator's Guide or the online help

Smart Protection

Smart Scan

Smart Scan shifts much of the malware and spyware scanning functionality to a Smart Protection Server. Instead of downloading a complete malware pattern file to the local computer, a much smaller version of the pattern is downloaded which can 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. This method keeps local pattern files small and reduces the size and number of updates required by Agents/Appliances.

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 Service for File Reputation supplies file reputation information required by Smart Scan. Select whether to connect directly to Trend Micro's Smart Protection service or whether to connect to one or more locally installed Smart Protection Servers.

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: *You can view and edit the list of available proxies on the* ***Proxies*** *tab on the* ***Administration > System Settings*** *screen.*

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.

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.*

Advanced

Quarantined Files

Maximum disk space used to store quarantined files: This setting determines how much disk space can be used to store quarantined files. It applies globally to all computers: physical machines, virtual machines, and Virtual Appliances. The setting can be overridden at the Policy level and at the Computer level. If you are using a Virtual Appliance to provide protection to virtual machines, all quarantined files from the Agentless VMs will be stored on the Virtual Appliance. As a result, you should increase the amount of disk space for quarantined files on the Virtual Appliance.

Quarantined files will be automatically deleted from a Virtual Appliance under the following circumstances:

- If a VM undergoes vMotion, quarantined files associated with that VM will be deleted from the Virtual Appliance.
- If a VM is deactivated from the Deep Security Manager, quarantined files associated with that VM will be deleted from the Virtual Appliance.
- If a Virtual Appliance is deactivated from the Deep Security Manager, all the quarantined files stored on that Virtual Appliance will be deleted.
- If a Virtual Appliance is deleted from the vCenter, all the quarantined files stored on that Virtual Appliance will also be deleted.

Scan Limitation

Maximum file size to scan: Files exceeding this file size will not be scanned. (Setting a value of 0 means that there is no maximum size. All files will be scanned.)

Resource Allocation for Malware Scans

Use multithreaded processing for Malware Scans (if available): Enables multithreaded processing on systems that support this capability. It only applies to Manual/Scheduled Scans, not to Real-Time Scanning.

Note: *Using multithreaded processing may reduce the resources available to other processes running on the computer. Note that you will have to restart the computers on which you are enabling multithreaded processing for the setting to take effect.*

Allowed Spyware/Grayware

Allowed Spyware/Grayware: Use this setting to maintain a list of allowed applications that have been identified as spyware/grayware by Deep Security.

Note: *This option is only effective on Windows computers. On Linux computers, you can achieve a similar result by using **Scan Exclusion File Lists** to identify specific files that should be ignored during Malware scans. Scan Exclusion objects are a property of **Malware Scan Configurations,** and Malware Scan Configurations are a property of **Security Policies**.*

To specify a Scan Exclusion File List in a Malware Scan Configuration:** in the Deep Security Manager, go to **Policies > Common Objects > Malware Scan Configurations**. You can specify a File List in the **Scan Exclusions

__Area__ on the __Exclusions__ tab of the Malware Scan Configuration's __Properties__ window.

__To select a Malware Scan Configuration in a Security Policy:__ open the Policy Editor and on the __General__ tab, select the Malware Scan Configuration from the drop-down list in any of the __Real-Time Scan__, __Manual Scan__, or __Scheduled Scan__ areas.

Note: *Applications in the __Allowed Spyware/Grayware__ list will be ignored by the Spyware/Grayware scan engine. The presence of the applications will not be recorded or stored as Anti-Malware Events.*

Spyware/grayware can be added to the approved list in one of two ways. You can add it using an Anti-Malware Event where the application was detected or you can manually enter the name of the spyware/grayware.

To add spyware/grayware to the list of allowed spyware/grayware using an Anti-Malware Event:

1. Find the detection Event in the **Anti-Malware Events** page.
2. Right-click on the Event.
3. Select **Allow**.

If the application has already been detected by the scan engine, it may already have been quarantined or deleted, depending on what your current spyware/grayware settings are. If it has been quarantined you will have to restore or reinstall the application. See **Anti-Malware > Quarantined Files** for information on restoring quarantined files. Alternatively, you can run a spyware/grayware scan with **Action** set to "Pass" mode so that all spyware/grayware detections are recorded on the **Anti-Malware Events** page but "passed" over and neither quarantined nor deleted. You can then add the selected spyware/grayware to the allowed list using this method and afterwards set **Action** to "Quarantine" or "Delete" modes.

To manually add spyware/grayware to the list of allowed spyware/grayware:

Note the name of the application as it is displayed in the Anti-Malware Event log and add it manually to the **Allowed Spyware/Grayware List**.

Note: *Entries in this list are case-sensitive. They must appear exactly as they do in the Event log.*

Note: *Refer to the Trend Micro Spyware/Grayware Encyclopedia for information about detected spyware/grayware.*

Local Event Notification

Display local notifications when malware is detected: This setting determines whether the Deep Security Notifier (if it is installed locally on the computer) will display a pop up notification that malware has been detected.

VM Scan Cache

Scan Caching is used by the Virtual Appliance to maximize the efficiency of Malware and Integrity Monitoring Scans of virtual machines. For information on Scan Cache configurations, see **Virtual Appliance Scan Caching** in the Deep Security Manager Administrator's Guide or the online help.

NSX Security Tags

Deep Security can apply **NSX Security Tags** to protected VMs upon detecting a malware threat. NSX Security Tags can be used with NSX Service Composer to automate certain tasks, such as quarantining infected VMs. Consult your VMware NSX documentation for more information on NSX Security Tags and dynamic NSX Security Group assignment.

Note: *NSX Security Tags are part of the VMware vSphere NSX environment and are not to be confused with Deep Security Event Tags. For more information on Deep Security Event Tagging, see* **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help*.*

You can choose to only apply the NSX Security Tag if the remediation action attempted by the Anti-Malware engine fails. (The remediation action is determined by the Malware Scan Configuration that is in effect. To see which Malware Scan Configuration is in effect, go to the **Computer/Policy Editor > Anti-Malware > General** tab and check the **Real-Time Scan**, **Manual Scan**, and **Scheduled Scan** areas.)

You can also choose to have the Security Tag removed if a subsequent Malware Scan does not detect any malware. You should only use this setting if all Malware Scans will be of the same kind.

Quarantined Files

Quarantined Files are displayed the same way as they are in the main Deep Security Manager window except that only files that were quarantined on this computer are listed. (See ***Quarantined Files (page 16)***.)

Events

Anti-Malware Events are displayed the same way they are in the main Deep Security Manager window except that only events associated with this Policy or specific computer are displayed. (See ***Anti-Malware Events (page 13)***.)

Web Reputation

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 Web sites that users are attempting to access. The Web site's reputation is correlated with the specific Web reputation policy enforced on the computer. Depending on the Web Reputation Security Level being enforced, Deep Security will either block or allow access to the URL.

The Web Reputation configuration for this Policy or computer inherits its on or off state from either its parent Policy unless you choose to override it.

The Web Reputation Service page has the following tabbed sections:

- ***General (page 116)***
- ***Exceptions (page 119)***
- ***Smart Protection (page 117)***
- ***Advanced (page 118)***
- ***Events (page 120)***

General

Web Reputation

You can configure this Policy or Computer to inherit its Web Reputation On/Off state from its parent Policy or you can lock the setting locally.

Security Level

The Web Reputation rating system assigns the following risk levels to URLs:

- **Dangerous:** A URL that has been confirmed as fraudulent or a known source of threats
- **Highly Suspicious:** A URL that is suspected to be fraudulent or a known source of threats
- **Suspicious:** A URL that is associated with spam or possibly compromised
- **Safe:** A URL that is not a risk

Select a security level to implement:

High: blocks pages that are:

- Dangerous
- Highly suspicious
- Suspicious

Medium: blocks pages that are:

- Dangerous
- Highly suspicious

Low: blocks pages that are:

- Dangerous

Block pages that have not been tested by Trend Micro: Blocks pages that are:

- Unrated by Trend Micro

Smart Protection

Smart Protection Server for Web Reputation Service

Smart Protection Service for Web Reputation supplies web reputation information required by the Web Reputation module. Select whether to connect directly to Trend Micro's Smart Protection service or whether to connect to one or more locally installed Smart Protection Servers.

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: *View the list of available proxies on the* ***Administration > System Settings > Proxies*** *tab.*

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.

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.*

Advanced

Blocking page

When users attempt to access a blocked URL, they will be redirected to a blocking page. Provide a link they can use to request access to the blocked URL.

Alert

Select whether to raise an Alert when a Web Reputation event is logged.

Ports

Select specific ports to monitor for potentially harmful web pages.

Local Event Notification

Display local notifications via the Deep Security Notifier when access to a malicious Web site is blocked. (See **Deep Security Notifier** in the Deep Security Manager Administrator's Guide or the online help.)

Exceptions

Exceptions are lists of URLs that are blocked or allowed regardless of their safety ratings.

> *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.*

Allowed

URLs included in the Allowed list will be accessible regardless of their safety ratings. Multiple URLs can be added at once but they must be separated by a line break. When adding URLs to the Allowed list, select whether to allow all URLs with the same domain or the URL:

- **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.

Blocked

URLs and URLs containing specified keywords included in the Blocked list are always blocked (unless there is an overriding entry in the Allowed list). Multiple URLs or keywords can be added at once but they must be separated by a line break. When blocking URLs, you select whether to block all URLs from a domain, to block the URL, or to block URLs that contain a specific keyword.

- **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.

Events

Web Reputation Events are displayed the same way they are in the main Deep Security Manager window except that only events relating to computers using this Policy are displayed.

Firewall

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 page contains the following tabbed sections:

- ***General (page 122)***
- ***Interface Isolation (page 123)***
- ***Reconnaissance (page 124)***
- ***Advanced (page 126)***
- ***Events (page 127)***

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.

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.

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 **Policy/Computer Editor > Settings > Scanning > Open Ports > Ports to Scan**.

Note: *Regardless of the ports configured to be scanned, Deep Security Manager will always scan the default Agent/Appliance port (4118).*

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 de-select Rules.

From an Editor window, you can edit a Firewall Rule so that your changes apply only locally in the context of your editor (either the Computer or Policy 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, select the Rule and click Properties... (▤) or right-click the Rule and click **Properties...**

To edit the Rule globally, right-click the Rule and click **Properties (Global)...**

See also:

- **Policies, Inheritance and Overrides** in the Deep Security Manager Administrator's Guide or the online help

Interface Isolation

Interface Isolation

You can configure this Policy or Computer to inherit its Interface Isolation enabled/disabled state from its parent Policy or you can lock the setting locally.

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).

See also:

- **Policies, Inheritance and Overrides** in the Deep Security Manager Administrator's Guide or the online help

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 and helps to prevent attacks.

- **Reconnaissance Scan Detection Enabled:** Turn the ability to detect reconnaissance scans on or off.
- **Computers/Networks on which to perform detection:** Choose from the drop-down 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 **Policy/Computer Editor > Firewall > General** tab. You should also go to the **Policy/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.*

For each type of attack, the Agent/Appliance can be instructed to send the information to the Deep Security Manager where an Alert will be triggered. You can configure the 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.

Note: *For the "Notify DSM Immediately" option to work, the Agents/Appliances must be configured for **Agent/Appliance initiated** or **bidirectional** communication in **Policy/Computer Editor > Settings > Computer.**) If enabled, the Agent/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/Appliances to block traffic from the source IPs for a period of time. Use the **Block Traffic** drop-down lists to set the number of minutes.

- **Computer OS Fingerprint Probe:** The Agents/Appliances will recognize and react to active TCP stack OS fingerprinting attempts.
- **Network or Port Scan:** The Agents/Appliances will recognize and react to port scans.
- **TCP Null Scan:** The Agents/Appliances will refuse packets with no flags set.
- **TCP SYNFIN Scan:** The Agents/Appliances will refuse packets with only the SYN and FIN flags set.
- **TCP Xmas Scan:** The Agents/Appliances will refuse 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/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/Appliance 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. 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/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/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.

The statistical analysis method used in computer/port scan detection is derived from the "TAPS" algorithm proposed in the paper "Connectionless Port Scan Detection on the Backbone" published by Sprint/Nextel and presented at the Malware workshop, held in conjunction with IPCCC, Phoenix, AZ, USA in April, 2006.

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.*

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 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.

Intrusion Prevention

The **Intrusion Prevention** module protects computers from being exploited by attacks against known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities. Shields vulnerabilities until code fixes can be completed. It identifies malicious software accessing the network and increases visibility into, or control over, applications accessing the network.

The **Intrusion Prevention** page has the following tabbed sections:

- ***General (page 129)***
- ***Advanced (page 131)***
- ***Events (page 134)***

General

Intrusion Prevention

You can configure this Policy or Computer to inherit its Intrusion Prevention On/Off state from its parent Policy or you can lock the setting locally.

Set the Intrusion Prevention behavior to "Prevent" or "Detect".

When first applying a new set of Intrusion Prevention Rules you can choose to set the Intrusion Prevention behavior to "Detect". When in Detect mode, the Intrusion Prevention engine will apply all the same Intrusion Prevention Rules to traffic but instead of dropping packets, it will only log an Event and let the traffic pass. Use this behavior to ensure the new Intrusion Prevention Rules will not interfere with legitimate traffic.

> Note: *This setting only applies when the Network Engine is operating Inline; that is, live traffic is being streamed through the Deep Security network engine. The alternative to Inline mode is Tap mode, where the live traffic is cloned, and it is only this cloned traffic that is analyzed by the network engine. Prevent mode is impossible when in Tap Mode because the network engine does not control the live traffic stream.*
>
> *To switch between Inline and Tap mode, open a Policy or Computer Editor and go to **Settings > Network Engine > Network Engine Mode**.*

Assigned Intrusion Prevention Rules

Displays the Intrusion Prevention Rules that are in effect for this Policy or computer. To add or remove Intrusion Prevention Rules, click **Assign/Unassign...** This will display a window showing all available Intrusion Prevention Rules from which you can select or de-select Rules.

From an Editor window, you can edit an Intrusion Prevention Rule so that your changes apply only locally in the context of your editor (either the Computer or Policy 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, select the Rule and click Properties... (▤) or right-click the Rule and click **Properties...**

To edit the Rule globally, right-click the Rule and click **Properties (Global)...**

Recommendations

Deep Security can perform regular Recommendation Scans which scan a computer and make recommendations about the application of various security Rules. Selecting this checkbox will automatically assign recommended rules for the computer and automatically unassign rules that are not required.

> Note: *If you select this option, you should also opt to allow Deep Security Rule Updates to automatically assign new Intrusion Prevention Rules. Go to **Administration > System Settings > Updates** and select **Automatically apply new Rule Updates to Policies** in the **Rule Updates** area.*

To schedule periodic Recommendation Scans, in the Deep Security Manager go to **Administration > Scheduled Tasks** and create a new Scheduled Task.

See also:

- **Policies, Inheritance and Overrides** in the Deep Security Manager Administrator's Guide or the online help

Advanced

Event Data

Allow Intrusion Prevention Rules to capture data for first hit of each rule (in period): Determines whether Deep Security will save the packet data which triggered an Intrusion Prevention Rule. This setting works in conjunction with the advanced ***Network Engine settings (page 150)*** that can be found in **Computer\Policy Editor > Settings > Network Engine > Advanced Network Engine Settings**.

- **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.

Rule Updates

Automatically assign new Intrusion Prevention Rules as required by updated Application Types and Intrusion Prevention Rule dependencies: Security Updates sometimes include new or updated Application Types and Intrusion Prevention Rules which require the assignment of secondary Intrusion Prevention Rules. This setting will allow Deep Security to automatically assign these Rules if they are required by the Application Types or Intrusion Prevention Rules that were assigned to a Policy or computer during a Security Update.

SSL Configurations (Computer editors only)

Deep Security Manager supports Intrusion Prevention analysis of SSL traffic. The SSL Configurations page allows you to create SSL Configurations for a given certificate-port pair on one or more interfaces. Certificates can be imported in **P12** or **PEM** format and Windows computers have the option of using **Windows CryptoAPI** directly.

To create a new SSL Configuration, click **New** and follow the steps in the **SSL Configuration** wizard.

If the computer you are configuring is being installed on the computer hosting the Deep Security Manager, the wizard will let you use credentials already stored in the Deep Security Manager.

Double-click an existing configuration to display its **Properties** window.

Assignment

- **General Information:** The name and description of the SSL configuration, and whether it is enabled on this computer.

- **Interface Assignments:** Which interfaces this configuration is being applied to.
- **IP Assignment:** Which IP(s) this configuration applies to.
- **Port Selection:** Which port(s) this configuration applies to.

Credentials

The **Credentials** tab lists the current credentials, and has an **Assign New Credentials...** button which lets you change them.

Note: *Filtering of SSL traffic is only supported by the Deep Security Agent, not the Deep Security Appliance. The Agent does not support filtering SSL connections on which SSL compression is implemented.*

For information on setting up SSL filtering, see **SSL Data Streams** in the Deep Security Manager Administrator's Guide or the online help.

NSX Security Tagging

Deep Security can apply **NSX Security Tags** to protected VMs upon detecting a malware threat. NSX Security Tags can be used with NSX Service Composer to automate certain tasks, such as quarantining infected VMs. Consult your VMware NSX documentation for more information on NSX Security Tags and dynamic NSX Security Group assignment.

Note: *NSX Security Tags are part of the VMware vSphere NSX environment and are not to be confused with Deep Security Event Tags. For more information on Deep Security Event Tagging, see* **Event Tagging** in the Deep Security Manager Administrator's Guide or the online help*.*

Intrusion Prevention Events have a severity level that is determined by the severity level of the Intrusion Prevention Rule that caused it.

Note: *The severity level of an Intrusion Prevention Rule is configurable on the* ***Rule Properties > General*** *tab.*

Intrusion Prevention Rule severity levels map to NSX tags as follows:

IPS Rule Severity	NSX Security Tag
Critical	IDS_IPS.threat=high
High	IDS_IPS.threat=high
Medium	IDS_IPS.threat=medium
Low	IDS_IPS.threat=low

You can configure the sensitivity of the tagging mechanism by specifying the minimum Intrusion Prevention severity level that will cause an NSX security tag to be applied to a VM.

The options for the **Minimum rule severity to trigger application of an NSX Security Tag** setting are:

- **Default (No Tagging):** No NSX tag is applied.
- **Critical:** An NSX tag is applied to the VM if an Intrusion Prevention Rule with a severity level of **Critical** is triggered.
- **High:** An NSX tag is applied to the VM if an Intrusion Prevention Rule with a severity level of **High** or **Critical** is triggered.
- **Medium:** An NSX tag is applied to the VM if an Intrusion Prevention Rule with a severity level of **Medium**, **High**, or **Critical** is triggered.

- **Low:** An NSX tag is applied to the VM if an Intrusion Prevention Rule with a severity level of **Low**, **Medium**, **High**, or **Critical** is triggered.

Separate settings are provided for Rules that are operating in Prevent mode and for Rules that operating in Detect-only mode.

Note: *Whether an IPS Rule is operating in Prevent or Detect-only mode is determined not only by the Intrusion Prevention module setting (**Computer/Policy Editor > Intrusion Prevention > General** tab), but also by the configuration of the individual Rule itself (**Rule Properties > General tab > Details**).*

Events

Intrusion Prevention 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.

Integrity Monitoring

The **Integrity Monitoring** module monitors specific areas on a computer for changes. It can monitor installed software, running services, processes, files, directories, listening ports, registry keys, and registry values. It functions by performing a baseline scan of the areas on the computer specified in the assigned rules and then periodically rescanning those areas to look for changes.

The **Integrity Monitoring** page has the following tabbed sections:

- ***General (page 136)***
- ***Advanced (page 137)***
- ***Events (page 138)***

General

Integrity Monitoring

You can configure this Policy or Computer to inherit its Integrity Monitoring On/Off state from its parent Policy or you can lock the setting locally.

Integrity Scan (Computer Editor only)

Click **Scan For Integrity** to perform on an on-demand Integrity Scan on this computer.

Baseline (Computer Editor only)

The Baseline is the original secure state that an Integrity Scan's results will be compared against. Click **Rebuild Baseline** to create a new Baseline for Integrity Scans on this computer. Click **View Baseline** to view the current Baseline data.

Assigned Integrity Monitoring Rules

Displays the Integrity Monitoring 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 de-select Rules.

From an Editor window, you can edit a Integrity Monitoring Rule so that your changes apply only locally in the context of your editor (either the Computer or Policy 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, select the Rule and click Properties... (☰) or right-click the Rule and click **Properties...**

To edit the Rule globally, right-click the Rule and click **Properties (Global)...**

Recommendations

Displays when the last Recommendation Scan occurred and number of recommended Integrity Monitoring Rules.

See also:

- **Policies, Inheritance and Overrides** in the Deep Security Manager Administrator's Guide or the online help

Advanced

Content Hash Algorithms

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.

VM Scan Cache

For information on Integrity Monitoring Scan Cache Configurations, see **Virtual Appliance Scan Caching** in the Deep Security Manager Administrator's Guide or the online help.

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:

- **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

Events

Integrity Monitoring 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.

Log Inspection

The **Log Inspection** module identifies security events contained in a computer's log files. Suspicious events can be forwarded to a SIEM system or centralized logging server for eventual correlation, reporting and archiving. It functions by implementing the open-source software available at OSSEC.net.

The Log Inspection page has the following tabbed sections:

- ***General (page 140)***
- ***Advanced (page 141)***
- ***Events (page 142)***

General

Log Inspection

You can configure this Policy or Computer to inherit its Log Inspection On/Off state from its parent Policy or you can lock the setting locally.

Assigned Log Inspection Rules

Displays the Log Inspection Rules that are in effect for this Policy or computer. To add or remove Log Inspection Rules, click **Assign/Unassign...** This will display a window showing all available Log Inspection Rules from which you can select or de-select Rules.

From an Editor window, you can edit a Log Inspection Rule so that your changes apply only locally in the context of your editor (either the Computer or Policy 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, select the Rule and click Properties... (▤) or right-click the Rule and click **Properties...**

To edit the Rule globally, right-click the Rule and click **Properties (Global)...**

Recommendations

Displays when the last Recommendation Scan occurred and number of recommended Log Inspection Rules.

See also:

- **Policies, Inheritance and Overrides** in the Deep Security Manager Administrator's Guide or the online help

Advanced

Severity Clipping

Send Agent/Appliance events to syslog when they equal or exceed the following severity level: Log Inspection Rules have a severity level. This setting determines which Events triggered by those rules get sent to the syslog server (if syslog is enabled.) (To enable syslog, go to **Administration > System Settings > SIEM** .)

Store events at the Agent/Appliance for later retrieval by DSM 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.

Events

Log Inspection 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.

SAP

Trend Micro Deep Security supports integration with the SAP NetWeaver platform. The **SAP** page in the Computer/Policy editor allows you to enable the SAP integration module for individual computers or policies. For additional information about the how to set up SAP integration, see the *Deep Security Manager Integration Guide for SAP*.

The SAP page contains these settings:

- **Configuration:** Enables or disables the SAP integration module. The setting can be **On**, **Off**, or **Inherited** from the parent policy.
- **Version:** Displays the version number of the Virus Scan Adapter (VSA) reported from the Deep Security Agent.
- **State:** Provides information about the state of the SAP integration module. This reflects the state of the module on the Agent as well as its configuration in Deep Security Manager. A state of "On" indicates that the module is configured in Deep Security Manager and is installed and operating on the Deep Security Agent. If the state is "Off", the state displays additional information about why it is off.

Interfaces/Interface Types

Interfaces (Computer Editor)

Displays the interfaces detected on the computer. If a Policy with multiple interface assignments has been assigned to this computer, interfaces that match the patterns defined in the Policy will be identified.

Interface Types (Policy Editor)

Displays the interfaces detected on the computer. If a Policy with multiple interface assignments has been assigned to this computer, interfaces that match the patterns defined in the Policy will be identified.

Network Interface Specificity

If you have computers with more than one interface, you can assign various elements of a Policy (Firewall Rules, etc.) to each interface. To configure a Policy for multiple interfaces, select **Rules can apply to specific interfaces** and type names and pattern matching strings in the fields below.

The interface type name is used only for reference. Common names include "LAN", "WAN", "DMZ", and "Wi-Fi" though any name may be used to map to your network's topology.

The Matches defines a wild-card based interface name match to auto map the interfaces to the appropriate interface type. Examples would be "Local Area Connection *", "eth*", and "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 interfaces are detected on the computer that don't match any of these entries, the Manager will trigger an Alert.*

Interface Types (Interface Patterns)

To enforce interface isolation, set the **Enable Interface Isolation** option on the **Policy/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).

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*

Note: *If you enter a string pattern that matches more than one interface on a computer, traffic will be allowed on all of those matching interfaces. To make sure that only one interface is active, set the* ***Limit to one active interface*** *option.*

Settings

The **Settings** page has the following tabbed sections:

- ***Computer (page 146)***
- ***Network Engine (page 150)***
- ***Scanning (page 157)***
- ***SIEM (page 158)***

Computer

Communication Direction

- **Bidirectional:** By default, communications are bidirectional. This means that the Agent/Appliance normally initiates the heartbeat but still listens on the Agent port for Manager connections. The Manager is still free to contact the Agent/Appliance in order to perform operations as required. This allows the Manager to apply changes to the security configuration to the Agent/Appliance as they occur.

  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:** With this option selected, all Manager to Agent/Appliance communications are initiated by the Manager. This includes security configuration updates, heartbeat operations, and requests for Event logs.
- **Agent/Appliance Initiated:** With this option selected, the Agent/Appliance does not listen on port 4118. Instead it contacts the Manager on the heartbeat port (4120 by default) as dictated by the heartbeat settings. Once the Agent/Appliance has established a TCP connection with the Manager all normal communication takes place: the Manager first asks the Agent/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 (e.g., the Policy needs to be updated), these operations are performed before the connection is closed. In this mode, communications between the Manager and the Agent/Appliance only occur on every heartbeat. If an Agent/Appliance's security configuration has changed, it will not be updated until the next heartbeat.

  Note: *Before configuring an Agent/Appliance for Agent/Appliance initiated communication, ensure that the Manager URL and heartbeat port can be reached by the Agent/Appliance. If the Agent/Appliance is unable to resolve the Manager URL or is unable to reach the IP and port, Agent/Appliance initiated communications will fail for this Agent/Appliance. The Manager URL and the heartbeat port are listed in the **System Details** area in the **Administration > System Information** page.*

Note: *Agents/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/Appliance initiated or bidirectional communication to work.*

Note: *To enable communications between the Manager and the Agents/Appliances, the Manager automatically implements a (hidden) Firewall Rule (priority four, Bypass) which opens port 4118 on the Agents/Appliances to incoming TCP/IP traffic. The default settings open the port to 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, which only allows incoming TCP/IP traffic from specific IP and/or MAC addresses. This new Firewall Rule will replace the hidden Firewall Rule if the settings match the following:*

***action:** force allow or bypass*
***priority:** 4 - highest*
***packet's direction:** incoming*
***frame type:** IP*
***protocol:** TCP*
***packet's destination port:** 4118 (or a list or range that includes 4118)*

As long as these settings are in effect, the new rule will replace the hidden rule. You can then type Packet Source information for IP and/or MAC addresses to restrict traffic to the computer.

Heartbeat

- **Heartbeat Interval (in minutes):** How much time passes between heartbeats.
- **Number of Heartbeats that can be missed before an Alert is raised:** This setting determines how many missed heartbeats are allowed to go by before the Manager triggers an Alert. (For example, entering three will cause 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/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) 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 (non-Windows Agents), the Manager monitors the system time reported by the Agent at each heartbeat operation and will trigger 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 or paused.

Send Policy Changes Immediately

By default, the value for the **Automatically send Policy changes to computers** setting is "Yes". This means that any changes to a security policy are automatically applied to the computers that use the policy. If you change this setting to "No", you will need find affected computers on the **Computers** page, right-click them, and choose "Send Policy" from the context menu.

Troubleshooting

You can increase the granularity of the logging level and record more events for troubleshooting purposes, however you should exercise caution when using this option since this can significantly increase the total size of your Event logs.

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").

Agent Self-Protection

> Note: *The Agent Self-Protection feature is available only with Windows Agents.*

Use these settings to prevent local users from interfering with Agent functionality.

- **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent:** This will prevent local users from uninstalling the Agent, stopping the Agent service, modifying Agent-related Windows Registry entries, or modifying Agent-related files. These restrictions can be overridden by issuing local instructions from the command line. (See **Command-Line Utilities** in the Deep Security Manager Administrator's Guide or the online help.) When Agent Self-Protection is enabled, attempts to make modfications to the Agent via the local operating system graphical user interface will be met with a message similar to "Removal or modification of this application is prohibited by its security settings".

  - **Local override requires password:** It is possible that a Deep Security Manager loses the ability to communicate with an Agent. In such cases you will have to interact with the Agent locally using the Agent's command-line interface. Enter a password here to password-protect the local command-line functionality. (Recommended.)

    > Note: *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.*

Anti-Malware protection must be "**On**" to prevent the following:

- Stopping the Agent service
- Modifying Agent-related Windows Registry entries
- Modifying Agent related files

Anti-Malware protection is not required to prevent local users from uninstalling the Agent.

To turn Agent Self-Protection off or on from the command line:

1. Log in to the local computer as an Administrator
2. Run a command prompt from the Agent's (or Relay's) installation directory
3. Enter the following command (where "**password**" is the password set using the **Local override requires password** setting):
   - to turn Self-Protection off:
     ```
     dsa_control --selfprotect=0 --passwd=password
     ```
   - to turn Self-Protection on
     ```
     dsa_control --selfprotect=1 --passwd=password
     ```

   > Note: *If no password was set, omit the "**--passwd**" parameter.*

> Note: *In Deep Security 9.0 and earlier, this option was **--harden=<num>***

Alternatively, you can use the **reset** parameter which will reset the Agent and disable Agent Self-Protection:

- `dsa_control --reset`

Environment Variable Overrides

Environment variables are used by the Integrity Monitoring module to represent some standard locations in the directory system of 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 this way 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.*

The following are the default environment variables used by the Integrity Monitoring module:

Name	Value
ALLUSERSPROFILE	C:\ProgramData
COMMONPROGRAMFILES	C:\Program Files\Common Files
PROGRAMFILES	C:\Program Files
SYSTEMDRIVE	C:
SYSTEMROOT	C:\Windows
WINDIR	C:\Windows

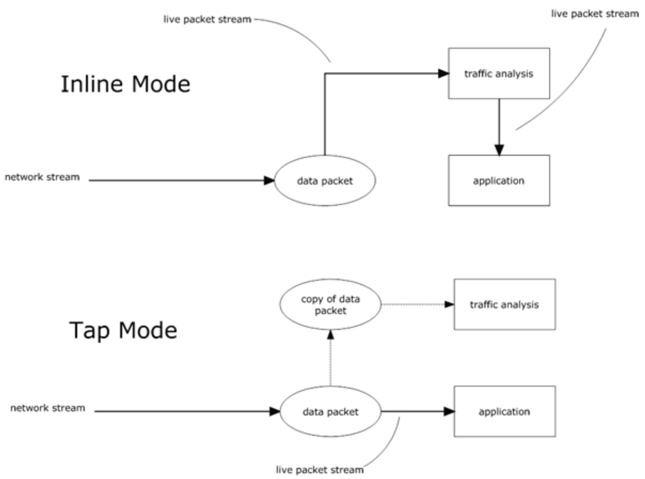
To override any of these environment variables:

1. Click the **View Environment Variables...** button to display the **Environment Variable Overrides** page.
2. Click **New** in the menu bar and enter a new name/value pair (for example, **WINDIR** and **D:\Windows**) and click **OK**.

Network Engine

Network Engine

The Agent/Appliance's network engine can operate Inline or in Tap Mode. When operating Inline, the live 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 Rules can be applied to payload content. When operating in Tap Mode, the live packet stream is cloned and diverted from the main stream. In Tap Mode, the live packet stream is not modified; all operations are carried out on the cloned stream.



Events

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 4MB log file will hold about 20,000 log entries. How quickly your log files fill up depends on the number of rules in place.

- **Maximum size of the event log files (on Agent/Appliance):** Adjust these settings if you begin to see "Insufficient Disk Space" Alerts for one or more computers.
- **Number of event log files to retain (on Agent/Appliance):** Adjust these settings if you begin to see "Insufficient Disk Space" Alerts for one or more computers.

> *Note:* ***Events*** *are records of individual events.* ***Counters*** *are a record of the number of times individual events have occurred. Events are used to populate the* ***Events*** *pages. Counters are used to populate the Dashboard Widgets (number of Firewall Events over the last 7 days, etc.) and the Reports. You might want to collect only counters if, for example, you are using syslog for event collection; events can potentially take up a lot of disk space and you may not want to store the data twice.*

- **Do Not Record Events with Source IP of:** This option is useful if you want Deep Security to not 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/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/Appliances need to cache the entries in memory while they are being aggregated before writing 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 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.*

Anti-Evasion Settings

Anti-Evasion settings control the network engine handling of abnormal packets that may be attempting to evade analysis.

Posture: There are three options for the Posture setting. This setting can be inherited from the parent policy:

- **Normal:** This is the default setting. It is tuned to prevent the evasion of IPS rules, without false positives.
- **Strict:** Strict mode performs more stringent checking than Normal mode but it could result in 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 **Ignore** (Deep Security sends the packet through to the system), **Ignore & Log** (same behavior as Ignore, 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):
  - **Invalid TCP Timestamps:** Action to take when a TCP timestamp is too old.
  - **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).
  - **Timestamp PAWS Zero Allowed:** Action to take when a TCP timestamp is zero.
  - **Fragmented Packets:** Action to take when a packet is fragmented.
  - **TCP Zero Flags:** Action to take when a packet has zero flags set.
  - **TCP Congestion Flags:** Action to take when a packet has congestion flags set.
  - **TCP Urgent Flags:** Action to take when a packet has urgent flags set.
  - **TCP Syn Fin Flags:** Action to take when a packet has both SYN and FIN flags set.

  - **TCP Syn Rst Flags:** Action to take when a packet has both SYN and RST flags set.
  - **TCP Rst Fin Flags:** Action to take when a packet has both RST and FIN flags set.
  - **TCP Syn with Data:** Action to take when a packet has a SYN flag set and also contains data.
  - **TCP Split Handshake:** Action to take when a SYN is received instead of SYNACK, as a reply to a SYN.
  - **RST Packet Out of Connection:** Action to take for a RST packet without a known connection.
  - **FIN Packet Out of Connection:** Action to take for a FIN packet without a known connection.
  - **OUT Packet Out of Connection:** Action to take for an outgoing packet without a known connection.
  - **Evasive Retransmit:** Action to take for a packet with duplicated or overlapping data.
  - **TCP Checksum:** Action to take for a packet with an invalid checksum.

Advanced Network Engine Settings

Generate an Alert when Agent configuration package exceeds maximum size: Yes or No. The default is Yes.

If you deselect the **Default** checkbox, 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 and/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 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/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.
    - **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. **Normal:** All Events are logged except dropped retransmits.
    - **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* **Advanced Logging Policy Modes** in the Deep Security Manager Administrator's Guide or the online help *in the* ***Reference*** *section.*

- **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.
- **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.

Scanning

Open Ports

Select a port list to be used when the Deep Security Manager performs a port scan on discovered computers. (The port lists in the drop-down list are the same ones defined in the **Port Lists** page in the **Shared** section.)

Recommendations

Periodically, the Agents can scan their computer for common applications and then make rule recommendations based on what is detected. This setting sets the interval between scans on computers that have been configured to allow them.

Note: *This setting is not the same as a Scheduled Task to perform Recommendation Scans. If you wish to regularly scan for Recommendations, you should select this option or create a Scheduled Task (**Administration > Scheduled Tasks**), but not both. For more information on Scheduled Tasks, see **Scheduled Tasks (page 188)**.*

Virtual Appliance Scans (Policy editor only)

The Virtual Appliance has various settings that can significantly improve the efficiency of security scans in large virtual machine environments where Agentless protection has been implemented.

- **Max Concurrent Scans:** Scan requests are queued by the Virtual Appliance and carried out in the order in which they arrive. However, the Virtual Appliance is capable of carrying out concurrent scans on multiple VMs. The recommended number of concurrent scans is five. Beyond 10, the performance of the Virtual Appliance may begin to decline. This setting applies to Manual/Scheduled scans.
- **Max On-Demand Malware Scan Cache Entries:** This determines, for Manual (on-demand) Malware Scans, the maximum number of records that identify and describe a file or other type of scannable content to keep. One million entries will use approximately 100MB of memory.
- **Max Real Time Malware Scan Cache Entries:** This determines, for Real-Time Malware Scans, the maximum number of records that identify and describe a file or other type of scannable content to keep. One million entries will use approximately 100MB of memory.
- **Max Integrity Monitoring Scan Cache Entries:** This determines, for Integrity Monitoring, the maximum number of entities included in the baseline data for Integrity Monitoring. Two hundred thousand entities will use approximately 100MB of memory.

SIEM

Event Forwarding Frequency (From the Agent/Appliance)

Select how often events are sent from the Agent/Appliance to Alert recipients. (Enter syslog configuration in the Event Forwarding areas.)

Event Forwarding

The Events from each of the protection modules can be forwarded to a remote computer via syslog. For information on configuring Syslog, see **Syslog Integration (SIEM)** in the Deep Security Manager Administrator's Guide or the online help.

Updates (Computer Editor only)

If the Relay module is enabled for this computer, the Security Updates page displays the Components (Patterns) that the Relay is currently distributing to the Agents/Appliances that rely on it for Security Updates. If the Anti-Malware module is enabled for this computer, this page also displays the set of patterns that are in effect locally on this computer.

Download Security Updates: gets the latest Security Update available from the Deep Security Relay Group assigned to this computer.

Rollback Security Updates: rolls back the current Security Update to the one previously in effect on this computer. This button does not appear for Relays.

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 create multiple levels of child Policies which 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. This **Overrides** page shows you whether and how many settings have been overridden at this Policy or specific computer level. To undo the Overrides at this level, click the **Remove** button.

For more information, see **Policies, Inheritance and Overrides** in the Deep Security Manager Administrator's Guide or the online help.

Administration

The Administration section of the Deep Security Manager includes the following sections:

- The ***System Settings (page 162)*** section lets you control the administration of the Deep Security system.
- The ***Scheduled Tasks (page 188)*** section provides the ability to configure recurring automated tasks.
- The ***Event-Based Tasks (page 190)*** section provides the ability to configure tasks that will be performed upon the occurrence of specific events.
- The ***Manager Nodes (page 194)*** page displays a list of all active Manager nodes.
- The ***License (page 197)*** page displays details about your Trend Micro product license such as which Deep Security protection modules are available and how many computers you are licensed to install Agent/Appliance software on.
- Use the ***Users (page 198)*** section to create and modify User accounts for Users of the Deep Security Manager.
- Use the ***Roles (page 202)*** section to define various Roles with different rights. Roles are then assigned to Users.
- Use the ***Contacts (page 206)*** section to create and modify contacts. Contacts
- The ***System Information (page 208)*** page contains details about the current state of the Deep Security Manager.
- The ***Updates (page 210)*** section is for managing Security and Software Updates.

System Settings

The **System Settings** page contains the following tabbed pages:

- *Tenants (page 163)*
- *Agents (page 166)*
- *Alerts (page 169)*
- *Contexts (page 170)*
- *SIEM (page 171)*
- *SNMP (page 172)*
- *Ranking (page 173)*
- *System Events (page 175)*
- *Security (page 176)*
- *Updates (page 178)*
- *Smart Feedback (page 181)*
- *SMTP (page 182)*
- *Storage (page 183)*
- *Proxies (page 184)*
- *Advanced (page 185)*

Tenants

The **Tenants** tab appears only if you have enabled Multi-Tenant mode.

Multi-Tenant Options

- **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 "Backup" Scheduled Task:** Determines if the **Backup** Scheduled Task should be available to Tenants. In most cases backups should be managed by the database administrator and this option should be left checked.
- **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 if vCenter connectivity should be exposed. If the deployment is intended for a public service, this option should most likely be disabled since there will not be a route to the vCenter from a hosted service.
- **Allow Tenants to add 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 for a public service, this option should most likely be disabled since there will not be a route to the directory from a hosted service.
- **Allow Tenants to configure SNMP settings:** Allow Tenants to forward System Events to a remote computer (via SNMP)
- **Show Introduction to Tenants (Recommended only if all "add" and "synchronize" options are enabled):** Automatically displays the introductory slide show to Tenants when they first sign in. (The slide show can be accessed by clicking the **Support** link at the top right of the Deep Security Manager window and selecting **Introduction**.)
- **Show "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 "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 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" (for unassigned Relays):** 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.*

- **New Tenants automatically download the latest Security Updates:** 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 (all Tenants will use the options configured for the primary Tenant):**
  - **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 "SIEM" Tab (All Tenants use the settings located on the SIEM tab for ALL event types and syslog is relayed via the Manager):** Allows the primary Tenant to configure syslog for all Tenants at once. In CEF format the Tenant name is included as `TrendMicroDsTenant`.
  - **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 Deep Security Manager was installed with. In order to provide additional scalability Deep Security Manager supports adding additional database servers.

For SQL Server the secondary database server requires a hostname, username and password (domain and named instance are optional). The TCP/Named Pipes setting has to be the same as the primary database (TCP is always recommended). The user (the Deep Security Manager) must have the following permissions:

- create databases,
- delete databases and
- 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.

For information on setting up database user accounts for multi-tenancy see **Multi-Tenancy** in the Deep Security Manager Administrator's Guide or the online help.

Database servers (other than the primary) can be deleted provided there are no Tenants located on the server.

If the hostname, username, password or any details change the GUI can be used to change for database servers (other than the primary). To change values for the primary the Deep Security Manager must be shutdown (all nodes) and the dsm.properties file edited with the new details.

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 involves:

1. Creating a new Tenant
2. Logging in as that Tenant
3. Customizing the example Policies (adding/removing/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

All future Tenants will have the example policies and rule update version included in the snapshot.

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 additional Tenant computer details are recorded.

Agents

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. (Deep Security Manager always identifies computers by using a unique fingerprint, not their IP addresses or hostnames.)

Update the "Hostname" entry if an IP not is used as a hostname and a change in hostname is detected on the computer after Agent/Appliance-initiated communication or discovery: Updates the hostname displayed in the computer's "Hostname" property field if a hostname change is detected. (Deep Security Manager always identifies computers by using a unique fingerprint, not their IP addresses or hostnames.)

Agent-Initiated Activation

The standard method of installing and activating an Agent on a computer is to install the Agent on a computer and then to use the Deep Security Manager to "activate the Agent". This activation sends a unique encrypted fingerprint from the Manager to the Agent and the Agent will now refuse any instructions that are not identified as coming from the Manager by that fingerprint.

There may be circumstances, however, where it is desirable for the activation to be initiated by the Agent rather than by the Manager. (Large, distributed installations, for example.) In this case the Manager must be configured to allow Agents to communicate with it and initiate activation. Use the **Agent-Initiated Activation** panel to set restrictions on which computers can initiate their own Agent activations.

Agent-initiated activation is performed from the command-line. The following are the Agent's activation-related command-line options:

Usage: `dsa_control [-a <str>] [-g <str>] [-c <str>] [-r]`		**Notes**
`-a <str>`	**Activate** Agent with Manager at specified URL. URL format must be "dsm://hostOrIp:port/"	"port" is the Manager's Heartbeat port. (4120 by default.)
`-g <str>`	**Agent** URL. Defaults to "https://127.0.0.1:4118/"	
`-c <str>`	**Certificate** file. Default is "ds_agent.crt".	dsa_control will use the correct certificate automatically. There is no need to use this option unless you have multiple Agents installed in different directories, or you are trying to control an Agent on another computer.
`-r`	**Reset** Agent configuration	

Note: *You can instruct Deep Security Manager to send a default Policy to self-activating Agents which do not already have a Policy assigned to them. Use the* ***Policy to assign (if Policy not assigned by activation script)*** *option to select a Policy.*

If you allow Agent-Initiated Activated Activation, there are several further options you can configure:

Specify on which computers you will 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.*

If a computer with the same name already exists: If an computer with the same hostname is already listed on the **Computers** page the Deep Security Manager can take the following actions:

- **Do not allow activation:** The Deep Security Manager will not allow the Agent to be activated.
- **Activate a new computer with the same name:** If the listed computer is not activated, the Agent-Initiated Activation will be allowed to proceed and the new computer will take the place of the already listed computer on the Computers page.
- **Reactivate the existing computer:** The new computer will be activated/reactivated and take the place of the listed computer, whether the listed computer is activated or not.

Allow reactivation of cloned VMs: When a new VM clone which 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 and reactivate it as a new computer. No Policies or Rules that may have been in place on the original VM will be assigned to the new VM. It will be just a like a newly activated computer.

Allow reactivation of unknown VMs: This setting allows previously activated VMs which have been removed from their cloud environment and deleted from the Deep Security Manager to be reactivated if they are added back to the inventory of VMs. Deep Security Manager will recognize a valid certificate on VM and allow it to be reactivated. No Policies or Rules that may have been in place on the original VM will be assigned to the new VM. It will be just a like a newly activated computer.

Agent activation secret: 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 **tenantPassword** 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/ "tenantPassword:secret"
```

Note: *In a multi-tenant environment, the **Agent activation secret** setting applies only to the primary tenant.*

Note: *For more information on Agent-Initiated Activation, see* **Command-Line Utilities** in the Deep Security Manager Administrator's Guide or the online help *and* **Deployment Scripts** in the Deep Security Manager Administrator's Guide or the online help.

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.

Alerts

Alerts

View Alert Configuration...: Configure all of Deep Security Manager's possible Alerts. For the most part, this means turning them on or off, setting their severity levels, and configuring the Alert's email notification settings.

Length of time an Update can be pending before raising an Alert: The 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.

Alert Event Forwarding (from the Manager)

Enter an email address to which all Alert emails will be sent regardless of whether any Users have been set up to receive notifications. (Which Alerts will trigger the sending of an email can be configured in the **Alerts** section of the Deep Security Manager.)

Contexts

Use this page to configure the settings Deep Security will use to determine whether a protected computer has Internet connectivity or not. Some Deep Security Rules can be applied conditionally depending on the computer's network connectivity conditions. This is known as "Location Awareness". The Internet connectivity condition options for a particular rule can be configured on the **Options** tab of the rule's **Properties** window. The Internet Connectivity Test can also be used when implementing Interface Isolation. (See ***Interface Isolation (page 123)*** and ***Interfaces/Interface Types (page 144)***.)

Internet Connectivity Test

- **URL for testing Internet Connectivity Status:** The URL to which an HTTP request will be sent to test Internet Connectivity. (You must include "http://".)
- **Regular Expression for returned content used to confirm Internet Connectivity Status:** A regular expression which 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.)

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*

- **Test Interval:** The time interval between connectivity tests.

Example

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.

SIEM

System Event Notification (from the Manager)

Forward System Events to a Remote Computer (via Syslog): Notifications can be sent to a Syslog server. Type the details of your syslog server here.

Forwarding protection module Events is configured at the Policy and computer level. To configure protection module Event forwarding, go to **Policy/Computer Editor > Settings > SIEM**.

For information on configuring Syslog, see **Syslog Integration (SIEM)** in the Deep Security Manager Administrator's Guide or the online help.

SNMP

Forward System Events to a Remote Computer (via SNMP)

Deep Security supports SNMP for forwarding System Events to a computer from the 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`.

Ranking

Ranking

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** drop-down 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 drop-down list for all computers.)

System Events

System Events

System Events include activities and changes to the configuration of an Agent/Appliance, the Deep Security Manager, or Users. They also include errors that may occur during normal operation of the Deep Security system.

This page enables you configure the **Record** and **Forward** options for each type of System Event:

- **Record:** Deep Security Manager will record this type of event and list them on the **Events & Reports** > **Events** > **System Events** page.
- **Forward:** Deep Security Manager will forward this type of event to a remote computer, if you have configured System Event notifications on the **Administration > System Settings > SIEM** or **Administration > System Settings > SNMP** page.

For a list of all possible System Events, see **System Events** in the Deep Security Manager Administrator's Guide or the online help in the **Reference** section. Events are kept for a period of time, which can be set from the **Administration** > **System Settings** > **Storage** page.

Security

User Security

- **Session timeout:** Specify the period of inactivity after which a User will 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 he is locked out. Only a User with "Can Edit User Properties" rights can unlock a locked-out User.
- **Number of concurrent sessions allowed per User:** Maximum number of simultaneous sessions allowed per User.
- **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.

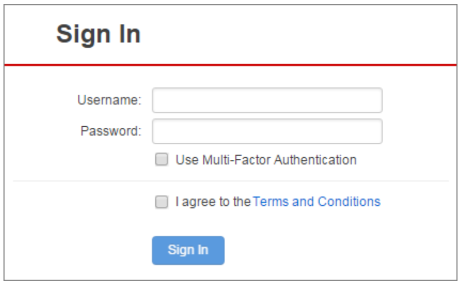
Note: *For greater security, enforce stringent password requirements: minimum 8 characters, include both numbers and letters, use upper and lower case, include non-alphanumeric characters, and expire regularly.*

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.*

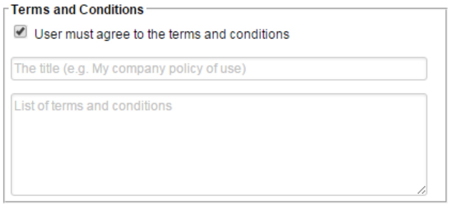
Note: *If a User gets locked out for a particular reason (too many failed sign-in attempts, for example), and no User remains with the sufficient rights to unlock that account, please contact Trend Micro for assistance.*

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:


Sign In
Username:
Password:
□ Use Multi-Factor Authentication
□ I agree to the Terms and Conditions
Sign In

To enable this feature, select **User must agree to the terms and conditions**. 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.



Terms and Conditions

☑ User must agree to the terms and conditions

The title (e.g. My company policy of use)
List of terms and conditions

Sign In Page Message

Enter text that will be displayed on the Deep Security Manager's sign in page.

Trusted Certificates

Click **View Certificate List** to view a list of all security certificates accepted by Deep Security Manager.

Key Pair Generation

Before adding a Microsoft Azure resource to Deep Security Manager, you will need to generate a certificate and key pair. After generating the required files, you will import the certificate (.cer file) into Azure Web Services Console. You will upload the key pair (.pem file) to Deep Security Manager when you add you Microsoft Azure resources.

To create a certificate and key pair:

1. In the Deep Security Manager, go to **Administration** > **System Settings** > **Security**.
2. Under **Key Pair Generation**, click **Generate Key Pair**.
3. Click **Create Key Pair**.
4. Save the .pem file locally.
5. Click **Export Certificate**.
6. Save the .cer file locally.
7. Click **Close**.

Updates

To ensure maximum protection you must keep your Software and Security Rules and Patterns up to date. The **Updates** tab on the **Administration > System Settings** page allows you to set the location where Deep Security Manager checks for updates. To see the status of current updates, go to the **Administration > Updates** page.

Security Updates

Primary Security Update Source

- **Trend Micro Update Server:** Connect to the default Trend Micro Update Server.
- **Other Update Source:** If you were given an alternative source for updates, enter the URL here including "http://" or "https://". (SSL connections are supported.)

Patterns

- **Allow Agents/Appliances to download Pattern Updates from Primary Update Source if Relays are not available:** If an Agent/Appliance cannot communicate with the Relay, it will download pattern files directly from the Trend Micro Update Server (or other update source).
- **Allow Agents/Appliances to download Pattern Updates when Deep Security Manager is not accessible:** Normally, the Deep Security Manager instructs Agents/Appliances to download Pattern Updates. When this option is selected, even though an Agent cannot communicate with the Deep Security Manager, it will continue to download updates from its configured source.

Rules

- **Automatically Apply Rule Updates to Policies:** With this option selected, newly downloaded Security Rule Updates 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.

Note: *By default, changes to Policies are automatically applied to computers. You can change this behavior by opening a **Policy/Computer Editor > Settings > Computer** window and changing the **Automatically send Policy changes to computers** setting in the **Send Policy Changes Immediately** area.*

Relays

- **Support 9.0 (and earlier) Agents:** Deep Security Security Update packages in versions 9.5 and later are in a different format than those from Deep Security 9.0 and earlier. If you are not running and Deep Security 9.0 Agents or Appliances, you should uncheck this option so you are not downloading unnecessary content.
- **Download Patterns for all Regions:** If this option is unchecked, a Relay will only download and distribute Patterns for the region (locale) the Deep Security manager was installed in. If you are operating in Multi-Tenancy mode and

any of your Tenants are running their Deep Security installations in regions other than your own, you should keep this option checked.

- **Use the Primary Tenant Relay Group as my Default Relay Group (for unassigned Relays):** By default, the Primary Tenant gives Tenants access to the its Relays, which means that Tenants do not need to set up their own Relays for security updates. If you do not want your Tenant environment to use those shared Relays, deselect this option and set up dedicated Relays for this Tenant.

  Note: *If your Primary Tenant has chosen to not share their Default Relay group, when you click* ***Administration*** *>* ***Updates*** *>* ***Relay Groups****, the Relay Group Name will be "Default Relay Group" rather than "Primary Tenant Relay Group", and you will need to set up your own dedicated Relays.*

  Note: *This setting appears only if you have enabled Multi-Tenant mode.*

Software Updates

Trend Micro Download Center

- **Automatically download updates to imported software:** Select this option to automatically download updates to any software that you have already imported to Deep Security. This setting will download the software to the Deep Security but will not automatically update your Agent or Appliance software.

  Note: *Updating the Deep Security software on your computers must be done manually by either selecting the computer(s) on the* ***Computers*** *page and selecting* ***Upgrade Agent...*** *from the* ***Actions*** *menu, or by opening the computer's editor Window, going to* ***Overview > Actions > Software*** *and clicking* ***Upgrade Agent...*** *.*

- **Allow Relays to download software updates from Trend Micro Download Center when Deep Security Manager is not accessible:** Select this option to enable Relays to download software updates directly from the Trend Micro Download Center when they cannot connect to the Deep Security Manager. This 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 ports into your enterprise environment from the cloud.

Alternate software update distribution server(s) to replace Deep Security Relays:

Deep Security Relays are usually used to host Agent Software Updates. However, you can optionally use your own web servers to distribute Agent software packages. To use your own web servers for software distribution, enter the URL to the directory hosting the software.

Note: *Even though you are using your own web servers to distribute software, you must still import Agent software from the Trend Micro Download Center into the Deep Security Manager using the options on the* ***Administration > Updates > Software*** *screens. 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. For more information on configuring your own software distribution web servers, see* **Configuring a Software Web Server** in the Deep Security Manager Administrator's Guide or the online help*.*

Virtual Appliance Version Control

The Deep Security Virtual Appliance uses the same Protection Module plug-in software packages as the 64-bit Red Hat Enterprise Linux Agent. Upon activation of the Virtual Appliance, Deep Security will check the inventory of imported software for the latest version of the Red Hat Enterprise Linux Agent to see if there are updates available. You can use this control to manage the version of the Red Hat Enterprise Linux Agent software that will be used to update any newly activated Virtual Appliances.

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.

Note: *Smart Feedback will use the* ***Agents, Appliances, and Relays (Security Updates)*** *proxy specified on the* ***Administration > System Settings > Proxies*** *tab.*

Smart Feedback is part of the Trend Micro Smart Protection Network. The Smart Protection Network uses a global network of threat intelligence sensors to continually update email, web, and file reputation databases in the cloud, identifying and blocking threats in real time.

Deep Security can access the Smart Protection Service directly or you can install local Smart Protection Servers. Smart Protection Servers are designed to localize operations to the corporate network to optimize efficiency. Smart Protection Server software along with installation and configuration instructions are available from the Trend Micro Download Center at http://downloadcenter.trendmicro.com.

Note: *You can enter the addresses of several Smart Protection Servers. Trend Micro recommends that you install multiple local servers to ensure availability in case of hardware, software, or connectivity failure.*

SMTP

SMTP

Type the address of your SMTP mail server. (You only need to specify the port if it differs from the default SMTP port 25.) Enter a "From" email address from which the emails should be sent. Optionally enter a "bounce" address to which delivery failure notifications should be sent if the Alert emails can't be delivered to one or more Users. If your SMTP mail server requires outgoing authentication, enter the username and password credentials. Select STARTTLS if your SMTP server supports the protocol.

Once you've entered the necessary information, use the **Test SMTP Settings** to test the settings.

Storage

Data Pruning

These settings define how long to store Event records and Counters, older Security Updates, and other stored objects before purging them from the database.

With respect to the Event settings, your decisions should be based on the robustness of the database system you are using, the amount of available storage space, and which events you have decided to log.

Some tips on Event logging:

- Modify the amount of log collection for computers that are not of interest. This can be done in the **Events** and **Advanced Network Engine Settings** areas on the **Policy/Computer Editor > Settings > Network Engine** tab.
- Consider reducing the Event logging of Firewall Rule activity by disabling the Event logging options in the Firewall Stateful Configuration. (For example, disabling the UDP logging will eliminate the unsolicited UDP log entries)
- For Intrusion Prevention Rules the best practice is to log only dropped packets. Logging packet modifications may result in a lot of 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 source of attacks. Otherwise leaving packet data on will result in much larger log sizes.

Note: ***Counters*** *are data aggregated from the Event logs. They are used to generate Reports and populate the Dashboard widgets.*

Note: ***Server Logs*** *are a record of the Deep Security Manager web server activity. They do not contain information related to the security of the computers on your network.*

Proxies

Proxy Server Use

- **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/Appliances get the Anti-Malware components of their Security Updates from Deep Security Relays. However, if Agents/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/Appliances will also use this proxy.*

- **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.)*

- **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.

You can view and edit the list of available proxies on the **Proxies** tab on the **Administration > System Settings** screen.

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 in **Policy/Computer Editor > Anti-Malware > Smart Protection**).

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

Service	Origin	HTTP Support	SOCKS4 Support	SOCKS5 Support
Software Updates	DSM	Yes	Yes	Yes
Security Updates	DSA/DSVA/DSR	Yes	Yes	Yes
Licensing and product registration	DSM	Yes	Yes	No
Certified Safe Software Service	DSM	Yes	No	No
Smart Feedback	DSA/DSR	Yes	Yes	Yes
Amazon AWS Cloud Account	DSM	Yes	No	No
VMware vCloud Cloud Account	DSM	Yes	No	No
Microsoft Azure Cloud Account	DSM	Yes	No	No

Advanced

Primary Tenant Access

By default, the Primary Tenant is able to access your Deep Security environment. However, the Primary Tenant may have enabled the "Primary Tenant Access" settings in your environment. These settings allow you to prevent the Primary Tenant from accessing your Deep Security environment or to grant access for a limited amount of time.

Load Balancers

When the Deep Security Manager and Deep Security Relays are deployed without load balancers, Agents are provided with the list of Manager and Relay hostnames and will automatically contact these servers using a random round robin sequence.

You may choose to put a load balancer in front of the Manager or Relay nodes to accommodate auto-scaling. You can do so without having to update the Agents' address by entering the load balancer settings here. The hostnames and ports you supply here will override those currently used by the Agents.

Note: *The Manager web console and Relay Ports can be deployed behind a normal terminating SSL load balancer. The Agent's heartbeat port (defaulted to 4120) must be a non-terminating load balancer because of the mutual SSL authentication used in the heartbeat communication.*

Note: *The load balancer settings supplied here will also override the addresses generated by the Deployment Script Generator. (The script generator writes the address of the Manager that the user is connected to.) This ensures that the scripts continue to function even if one of the Manager nodes is removed.*

Multi-Tenant Options

To run Deep Security Manager in Multi-Tenant mode:

1. Click Enable Multi-Tenant Mode.
2. In the wizard that appears, enter your Multi-Tenant Activation Code and click Next.
3. Choose a license mode to implement:
   - **Inherit Licensing from Primary Tenant:** Gives all Tenants the same licenses as the Primary Tenant.
   - **Per Tenant Licensing:** In this mode, Tenants themselves enter a license when they sign in for the first time.
4. Click Next to finish enabling Multi-Tenancy in your Deep Security Manager.

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 encoding used when you export data files from the Deep Security Manager.

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 the **Administration > System Information** page.

Whois

The Whois lookup to be used when logging 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 the **Administration > User Management > Users > Properties** window).

Scan Cache Configurations

Click **View Scan Cache Configurations...** to display a list of saved Scan Cache Configurations. Scan Cache Configurations are settings used by the Virtual Appliance to maximize the efficiency of Anti-Malware and Integrity Scans in a virtualized environment. See **Virtual Appliance Scan Caching** in the Deep Security Manager Administrator's Guide or the online help for more information.

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**.

NSX

If Deep Security is being used to protect virtual machines in a VMware NSX environment and if it is installed with multiple Deep Security Manager nodes, this setting will determine which Deep Security Manager node communicates with the NSX Manager. (For more information on integrating Deep Security with an NSX environment, see the **Trend Micro Deep Security Installation Guide for VMware NSX**. For more information on multiple Deep Security Manager Nodes, see **Multi-Node Manager** in the Deep Security Manager Administrator's Guide or the online help.)

Logo

You can replace the Deep Security logo at the top-right of the Deep Security Manager with your own. (The logo also appears on the sign-in page and at the top of Reports.) The graphic has to be a PNG image 320 pixels wide, 35 pixels high, and smaller than 1MB. (A template is available in the "installfiles" directory of the Deep Security Manager.)

Click **Import Logo...** to import your own graphic, or **Reset Logo...** to reset the log to its default.

Scheduled Tasks

The **Scheduled Tasks** page lets you automate and schedule certain common tasks.

From the main page you can:

- Create **New** Scheduled Tasks ()
- **Delete** a Scheduled Task (🗑)
- Examine or modify the **Properties** of an existing Scheduled Task ()
- **Duplicate** (and then modify) existing Scheduled Tasks ()
- **Run** (▶) a selected Scheduled Task

Click **New** () and select "New Scheduled Task". The wizard that appears will guide you through the steps of creating a new Scheduled Task. You will be prompted for different information depending on the type of task.

Scheduled Tasks

The following Tasks can be scheduled:

- **Backup:** Perform regular database backups. (This option is only available if you are using a Derby or Microsoft SQL Server database.)
- **Check for Security Updates:** Regularly check for security updates and import them into Deep Security when they are available.
- **Check for Software Updates:** Regularly check for Deep Security 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.
- **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 the same as that specified on the **Policy/Computer Editor > Anti-Malware** page for each computer.
- **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. The ports that will be scanned are those defined on the **Scanning** tab in the **Policy/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.
- **Send Outstanding Alert Summary:** Generate an email listing all outstanding (unresolved) Alerts.
- **Send Policy:** Regularly check for and send updated policies.

- **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/Contacts:** 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.)
- **Synchronize VMware vCenter:** Synchronize the **Computers** list with an added VMware vCenter. (Only available if you have added a VMware vCenter to the Deep Security Manager.)

Enabling or Disabling a Scheduled Task

Existing Scheduled Tasks can be enabled or disabled. For example, you may 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.

Event-Based Tasks

Event-based Tasks let you monitor protected computers for specific Events and perform Tasks based on certain conditions.

From the main page you can:

- Create **New** Event-based Tasks ( )
- Examine or modify the **Properties** of an existing Event-based Task ()
- **Duplicate** (and then modify) existing Event-based Tasks ()
- **Delete** a Event-based Task ( )

Click **New** () and select **New Event-based Task**. 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.

Events

The following Events can be monitored:

- **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

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** (http://docs.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html) to match patterns in the following fields:

- **Cloud Instance Image ID**: Cloud instance Image ID.

> Note: *The **Cloud Instance Security Group Name** 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: *The **Cloud Instance Metadata** 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: *The **Cloud Instance Security Group Name** match condition is only available for AWS cloud instances.*

- **Cloud Account Name**: The "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.
- **Folder Name**: The name of the folder or directory in which the computer is located in its local environment.

> Note: *The **Folder Name** 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+ **or** FIN-.*
RD-ABCD	RD-\w+ **or** RD-.*

AB **or** ABC **or** ABCCCCCCCCCC	ABC*
Microsoft Windows 2003 **or** Windows XP	.*Windows.*
Red Hat 6 **or** Some_Linux123 **or** abcFreeBSD	.*Red.*|.*Linux.*|.*FreeBSD.*

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 of two minutes before activation to allow any pending VMware administrative tasks to complete.*

> *Note:* *Activation will only occur if the computer is not already activated. That is, activation will only occur if the computer does not already have Agent or Virtual Appliance protection, or if the computer only has Agent protection but Virtual Appliance protection is available.*

- **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.

Enabling or Disabling an Event-Based Task

Existing Event-Based Tasks can be enabled or disabled. 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. The control to enable or disable an Event-Based Task is on the **General** tab of the Task's **Properties** window.

Manager Nodes

The **Manager Nodes** page displays a list of all active Manager nodes. Double-click on a Manager node in the list to display its **Properties** window:

- **Hostname:** The hostname of the Deep Security Manager host computer.
- **Description:** A description of the Manager node.
- **Performance Profile:** A 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 "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. The following table gives an indication of how some common concurrent operations are 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/Appliance-Initiated Heartbeats	20 Active 40 Queued	50 Active 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. The following table gives an indication of how some common concurrent operations are 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/Appliance-Initiated Heartbeats	20 Active 40 Queued	50 Active 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
Check Status	100	Same (100)

Operation	2-core system	8-core system
Agent/Appliance-Initiated Heartbeats	20 Active 40 Queued	50 Active 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 whether the Deep Security Manager node whose properties you are viewing is online and active from the perspective of the Deep Security Manager node you are logged into.
- **Options:** You can choose to decommission the Manager node. The node has to be offline (uninstalled or service halted) to be decommissioned.

For more information on multi-node Deep Security Manager installations, see **Multi-Node Manager** in the Deep Security Manager Administrator's Guide or the online help.

Tenants

The **Tenants** page displays the list of Tenants registered with this installation of Deep Security. From the main page you can:

- Create a **New Tenant**( )
- **Delete** a Tenant ( )
- Examine or modify the **Properties** of an existing Tenant ( )
- **Sign In As Tenant**, which enables you to use Deep Security Manager as if you are the Tenant.

> Note: *If you selected the **Administration** > **System Settings** > **Tenants** > **Allow Tenants to control access from Primary Tenant** option, the Tenant can disable your ability to sign in as the Tenant.*

- If a Tenant upgrade has failed, you can use the **Database Upgrade** button to force the upgrade process.
- **Export** ( ) one or more Tenants to a CSV file. (Either export them all by selecting **Export to CSV...** from the drop-down list or export only those that are selected by choosing **Export Selected to CSV...**)
- **Add/Remove Columns** ( ) columns can be added or removed by clicking **Add/Remove Columns**. The order in which the columns are displayed can be controlled by dragging them into their new position. Listed items can be sorted and searched by the contents of any column.

Clicking **New** ( ) or **Properties** ( ) displays the Tenant **Properties** window.

Licenses

Displays details about your Trend Micro Deep Security product licenses. Deep Security consists of five module packages: Anti-Malware and Web Reputation; Firewall and Intrusion Prevention; Integrity Monitoring; Log Inspection; and 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 will be immediately available.

When a license expires, existing functionality will persist but updates will no longer be delivered.

Alerts will be raised if any module is about to expire or has expired.

Licensing for AWS Marketplace

On the AWS Marketplace, there are two separate Deep Security Manager AMIs, each providing a different licensing option: "Bring your own license" or "Pay per use". The type of license you are using is displayed in the Deep Security Manager console, under **Administration** > **Licenses**.

- **Bring-Your-Own-License** (BYOL) is for customers who have already obtained a license to use Deep Security 9.5 from another source. This type of licensing works the same way as standard Deep Security licensing, described above.
- **Pay-Per-Use** (PPU) enables customers to pay based on the size of the AWS instance they are running. With PPU, each EC2 instance type has an associated seat count limit (the seat count is the number of Deep Security Agents that you can run). You can change the size of your instance at any time. You can also run more than one instance to increase your seat count limit. When you install Deep Security Manager on an additional instance, on the Database tab, select "This Deep Security installation will act as an additional Manager node in an already-deployed Deep Security installation". This option specifies that each node will use the same database. Here are the seat count limits for each type of EC2 instance supported for Deep Security Manager:
    - **M3 Large (m3.large):** Up to 25 Agents
    - **M3 XL (m3.xlarge):** Up to 50 Agents
    - **M3 2XL (m3.2xlarge):** Up to 100 Agents
    - **C3 4XL (c3.4xlarge):** Up to 200 Agents

  As you launch or shut down Deep Security Manager nodes, the seat-count usage for the hour is re-calculated and the remaining seat limit is displayed on the **Administration** > **Licenses** page.

Note: *Deep Security on the AWS Marketplace does not support the use of vCenter and the Deep Security Virtual Appliance (DSVA). Additionally, the PPU license does not provide Multi-Tenant support.*

Users

"Users" refers to all Deep Security Manager account holders. Use this section to create, modify, and delete User accounts. From the **Users** page, you can:

- Create **New** User accounts ( )
- Examine or modify the **Properties** of an existing User account ( )
- Set (or change) the **Password** for a User account ( )
- **Delete** a User account ( )
- **Search** ( ) for a particular User
- **Synchronize** ( ) with a **Directory** list of Users
- View **System Events** ( ) associated with this User
- Set or change the **Role** ( ) for this User

Clicking **New** ( ) or **Properties** ( ) displays the **User Properties** window.

General

General Information

- **Username:** The username associated with this User's password.
- **Name:** The name of the account holder.
- **Description:** a description of the account holder.
- **Role:** Use the drop-down list to assign a pre-defined Role to this User. (Assigning Roles can also be done using the right-click menu when in List View mode.)

Note: *The Deep Security Manager comes pre-configured with two Roles: Full Access and Auditor. The "Full Access" Role grants the User all possible privileges in terms of managing the Deep Security system such as creating, editing and deleting computers, computer groups, Policies, Rules, etc. The "Auditor" Role gives the User the ability to **view** all the information in the Deep Security system but not the ability to make any modifications except to his personal settings (password, contact information, view preferences, etc.) Roles with various levels of system access rights can be created and modified in the **Roles** page or by selecting "New..." in the **Roles** drop-down 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.

Sign-In Credentials

- **Set password:** Click this button to change your password. You will be prompted for your old password and new password.
- **Password never expires:** When this option is selected, the user's password will never expire.
- **Locked Out (Denied permission to sign in):** Checking this will keep this User from being able to sign in to the Manager. (If a User enters the wrong password too many times when trying to sign in, he will be locked out automatically. Clear this if you have resolved this situation.) (Locking or unlocking a User can also be done from the right-click menu when in List View Mode.)

Multi-Factor Authentication (MFA)

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 **Multi-Factor Authentication (MFA)** in the Deep Security Manager Administrator's Guide or the online help.

Contact Information

This User's contact information. Checking the **Receive Notifications** checkbox will include this User in the list of Users who receive email notifications when Alerts are triggered.

Settings

Module

- **Hide Unlicensed Modules:** 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 Manager's status bar 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.
- **Menu/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 window:** 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.
- **Optimal 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 show on a single page:** Many lists on the Deep Security Manager are grouped into categories. For example, Intrusion Prevention Rules can be grouped according to Application Type. The Deep Security Manager will try to avoid splitting these groups when paginating and can override the "Optimal" setting (above) to keep items in the same group together. Use this setting to set a firm maximum on the number of items to display per page. If the number of items in a group exceeds this number, the group will be split and the group title will display information that this has been done.
- **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:** Determines if Reports exported in PDF format are password protected.

Reset to Default Settings: Reset all settings on this page to their defaults.

Synchronizing with a Directory

The User list can be synchronized with an Active Directory, allowing Users to sign in with the password stored in the directory. Clicking **Synchronize with Directory** in the toolbar will display the **Synchronize with Directory** wizard. Type the name of the directory server and your access credentials. 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've 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 Manager.

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 delete a User from Deep Security Manager who was added as a result of synchronizing with an Active Directory and then re-synchronize with the directory, the User will reappear in your User list (if they are still in the Active Directory).*

Filtering the Active Directory

The first page of 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 and/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 http://datatracker.ietf.org/doc/rfc4515/.

Note: *The new Users, although being in the "locked out" state, are given the "Full Access" User Role.*

Roles

Deep Security uses Role-based access control to restrict Users' access to various parts of the Deep Security system. Once you have installed the 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.

Deep Security comes pre-configured 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 the Manager interface will be either visible and changeable, visible only but disabled, or hidden. For a list of the rights granted in the pre-configured Roles, as well as the default rights settings when creating a new Role, see* **User Management** in the Deep Security Manager Administrator's Guide or the online help*.*

You can create new Roles which 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, etc.). 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.*

From the main page you can:

- Create **New** Roles ( )
- Examine or modify the **Properties** of an existing Role ( )
- **Duplicate** (and then modify) existing Roles ( )
- **Delete** a Role ( )

Clicking **New** ( ) or **Properties** ( ) displays the **Role properties window** with six tabs (**General, Computer Rights, Policy Rights, User Rights, Other Rights,** and **Assigned To**).

General

General Information

The name and description of this Role.

Access Type

Select whether Users with this Role will have access to the Deep Security Manager's Web-based user interface or the Deep Security Manager's Web service API, or both.

*Note: To enable the Web service API, go to **Administration > System Settings > Advanced > SOAP Web Service API**.*

Computer Rights

Computer and Group Rights

Use the **Computer and Group Rights** panel 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.

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/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, etc.)

  Note: The previous two settings affect data Users have access to. Although Users' abilities 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 sub-groups within the computer groups they have access to.

Advanced Rights

- **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.
- **Allow Cloud Providers to be added, removed, and sychronized:** Allow Users in this Role to add, remove, and synchronize Cloud Providers.

Policy Rights

Determines the rights a User in a particular Role has to create, delete, modify, or import Policies.

Policy Rights

Use the **Policy Rights** panel 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, select the **Selected Policies** radio button and put a check next to the policies that Users in this Role will have access to.

Note: *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/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.

Advanced Rights

- **Allow Policy imports:** Allow Users in this Role to import policies using files created with the Deep Security Manager's **Export** option on the **Policies** tab.

User Rights

User Rights

The options on the **User Rights** tab allow you to set what kind of authority Users in this Role have over other Users.

- **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.

> *Note:* *Be careful when using this last option. If you assign this option 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 Rights

You can further restrict Users' ability to view/create/edit/delete Users and Roles by selecting **Custom** and using the options in the **Custom Rights** panel. Some options may be restricted for certain users if the **Can only manipulate Users with equal or lesser rights** option is selected (see below).

Delegate Authority

Selecting the **Can only manipulate Users with equal or lesser rights** option will limit 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.

When this option is selected, 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** area:

- **Can Create New Users:** Can only create Users with equal or lesser rights.
- **Can Edit User Properties:** Can only edit a User (or set/reset password) with equal or lesser rights.
- **Can Delete Users:** Can only delete Users with equal or lesser rights.

Other Rights

Roles can be restricted with respect to the Deep Security objects they can manipulate. Default settings for new Roles are "View Only" or "Hide" for each element, but these rights can be expanded to "Full Control", or customized by choosing "Custom" from the drop-down list.

Assigned To

The **Assigned To** tab displays a list of the Users who have been assigned this Role.

Contacts

Users can create "Contacts". Contacts cannot sign in to the Deep Security Manager but they 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.

From the **Contacts** page, you can:

- Create **New** Contacts ( )
- Examine or modify the **Properties** of an existing contact ( )
- **Delete** a contact ( )
- **Synchronize** ( ) with an **Directory** list

Clicking **New** ( ) or **Properties** ( ) displays the **Contact properties window**.

General Information

The name, description, and preferred language of this contact.

Contact Information

The email address entered here is 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.)

Clearance

The Role specified here determines the information this contact will be allowed to see. For instance, 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.

Reports

Select whether or not reports will be encrypted for this User.

Synchronizing with a Directory

The Contact list can be synchronized with an Active Directory. Clicking **Synchronize with Directory** in the toolbar will display the **Synchronize with Directory** wizard. Type the name of the directory server and your access credentials. You will then be prompted to select which group of Users to import and whether they will be Users or Contacts. Once they've 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.

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".)*

System Information

Create a Diagnostic Package...

Clicking **Create Diagnostic Package...** in the Toolbar displays the **Diagnostic Package** wizard which will create a zip file containing Install/Uninstall and Debug Logs, System Information, Database Contents (last hour only for time-sensitive items), File Listing, and Properties Files (Passwords Removed). This information can be given to your support provider to help troubleshoot any problems.

Note: The default maximum size of a diagnostic package is 256MB. A command line instruction is available to increase the size of the diagnostic package:

```
dsm_c -action changesetting -name configuration.diagnosticMaximumFileSize -value ####
```

The following example increases the size of the package to 1GB (1000MB):

```
dsm_c -action changesetting -name configuration.diagnosticMaximumFileSize -value 1000
```

Do not change the size of the diagnostic package unless instructed to do so by your support provider.

Extensions...

Extensions can be reports or plug-ins for the Deep Security Manager.

Demo Mode...

If you are evaluating Deep Security in a test environment and want to see what a full Deep Security installation in an enterprise environment looks like, you can enable Demo Mode by clicking **Demo Mode...** on the **System Information** page toolbar.

When in Demo Mode, the Manager populates its database with simulated 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.

*Note: While Demo Mode can be used with mixed real and simulated computers, it is **not** intended to be used in a production environment!*

Demo mode can be turned off the same way.

System Activity (Over The Last Hour)

This panel displays various graphs detailing activities carried out by the different Manager nodes. For details on the information displayed in the **System Activity** panel, see **Multi Node Manager** in the Deep Security Manager Administrator's Guide or the online help.

System Details

This panel displays detailed system information used for troubleshooting by your support provider.

Updates

The Updates section of the Deep Security Manager includes the following sections:

- The ***Security (page 211)*** section enables you to manage your security updates.
- The ***Software (page 216)*** section enables you to manage your software updates.
- The ***Relay Groups (page 221)*** section enables you to create and modify groups of Deep Security Relays.

Security Updates

The Security Updates Overview page displays the state of your Security Updates from the Trend Micro Update Server through to your Deep Security distribution network and down to your protected computers.

Pattern Updates are used by the Anti-Malware module.

Rule Updates are used by these modules:

- Firewall
- Intrusion Prevention
- Integrity Monitoring
- Log Inspection Security

Pattern Updates

Trend Micro Update Server

Indicates whether Deep Security Relays can connect to the Trend Micro Update Server to check for the latest Pattern Updates.

Deep Security

- **Last check for updates:** The last time a successful check for Pattern Updates was performed.
- **Check for Updates and Download...:** Check for available Pattern Updates. If new Updates are available, they will be automatically downloaded.
- **Last Download:** The last time that a new Pattern Update was downloaded after a successful check for Updates.
- **All Relays in Sync:** Indicates whether 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 here.
- **Next scheduled check:** The next time a Scheduled Task to check for Pattern Updates is due to run.

Computers

- **All Computers are up to date/Computers out of Date:** Indicates whether or not any computers are out of date *with respect to the Pattern Updates being stored in the Relays.*
- **Send Patterns to Computers:** instructs all computers to retrieve the latest Pattern Updates from their assigned Relays.

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.*

Rule Updates

Trend Micro Update Server

Indicates whether Deep Security Relays can connect to the Trend Micro Update Server to check for the latest Rule Updates.

Deep Security

- **Last check for updates:** The last time a successful check for Rule Updates was performed.
- **Check for Updates and Download...:** Check for available Rule Updates. If new Updates are available, they will be automatically downloaded.
- **Last Download:** The last time that a new Rule Update was downloaded after a successful check for Updates.
- **Apply Rules to Policies...:** Apply the latest downloaded Rule Updates to your Security Policies. (This will be done automatically if you have the **Automatically apply new Rule Updates to Policies** option selected on the **Administration > System Settings > Updates** tab.)
- **Policies are using Rule Update xx-yyy:** The Rule set that is currently being applied by the Security Policies. A warning will be displayed if you are not using the latest downloaded update.
- **Next scheduled check:** The next time a Scheduled Task to check for Rule Updates is due to be.

Computers

- **All Computers are up to date/Computers Out of Date:** Indicates whether or not any computers are out of date *with respect to the Rule Updates that have been applied to the Policies stored in the Deep Security Manager.*
- **Send Policies to Computers:** click to send Policies with updated Rule sets to any Computers that do not yet have them.

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.*

Rules

Displays a list of the most recent Intrusion Prevention, Integrity Monitoring, and Log Inspection Rules that have been downloaded to the Deep Security Manager's database. If required you can reapply the current Rule set to computers being protected by Deep Security or rollback to a previous Rule set. You can configure the number of Rule Updates that are kept in the Deep Security Manager's database by going to the **Administration > System Settings > Storage** tab.

From the **Rule Updates** page, you can:

- **Import** (🔒) a Rule Update
- **Delete** (🗑) a Rule Update
- **View** the Properties (▤) of a Rule Update
- **Rollback** (✓) to an earlier Rule Update
- **Export** (📄) a Rule Update

Import

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 asked to do so by your support provider.

View Properties

The **Properties** window for a Rule Update displays:

General Information

- **Name:** the name of the Rule Update file
- **Version:** the version number of the Rule Update
- **Released:** the date the Rule Update was issued by Trend Micro
- **Imported:** the date the Rule Update was imported into Deep Security
- **Applied:** the date the Rule Update was applied Policies

Contents

Itemizes new objects included in the Rule Update.

Rollback

If a recent Rule Update has caused problems in your environment, you may want to rollback to a previous Rule Update. If you rollback to a previous Update, all Policies affected by the rollback will be immediately updated on *all computers using those Policies*.

Export

Under normal circumstances you should not have to export a Rule Update unless asked to do so by your support provider.

Patterns

The **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.

Indicates whether Deep Security Relays can connect to the Trend Micro Update Server to check for the latest Pattern and Rule Updates.

- **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.

The version numbers of the Security Update components in effect on a specific computer can be found on the **Computer Editor > Updates** page.

Software Updates Overview

The **Software Updates Overview** page displays the state of your Software Updates from the Trend Micro Update Server through to your Deep Security distribution network and down to your protected computers.

Trend Micro Download Center

This area of the overview page displays whether there are any updates available for the software that has already been imported to Deep Security.

Note: *Deep Security will only inform you of updates to the minor versions of your imported software. For example, if you have Agent version **9.5.100**, and Trend Micro releases Agent version **9.5.200**, Deep Security will tell you that updates to your software are available. However, if Trend Micro then releases Agent version **9.6.xxx** and you don't have any earlier **9.6** Agents in your database inventory, you will not receive a notification that updates are available (even though you have a **9.5.100** Agent).*

Deep Security

This area of the overview page displays the last time a check for software Updates was performed and whether the check was successful. The **Check for updates** button performs an on-demand check. The date of the next Scheduled task for a software update is displayed. There will be a warning if no Scheduled Task exists.

Computers

Displays whether any computers are running Agents for which updates available. The check is only performed against software that has been downloaded to Deep Security, not against software available from the Download Center. If any computers are out of date, you can click the **Upgrade Agent/Appliance software** button, which takes you to the **Computers** page filtered to display out-of-date computers.

Note: *Deep Security considers computers out of date only if an update to the minor version of the Agent is available in the Deep Security database inventory. For example, if you have a computer running Agent version **9.5.100**, and you import Agent version **9.5.200** from Trend Micro Download Center, Deep Security will tell you that the computer is out of date. However, if you are running Agent version **9.5.200** and you then import Agent version **9.6.xxx**, Deep Security will not consider the computer out of date and you will see a green check mark indicating that your computers are up to date.*

Upgrading Agent/Appliance Software

The Agent software on Computers must be upgraded manually. To upgrade all Agents, click **Upgrade Agent/Appliance Software...**. To upgrade the Agent software on individual computers, go the **Computers** page and select **Actions > Upgrade Agent** from the context menu.

Download Center

Displays a list of the latest software available for download from the Trend Micro Download Center. Software packages will include new versions of the Manager, the Agents, the Virtual Appliance, and the Filter Driver.

Note: *Only the most recent Deep Security software is listed on this page. For older versions, go directly to Download Center web site at http://downloadcenter.trendmicro.com/*

- **Name:** the file name of the software package
- **Release Notes:** a link to the release notes for the software package
- **Platform:** the platform for the software package
- **Imported:** a checkmark is displayed if the software is already downloaded to your Deep Security database
- **Version:** the software version number
- **Release Date:** the date the software was made available by Trend Micro
- **Direct Import Capable:** an icon(🌐) is displayed if the software package can be imported to the Deep Security Manager directly from the Download Center. Packages that cannot be imported directly must be downloaded to a local folder from the Trend Micro Download Center web site and manually imported on the **Administration > Updates > Software > Local** page.

Import

Use this Import function to manually import software from the Trend Micro Download Center.

Local Software

The **Local Software** page lists the software that has been imported into Deep Security.

Software must be imported from the Trend Micro Download Center into the Deep Security database for it to be available to the computers on your network. When an Alert is raised that the software on a computer is out of date, it is because a more recent version of the Agent or Appliance software is available locally in Deep Security. That is, 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.)

To install a Deep Security Agent or Appliance on a computer, you first have to import the software from the Download Center into Deep Security and then extract the installer package.

From the **Local Software** page, you can:

- **Import** ( ) a Software Update
- **Delete** ( ) a Software Update
- **View** the Properties ( ) of a Software Update
- **Export** ( ) a Package or Installer
- **Generate Deployment Scripts** ( ) for the installation of Agents on computers

Import

Under normal circumstances, software is imported from the Download Center either automatically, or manually from the **Administration > Updates > Software > Download Center** page. Use this Import function to manually import software from locations other than the Trend Micro Download Center.

Delete

Delete a software package from the Deep Security database.

The Deep Security database must contain a copy of all software currently installed on managed computers. When a Deep Security Agent is first activated, only those Protection Modules that are "On" in the Security Policy being applied are installed on the computer. If you turn on a Protection Module at a later time, Deep Security will retrieve the plug-in for the new Security Module from the Agent software package in the database to install it on the computer. If that software is missing, the Security Module plug-in cannot be installed.

To save space, Deep Security will periodically remove unused packages from the Deep Security database. There are two types of packages that can be deleted: Agent packages and Kernel Support packages.

Note: *The Deep Security Virtual Appliance relies on the Protection Module plug-ins found in the 64-bit Red Hat Enterprise Linux Agent software package. If you have an activated Virtual Appliance and try to delete a 64-bit Red Hat Enterprise Linux Agent, you will get an error message telling you the software is in use.*

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. The number of old software packages kept in the database is configured on the **System Settings > Storage** tab. You can also manually delete unused Agent packages. If you try to delete software that is being used on one of your managed computers, you will get a warning and be unable to delete the software.

Note: *For the Windows and Linux Agent packages, only the in-use 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 will 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.

Note: *For Linux Kernel Support packages, only the latest one cannot be deleted.*

Deleting Kernel Support packages

In both single and multi-tenancy mode, Deep Security automatically deletes unused Kernel Support packages (KernelSupport-*platform*-*version*.zip). The number of old packages kept in the database is configured on the **System Settings > Storage** tab. A Kernel Support package can be deleted if both of these conditions are true:

- There is no Agent package with the same group identifier.
- There is another Kernel Support package with the same group identifier and a later build number.

You can also manually delete unused Kernel Support packages.

View Properties

The **Properties** window for a Software Update displays:

General Information

- **Name:** the name of the Software Update file
- **Platform:** the operating system the software is built for
- **Version:** the version number of the Software Update
- **Fingerprint:** The digital fingerprint of the file.
- **Imported:** the date the Rule Update was imported into Deep Security
- **Notes:** any miscellaneous notes you wish to attach to the file

Export

Export Package: This option will export the entire software package. Use this option to export software for use with an optional Update Web Server. (Update Web Servers are web servers under your control which can be used as software distribution points instead of Relays. Update Web Servers are configured on the **Administration > System Settings > Updates**

tab. For more information on Update Web Servers, see **Software Updates** in the Deep Security Manager Administrator's Guide or the online help in the User's Guide.)

Export Installer: This option extracts the core Agent installer from the Agent package. The core Agent installer is used to install the core Agent software on a computer. It is a lightweight package that does not contain any of the plug-ins required for any of the Protection Modules. When you activate the Agent and turn on a Protection Module, Deep Security Manager retrieves the required plug-in from the software package in the Deep Security database and sends it out to the Agent to be installed on the computer. For information on installing Deep Security Agents, consult the Installation Guide.

Generate Deployment Scripts

Installing an Agent, activating it, and applying protection with a Security Policy is multi-step process that can be scripted from the command line on the computer you want to protect. The Deployment Script Generator tool will generate a customized script to be run on the computer which will download the Agent software from the Deep Security Manager, install and activate it, and then apply a Security Policy. For information on using the Deployment Script Generator, see **Deployment Scripts** in the Deep Security Manager Administrator's Guide or the online help.

Relay Groups

Deep Security Relays are part of the network that distributes Security and Software Updates from Trend Micro to your protected resources. You must have at least one functioning Deep Security Relay if you want keep your protection up to date. Relay functionality is included in all 64-bit Windows and Linux Deep Security 9.5 or later Agents.

Each Relay belongs to a Relay Group (even if it's just a group with a single member). Agents/Appliances are assigned to Relay Groups, not individual Relays. This provides some redundancy in case a single Relay within a group goes offline. There is a group called "Default Relay Group" to which all new Relays are assigned by default. You can have multiple Relay Groups, and the Relays Groups can be arranged in a hierarchy so a single top level Group gets its updates from the Trend Micro Update Server and then passes them down through a hierarchy of sub-Groups.

> Note: *A Relay can obtain security updates from another Relay Group, but not from another Relay (even if they are both part of the same Relay Group). A Relay must obtain updates from another Relay Group further up the hierarchy or another configured security update source. For more information on configuring security updates, see* **Security Updates** in the Deep Security Manager Administrator's Guide or the online help*.*

For information on enabling Relay functionality in an Agent, see **Relay Groups** in the Deep Security Manager Administrator's Guide or the online help in the User's Guide.

From the **Relay Groups** page, you can:

- Create a **New** ( ) Relay Group
- **Delete** ( ) a Relay Group
- View the **Properties** ( ) of a Relay Group

Relay Group Properties

General

General Information: The name and description of the Relay Group.

Security Updates: Select the source from which this Relay Group will download and distribute Security Updates. The Default Relay Group will always use the primary update source defined in the **Administration > Updates > Relay Groups**. However, any additional Relays Groups you create can use either the primary update source or another one that you have configured.

Proxies: Specify the proxy server that must be used to access the Primary Security Update Source. The Primary Security Update Source is usually Trend Micro Update Server, and is configured on the **Administration > System Settings > Updates** tab. The proxy will be used by the Relays in this Group if this Relay Group is configured to use the Primary Security Update Source. If this Relay Group is configured to get its Security Updates from another Relay Group, the proxy will only be used if connectivity with the other Relay Group is lost and this Group from must fall back to the Primary Security Update Source.

Members: Relays that are members of the group

Assigned To

The **Assigned To** tab shows the computers that are using this Relay as the source of the Security and Software Updates.

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM97216/150921b