



9.6 Deep Security

Service Pack 1

Best Practice Guide



Cloud & Data Center



Complete End User



Cyber Threats

About this guide

Deep Security provides a single platform for server security to protect physical, virtual, and cloud servers as well as hypervisors and virtual desktops. Tightly integrated modules easily expand to offer in-depth defenses, including anti-malware, web reputation, intrusion prevention, firewall, integrity monitoring, and log inspection. It is available in agentless and agent-based options that can all be managed through a single console across physical, virtual, and cloud server deployments.

This guide is intended to help users to get the best productivity out of the product. It contains a collection of best practices that are based on knowledge gathered from previous enterprise deployments, lab validations, and lessons learned in the field.

Examples and considerations in this document serve only as a guide and not a representation of strict design requirements. These guidelines do not apply in every environment but will help guide you through the decisions that you need in configuring Deep Security for optimum performance.

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 file and the latest version of the applicable user documentation.

This Best Practice Guide contains:

- Deployment considerations and recommendations
- Guidance in sizing server and storage resources for Deep Security implementation
- Upgrade guidelines and scenarios
- Recommended configuration to maximize system performance and reduce administrative overhead
- Best practice tips for VDI, private and public cloud environments

Acknowledgements

This guide was made by the following individuals who volunteered their time and expertise to this project:

Marlon Beriña, Aldrin Ceriola, Saif Chaudhry, Jennifer Chua, Jason Dablow, Erwin Dusojan, Mohamed Inshaff, Jill Maceda, Marion Mora, Robert See, Hugo Strydom, Anthony Pan, Cunlin Yu, Simon Zhang, Charles Deng, and Andy Dai.

We would also like to thank the following people for their significant support and contribution during development and review:

Mahmood Azmat, Cenen Enalbes, Evgeny Faddeenkov, Fernando Fontana, Mason Lee, Will C Lin, Robert Littlefield, Hao Liu, Jason Liu, Dave Lu, Ryan Mao, Dietmar Metzler, Rodel Villarez, Jay Yaneza, Robert Ynares, Alwin Yu, Keanu Beltran, Patty Macapinlac, Justin Foster, Nick Willan, Jeffery Mei, and Khalil Jiwa.

Document version: 1.2

Release date: Apr 12, 2017

Table of Contents

1	Environment.....	7
1.1	OPERATING SYSTEMS AND DATABASE SYSTEM.....	7
1.2	VMWARE VSPHERE AND VSHIELD COMPATIBILITY WITH DEEP SECURITY	7
1.3	VMWARE TOOLS AND VSHIELD ENDPOINT DRIVERS (FOR AGENTLESS ANTI-MALWARE)	7
1.4	ENVIRONMENTAL RECOMMENDATIONS FOR TCM INTEGRATION	8
2	Sizing Considerations	9
2.1	DEEP SECURITY MANAGER.....	9
2.2	DATABASE	9
2.3	DEEP SECURITY VIRTUAL APPLIANCE.....	10
2.4	DEEP SECURITY RELAY	10
3	Installation and Deployment.....	12
3.1	DEEP SECURITY COMPONENTS.....	12
3.1.1	<i>Deep Security Manager.....</i>	<i>12</i>
3.1.2	<i>Deep Security Agent/Relay.....</i>	<i>14</i>
3.1.3	<i>Deep Security Virtual Appliance.....</i>	<i>17</i>
3.1.4	<i>Database.....</i>	<i>20</i>
3.2	VMWARE COMPONENTS	21
3.3	DEPLOYMENT SCENARIO SAMPLES	24
3.4	TESTING DEEP SECURITY.....	25
4	Upgrade and Migration	26
4.1	GENERAL UPGRADE RECOMMENDATIONS:	26
5	Configuration	27
5.1	UI CONFIGURATIONS.....	27
5.1.1	<i>Dashboard</i>	<i>27</i>
5.1.2	<i>Alerts</i>	<i>27</i>
5.1.3	<i>Policies.....</i>	<i>27</i>
5.2	MODULE CONFIGURATIONS.....	29
5.2.1	<i>Anti-Malware.....</i>	<i>29</i>
5.2.2	<i>Web Reputation.....</i>	<i>37</i>
5.2.3	<i>Firewall.....</i>	<i>37</i>
5.2.4	<i>Intrusion Prevention.....</i>	<i>41</i>
5.2.5	<i>Integrity Monitoring.....</i>	<i>43</i>
5.2.6	<i>Log Inspection.....</i>	<i>45</i>
5.3	ADMINISTRATION AND SYSTEM SETTINGS	46
5.3.1	<i>Recommendation Scan</i>	<i>46</i>
5.3.2	<i>System Settings.....</i>	<i>47</i>
6	Performance Tuning and Optimization	51
6.1	DEEP SECURITY MANAGER.....	51
6.1.1	<i>Configure Deep Security Manager's Maximum Memory Usage.....</i>	<i>51</i>
6.1.2	<i>Configure Multiple Managers.....</i>	<i>51</i>
6.1.3	<i>Performance Profiles.....</i>	<i>52</i>
6.2	DATABASE	55
6.2.1	<i>Exclude Database files from Anti-Malware scans.....</i>	<i>55</i>
6.2.2	<i>Auto-growth and Database Maintenance</i>	<i>55</i>
6.2.3	<i>Database Indexing.....</i>	<i>55</i>
6.3	NSX.....	55
6.3.1	<i>NSX Firewall.....</i>	<i>55</i>

6.3.2	<i>NSX Security Policy</i>	56
7	Disaster and Recovery	57
7.1	HIGH AVAILABILITY	57
7.2	REMOVING A VIRTUAL MACHINE FROM DEEP SECURITY PROTECTION IN A DISASTER	57
7.3	RECOVERING A PHYSICAL MACHINE (WITH DSA) IN A DISASTER	58
7.4	RECOVERING AN INACCESSIBLE DSWA	59
7.5	ISOLATING A DEEP SECURITY ISSUE	59
8	Other Deployment Scenarios	62
8.1	MULTI-TENANT ENVIRONMENT	62
8.2	ENVIRONMENTS USING TEAMED NICs	63
8.3	AIR-GAPPED ENVIRONMENTS	63
8.4	SOLARIS ZONES	64
8.5	MICROSOFT CLUSTER SERVERS	64
8.6	MICROSOFT HYPER-V	64
8.7	VIRTUALIZED ENVIRONMENTS (VDI)	65
8.8	PRIVATE, PUBLIC & HYBRID CLOUD ENVIRONMENTS	67
8.9	VMWARE SRM (SITE RECOVERY MANAGEMENT) ENVIRONMENT	68
8.10	SAP	69
8.11	IBM RATIONAL CLEARCASE	70
8.12	AM EXCLUSION FOR VEEAM	70

1 Environment

Deep Security 9.6 SP1 consists of several components working together to provide protection. The information provided in this section will help you determine the compatibility and recommended software for:

- a) Operating Systems
- b) Database Systems
- c) VMware vSphere and vShield Compatibility
- d) VMware Tools and vShield Endpoint Driver

1.1 Operating Systems and Database System

Please refer to IG:

http://docs.trendmicro.com/all/ent/ds/v9.6_sp1/en-us/Deep_Security_96_SP1_Install_Guide_basic_EN.pdf

1.2 VMware vSphere and vShield Compatibility with Deep Security

VMware and Deep Security compatibility charts change often, especially as new versions of vSphere are released.

To get up-to-date information for the latest compatibility chart, refer to

<http://esupport.trendmicro.com/solution/en-US/1060499.aspx>

1.3 VMware tools and vShield Endpoint Drivers (for Agentless Anti-Malware)

The agentless anti-malware operations provided by Deep Security require the vShield Endpoint Driver to be installed on the virtual machines to be protected.

VMware includes the VMware vShield Endpoint Driver in VMware Tools 5.x, but the installation program does not install it on guest VMs by default. To install it on a guest VM, review the installation options in the table below:

Available VMware Tools Installation Options		
Installation Option	vShield Endpoint	Action
Typical	vShield Endpoint does NOT install	DO NOT select this option
Complete	vShield Endpoint installs	Select if you want all features
Custom	You must explicitly install vShield Endpoint	Expand VMware Device Drivers > VMCI Driver
		Select vShield Drivers and choose "This feature will be installed on local drive".

Note:

The vShield Endpoint Driver bundled with VMware Tools is now called **Guest Introspection** upon upgrading vSphere to version 5.5 Update 2. However, Guest Introspection service is used for NSX 6.1. If you are using NSX 6.0 and below, the name of this service is VMware Endpoint.

<https://www.vmware.com/support/vsphere5/doc/vsphere-esxi-55u2-release-notes.html>

Network Copy Performance Issue with vShield Endpoint

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2034490

The vShield Endpoint Driver that came with ESXi 5.0 Patch 4 causes an issue where files copied over the network was slow. VMware released a fix, which is bundled into the VMware Tools that came with ESXi 5.0 U2.

http://www.vmware.com/support/vsphere5/doc/vsp_esxi50_u2_rel_notes.html

The fix for this issue in 5.0 U2 was not carried over to 5.1. Users getting this problem on a 5.1 environment must apply 5.1 U1.

<http://www.vmware.com/support/vsphere5/doc/vsphere-esxi-51u1-release-notes.html>

1.4 Environmental recommendations for TMCM integration

Control Manager (TMCM) drill down feature on historical diagram has improper behavior but this issue has been fixed in TMCM 6.0 SP1. We recommend using TMCM 6.0 SP1 or higher versions.

2 Sizing Considerations

Sizing recommendations rely greatly on the type of environment and other various factors such as network, hardware, software, applications, etc. These estimates were based on experience and previous enterprise deployments.

The recommendations below may not accurately reflect the required settings for every configuration, but they provide a guideline to determine the best environment for running Deep Security.

They have been classified into **Small** (1 to 10,000), **Medium** (10,000 to 20,000), and **Large** (20,000 and above) deployments.

2.1 Deep Security Manager

Deep Security Manager				
Number of Agents	# of CPUs	System RAM	Memory allocated to DSM JVM process	# of DSM nodes
1 - 10,000	2	8-12 GB	4-8 GB	1-2
10,000 - 20,000	4	16 GB	12 GB	2
20,000 - above	4	24 GB	16 GB	2-3

*To change the default allocated memory for the DSM JVM process, refer to [Maximum Memory Usage](#).

Note: We always recommend deploying two (2) DSM nodes instead of three (3) when there are more than 10,000 agents.

However, sometimes if there is a special demand, for example, frequent/time-boxed recommendation scan (which is DSM CPU intensive), three (3) nodes will be suggested.

2.2 Database

Database	
Number of Agents	HDD Size
1 - 10,000	10-20 GB
10,000 - 20,000	20-30 GB
20,000 - above	30-40 GB

The table above

determines the initial database size to set for the Deep Security database. These estimates are provided based on the following assumptions:

- Log Inspection and Web Reputation Service (WRS) are disabled.
- Intrusion Prevention is enabled properly with very few false positive events.
- Anti-Malware (AM) events are insignificant in terms of size and are not part of the calculation.
- Anti-Malware only logs events occasionally, unless there is an outbreak in place.

- Log Retention Period is 30 days.
- Firewall events are 50 per day.

Notes:

1. Other factors, such as the modules in use, number of security updates held, the number of policies, etc, will affect the database size. In general, centrally collected Firewall and Intrusion Prevention event logs form the bulk of the database volume.

Event retention (**DSM > Administration > System Settings > Storage**), is relevant to maintain a reasonable sized database. Make sure to review these settings as this will help determine how much space is needed.

- One (1) Firewall event log entry takes up roughly 250 bytes.
- One (1) Intrusion Prevention event log entry takes up roughly 300-1024 bytes depending on the rule type.

2. For environments where a significant amount of Firewall events are anticipated, consider disabling “Out of allowed policy” events. This can be done on each agent or on the policy (**DSM > Policy > Firewall > Advanced**).
3. Environments with large retention requirements should rely on SIEM or Syslog server for log storage. If logs are stored in SIEM or Syslog, fewer data would be stored in the Deep Security database, and thus requires lesser space.
4. Imported software in the Deep Security Manager also plays a big part in terms of space usage. Always review the number of software versions you plan to keep in the database and remove unnecessary versions.

2.3 Deep Security Virtual Appliance

The sizing recommendation chart below shows how much memory and CPU the Deep Security Virtual Appliance (DSVA) requires to manage (x) number of guests (protected virtual machines per ESXi Host). Recommendations assume full-policy use, running the firewall, intrusion prevention, anti-malware, integrity monitoring, and web reputation service modules.

Deep Security Virtual Appliance		
Number of Protected Virtual Machines*	vCPU	RAM
1 - 25	2	6 GB
26-50	2	8 GB
51 - 100	2	10 GB
101 - 150	4	12 GB
151 - 200	4	16 GB
201 - 250	6	20 GB
251-300	5	24 GB

Note: Recommendations for 251-300 virtual machines assumes that the integrity monitoring module is not used.

2.4 Deep Security Relay

Deep Security Relay	
Number of Agents	# of Relays
1 - 10,000	1-2
10,000 - 20,000	2-3
20,000 - above	3-4

In determining the number of Deep Security Relays required for an environment, review the expected number of download connections from Deep Security Agents (DSA) and Deep Security Virtual Appliances (DSVA).

Establish how much of the DSA and the DSVAs need to be updated within an expected time frame (e.g. 50 agents need to get the updates in an hour).

Notes:

1. The Deep Security Relay (DSR) throughput is dependent on the size of the packages downloaded by the DSA/DSVA. For example, the download package size for the initial activation of an agent may be between 50 - 100 MB, but the typical updates after initial activation will be less than this (e.g. 1 – 10 MB).
2. The main load a DSR would expect to serve is during the initial activation. Thus, it is strongly recommended to do rollouts by phase. Stage the deployment and gradually add endpoints to the system.
3. To rollout an update to an endpoint as fast as possible, more relay servers are required. Increasing the number of relays means that the updates get pushed out faster to the endpoints.

Example:

- To rollout a 10 MB update to 20,000 endpoints within 30 minutes, deploy four (4) Deep Security Relays.
- To rollout a 10 MB update to 20,000 endpoints within 1-2 hours, two (2) Deep Security Relays are sufficient.

3 Installation and Deployment

Deep Security is composed of several components that need to communicate with each other. When deploying in a highly segmented network environment, knowledge about the various ports it uses will be useful for preventing unintended functionality disruptions. Make sure to note all ports that are required are open and, not reserved for other purposes.

Refer to the article below for a list of ports required in Deep Security:

<http://esupport.trendmicro.com/solution/en-us/1060007.aspx>

3.1 Deep Security Components



3.1.1 Deep Security Manager

A. Deployment Considerations

1. Use the Fully Qualified Domain Name.

Define DSM to use its fully qualified domain name, which is resolvable by all other components.

If this was not defined correctly during the install, this can be modified under **DSM > Administration > System Information**.

The manager address/name specified in the "Network Map with Activity Graph" screen will be the one used by the other components to contact DSM.

2. Deploy at least one (1) secondary DSM node.

This is always recommended to be deployed for redundancy. See [Configure Multi-Node Managers](#).

Multi-node deployment is not meant to address geographic dispersion. Therefore, DSM nodes and database must be in the same network segment (i.e. NO DSM1/DB in London with DSM2 in Paris connected via WAN).

B. Other Recommendations

1. Maximum Memory for the DSM installer

The installer is configured to use 1 GB of contiguous memory by default. If the installer fails and you receive a "*java.lang.OutOfMemoryError*" error during installation, you may need to configure the installer to use less memory.

2. Load Balancer Support

Deep Security Manager can now specify hostname and port that supersede the defaults in order to put a load balancer in front of:

- The manager user interface port (4119)
- The manager heartbeat port (4120)
- The relay port (4122)

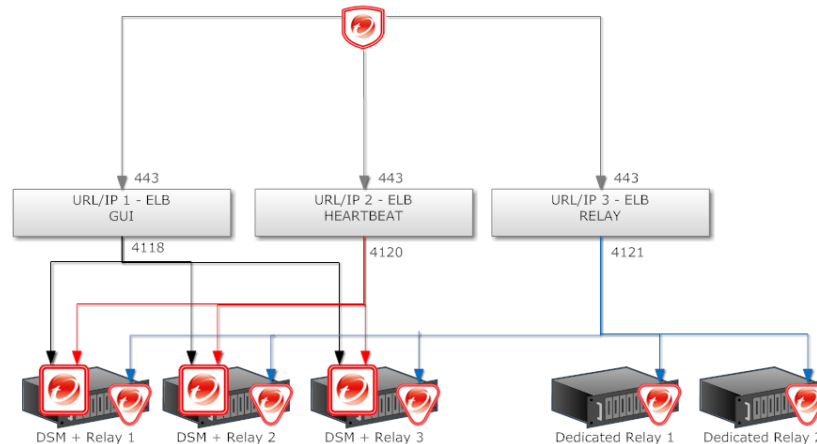
To configure the load balancers, go to **DSM > Administration > System Settings > Advanced > Load Balancers**.

This setup is recommended for Multi-Tenant (Service Provider) environments especially in the cloud.

Using a load balancer allows the following:

- Tunneling for 4119, 4120, and 4122 traffic over 443 (three load balancers with three addresses).
- Ability to add and remove DSM nodes on demand, without generating update traffic going to each DSA and DSVA in the environment.

Load balancers can be configured to use different ports for different traffic. If the load balancer supports port re-direction, it can be used to expose all of the required protocols over port 443 (using three (3) load balancers).



In all cases, the load balancers should be configured as TCP load balancers (not SSL Terminating). This ensures a given communication exchange will occur directly between Agent/Virtual Appliance and the Manager from start to finish. The next connection may balance to a different node.

On environments with a fixed number of DSM nodes, there is no need to use a load balancer in front of DSM.

For high availability and scalability, the Deep Security Manager by default, provides the URL address of all nodes to all agents and virtual appliances. The agents and virtual appliances use the list to randomly select a Manager node and continue to try the rest of the list until a node can be reached. If it cannot reach any nodes, it will wait until the next heartbeat and try again.



3.1.2 Deep Security Agent/Relay

A. Deployment Considerations

1. DNS Resolution

Ensure that each computer can resolve the fully qualified domain name of the Deep Security Manager for a successful deployment.

2. Time Synchronization

The clock on a Deep Security Agent/Relay (DSA/DSR) machine must be synchronized with Deep Security Manager (DSM) within a period of 24 hours.

3. Take time to decide on the best deployment method to use for your environment.

The Deep Security Agent can be deployed using various methods, including but not limited to:

- Manual deployment
- Group Policy (msiexec in Silent Mode)
- Enterprise Deployment Software (i.e. SCCM)
- Bundled in Templates
- Custom Scripts

The type of agent deployment mechanism used will help prepare you for future DSA/DSR upgrades.

Sample Scenarios:

- If GPO or Enterprise Deployment Software is used, it will be easier to perform an agent upgrade as the update package can just be pushed via the same method.
- If the agent is bundled with virtual machine templates, then you will need to remember to update the templates as part of the overall agent upgrade process.

Deployment via DSM is not an available option; however, pushing software updates/upgrades through DSM is possible. If you plan on performing upgrades via DSM, the overhead of pushing all of these upgrade packages via network should be taken into consideration.

4. Installation via Remote Desktop

Installing the Deep Security Relay/Agent over Windows Remote Desktop is NOT recommended because of the temporary loss of connectivity during the installation process. Using the following command line switch when starting Remote Desktop will allow the installation program to continue on the server after the connection is lost:

mstsc.exe /admin (mstsc.exe /console - for earlier Windows versions)

5. Other Anti-Malware software on the same machine

Only one (1) Anti-malware or one (1) firewall application is allowed in a machine. Make sure to remove other Anti-malware or firewall application.

6. OfficeScan Client and Deep Security

If the client machine where DSA/DSR will be installed on has a previous OfficeScan client, make sure that the drivers (tmactmon, tmevtmgr, and tmcomm) are fully uninstalled prior to installation. DSA and

OfficeScan client use the same name for drivers, however, DSA cannot use OfficeScan client's drivers and vice versa.

7. Combined Mode Protection

There is a Combined Mode feature in Deep Security 9.6 that allows the Deep Security Virtual Appliance (DSVA) and Deep Security Agent (DSA) to work together in providing security.

In Combined Mode, the features are distributed such that some protection is supplied by DSA and other protection is given by DSVA. There is no concept of redundancy or standby, so if either of these agents fails, then the corresponding protection/feature is lost.

Consider using coordinated protection (DSA + Agentless). When virtual machines are protected by the coordinated approach, if the agent goes offline, protection from the appliance is automatically activated.

When a VM is protected by both DSVA and DSA in Combined Mode, the user is unable to deactivate DSVA protection from the Deep Security Manager (DSM) User Interface (UI) console.

Trend Micro provides a workaround to disable agentless protection and keep only agent protection for a VM with Combined Mode protection. Refer to the following KB link:

<http://esupport.trendmicro.com/solution/en-US/1112971.aspx>

8. Check the FQDN of the machine before and after DSA installation

A brief network interruption occurs during the agent installation process. Sometimes, this can affect DHCP auto registration. It is recommended to verify the computer's FQDN (`ping -a <ip or server name>`) before and after the install. Should an issue with auto registration be encountered, use `ipconfig /registerdns` or reboot the computer.

9. Using DSA with iptables (on Linux agents) or Windows Firewall

To avoid conflict, the DSA installation will disable iptables (Linux) or Windows Firewall (Windows) by default. In situations where the DSA firewall feature is NOT used, refer to the steps below to prevent the installer from disabling iptables or from making any changes to the native Windows Firewall.

For Windows:

Refer to the following article for details on how to modify the DSA MSI package to prevent it from changing the Windows Firewall:

<http://esupport.trendmicro.com/solution/en-us/1055458.aspx>

For Linux:

In order to leave iptables untouched by the DSA, the user must create or touch an empty file with the following path:

`/etc/use_dsa_with_iptables`

If that file is present then the DSA scripts will not disable iptables.

```
# touch /etc/use_dsa_with_iptables
# service iptables restart
# service ip6tables restart
```

10. Install multiple Deep Security Relays

At least one (1) Deep Security Relay is required for a Deep Security environment. Trend Micro recommends installing multiple Relays to achieve redundancy and optimize the bandwidth usage.

11. Relay Groups

Set up relay groups for redundancy. If a Relay Group has multiple Relay members, each Relay acts as a backup for the others. If you have multiple sites in geographic region or office, it is recommended to setup Relay Groups for each site.

12. Deep Security Relay communication direction

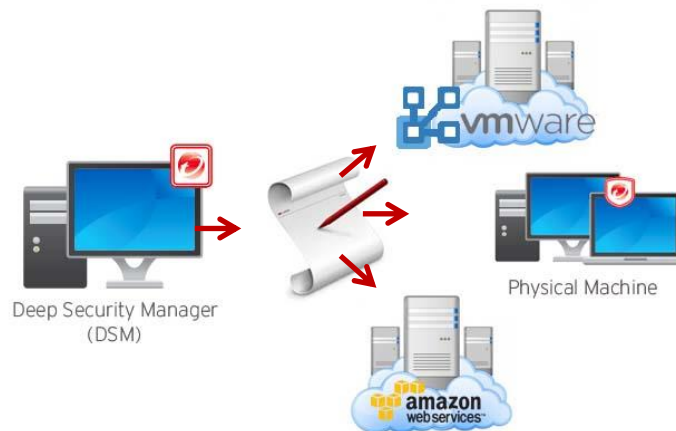
The communication direction for DSR must be set to bidirectional. Otherwise, the rule update may fail to apply.

13. Install with installer, not package

When installing DSA, send only the installer (msi, rpm) file to the destination machine. The plug-ins can be deployed to DSA based on policy.

B. Agent Deployment Scripts

Deep Security Manager's deployment script generator can be used to generate scripts that can be run on computers where the agent will be installed. The script can be modified to optionally perform subsequent tasks like activation and policy assignment.



Consider using deployment scripts in these scenarios:

- Environments where there is a need to deploy and activate multiple agents.
- Automate the activation process and deployment of policies.
- Activate and deploy to clients in environments where the server cannot communicate/discover clients directly but clients can reach the server without problem.
- In Amazon Elastic Compute Cloud (Amazon EC2) environments, it can be bundled with the endpoint and used while instances are being auto scaled.

Notes:

1. Deployment Scripts support basic function only. It cannot fulfill all the needs for all environments so customers should adjust the scripts for their specific need.

Some environments might experience a delay in starting the ds_agent service. If the dsa_control activation signal is sent before the ds_agent service is started, this might prevent the activation from working successfully. Extend the sleep time in the scripts to prevent this.

Example:

In AWS testing, concurrent launching of 100 instances had better results when the sleep time is set to more than 60 seconds. This highly depends on AWS' system loading. Disk I/O, CPU loading, network bandwidth, and database configuration.

2. In Amazon Web Services (AWS EC2) environments, the new instances must be able to access the

URLs specified in the generated deployment script. This means that DSM must be either internet facing, connected to AWS via VPN/Direct Link, or deployed on Amazon Web Services as well.

3. The base tenant **MUST** import the agent packages before using deployment scripts (for both single and multi-tenant deployments).
4. Agent-Initiated Activation feature must be configured correctly in DSM, if scripts will be used to do activation tasks.

Allow Agent-Initiated Activation option must be enabled on the Administration > System Settings > Agents tab.

5. By default, port 4118 is not open on the security group (firewall) of AWS. To activate from the DSM console, the DS agent must be able to communicate on port 4118 of AWS. To allow 4118 on the security group of AWS:
 - Open the AWS web console.
 - Go to **Network and Security**.
 - Select **Security Group**.
 - Under TCP Port (Service), check if 4118 is listed. If not, select "Create a rule" to add.
 To verify, you can telnet to the machine to verify communication on port 4118.

To automatically protect a new instance of Amazon Web Services (AWS), please refer to the following KB: <http://esupport.trendmicro.com/solution/en-US/1098564.aspx>



3.1.3 Deep Security Virtual Appliance

A. Deployment Considerations

1. DSVA Package

It is required to download the DSVA installer package into Deep Security Manager prior to the deployment of DSVA and addition of the vCenter server to DSM.

2. DNS Resolution

Ensure that the DSVA can resolve the FQDN of the Deep Security Manager and that the ESX server is able to connect to the DSM FQDN at port 4119. There will be issues in installing the driver and deploying DSVA if ESX cannot do so.

Ensure that the DSM and vShield Manager FQDN can be resolved by DSVA.

3. VMware Tools

There is no need to update the VMware Tools within the Deep Security Virtual Appliance. DSVA uses the device drivers that come with the version of tools it was built with. When a tool upgrade is implemented, DSVA may not start.

4. Change the default password

Default password for the deployed DSVA image is “dsva”. We recommend you to change this after the installation. To do so, press <F2> and select the option “**Configure Password**” on the console.

5. Do not vMotion DSVAs

Make sure that the DSVAs do not vMotion. For this reason, the recommended naming convention for the appliance is to use the name of the ESXi host (it is located on) pre-fixed or suffixed.

Example:

ESXi Hostname (Delta-12)

DSVA Hostname (Delta-12-DSVA)

Doing it this way allows you to easily identify which DSVA belongs to which ESXi host. The DSVA deployment wizard will set the “Automation Level” to “Disabled” in the DRS settings for the cluster. This means that the DRS will not vMotion the DSVA by default.

6. Doing a storage vMotion on the DSVA is also not recommended

When performing a storage vMotion operation on DSVA, network connectivity on the protected virtual machines will be interrupted. Security Appliances, such as the DSVA, are not intended to be vMotioned and are not supported by VMware.

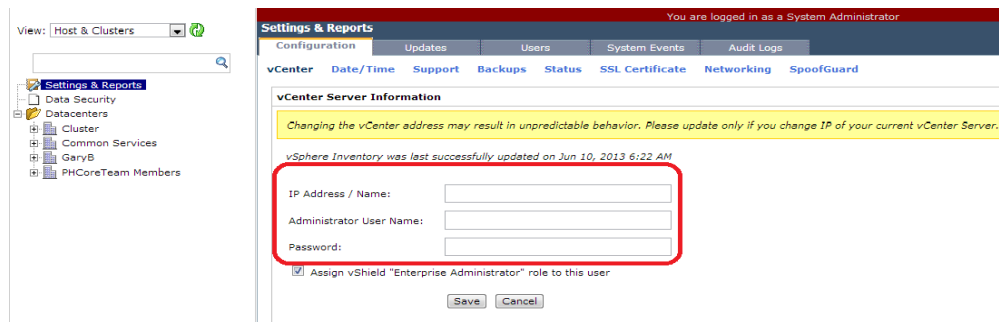
7. Make sure DSVAs are always on and the first to start up after maintenance

If maintenance is required on the ESXi host and DSVA needs to be shut down, ensure that it is the first VM to start running after the maintenance.

8. vCenter account in vShield Manager/NSX

Make sure vShield Manager has the correct vCenter settings, specifically the vCenter account.

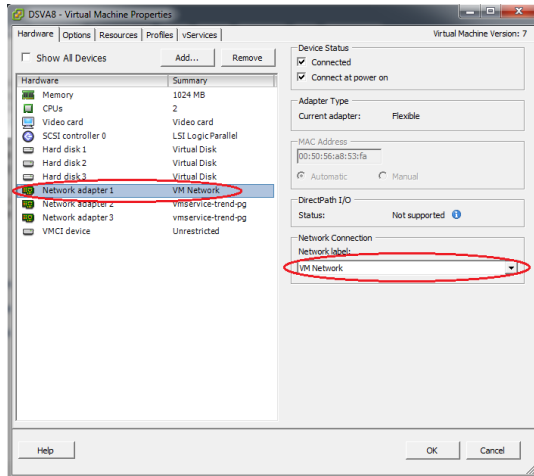
In the **vShield Manager console > Setting and Reports**:



9. Management Interface

Once DSVA is deployed, when configuring the network settings, make sure that its management interface has a connection to DSM.

On vCenter, right-click the DSVA image and select “**Edit Properties**”, then check the connection for the **Flexible Network Adapter** (Network adapter 1 by default):



10. Protected Virtual Machines

When creating VMs to be protected by DSVA, note the following considerations:

- VMware Tools 5.0 or later with the vShield driver installed.
*VMware vShield Manager and VMware vShield Endpoint Drivers are required if you want to implement Anti-Malware protection on your virtual machines.
- Virtual Disks Supported: LSI Logic parallel, LSI SAS, or VMware paravirtual SCSI driver (Buslogic is unsupported)

11. DSVA thick or thin provisioning mode

For production, we recommend to use thick provisioning mode while deploying DSVA to improve disk performance.

12. DSVA memory over assignment and reservation

We have the following KB to describe the memory assignment about DSVA:

<http://esupport.trendmicro.com/solution/en-US/1103564.aspx>

However, for performance enhancement, we have disabled the swap function of Linux kernel for DSVA. If DSVA's memory is really insufficient, as there's no swap partition or file for DSVA, Linux kernel will start to kill processes to recycle memory using OOM-Killer. This behavior may cause some unexpected result such as interrupted VM network.

To prevent the issue, we suggest to assign some more memory to DSVA, the suggestion will be the same as Windows virtual memory allocation (1.5 multiply), but you can set memory reservation to DSVA.

For example, you have more than 50 VMs but less than 100VMs per ESXi host, based on the KB above, you need to assign 4 GB memory to DSVA. To avoid the OOM-Killer, you can assign an additional 2 GB memory to DSVA and set memory reservation to 4 GB on the "Resources" tab of DSVA properties.

This setting means ESXi will only reserve 4 GB physical memory for DSVA. So if the ESXi host resource is enough, ESXi will allocate 6 GB physical memory to DSVA. But if your business needs more memory and ESXi lacks physical memory for your VMs, ESXi will reclaim 2 GB physical memory from DSVA to your VMs and provide page files as virtual memory for the DSVA instead.

For issues involving the Anti-Malware module, you may refer to the following articles:

<http://esupport.trendmicro.com/solution/en-US/1098103.aspx>

<http://esupport.trendmicro.com/solution/en-us/1060525.aspx>

B. Other Recommendations

Smart Protection Server

In agentless anti-malware environment, the actual scanning of the files takes place on the Deep Security Virtual Appliance, as there is no agent on the endpoint.

DSVA uses the conventional scanning method (recommended) that does not use Smart Protection Server. There is a feature called “Web Reputation” which is used by the DSVA. When someone tries to access a URL on the VM, the rating of that URL is checked by the DSVA first. It makes sure that the URL is not a malicious URL. To check the rating of the URL, DSVA has to send that query to the Smart Protection Server.

Smart Protection Network is globally available on the Internet courtesy of Trend Micro. By default, DSVA will use it. Please refer to KB <http://esupport.trendmicro.com/solution/en-US/1102863.aspx> to know the complete list of URLs which Deep Security needs to access. Ensure that those URLs are allowed on your company firewall/proxy.

To void Internet traffic going to the global servers, it is recommended to install a local standalone Smart Protection Server 3.0 or above.

3.1.4 Database

A. Deployment Considerations

1. Place the database on the same network as the Deep Security Manager.

The DSM must be co-located on the same network as its database, with the connection speed of 1 GB LAN or higher. Connections over WAN are discouraged.

DSM relies heavily on the database to function. Any increase in latency can have a serious negative impact on DSM performance and availability.

2. Dedicated Database Server

It is recommended to install the database server on a separate machine.

3. It is recommended to use Microsoft SQL Enterprise or Oracle.

A. Microsoft SQL Enterprise Server

- Create first the DSM database in SQL prior to DSM installation.
- Make sure that “Remote TCP connections” is enabled in your Database Server.
[http://msdn.microsoft.com/en-us/library/bb909712\(v=vs.90\).aspx](http://msdn.microsoft.com/en-us/library/bb909712(v=vs.90).aspx)
- The database account that will be used should have **db_owner** rights for the DSM database.
- The **dbcreator** server role is required if Multi-Tenancy is used.
- Set the database with Simple Recovery model.
<http://technet.microsoft.com/en-us/library/ms189272.aspx>

B. Oracle Database Server

- Ensure that the Oracle Listener service is started and accepts remote TCP connections on your Database Server.
- Create the ***'dsm'** database user.
*Any other user name may be used.
- Grant the **CONNECT**, **RESOURCE** roles and the **UNLIMITED TABLESPACE** system privilege to the user **'dsm'**.
- Assign the **CREATE SEQUENCE**, **CREATE TABLE** and **CREATE TRIGGER** system privileges to the user **'dsm'**.
- If you plan to use multi-tenancy, grant the **CREATE USER**, **DROP USER**, **ALTER USER**, **GRANT ANY PRIVILEGE** and **GRANT ANY ROLE** system privileges to the user **'dsm'**.

4. Use a TCP/IP connection to the database.

Connecting to the database via TCP/IP channel is recommended.

In situations where the use of named pipes is required to connect to the SQL Server, a properly authenticated Microsoft Windows communication channel must be available between Deep Security Manager's host and the SQL Server host.

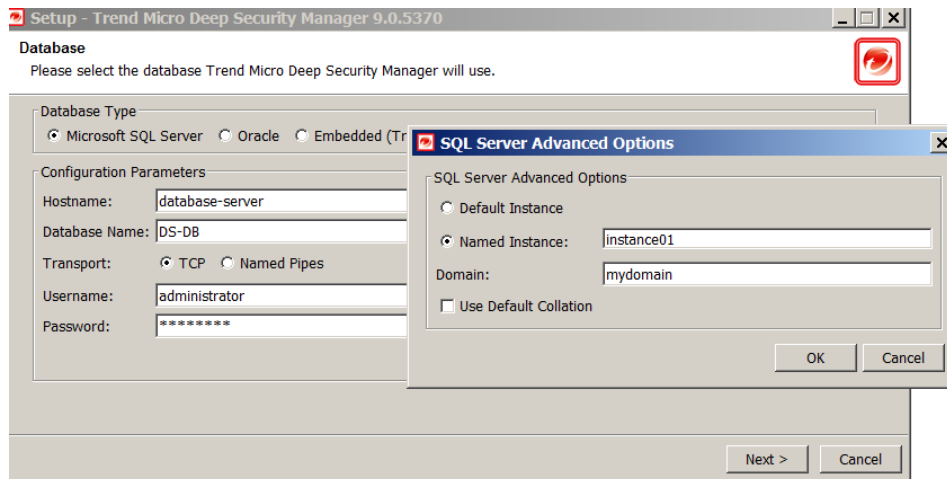
This may already exist if:

- The SQL Server is on the same machine as Deep Security Manager
- Both servers are members of the same domain
- A trust relationship exists between the two servers

If no such communication channel is available, Deep Security Manager will fail to communicate with the SQL Server over named pipes.

5. Ensure correct connection settings are used during installation.

During installation, the DSM installer would ask you for database connection details. Make sure to properly enter the database hostname under "Hostname" and the pre-created database for Deep Security under "Database Name".



The installation supports both SQL and Windows Authentication. When using Windows Authentication, click the "Advanced" button to display additional options. The screenshot above shows an example for connecting to a named SQL instance using Windows Authentication.

6. Avoid using special characters for the database user (Oracle).

Although Oracle allows special characters when configuring the database user object, if they are surrounded by quotes. Deep Security does not support special characters for the database user.

7. Keep the database name short (Microsoft SQL).

If Multi-tenancy is planned for the environment, keeping the main database name short will make it easier to read the database names of your tenants. For example, if the main database is "MAINDB", the first tenant's database name will be "MAINDB_1", the second tenant's database name will be "MAINDB_2", and so on.

8. Database account expiry

In some customers' environments, for security reasons, the account/password of database has expiration settings. In this case, customer can follow the published KB below to change the account/password of database for Deep Security Manager: <http://esupport.trendmicro.com/solution/en-US/1095714.aspx>

3.2 VMware Components



VMware ESXi Server



VMware vCenter

VMware vShield
Manager

A. Deployment Considerations

1. Ensure the latest security patches are applied to vCenter, ESXi, and vShield/NSX Manager.

For version compatibility details, refer to:

<http://esupport.trendmicro.com/solution/en-US/1060499.aspx>

2. Ensure all VMware components are tied to an NTP server.

It is recommended to use the same NTP server for the entire environment, and ensure they are all synchronized.

3. Use vShield 5.1 and above to take advantage of the new features of Deep Security 9.6.

Features such as Agentless Recommendation Scan, Scan Cache, and Hypervisor Integrity Monitoring require at least vShield 5.1.

4. Deploying vShield Manager/NSX

The OVA package for the vShield Manager Appliance can be downloaded from the VMware's web site. It is located under "vCloud Networking and Security" section of the web site. This appliance can be deployed on any vCenter. It does NOT have to be on the vCenter that it will be connecting to. You will need one vShield Manager to connect to each vCenter.

5. vCenter and vShield Manager/NSX Passwords

Login credentials with access to vCenter and vShield Manager are required when connecting the components to Deep Security. Always remember to update the connection details in Deep Security each time the password for these accounts change to avoid synchronization issues.

This can be done via DSM > Computers > right-click on vCenter > Properties.

For more details on the permissions, refer to:

<http://esupport.trendmicro.com/solution/en-US/1098184.aspx>

6. Deploying the vShield driver on VMs

A. For VDI environments:

- Enable the driver in the gold image.

B. For mass deployments:

- Run the command below from a command prompt to automatically install the Endpoint Driver without user intervention:

```
setup.exe /S /v "/qn REBOOT=R ADDLOCAL=ALL REMOVE=Hgfs"/v "/qn  
ADDLOCAL=VMCI,VShield REMOVE=Hgfs"
```

C. For environments where VMs are already up and running and could not be reconfigured and recomposed:

- Login to vCenter using vSphere client
- In the **Inventory > Hosts and Clusters** view, select the host, cluster, or datacenter and click the Virtual Machines tab.

- Control-click or Shift-click to select the virtual machines.
- Right-click the selected virtual machines and click **Guest > Install/Upgrade VMware Tools**.
- Choose “**Automatic tools upgrade**” option and enter the listed MSI arguments below in the text field box. This will specify which VMware Tools components to include/exclude.

/S /v "/qn ADDLOCAL=VMCI,VShield REMOVE=Hgfs"

More details about the MSI parameters can be found here:

<http://pubs.vmware.com/vsphere-50/index.jsp?topic=/com.vmware.vmttools.install.doc/GUID-CD6ED7DD-E2E2-48BC-A6B0-E0BB81E05FA3.html>

- Verify on random VMs to ensure the driver is running using “*sc query vsepflt*” in the command prompt.

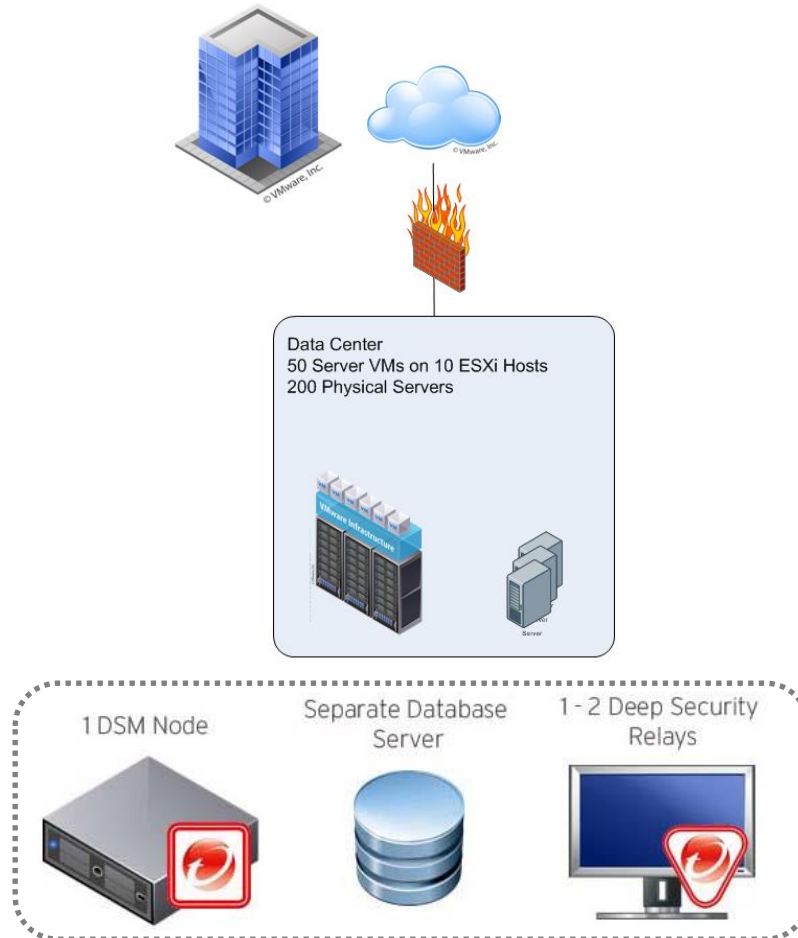
7. Multiple vCenters

Deep Security supports multiple vCenter servers. Virtual Machine UUIDs must be unique across all vCenter instances. For example, adding a VM to the inventory on multiple vCenter servers can result in duplicate UUID issues.

When using “Linked Mode” each linked vCenter server must be added individually to DSM.

3.3 Deployment Scenario Samples

A. Standard Small Scale Deployment

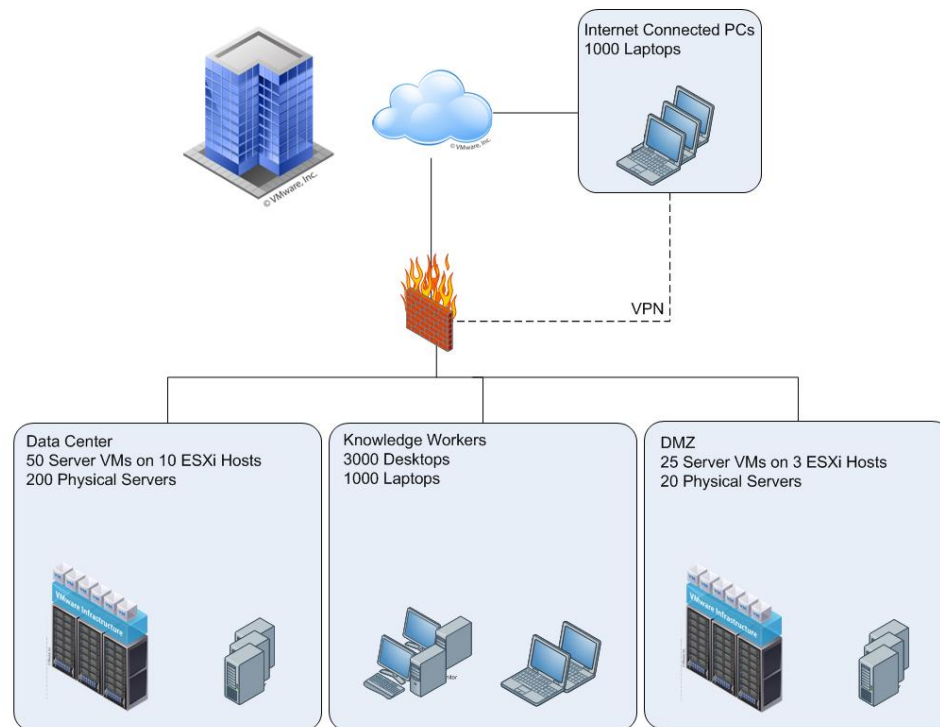


This small standard deployment only requires a single DSM infrastructure.

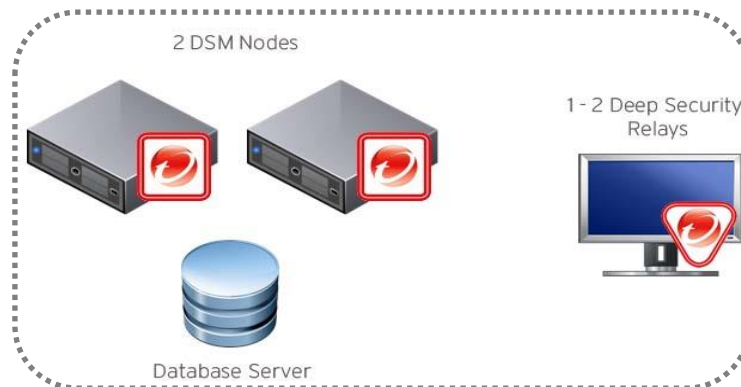
- Database installed on a separate machine.
- Both DSM and database should be located in the same datacenter.
- One to two Relays for updates.
- Use 10-minute heartbeat for all systems.

Refer to the [heartbeat](#) section for additional details on heartbeat.

B. Medium Scale Deployment with VPN users



Scenario: Remote systems connect to VPN regularly



Two (2) DSM nodes are recommended for redundancy.

- DSM and DB both located in the datacenter
- Bi-directional communication is used
- One to two Relays for updates
- 10-minute heartbeat for servers
- 60-minute heartbeat for desktops and internal laptops
- 10-minute heartbeat for remote laptops
(may vary; heartbeat frequency needs to be less than average VPN session frequency)

Refer to the [heartbeat](#) section for additional details on heartbeat and communication methods.

3.4 Testing Deep Security

Validate and test Deep Security features and functionality after deployment. You may refer to the following link for guidelines on testing each module of Deep Security. The link also provides the procedure for testing the integration with VMware, Active Directory, and SIEM tools, along with failover/high availability tests and scenarios:

4 Upgrade and Migration

4.1 General Upgrade Recommendations:

1. Before upgrading the Deep Security Manager, make a full backup of the Deep Security Manager database. In rare event when you have difficulty in upgrading, this will allow you to roll back by installing the previous manager (with a temp database) and re-pointing it at the restored database (in dsm.properties).
2. Perform the upgrade on a non-peak hour or low-peak hours.
3. For multi-node DSM:
 - a) Upgrade must be done on all DSM nodes.
 - b) Example: Upgrade DSM node 1, then node 2, and then node 3.
All nodes must run on the same version prior to upgrade.
 - c) If the database size is very big, it's recommended to manually upgrade the DSM database schema by following this KB:
<http://esupport.trendmicro.com/solution/en-us/1112218.aspx>
4. If a previous version of Deep Security Manager is installed on your system, choose between the "Upgrade the existing installation" and the "Overwrite the existing installation":
 - a) Upgrading the installation will upgrade the Deep Security Manager to the latest version but will not overwrite your policies, Intrusion Prevention Rules, Firewall Rules, Application Types, etc. or change any of the security settings being applied on the computers in your network.
 - b) Overwriting the existing installation erases all the data associated with the previous installation and then installs the latest filters, rules, policies, etc.
5. In a Multi-Tenants environment:
 - a) When the installer runs and detects an existing installation, it offers an upgrade option. If upgrade is selected, the installer first notifies other nodes to shut down and then begins the process of upgrading.
 - b) The primary tenant is upgraded first, followed by the tenants in parallel (five at a time). Once the installer finishes, the same installer package would be executed on the rest of the Manager nodes.
6. For environments with large databases, schema modification during an upgrade can take significant amount of time (8+ hours), so make sure to plan ahead.
7. DSM supports managing the components running 1 major version back (i.e. DSM 9.6 can manage DSA/DSVA 9.5), but DSM still can manage the latest 8.0 agents for Windows 2000 support.

Currently, upgrading directly from DSVA 9.0 to 9.6 is not supported. Customer needs to delete or power off the old virtual appliance and deploy the new one with version 9.5, then upgrade virtual agent to version 9.6 with RHEL 64-bit agent package.

5 Configuration

Because Deep Security is a modular solution that can be adapted to different environments, there is no right or wrong way to configure the product. Below are some common settings, exclusions, and other helpful configurations which appear in most Deep Security deployments. Always double-check with your company's policies before adapting these recommendations.

5.1 UI Configurations

5.1.1 Dashboard

We recommend that at least the following widgets are included and placed on the area best seen on the dashboard page:

- a. Alert Status – This keeps you informed on any critical items that may need immediate attention such as security updates and protection on computers getting offline.
- b. Computer Status – This gives you a good overview of agents' status.
- c. My Account Status – This shows information about the user currently logged in.
- d. Security Update Status – This shows information about out-of-date vs. up-to-date agents.

Create multiple dashboards and group them by usage (i.e. General, Anti-Malware Dashboard, Updates, etc.). This allows easier management of large scale environments. The tabbed view allows administrators to easily switch between them. Each dashboard has a different time and computer filter allowing for many different views into the system.

5.1.2 Alerts

By default, most alerts are enabled. In large environments, it might be beneficial to remove some alerts so only the ones requiring an action will be triggered. With all alerts enabled, a manager or less technical savvy person will get the idea that Deep Security isn't working properly. Alerts should be tweaked to give you the most relevant information so you can take action(s) on them accordingly. From the alerts page, user can select "Configure Alerts" link to enable or disable alerts.

5.1.3 Policies

Policies provide a logical way of replicating security settings to servers and desktops that share similar security requirements. We recommend that machines with similar settings, software installed, application, or function should be grouped strategically when assigning policies.

Note that the default policies built in with Deep Security are meant to be examples and should not be used without prior configuration.

a. Policies vs. Computer Level Rule and Configuration Assignment

The best practice is to assign most rules through Policies for ease of management.

Advantages for using Policies:

- User can change or test the policy settings before assigning it to the machines.
- It allows a quick removal of rules and configuration by simply taking out a machine from the policy or assigning it an entirely new one.
- Duplicate the policy and use it as a baseline setting for succeeding policies to be created.

When to use Computer Level rule assignment:

- When leveraging automatic assignment

- When there are many varying computers (i.e. each machine uses different applications, different OS updates, etc. making them virtually impossible to group)
 Note: When using a combination of both policy and computer level assignments, keep in mind that if you un-assign a policy from a computer, rules may still apply on the computer if they were assigned independently of the policy.

b. Policy Groupings

Below are some recommended machine groupings to effectively take advantage of policies:

- By Operating System
 (e.g. Windows 2008 Servers, Windows XP Machines, and Linux)
- By Server Function
 (e.g. Mail Servers, Web Servers, User Laptops, and Point of Sale Systems)
- By Application installed/version
 (e.g. OfficeScan Servers, Oracle 10 Database Servers, MS SQL 2005 Servers)

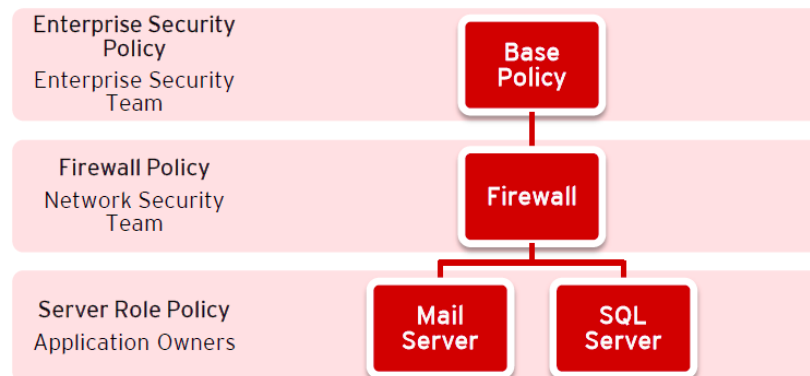
Properly grouping the machines is the key to an effective management of recommendation scans.

When a Recommendation Scan is performed on an individual member of a policy, the recommendations for that particular agent (DSA) will be seen on the policy as well.

Accepting or applying the recommendations at the policy level will apply the rules to all members of the policy. The advantage of this method is the ease of maintenance. The disadvantage, however, is the possibility of assigning rules to members that do not actually need them. This is the reason why it is recommended to group the machines accordingly if users don't want to see the vulnerability being triggered for machines that should not be affected.

Deep Security 9.6 supports multiple levels of policy inheritance. A newly-created policy can be configured to inherit all or some of its settings from a parent policy. It lets you create a tree structure of security policies. For example, you can create a parent policy called "Windows Server" and two child policies, "Windows Server 2008" and "Windows Server 2003", inherited from their parent policy. Each of those child policies can have child policies of their own for different editions of Windows Server.

Sample Policy grouping with policy inheritance:

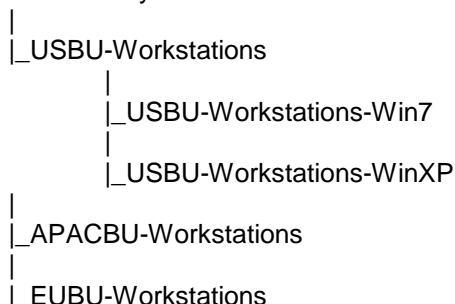


c. Policy Names

As a best practice, using a naming convention for policies can lessen the burden of managing multiple policies in an environment.

Example:

Workstation Base Policy



5.2 Module Configurations

5.2.1 Anti-Malware

a. Configuration

Policies > Common Objects > Other > Malware Scan Configuration > Scan Settings

Recommended Real-Time Scan Configuration	
General	Recommendation
Files to Scan	All Files
Directories to Scan	All directories
Actions	
Active Action	Disabled
Custom Actions:	Enabled
For Virus	Clean
For Trojans	Delete
For Packer	Quarantine
For Spyware	Quarantine
For Other Threats	Quarantine
Possible Malware upon Detection	Quarantine
Options	
Enable Spyware / Grayware Scan	Enabled
Scan Compressed Files	Enabled
Maximum size of individual extracted files	30
Maximum Levels	2
Maximum number of files to extract	10
Scan Embedded Microsoft Office Objects	Enabled
Scan for Exploit Code in Microsoft Office Objects	Enabled
OLE Layers to Scan	3
Enable IntelliTrap*	Disabled
Enable Network Directory Scan	Enabled**

Scan Files When	Read/Write
Alert when ...	Enabled

* IntelliTrap helps block real-time compressed executable files and pairing them with other malware characteristics. Since IntelliTrap identifies such files as security risks and may incorrectly block safe files, you may disable IntelliTrap if users regularly exchange real-time compressed executable files. (IntelliTrap only works in Real-Time mode.)

**Network scanning should be disabled to maintain maximum performance during Real-Time Scan. However, these network resources must be protected by a local AV scanner. Leave enabled if there is no other file scanner for these network shares.

Recommended Scheduled Scan Configuration	
Files to Scan	All Files
Directories to Scan	All directories
Actions	
Active Action	Disabled
Custom Actions	Enabled
For Virus	Clean
For Trojans	Delete
For Packer	Quarantine
For Spyware	Quarantine
For Cookie	Delete
For Other Threats	Quarantine
Possible Malware – Upon Detection	Quarantine
Options	
Enable Spyware / Grayware Scan	Enabled
Scan Compressed Files	Enabled
Maximum size of individual extracted files	60
Maximum Levels	3
Maximum number of files to extract	10
Scan Embedded Microsoft Office Objects	Enabled
Scan for Exploit Code in Microsoft Office Objects	Enabled
OLE Layers to Scan	3
CPU Usage	Medium
Alert when...	Enabled

Recommended Manual Scan Configuration	
Files to Scan	All Files
Directories to Scan	All directories
Actions	
Active Action	Disabled

Custom Actions	Enabled
For Virus	Clean
For Trojans	Delete
For Packer	Quarantine
For Spyware	Quarantine
For Cookie	Delete
For Other Threats	Quarantine
Possible Malware – Upon Detection	Quarantine
Options	
Enable Spyware / Grayware Scan	Enabled
Scan Compressed Files	Enabled
Maximum size of individual extracted files	60
Maximum Levels	2
Maximum number of files to extract	10
Scan Embedded Microsoft Office Objects	Enabled
Scan for Exploit Code in Microsoft Office Objects	Enabled
OLE Layers to Scan	3
CPU Usage	High
Alert when...	Enabled

Note:

In choosing actions to take when malware is detected, note that there is a corresponding secondary action that will be triggered when the initial action fails to execute.

Primary Action (configured on the console)	Secondary Action (hardcoded)
Quarantine	Pass
Clean	Quarantine
Delete	Clean
Deny	Quarantine

b. Scan Schedule Setting

In addition to scan configurations, there is also an option to set a schedule for Real-Time Scan. This can be useful when there is a specific timeframe wherein you would like to turn off real-time scanning to improve performance.

Example:

- File Server is scheduled to have a backup of all files every day at 2:00am - 4:00am.
- This server will most likely have high activity during this time and whitelisting the 2:00am -4:00am timeslot from Real-Time Scan activity would significantly help improve performance for both the backup task and server resource.

Note:

- Perform a full manual scan on a server before running the actual backup task.
- We recommend that weekly scheduled scans are performed on all protected machines.

c. Multi-threaded processing

Real-Time Scan uses multi-threaded scans by default. However, for on-demand and scheduled scans, this option needs to be configured depending on the environment.

Policy/Computer > Anti-Malware > Advanced > Resource Allocation for Malware Scans

Scan Limitation
☒ Default
Maximum file size to scan: MB

Resource Allocation for Malware scans
Use multithreaded processing for Malware scans (if available): Default (No)

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.

Enable the option for physical machines using the physical Deep Security Agent to improve the performance. Note that a restart of the machine is required for any change to take effect.

Below are the scenarios wherein this setting should NOT be enabled:

- It is NOT recommended to turn this option on for agentless environments.
- When multi-threading is not an option, since the machine resource is limited (i.e. common for CPU-bound tasks).
- When resource should be held by a single operator only at a time (i.e. common for IO-bound tasks).

d. Quick Scan vs. Full Scan

Deep Security 9.6 added the Quick Scan feature to improve agent-based (Windows only) scanning time. It enables scanning only those critical files most likely to be infected. This allows more frequent quick scans to be scheduled with lower impact and leaving full scans to be performed on a less frequent basis (e.g. weekly).

Full Scan:

- Runs a full system scan on all processes and files
- Utilizes the configuration set under Manual Scan (i.e. scans the files based on directories, extensions, files configured to be included in the scan)
- Can be run at scheduled times by creating a Scheduled Task, or manually (on-demand)
- Can be run on all platforms supporting Anti-Malware
- Takes longer to complete

Quick Scan:

- Fast high level scan of critical system areas for currently active threats
- 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.
- Only available for Windows Agent-based systems.
- No configurable settings and will not use any scan configuration (i.e. will not check settings like Directories to Scan or Files to Scan)
- Quick Scan is only available on-demand. You cannot schedule a Quick Scan as part of a scheduled task.

Malware scan

Last Manual Scan for Malware: 37 Minutes Ago
Last Scheduled Scan for Malware: N/A

e. Scan Cache

This feature is used by the Virtual Appliance to maximize the efficiency of Malware and Integrity Monitoring Scans of virtual machines. It enables de-duplication of scanning in Malware and Integrity Monitoring Scans, producing a performance increase on scan times for subsequent scans or similar VMs (e.g. VDI linked clones).

- Works best when VMs are linked clones (VDI is prime case)
- Designed to avoid scanning identical files twice
- Scan cache is stored in the DSVa memory
- When a VM is vMotioned to another host, the scan cache information is not moved with it to avoid conflicts with the target cache. The target DSVa's cache would apply to the newly migrated VM.

Recommendations:

To modify the scan cache configurations: Go to DSM > Administration > System Settings > Advanced > Scan Cache Configurations > View Scan Cache Configurations

- Anti-Malware Real-Time Scan Cache : 15 Minutes
 - Anti-Malware On-Demand Scan Cache: 1 Day
 - Integrity Monitoring Scan Cache: 1 Day
- Things to remember when changing the cache values:
- Shorter expiry periods on cache means it gets refreshed more frequently. Consider setting it to a lower value if you want to increase security.
 - Create dedicated Scan Cache policies for VMs that you want to keep separate and have their own Scan Cache. This might be appropriate if you have different departments sharing the same infrastructure.
 - If you have a very large number of VMs per host (e.g. VDI environment), monitor the disk I/O and CPU usage during scanning. If scanning takes too long, consider increasing the size of the cache or adjusting the Scan Cache Settings to achieve the required performance.
 - If you need to increase cache size, you may need to adjust DSVa system memory accordingly.
- When to use the USN Setting:

USN means 'Update Sequence Number (USN) change journal'. With the setting enabled, Deep Security can check the USN value of a file. During Real-Time Scans, it will read partial content of files to determine if files are identical.

More information can be found here:

<http://msdn.microsoft.com/en-us/library/aa363798%28v=VS.85%29.aspx>

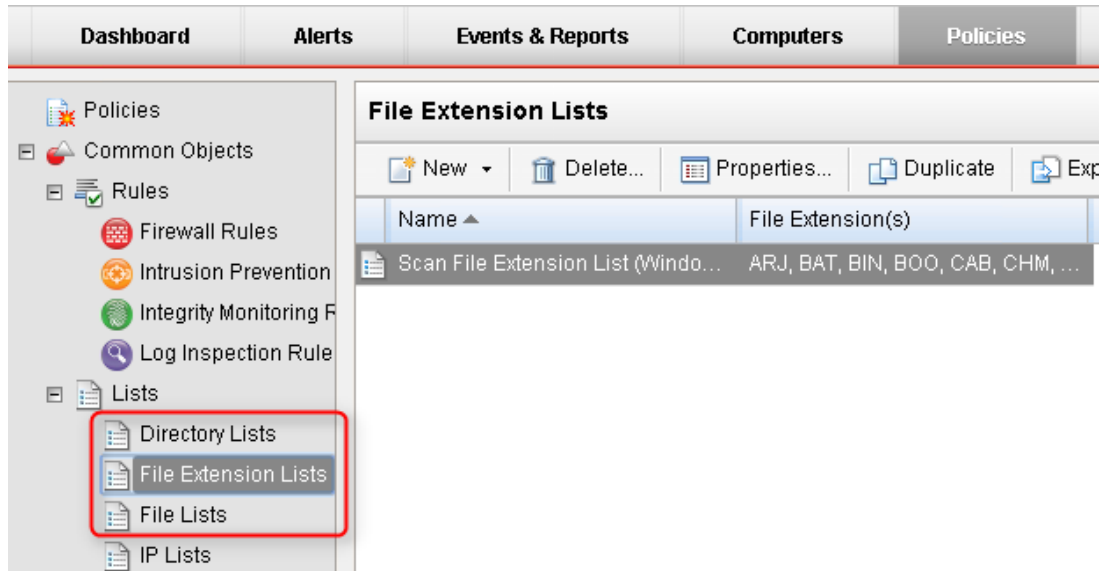
Using this setting reduces the performance and usually needs a higher cache setting. Use this setting only if stronger security is required.

Specific Scan Cache Settings for VMs and Policies can be changed under:

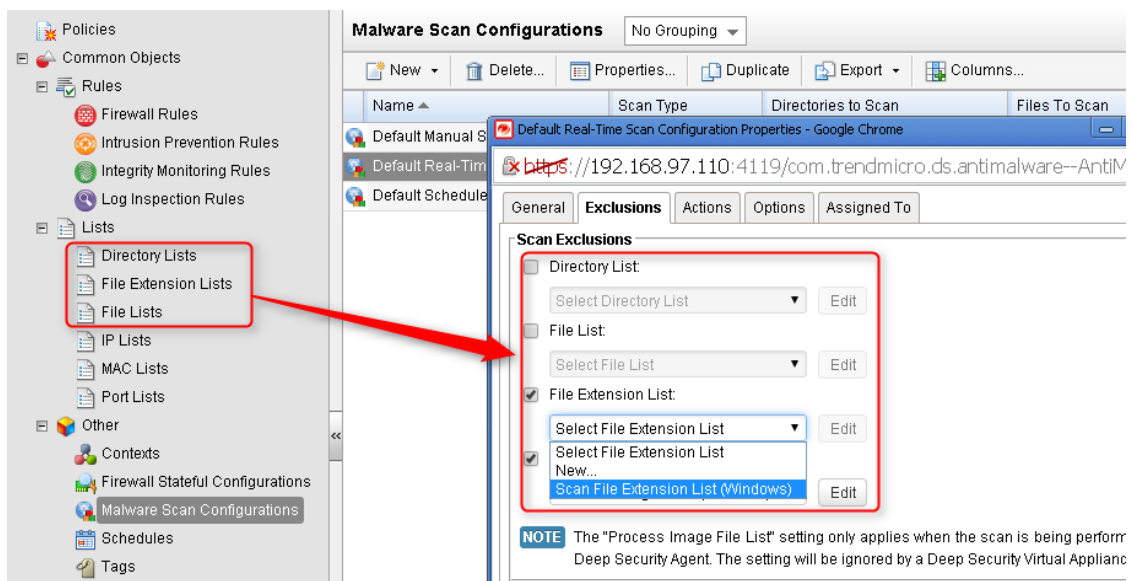
- Policy > Anti-Malware > Advanced > VM Scan Cache
- Policy > Integrity Monitoring > Advanced > VM Scan Cache

f. Scan Exclusions

The "Directory Lists/File Extension Lists/File lists" can be set in the Common Objects section of Policies tab.



These lists are then referenced on the Exclusions tab in the Malware Scan Configurations.



Note:

Please use this list as a starting point and refine it as per your environment and paths.

General Exclusions and Excluding Windows Update or Automatic Update Files

Files:

```
pagefile.sys
NTUser.pol
registry.pol
${Windir}\Software Distribution\Datastore\DataStore.edb
${Windir}\Software Distribution\Datastore\Logs\Edb*.log
${Windir}\Software Distribution\Datastore\Logs\Res1.log
${Windir}\Software Distribution\Datastore\Logs\Res2.log
${Windir}\Software Distribution\Datastore\Logs\Edb.chk
${Windir}\Software Distribution\Datastore\Logs\tmp.edb
```

```
{Windir}\Software Distribution\Datastore\Logs\hiberfil.sys  
{Windir}\Software Distribution\Datastore\Logs\pagefile.sys  
{Windir}\Software Distribution\Datastore\Logs\Edbres00001.jrs  
{Windir}\Software Distribution\Datastore\Logs\Edbres00002.jrs  
{Windir}\Security\*.edb  
{Windir}\Security\*.sdb  
{Windir}\Security\*.log  
{Windir}\Security\*.chk
```

Directories:

```
{allusersprofile}\  
{Windir}\system32\GroupPolicy\  
{Windir}\Cluster\
```

Extension Exclusions:

```
*.pst
```

Microsoft Windows Server Domain Controllers**Files:**

```
TEMP.edb  
EDB.chk
```

Directories:

```
{Windir}\SYSVOL\  
{Windir}\NTDS\  
{Windir}\ntfrs\  
{Windir}\system32\dhcp\  
{Windir}\system32\dns\
```

Microsoft SQL Server

Because scanning may hinder performance, large databases should not be scanned. Since Microsoft SQL Server databases are dynamic, exclude the directory and backup folders from the scan list. If it is necessary to scan database files, a scheduled task can be created to scan them during off-peak hours.

Directories:

```
{ProgramFiles}\Microsoft SQL Server\MSSQL\Data\  
{Windir}\WINNT\Cluster\ # if using SQL Clustering  
Q:\ # if using SQL Clustering
```

File Servers

Access to files over shared drives results in a degradation of performance. To scan some file types, only a fraction of content is required. Other file types require a full scan or even decompression and a full scan.

Trend Micro recommends that file servers are excluded from scanning and then perform the scanning on the local file server itself. With exclusions in place, there is no need to scan the file as it is accessed which increases performance.

It is also recommended to use agent protection for file server to get a better performance.

Note:

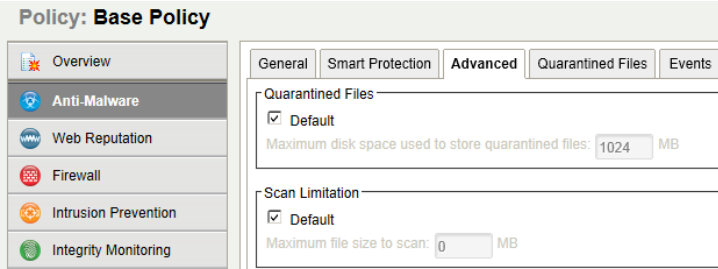
If there are any custom applications or applications not mentioned here, please contact the vendor of that software to get their recommended scan exclusions.

g. Quarantine Settings:

With agentless Anti-Malware feature, quarantined files are stored in the Deep Security Virtual Appliance (DSVA). Therefore, keep enough free space on a DSVA disk.

The default quarantined file settings are the recommended settings.

DSM > Policy > Anti-malware > Advanced



Policy: Base Policy

Overview | Anti-Malware | Web Reputation | Firewall | Intrusion Prevention | Integrity Monitoring

General | Smart Protection | **Advanced** | Quarantined Files | Events

Quarantined Files

☒ Default
Maximum disk space used to store quarantined files: 1024 MB

Scan Limitation

☒ Default
Maximum file size to scan: 0 MB

Maximum disk space used to store quarantined files: This represents the maximum space that the DSM sets aside for DSVA. Files from all protected VMs must share this space.

Maximum file size to scan: This is the largest file that can be quarantined.

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

- If a virtual machine (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.

h. Maximum performance configuration for Anti-Malware:

To maximize the performance of Anti-Malware feature, the following actions are recommended:

- a. Enable the scan cache and change the cache time based on your real situation
- b. Use Scan files when "Read" for files scanning.

Scan files when: ☒ Read
☐ Write
☐ Read/Write

- c. Add UNC path into the exclusion list. At the same time, make sure the Real-Time Scan is enabled to ensure that all VMs are being protected.
- d. Set up the proper exclusion list to exclude the folder, file, or extensions.
- e. Set the **scan limitation** to prevent scanning a file larger than the specified size.

Below are the reasons:

Read:

The system scans the virus when reading any files. This means you may download a test virus to your disk and till someone want to execute it, the system can catch the test virus when any file events are reading.

Write:

It is important but it affects the performance. Some FTP client and browsers download a file by splitting the body to several pieces.

For example: Download a 100 MB file.

The browser might download 1 MB each time (write 1 MB and close the file, write another 1 MB and close the file and so on until the whole file has been downloaded).

It means we have to scan this file for 100 times. The worst case is when the malware hide itself in the last bytes. If we do not scan on write and the file is a malware, it might be safe because we just put it on the disk without execution. We can scan it when it starts to be launched (read) and prevent its execution if a malware is found.

Write might detect malware in time, but really affects the performance.

5.2.2 Web Reputation

The default security level “Medium” is suitable for most users. However, if you want further security, you can adjust it to “High” level.

Web Reputation queries will go to the Smart Protection Server (if enabled) or to our cloud WRS servers. It is recommended to set up a local Smart Protection Server in house to limit the amount of required internet queries, which potentially leads to performance degradation.

Customer using products from Websense needs to be aware that there are potential incompatibilities between Deep Security Web Reputation and Websense’s URL filtration. We recommend disabling the Web Reputation if the protected computer is behind a Websense edge appliance.

If you have specific web pages to be allowed or blocked, configure them in the **Exceptions** tab. By default, Web Reputation is enabled to port 80 and 8080. If you have an HTTP proxy server using other ports, configure it in the **Advanced** tab.

1. Create a new Port List from Shared > Port Lists including you proxy port (e.g. 3128).
2. Choose the created Port List at Web Reputation > Advanced > Ports.

Other setting recommendations:

- Block pages that have not been tested by Trend Micro: Unchecked (could cause false positives if checked).
- Include internal company URLs in the Allowed list under Exceptions. Wildcards are supported.
- Ensure that your company’s firewall/proxy allows traffic going to **ds96-en.url.trendmicro.com** when using the global Smart Protection Server.

5.2.3 Firewall

Firewall configuration and administration must be performed carefully. There is no one set of rules that fits all environments. This guide aims to give users best practice tips and recommendations that can be used as reference and a guideline when building your own rules.

a. Inline vs. Tap Mode

- Always use Inline Mode (DSM > Policies > Settings > Network Engine > Network Engine 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.

- Use Inline Mode with rules set to “Detect” when there is a need to test the configuration and rules before deploying them into the production environment. This way, the real world process of analyzing the traffic takes place without having to perform any action such as blocking/denying of packets.

Running Deep Security in Tap Mode is NOT recommended and is not the best practice to perform tests or evaluate Deep Security. Traffic patterns in this mode do not represent how the network will behave should the administrator decide to switch to Inline Mode.

b. Firewall Rule Actions

Make sure you understand the difference between the firewall rule actions before creating your rules. Each rule can take one of the following actions:

- **Deny** - This action explicitly blocks traffic that matches the rule.
- **Force Allow** - If a packet matches a Force Allow rule, it is passed but still filtered by Intrusion Prevention. No events are logged. This action type must be used for UDP and ICMP traffic.
- **Bypass** - This allows traffic to bypass both Firewall and Intrusion Prevention analysis. It should always be created in pairs (for both incoming and outgoing traffic). Use this setting only for media-intensive protocols.
- **Log only** - If a packet matches a Log Only rule, it is passed and an event is logged. No other action will be taken.
- **Allow** - If a packet matches an Allow rule, it is passed and any other traffic not covered by a rule will be implicitly denied. Use it with caution.

c. Restrictive vs. Permissive Firewall

Typically firewall policies are based on one of two (2) design strategies. Either they permit any service unless it is expressly denied or they deny all services unless expressly allowed. It is best practice to decide what type of firewall you would like to implement. This helps reduce administrative overhead in terms of creating and maintaining the rules.

- **Permissive Mode (Reactive)**
 - This permits all traffic by default, and only blocks traffic it believes to be malicious based on signatures or other information.
 - Easy to implement, however, provides minimal security and requires complex rules.
 - This mode is rarely used except in cases where customers are not using the firewall but want to leverage it to block a port.
 - Deny rules are used to explicitly block traffic.
- **Restrictive Mode (Proactive)**
 - This is the recommended best practice from a security perspective.
 - It stops all traffic by default, and only allows traffic explicitly permitted.
 - If the primary goal of your planned firewall is to block unauthorized access, the emphasis needs to be on restricting rather than enabling connectivity.
 - It is easier to maintain and more secured.
 - Allow rules are used only to permit certain traffic across the firewall and deny everything else.

Note:

Allow rules explicitly allow traffic that matches it to pass. In addition, it implicitly denies everything else not defined. Be careful when creating Allow rules without defining the related rules correctly as doing so can cause one to block all traffic apart from what the Allow rule is created for.

d. Stateful Inspection

Stateful configurations should be used when the firewall is ON.

The stateful filtering engine inspects and validates each packet on an individual basis. This involves analyzing the packet within the context of traffic history, correctness of the packet's header values, and protocol state transitions. This enables protection against attacks such as denial of service, provided that a default configuration with stateful TCP/ICMP/UDP is enabled and only solicited replies are allowed.

If the UDP stateful option is enabled, **Force Allow** must be used when running UDP servers (e.g. DHCP). If there is no DNS or WINS server configured for the Deep Security Agents, a **Force Allow**, Incoming UDP Ports 137 rule may be required for NetBIOS.

Stateful logging should be disabled unless required for ICMP/UDP protocols.

e. Interface Isolation

Interface Isolation allows you to force a computer to use only one interface at a time. This feature prevents attackers from bridging across two interfaces. It is commonly used to protect users with wireless laptops.

Configure this via Policy > Firewall > Interface Isolation.

- Enter string patterns that will match the names of the interfaces on a computer (in order of priority).
- Limit the number of active interfaces to one at any given time.
- It is not recommended to enable this at the global level. Make sure it is enabled through the Policy instead.

Note: Interface patterns accept wildcards such as asterisk (*) as well as regex expressions.

f. Other Recommendations

● Bypass Rules

Bypass rules operate like **Force Allow** but also skip the rest of the packet processing pipeline so Intrusion Prevention is also skipped. Use this action for traffic that you prefer to allow across both the Firewall and Intrusion Prevention.

We recommend creating a pair of rules for each type of traffic. For example, create a rule bypassing the incoming traffic (request), and another outgoing rule to bypass the outbound traffic (response).

● Rule Priority

Rule priority determines the order in which filters are applied. This means, high priority rules get applied before low priority rules. When actions share the same priority, the orders of precedence for rules are: **Bypass**, **Force Allow**, and then **Deny**. However, a **Deny** action with a higher priority will take precedence over a **Bypass** action with a lower priority.

Note that **Allow** rules can only have a priority of 0. Keep this in mind when using **Allow** rules to implicitly deny traffic (any traffic not matching the **Allow** rules are denied). This means, when a **Deny** rule is added on the list, it will take precedence over all the existing **Allow** rules in place. For traffic that must always be allowed (such as ARP), it is recommended to use the action **Force Allow**.

To simplify administration of firewall rules, consider reserving certain priority levels to specific actions. For example, apply a default Priority 3 to rules that use **Bypass**, Priority 2 for **Force Allow** rules and Priority 1 for **Deny** rules. This reduces the potential for rule conflicts.

● ARP Traffic

Always allow ARP. If a computer relies on dynamic ARP, include an appropriate rule to allow ARP. ARP forms the basis of the TCP/IP stack. ARP facilities provide translation from IP addresses to Ethernet addresses, which are essential for sending packets to other systems on the local LAN segment. Without this conversion, there can be no other form of peer-to-peer IP communication.

It is important that Deep Security Manager does not instruct a Deep Security Agent to drop ARP packets, unless it is actually desired (configuration uses static ARP tables). To ensure this, please follow these guidelines:

- Enable the Trend Micro-provided ARP force allow rule.
- Do not prevent broadcast ARP packets.

- **Out Of Allowed Policy**

“Out of Allowed Policy (Open Port)” events can help quickly identify misconfigurations in rules. Generating these events for TCP, UDP, and ICMP advanced settings can assist with building and tweaking your policy.

Configure this under **Policy > Firewall > Advanced > Generate Firewall Events for packets that are Out of Allowed Policy**.

- **Use Port, IP, and MAC lists**

These lists are objects that can be reused by multiple rules. Using these lists in the configuration of multiple Firewall rules facilitates configuration changes since only a single common list must be updated. Modifications done on any of the lists are picked up by all the rules where they are used or assigned.

- **Number of rules**

Do not assign more than 300 rules as much as possible. Doing so can affect system performance.

- **Document all firewall rule changes**

Utilize the “Description” field of the firewall rule to note why, when, and for what purpose the rule was created for. Note when and why rules are created and deleted for easier maintenance.

- **Advanced Network Engine settings**

Configure this under Policies > Policy > Settings > Network Engine > Advanced Network Engine Settings.

ESTABLISHED Timeout:

This parameter defines the maximum time an idle connection can be kept. Certain applications may require keeping a connection active for a long time. Increase the value when you have such applications and there are “Out of Connection” event

Cold Start Timeout:

Specify the amount of time to allow non-SYN packets that could belong to a connection that was established before the stateful mechanism was started. Increasing this value can avoid “Out of Connection” event after restarting DSA or deploying a new profile.

Maximum TCP Connections and Maximum UDP Connections:

Maximum simultaneous TCP/UDP Connections allowed. Consider heap memory size before adjusting these two (2) parameters.

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 the 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.

Number of Packets to retain in Debug Mode:

Specify the number of packets to retain and log when the Debug Mode is on.

Log All Packet Data:

Record the packet data for events that are unassociated with specific Firewall or Intrusion Prevention rules. These are the log packet data for events such as “**Dropped Retransmit**” or “**Invalid ACK**”.

Minimum Fragment Size:

If legitimate traffic is blocked and there are "**First Fragment Too Small**" firewall events, change its value to "0" to disable the checking.

Minimum Fragment Offset:

If legitimate traffic is blocked and there are "**Fragment Offset Too Small**" firewall events, change its value to "0" to disable the checking.

For more tips and information about the Deep Security Firewall, you may refer to the following link:
<http://esupport.trendmicro.com/solution/en-us/1098015.aspx>

5.2.4 Intrusion Prevention

a. Modifying Rules

Intrusion Prevention (formerly called Deep Packet Inspection) rules must never be modified at the global level (DSM > Policy > Common Objects > Rules > Intrusion Prevention Rules) because there is no way to restore them. Configuration must be done by overriding the Policy or Computer. This way, the default master copy of the rules is kept on a global level and can be used as a reference should there be a need to revert back changes.

Bad customer rule may cause downtime. The customer can create a rule based on the signature only. For those advanced rules (Start/End/Patterns or XML format), please contact Trend Micro Technical Support to obtain a qualified rule.

b. Using Detect Only or Prevent Mode

- If a specific rule is causing false positives, place that rule in **Detect Only Mode** or un-assign it.
- Any rule requiring configuration should be assigned in **Detect Only Mode** until the rule can be configured for that computer.
- For new deployments, we recommend setting rules to **Inline Detect Mode** to make it easier to identify any false positives.
- Once the tests and additional configuration have been made, switch a rule to **Prevent Mode** to start blocking the packets that match the rule.

c. HTTP Protocol Decoding

The HTTP Protocol Decoding filter is the most important filter in the Web Server Common Application Type. This filter is responsible for decoding the HTTP traffic before the other rules inspect it. In addition, this filter also allows you to control various components of the decoding process.

This rule is required should you choose to use any of the Web Application Common or Web Server Common filters that requires it. The Deep Security Manager automatically assigns this rule when it is required by other rules. As each web application is different, the policy that uses this filter should run in a Detect Only Mode for a period of time before switching to Prevent Mode to determine if any configuration changes are required.

Quite often changes are required to the list of illegal characters.

Refer to the following KB articles for more details on this rule and how to tune it:

<http://esupport.trendmicro.com/solution/en-us/1098016.aspx>

<http://esupport.trendmicro.com/solution/en-us/1054481.aspx>

<http://esupport.trendmicro.com/solution/en-us/1096566.aspx>

d. Cross-Site Scripting and Generic SQL Injection Rules

Two of the most common application-layer attacks are SQL injection and cross-site scripting (XSS). Cross-Site Scripting and SQL Injection rules intercept the majority of attacks by default. Customization can be required to adjust the drop score for specific resources causing false positives.

Both rules are smart filters that need custom configuration for web servers. Customers who have output from Web Application Vulnerability Scanners should leverage that information when applying protection. For example, if the username field on login.asp page is vulnerable to SQL Injection, ensure that the SQL Injection rule is configured to monitor that parameter with a low threshold to drop on.

More details on this may be found here:

<http://esupport.trendmicro.com/solution/en-US/1098159.aspx>

e. Filtering SSL Data Streams

Deep Security Manager supports Intrusion Prevention analysis of SSL traffic and is able to filter SSL encrypted data streams. Filtering of SSL traffic is only supported by the Deep Security Agent, not the Deep Security Appliance. The Agent does not filter SSL connections that use compression.

This can be assigned and configured on individual computer. Open the Details window of the computer you wish to configure, go to Intrusion Prevention > Advanced > SSL Configurations > View SSL Configurations.

Note: When using this feature, there will be a performance impact. It is not recommended for servers with high numbers of connections per second.

If this feature is used, it is recommended to disable the inspection of HTTP responses to avoid any performance degradation. All web attacks that we protect against are included in the HTTP request and not the HTTP response, disabling inspection on responses will improve performance.

To configure this:

1. Go to the computer or policy > Intrusion Prevention.
2. Select a rule with Web Server Common app type, right-click Application Type > Properties.
3. Go to Configuration tab and uncheck Inherited.
4. Uncheck Monitor responses from Web Server.
5. Update the changes to the computer/policy.

f. Other Recommendations

- Set the rules only to log dropped packets to save disk space.
- If rules will be manually assigned, do not assign more than 300 rules as much as possible as it can affect system performance.
- Use Recommendation Scan to apply the necessary rules to get the best protection and performance.
- Only select the Always Include Packet Data option (Rule Properties > General > Events) when interested in examining the source of attacks. Otherwise, leaving the packet data logging on will result in much larger log sizes.
- Application Types under Intrusion Prevention rules should be checked prior to use.

Example:

The Trend Micro OfficeScan and Trend Micro OfficeScan NT Listener application types are inspecting incoming ports 8080, 4343, 26964, 24880, and 46485 by default.

OfficeScan ports can be changed, especially the random 5-digit client port. Make sure that these rules are re-configured to match your OfficeScan settings before assigning.

- It is a current limitation that one port cannot be assigned to more than eight (8) application types. Otherwise, the rules cannot work on that port.

g. Interface Tagging

"Interface Types" is a very useful feature that is used in conjunction with Firewall or Intrusion Prevention rules. We use Interface Types when we need to assign firewall or IP rules to a specific interface on machine that has multiple interfaces.

By default, the Firewall and Intrusion Prevention rules are assigned to all interfaces on the computer. If there are some special rules, for instance, you want to apply only to the wireless network interface; this is where Interface Types comes into play.

Configured under Policy > Interface Types > Network Interface Specificity.

When creating a policy, think about the difference in protection for different interfaces. Consider populating the Interface Type based on the different networks available to all potential Deep Security Agent protected machines.

5.2.5 Integrity Monitoring

Monitoring the operating system and application files and directories is an excellent way to ensure the integrity of the data on your server. Unexpected changes to these files can be a good indicator that something suspicious has occurred and should be investigated. It is good to note that rules created for Integrity Monitoring should be as specific as possible to improve performance, avoid conflicts and false positives (e.g. do not try to create a rule that monitors the entire hard drive).

a. Using Integrity Monitoring to protect against malware

Integrity Monitoring can be used to monitor files and registries. Malware normally infects a system by modifying certain registry keys and various system files. The default Deep Security rules allow you to monitor the integrity of a machine by observing the things most commonly changed by malware in an infected system. Here are a few sample rules that are applicable for all types of situation in Windows platform:

- Rule 1002773 – Microsoft Windows – ‘Hosts’ file modified
- Rule 1002776 – Microsoft Windows – ‘All Users’ Startup programs modified
- Rule 1002778 – Microsoft Windows – System DLL or EXE file modified

Unless new software or security patch is installed, there is no clear reason why any of these files should be modified. When such an event is raised, the administrator can check what is happening on the machine to make sure the machine is not compromised.

It is also possible to create custom rules to monitor specific threats. When a user knows the behavior of a particular virus he is trying to contain in an environment, he can create a special monitoring rule that checks for certain registry keys or files created by the virus. This can determine if the spread of the virus is being contained or not.

Note that Integrity Monitoring detects changes made to the system, but will not prevent or undo the change.

b. Baselines

Baselines are automatically created when the Integrity Monitoring rules are assigned to a computer. Retrieving baselines is a must. Trend Micro recommends to “Scan Computers for Integrity Check” for computers.

c. Rules from a Recommendation Scan

Recommended Integrity Monitoring rules typically result in too many monitored entities and attributes. The best practice is to decide what is critical and what should be monitored, then create custom rules or tune out of the box rules.

Pay attention to the rules that monitor the frequently changed properties (i.e. process IDs, open ports, etc) as they can be very noisy and may need some tuning.

d. Trusted-Source-Based Event Tagging

When Integrity Monitoring feature is being used, depending on the rules and settings, you might find it difficult to search and determine which events are good and informational, and which events you need to investigate further.

The Deep Security auto-tagging feature helps to group and label multiple events to suppress security events for legitimate changes.

To configure this feature, go to **DSM > Events and Reports > Integrity Monitoring Events > Auto-Tagging > Trusted Source**.

Deep Security has taken this step further by allowing administrators to automatically tag authorized changes by using internal reference servers, Certified Safe Software Service that Trend Micro is hosting in the cloud, or by comparing it with other computers in a group. Certified Safe Software Service is a cloud-based database of signatures of Trend Micro certified known-good files. More information on how to enable Trusted-Source-Based Event Tagging can be found in the Online Help and Administrator's Guide of Deep Security.

Selecting the Trusted Source:

- **Local Trusted Computer**

Use this when implementing a "Golden Host" model wherein applications and files installed on the Golden Host are used as basis for comparison.

This model is most useful when:

There are in-house applications installed on the local trusted computer.

Software, service packs, patches, etc. are installed on the local trusted computer and can use it as reference for other computers.

The local trusted computer is malware-free and secure.

The local trusted computer contains Integrity Monitoring rules that are similar to the computer that will use it as reference.

Best Practices:

- The security events from the Trusted Computers must be collected before the security events from the other computers. You can use scheduled task to automatically scan Trusted Computers.
- Create two (2) scheduled Integrity Monitoring scans.
 - First scan only checks the trusted computers
 - Second scan excludes the trusted computers
- For customers who wish to only trust events that have been generated as part of a maintenance window, they can leverage the "Pause Collection" functionality available in the Auto-Tag Rule properties.

This functionality disables automatic addition of new information to the Known Good Store based on changes on the trusted source when the collection has been paused. When paused, the events from the associated computers related to previously trusted events will continue to be tagged. However, new information will not be added to the Known Good Store until collection is resumed.

- **Certified Safe Software Service**

Use this when there are no local reference servers and users are free to install and upgrade software by themselves or at any given time. In this scenario, files are compared against Trend Micro's database of known-good files.

Best Practices:

- Make sure that the DSM has connection to the internet in order to query this cloud-based service.
- Certified Safe Software Service only supports SHA-1. If this service will be used, make sure that **Policy > Integrity Monitoring > Advanced tab > Content Hash Algorithms** is set to SHA-1.
- Among the three (3) Trusted-Source-Based Event Tagging mechanisms, this is the most safe and secure since there is no need to maintain a reference server. Trend Micro is responsible for making sure that its cloud service only contains known-good files.
- Since Auto-Tag rules can have precedence over other Auto-Tag rules, it is recommended that it goes first (top priority).

- **Trusted Common Baseline**

Use this when a group of computers can use each other as reference. Baselines of the computers in this group will be added to the common baseline. The computers in this group should be secured and free of malware because changes in one computer will automatically be added to the baseline. When a similar event occurred on another computer in the group, the event will automatically be tagged.

Best Practices:

- Make sure that the Trusted Common Baseline Auto-tagging rule is in place before any Integrity Monitoring rules have been applied to the computers in the common baseline group.
- Group the computers sharing the same operating system and function (e.g. Microsoft SQL servers running on Windows 2008 R2).
- Note that the setup and maintenance compared to Local Trusted Computer are easier but the level of protection is lower because all computers in the group are considered trusted. Since Auto-Tag rules can have precedence over other Auto-Tag rules, it is recommended that this is the last (least priority).

5.2.6 Log Inspection

Events from the Windows event log and other application specific logs are a great source of information about the health of your server and applications. An automated solution to inspect these log files for suspicious events and alert is great functionality to include in your defense in depth strategy.

This feature is especially useful in having easier access to important events in monitored log files without manually tracing through it.

- Log Inspection rules must be properly configured to work correctly. Note that most recommended rules work fairly well but Windows Event rules need to be tuned to gather security events relevant to customer requirements. When improperly tuned, events for this feature can overwhelm the DSM database if too many log entries are triggered and stored.
- Severity Clipping
 - a. "Send Agent/Appliance events to syslog when they equal or exceed the following severity level"
 - This should normally be changed when a syslog server is used. This setting determines which event triggered by those rules is sent to the syslog server (if syslog is enabled).
 - b. "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 on the Log Inspection events screen. Custom rules can be made to monitor logs that are not in the built in set of rules.

5.3 Administration and System Settings

5.3.1 Recommendation Scan

The recommendation engine is a framework that exists within Deep Security Manager, which allows the system to suggest and automatically assign security configuration. The goal is to make configuration of computers easier and only assign security required to protect that computer.

Note: When running a recommendation scan, the performance impact affects the DSM, so make sure to schedule these when no other tasks are running.

a. Run Recommendation Scans weekly

Recommendation Scans can heavily tax the DSM so scanning with high frequency can result in poor DSM performance. Hence, systems that don't change often (servers) can be scanned less frequently. Systems that lack control over when changes occur (workstations) should be scanned more frequently.

Ongoing scans for recommendations are not advised, this setting should be set to 'No'.
(Policy/Computer > Settings > Scanning > Recommendations > Perform ongoing scans for recommendations)

Setting ongoing scans to automatically start means that administrators have no control over when it will occur. Best practice is to create a new scheduled task with type "Scan Computers for Recommendations" to take place once a week instead.

b. Run scans after a major change (application of a patch, installation of new application, etc.)

Scans should be performed after major changes to the computer to determine any additional required protection.

c. Run scans after applying a new Security Update.

This allows you to use the recently released rules and get the latest updates assigned/unassigned.

d. Assign recommended rules to the policy, not to the computer.

As a best practice, recommended rules should be assigned to the policy and not directly to computers. Rules recommended can be applied automatically only to the machine where the Recommendation Scan was run.

Refer to the [Policy](#) section for additional details.

e. Run the scan on computers with similar functions.

In environments with similar computers, scans can be performed on subset of computers to gather baseline recommendations for all.

f. Automatic Assignment of Intrusion Prevention Recommendations

This option is disabled by default (Policy/Computer > Intrusion Prevention > General > Recommendations). It is not recommended to enable this option on the computer level. An exception to this would be when the machine is on its own and cannot be associated with other machines in a group. When this is enabled, Intrusion Prevention rules will automatically be enabled on the machine when the rule is found to be applicable or a matching application is found on the machine related to the rule.

See [Policy vs Computer Level](#) for more details.

Disabling this setting will give administrators a better control on assigning and un-assigning recommended rules.

5.3.2 System Settings

a. Communication Direction

This option can be set at the policy or computer level. The default “**Bidirectional**” method is recommended and is used in most production deployments.

Manager-Initiated should typically only be used for machines in the DMZ that cannot reach the Manager in the Datacenter.

Agent-Initiated method is good for environments where the agent is behind a firewall, such as mobile workstations. A disadvantage in using this mode is that policies cannot be updated on demand. The system must wait for the next heartbeat before the policy change can be deployed.

To configure this setting, go to Policy/Computer > Settings > Computer > Communication Direction.

b. Heartbeat Settings

This can be configured at the policy or computer level. Look for it under **Policy/Computer > Settings > Computer > Heartbeat**.

- Heartbeat Interval

Servers – 10 Minutes

Desktops – 60 Minutes

The most important factor when choosing the interval setting is the acceptable amount of time between when an event triggers and when the events are delivered to the DSM. Choosing a high frequency can have a negative performance impact on the DSM.

Why would servers require a lower heartbeat?

They are typically more critical assets and administrators want to be notified of events more frequently.

If protection is still in place when roaming, why would administrators want a laptop to still connect to DSM when off network?

They may want the ability to update the policy on the laptop when roaming. Also, events are stored in the DSM with the event timestamp, not the timestamp when they were delivered to DSM. Historical events can quite often be overlooked for devices that haven't performed a heartbeat in the last 24 hours.

- Number of heartbeats that can be missed before an alert is raised
By default, the value is “2”. This means, if a heartbeat is missed after two (2) attempts, the agent will get tagged as offline. We recommend increasing this value in most environments so agents that are actually online would not be tagged as offline too often.

In addition, if a heartbeat fails, events are stored locally to DSAs or DSVAs until the connection is restored.

- When using a SIEM/Syslog server to store events, heartbeat setting becomes less of a concern. Agents send events via Syslog in real-time, without batching and waiting for the next heartbeat.

c. Agent-Initiated Activations

This option is most commonly used for environments with large distributed installations where it is more desirable for the activation to be initiated by the agent rather than by DSM.

- Very useful when a large number of computers are added to a Deep Security installation and script can be used to automate the activation process. See [Deployment Scripts](#).

- For Agent-Initiated Activation to succeed, the **Allow Agent-Initiated Activation** option must be enabled on the **Administration > System Settings > Agents** tab.
- Also used when server cannot communicate/discover clients directly but clients can reach server without problem.
- Deep Security Agents can initiate the activation process using a locally-run command-line tool.

To activate:

Use “Run as administrator” to open cmd.exe, and then run the command:

```
dsa_control /a dsm://dsmhost:4120/
```

During the activation, the agent can determine the assigned policy and apply it. Additionally, agents can request scans or updates after they have been activated. This could be used to tightly integrate scans to other changes such as patch management.

Refer to the product Online Help or Administrator’s Guide for additional details.

- **Allow reactivation of cloned VMs**
This is used in environments with VM clones (i.e. clone new VM/instance from pre-activated VM, templates, or AWS images, or when switching an orphan managed VM/instance back to the vCenter or cloud managed VM/instance).

If enabled, DSM recognizes the VM as a clone and reactivates it as a new computer.

Notes:

- VM/Instance must be managed under Cloud Account/vCenter.
- VM/Instance must have unique system IDs (BIOS UUID, MAC addresses, hostname, IP, etc.).
- Make sure the network communication in the environment has no communication issues, this helps prevent the host from becoming offline or getting a mismatch.
- Cloned VM – Original VM must remain activated
- Clone activation will not migrate any policies or settings from the original VM.

- **Allow reactivation of Unknown VMs**
This allows previously activated VMs, which have been removed from their cloud environment and deleted from DSM, to be reactivated if they are added back to the inventory of VMs.
This is useful when the server deleted the agent by accident or when the server deactivated agent but the agent did not receive the deactivation request.

Note:

- The VM **MUST** have valid server certificate but no activation record on current DSM server(s).
- Unknown activation will not migrate any policies or settings from the original VM.

d. Send Policy Changes Immediately

By default, this setting is turned on. This means if there is any change made to any setting within the Deep Security environment, all affected computers are immediately updated.

Change the setting via **Policy/Computer > Settings > Computer > Automatically send policy changes to computers**.

It is recommended that this option is disabled and instead, use a scheduled task to update and send policy changes to agents manually. Manual/scheduled updates allow more control for an administrator to follow the existing change control process. Scheduled tasks can be set to update machines during maintenance windows, off hours, etc.

To monitor when machines are last updated, administrators can use the “Last Successful Update” information on the **Computers** tab of DSM.

e. Agent Self-Protection

By default, if Anti-Malware functionality is installed, DSA can protect its services, installation directories and status from any modification, including shutdown via Self-Protection setting.

If this setting is turned on, make sure to enable and set a password for the local override setting **under Policy/Computer > Settings > Agent Self Protection**.

f. Scheduled Tasks

Tasks can be configured to automate certain common tasks by schedule. Below is a list of Recommended Tasks to set up:

- Download Security Updates (Frequency: Once Daily)
- Scan Computers for Malware (Frequency: Once Weekly, or in accordance to company policy)
- Scan Computers for Recommendations (Frequency: Once Weekly)

Note:

When scheduling Recommendation Scans, it is best practice to set the task by group (i.e. per policy, or for a group of computers, no more than 1,000 machines per group) and spread it in different days (e.g. database server scans are scheduled every Monday; mail server scans are scheduled every Tuesday, and so forth).

Recommendation Scans can be CPU-intensive on the DSM so setting different schedules per group will help avoid any performance issues. Schedule Recommendation Scans more frequently for systems that change often.

- Send Policy (Frequency: Once Weekly, and run as needed)

g. Log Retention

The best practice is to run the data pruning feature built into DSM. If there is a compliance requirement to keep log sets for a longer period of time, the recommendation is to use third-party SIEM products to store the data.

Configure this under Administration > System Settings > Storage.

- Event retention is relevant to maintain a reasonably sized database
- Default retention time settings are:
 - 7 days for security events (AM, FW, IPS, IM, LI)
 - “Never” for system/agent events (as these can be useful for audit history purposes)
 - 13 weeks for counters (used for reporting, and very small in comparison to the security event logs)

h. Using Tags for Events

Tagging events allow administrators to manually tag events with pre-defined or custom labels. The use of tags in events makes log monitoring and review more efficient.

To configure tags and do auto-tag rules, go to **Policies > Common Objects > Other > Tags**.

See also [Trusted-Source-Based Event Tagging](#).

i. Active Directory Synchronization for Users and Computers

Deep Security supports the discovery of computers using Active Directory and importing users for user management.

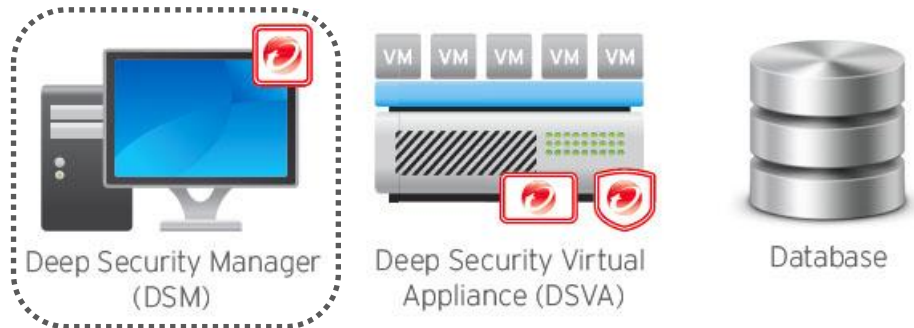
Non-SSL based LDAP is not supported to synchronize user account information because this information is considered sensitive and shouldn't be sent unencrypted. Domain controllers need to support LDAPS (port 636) for directory synchronization to work. Refer to the following links for more details on enabling LDAPS:

<http://support.microsoft.com/kb/321051>

<http://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx>

Discovering and synchronization of computers with Active Directory on the other hand can be done using standard LDAP (port 389) as the information retrieved is not sensitive (i.e. user credential information is not pulled down).

6 Performance Tuning and Optimization



6.1 Deep Security Manager

6.1.1 Configure Deep Security Manager's Maximum Memory Usage

The Deep Security Manager (DSM) default setting for maximum memory usage is 4 GB. Refer to the [Sizing Considerations](#) section to determine the recommended size allocated for the DSM.

To configure the amount of memory available to the Deep Security Manager:

For Windows:

1. Go to the Deep Security Manager directory, which is the same directory as **Deep Security Manager.exe** (e.g. C:\Program Files\Trend Micro\Deep Security Manager).
2. Create a new file called **Deep Security Manager.vmoptions**.
3. Edit the file by adding the line: **-Xmx8g** (in this example, "8g" will make 8 GB memory available to the DSM).
4. Save the file and restart DSM.

For Linux:

1. Go to the Deep Security Manager directory (/opt/dsm).
2. Create a new file called **dsm_s.vmoptions**.
3. Edit the file by adding the line: **-Xmx8g** (in this example, "8g" will make 8 GB memory available to the DSM).
4. Save the file and restart DSM.

You can verify the new setting by going to **System > System Information** and in the **System Details** area, expand **Manager Node > Memory**. The **Maximum Memory** value should now indicate the new configuration setting.

6.1.2 Configure Multiple Managers

Run and install multiple managers operating in a parallel using a single database. Running multiple nodes provides increased reliability, high availability, virtually unlimited scalability, and better performance.

Each node is capable of all tasks and no node is more important than any of the others. Users can log in to any node to carry out their tasks. The failure of any node cannot lead to any tasks not being carried out, and cannot lead to the loss of any data.

No more than three (3) manager nodes are recommended (up to five for non-multi-tenant). With three (3) nodes, it is possible to manage up to 100,000 endpoints.

Each node must run the same version of the Manager software.

Note: In a multi-node manager environment, all agents and virtual appliances have the addresses of all manager nodes.

- The agents and virtual appliances use the list of addresses to randomly select a node to contact.
- They continue to try the rest of the list until no nodes can be reached (or are all busy).

6.1.3 Performance Profiles

Performance profiles determine the number of concurrent operations that can take place for specific types of functionality. This includes the amount of Agent/Appliance-initiated connections that the manager will accept, and settings for scan storm avoidance in virtualized environments.

This setting allows you to tune the limits for a given DSM and set how loaded you want it to be. It allows users to control scans done in an environment (i.e. run unlimited scans, or choose to limit them to prevent performance issues).

You may change the performance profile via **DSM > Administration > System Information**. Click the desired Manager on the map, from here the Performance Profile can be changed via dropdown menu.

Refer to the tables below for a general idea on what each type of profile can handle:

1. **Aggressive Profile** - By default, new installations use the "Aggressive" performance profile which is optimized for a dedicated Manager. This means, the computer hosting the Manager does not perform any other task (database server, web server, etc.).

Operation	2-core system	8-core system
Activations	10	20
Updates	25	50
Recommendation Scans	5	12
Check Status	100	100
Agent/Appliance-Initiated Heartbeats	20 Active	50 Active
	40 Queued	40 Queued
Simultaneous Endpoint Disk & Network Jobs	50	50
Simultaneous Endpoint Disk & Network Jobs per ESX	3	3

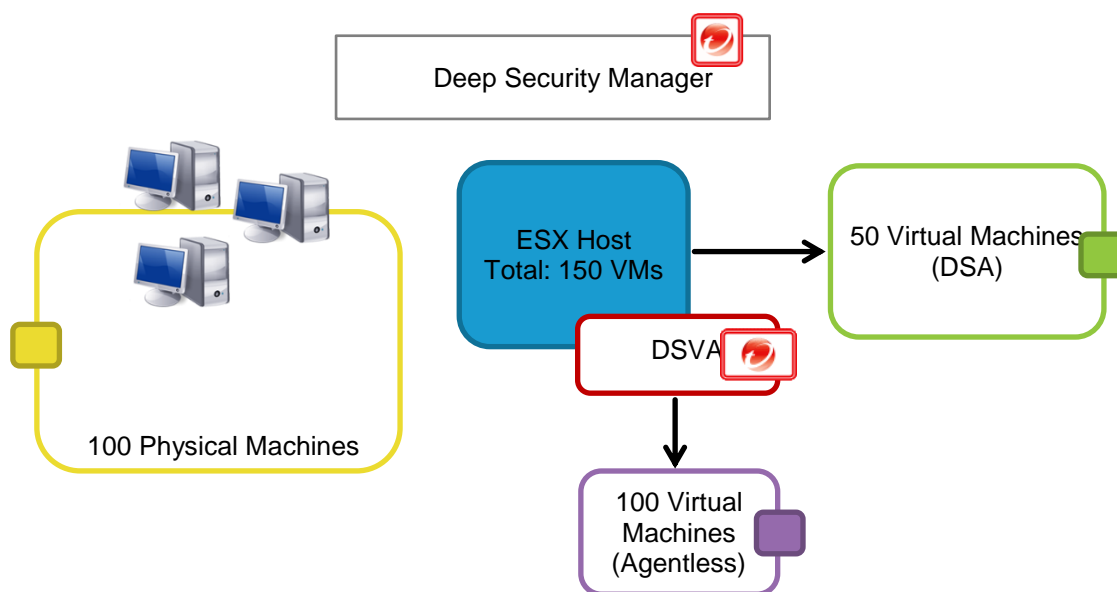
When to use:

- Virtualized Environments (Agentless deployment with DSVA and VMware)
- Hyper-V, Citrix, or other hypervisors where Physical Agents are used to provide protection

The default profile limits concurrent scans to three (3) per ESX host and 50 globally for Physical machines or VMs on other virtualization platforms to prevent scan storms.

Concurrent limit includes Anti-Malware Scans, Recommendation Scans, Integrity Scans, Baseline Rebuild, and Updates.

Sample Scenario:



When a scan is triggered for all 250 machines, Deep Security will process the request as below, instead of running the scan for all 250 machines at the same time:

- Scan the first three (3) VMs protected by DSA. The remaining 47 VMs will be placed in the queue. They will be seen in the console as “Scan Pending” and will be processed as soon as the first three finishes their scans.
- Scan the first 50 physical machines protected by DSA. The remaining 50 machines will be placed in the queue and will be processed as soon as the first 50 is finished with their scans.
- Scan one (1) VM protected by DSVA. The remaining 99 VMs will be placed in the queue. They will be seen in the console as “Scan Pending” and will be processed as soon as the one agentless VM finishes its scan.

Note:

Maximum concurrent scans for DSVA are set to “1” by default. However, this can be changed under the DSVA properties, go to **Settings > Scanning > Virtual Appliance > Max Concurrent Scans**.

Virtual Appliance	
Max Concurrent Scans:	Inherited (1)
Max On Demand Malware Scan Cache Entries:	Inherited (500000)

This setting determines the number of scans that the virtual appliance will perform at the same time. The recommended maximum number is “5”. If you increase the number beyond 10, scan performance may begin to degrade. Scan requests are queued by the Virtual Appliance and carried out in the order in which they arrive.

2. Standard Profile - Similar overall settings with aggressive, but is set to a lower limit.

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	50 Active
	40 Queued	40 Queued
Simultaneous Endpoint Disk & Network Jobs	50	50
Simultaneous Endpoint Disk & Network Jobs per ESX	3	3

When to use:

- Use only when the DSM is installed on a system with other resource-intensive software and resources are limited.

- 3. Unlimited Agent Disk & Network Usage** - This setting is identical to Aggressive but has no limit on endpoint disk and network usage operations.

Operation	2-core system	8-core system
Activations	10	20
Updates	25	50
Recommendation Scans	5	12
Check Status	100	100
Agent/Appliance-Initiated Heartbeats	20 Active	50 Active
	40 Queued	40 Queued
Simultaneous Endpoint Disk & Network Jobs	Unlimited	Unlimited
Simultaneous Endpoint Disk & Network Jobs per ESX	Unlimited	Unlimited

When to use:

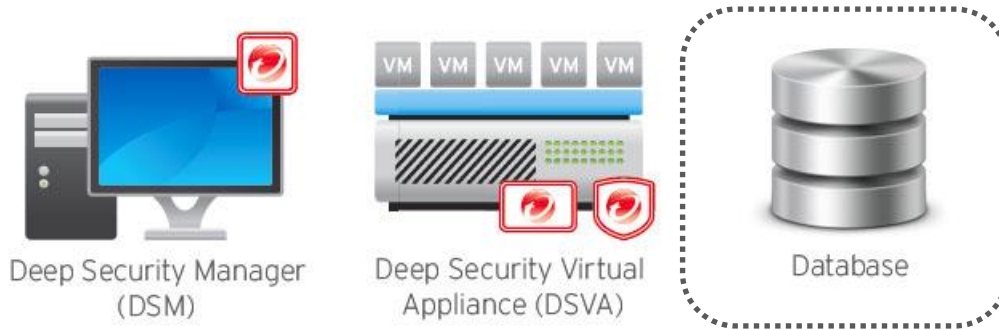
- Fully Physical Environments

Using this profile will concurrently run as many scans as possible and will assume no shared disk.

- 4. *Limited Disk and Network Usage** - This profile exists only on older versions of Deep Security. If you upgraded your Deep Security environment, you may see this as an additional profile.
- 5. Custom Performance Profile** - If further tuning of the default profiles is desired, please contact Trend Micro Technical Support for assistance.

Some of the symptoms that help determine if a custom performance profile is needed are:

- Frequent agent heartbeat rejections
- Recommendation Scans that take too long to complete
- Anti-Malware Scans that take too long to complete



6.2 Database

6.2.1 Exclude Database files from Anti-Malware scans

To optimize and establish a stable DB performance, make sure to exclude database related files (e.g. *dsm.mdf* and *dsm.ldf*) from any type of anti-malware scanning.

6.2.2 Auto-growth and Database Maintenance

For Microsoft SQL Databases, ensure less auto-growth events moving forward by adjusting the default auto-growth settings to a higher value.

Each time an auto-growth event is performed, SQL Server holds up database processing. This means that processing against that database will be held up until the auto-growth event completed. This could equate to slower response time for other SQL commands that are being processed against the database that is growing.

Monitor and perform database maintenance jobs to ensure things are working normally and to prevent having large fragmented database which could lead to performance issues.

6.2.3 Database Indexing

It's recommended to periodically rebuild the index of the database to improve performance.

Indexes are specialized data structures that operate on tables (and sometimes views) in the database engine used to aid in the searching for and sorting of data. Indexes are vital to the database engine returning results quickly.

As data is modified in the underlying tables that the indexes operate on, the indexes become fragmented. As the indexes become more and more fragmented, query times begin to suffer. The remedy to this situation is to either reorganize or rebuild the index in MS SQL or Oracle.

Below are some useful links with additional information on how to do this:

Rebuilding SQL Server Indexes

<https://msdn.microsoft.com/en-us/library/ms189858.aspx>

Index Rebuilding Techniques

http://www.remote-dba.net/tuning_index_rebuilding.htm

6.3 NSX

6.3.1 NSX Firewall

Use NSX firewall whenever possible to filter out unwanted traffic before sending to DSVA.

6.3.2 NSX Security Policy

To achieve better performance, define different security policy for different group of computers, which has different Deep Security functionalities enabled.

For example, define a security policy for computers which only have AM enabled. In this policy, do not specify any Network Introspection Services.

For the computers using Deep Security firewall, add one service in Network Introspection Services to redirect all traffic to DSVA.

If only IPS is used, consider to only redirect the ports which need DSVA to be checked when adding Network Introspection Services. For example, if it's a web server, only rules for the port 80 is assigned. Then, only redirect port 80 traffic in the NSX security policy, so that the other traffic can reach VM directly.

7 Disaster and Recovery

Deep Security utilizes a database for all of its configurations and settings. It is highly recommended that a proper disaster recovery plan is in place. This provides the best chance of successfully recovering a production environment in the quickest amount of time in case there is a disaster situation.



- It is important to make sure a regular backup of the Deep Security database is scheduled. This should be noted most specially when applying a patch or an upgrade to the software.
 - For Microsoft SQL Server database, Deep Security Manager can initiate a backup schedule task to do the database backup.
 - It is also recommended to use Microsoft SQL Server Management Studio to back up and restore the database. For detailed procedure, please refer: <https://msdn.microsoft.com/en-us/library/ms177429.aspx>
 - The Deep Security Manager cannot initiate a backup of an Oracle database. To back up and restore your oracle database, please consult Oracle support or refer to the Oracle article below to do the task using the Oracle Recovery Manager Tool:
https://docs.oracle.com/cd/E11882_01/install.112/e27508/backup.htm#DFSIG420
- Make sure you are not storing your backups in the same physical location as the database files. When your physical drive goes bad, you should be able to use the other drive or remote location that stored the backups in order to perform a restoration.
- Only restore the database from the same version number as the Deep Security Manager.

7.1 High Availability

Database clustering is supported in both Oracle and Microsoft SQL environments and is recommended for disaster recovery situations.

Oracle Data Guard and Microsoft SQL database mirroring both have no side effects in regular Deep Security functionality and can be safely used.

To recover from a disaster, make sure the database is fully mirrored or restored and available in the environment. Have a cold standby DSM ready and point it at the mirrored/restored database and start the service.

7.2 Removing a virtual machine from Deep Security protection in a disaster

If only a selected number of machines needs to be isolated and removed:

- Deactivate the affected virtual machines.
Go to **DSM > Computers > Locate the machines > Right Click > Actions > Deactivate**.
- If there is no immediate access to the DSM console, use one of the following:
 - If there is another ESXi host that has no Deep Security protection, vMotion the VM to this host.

- b. If all ESXi hosts are protected, login to the local DSVa VM and reset the appliance. Note that doing this will mean all VMs protected by that DSVa will now be unprotected.

If several VMs have the issue and need to be isolated and removed:

1. Deactivate the affected virtual machines.
Go to **DSM > Computers > Locate and right-click the machine > Actions > Deactivate**
2. Deactivate DSVa.
Go to **DSM > Computers > Locate and right-click the DSVa > Actions > Deactivate**
3. If necessary, unprepare the ESXi host and uninstall the vShield Endpoint.

To unprepare and remove the Deep Security Driver:

Go to **DSM > Computers > Locate and right-click the ESXi Host > Restore ESX...**

To remove the vShield Driver:

- Login to the vShield Manager console.
- Change the view to **Host & Clusters**.
- Expand datacenters and select the datacenter where the affected ESXi host resides.
- Click the affected ESXi and go to the **Summary** tab.
- Under the vShield Endpoint service, click Uninstall.

Note that when removing the filter driver, the ESXi host will be placed in maintenance mode and will be required to reboot.

In an agentless environment, Firewall and Stateful checks are done in the Filter Driver residing on the ESX host itself. As such, in a disaster scenario, shutting down the DSVa will only impair or shut down Anti-Malware, Integrity Monitoring, and Recommendation Scan functionalities. If the issue relates to a firewall rule blocking traffic on virtual machines, put the ESXi host in maintenance mode and un-prepare it.

7.3 Recovering a physical machine (with DSA) in a Disaster

Sometimes, assigning an incorrect policy or rule can completely isolate a machine from the network. To remove a faulty rule or policy, do one of the following:

1. If rules have been applied to the policy only, remove the faulty rule from the policy and trigger a Send Policy to the affected machines.
 - Go to **Policy > Double-click** the affected **Policy > Firewall/IP > Assign/Unassign** the rule and hit Save.
 - On the affected machines > **Right-click > Send Policy**
2. If rules have been applied directly on the machines, open the details for each affected machine and remove the faulty rule.
 - Go to the affected machine > Double-click for details > Firewall/IP > Assign/Unassign the rule and hit Save.
 - Under Overview > Actions > Send Policy or Right-click on the affected machine under Computers > Actions > Send Policy.
3. If you do not know which rule is at fault, remove the entire policy from the machine.
 - Right-click the affected machine > **Actions > Assign Policy > None**

- Right-click the affected machine > **Actions > Send Policy**
- 4. If the rule involved is a Firewall or Intrusion prevention rule, you can also consider turning off the Firewall and Intrusion Prevention State to “Off”. You can do this locally on the affected machine or on the Policy under the **General** tab.
- 5. If DSM can no longer communicate with the agents, log on locally to the machine and trigger an agent reset to completely clear all configurations on the agent and deactivate it.

On the command prompt of the local agent, run:

`dsa_control /r`

The “Reset” action does the following:

- Cleans up all DSA configuration settings and DSA memory
- Removes relation between DSA and DSM
- Removes corresponding entries from the Database

Refer to [Agent Self Protection](#) for more details.

- 6. Reactivate using a new policy without the recent change.

2

7.4 Recovering an inaccessible DSVA

Take the following steps to recover an inaccessible DSVA:

1. Reboot the DSVA.
2. If a reboot does not fix it, shut down the existing DSVA.
3. Login to DSM and attempt to deactivate the inactive DSVA and wait until you get the error “Deactivation Failed” (**Computers > DSVA > Right Click > Actions > Deactivate**).
4. Clear warnings and errors for that DSVA (**Computers > right-click the DSVA > Actions > Clear Warnings and Errors**).
5. Deploy a new DSVA from DSM (**Computers > right-click the ESX Host > Actions > Deploy Appliance**).
6. Activate the new DSVA (**Computers > right-click the DSVA > Actions > Activate**).
7. Reactivate all the VMs to the new DSVA.

Note that when you replace a faulty DSVA, all logs, settings, and quarantined files from the original DSVA will be lost.

7.5 Isolating a Deep Security Issue

1. As opposed to deactivating or uninstalling the agent, it is recommended to isolate the module causing the issue first. Ideally, check the related event logs first for information and clues regarding the issue on hand.

If no related logs are observed and multiple features are used, turn off the suspected module one by one to find the culprit.

For example, if the issue involves HTTP traffic being blocked, turning off WRS and then the Firewall would be the first thing to try.

2. For issues involving WRS:
 - If traffic to a certain site is blocked, consider adding it to the “Allowed” URLs. Do this by going to the **Policy/Computer > Web Reputation > Exceptions** tab. Enter the URL in the Allow list, save, and send the policy.
 - If adding the site to the Allow list does not help, turn off the Web Reputation (**Policy/Computer > Web Reputation > General > Web Reputation State**).
 - If WRS is already turned off and the issue still persists, consider checking other features enabled.

3. For issues involving the Firewall:

- Note if a new rule or a modification on a rule has taken place. Un-assign the suspected rule and verify if the issue persists.
- If you are not aware which rule is causing the issue, consider removing the policy assigned to the affected machine. Verify if the issue still persists.
- If no recent change has been done but traffic is blocked, turn the Firewall off. To do this, go to **Policy/Computer > Firewall > General > Firewall State**.
- If the firewall is disabled and the issue persists, verify that Firewall Stateful Configurations are also set to "None" (**Policy/Computer > Firewall > General > Firewall Stateful Configurations**).
- If both settings are turned off and the issue persists, switch the Network Engine to "Tap" mode. Do this via **Policy/Computer > Settings > Network Engine > Network Driver Mode**.

Should the issue still persist, check the other features that are enabled.

4. For issues involving Intrusion Prevention:

- Note if a new rule update has been applied or a modification on a rule has taken place. Un-assign the suspected rule or roll back the security update. Verify if the issue persists.
- If you are not aware which rule is causing the issue, consider removing the policy assigned to the affected machine. Verify if issue still persists.
- If no recent change or update has been applied, but traffic is blocked, switch the behavior from "Prevent" to "Detect" or turn off the Intrusion Prevention. Both settings may be found under **Policy/Computer > Intrusion Prevention > General > Intrusion Prevention State/Behavior**.
- If Intrusion Prevention is turned off and the issue still persists, switch the Network Engine to "Tap" mode. Do this via **Policy/Computer > Settings > Network Engine > Network Driver Mode**.
- Should the issue still persist, check the other features that are enabled.

5. For issues involving Anti-Malware:

Performance Related:

If there are performance or access issues experienced when the AM module is turned on, consider adding the directory/file being scanned to the exclusion list first. To do so, go to the Scan Configuration used by the Computer/Policy (**Policy/Computer > Anti-Malware > General > Select scan type > Configuration > Edit > Exclusions**). Verify if the issue still persists.

If adding the file/directory to the exclusion does not work, remove the policy assigned to the affected machine.

- If the issue persists, try to turn off Anti-Malware protection. Go to **Policy/Computer > Anti-Malware > General > Anti-Malware State**.
- If the issue continues, de-activate the agent.
- Should the issue still persist, check the other features that are enabled.

Detection Issues:

- If the issue involves malware not being detected, verify the Anti-Malware state and make sure it does not have any errors. Check for failed events under **Policy/Computer > Anti-Malware > Events**.
*Consult the following articles for Anti-Malware state verification:
<http://esupport.trendmicro.com/solution/en-US/1098103.aspx>
<http://esupport.trendmicro.com/solution/en-us/1060525.aspx>
- Verify Smart Protection settings and make sure there are no connection failures (**Policy/Computer > Anti-Malware > Smart Protection**).
- Should the issue persist, contact Trend Micro Technical Support.

6. For issues involving Integrity Monitoring:

- Note if a new rule update has been applied or a modification on a rule has taken place. Note the additional modifications made and review the configuration changes. You may also un-assign the suspected rule or roll back the security update. Verify if the issue persists.
- If no recent change or update has been applied, but alerts continue to be generated, turn off the Integrity Monitoring by going to **Policy/Computer > Integrity Monitoring > General > Integrity Monitoring State**.
- Should the issue still persist, check the other features that are enabled.

7. .For issues involving Log Inspection:

- Note if a new rule update has been applied or a modification on a rule has taken place. Note the additional modifications made and review the configuration changes. You may also un-assign the suspected rule or roll back the security update. Verify if the issue persists.
- If no recent change or update has been applied, but alerts continue to get generated, turn off the Log Inspection by going to **Policy/Computer > Log Inspection > General > Log Inspection State**.
- Should the issue still persist, check the other features that are enabled.

8 Other Deployment Scenarios

8.1 Multi-Tenant Environment

Multi-Tenancy allows you to create independent environments of Deep Security with the same manager and database infrastructure. It can be used by service providers or enterprises that require strong isolation between departments or lines of business.

Multi-Tenant vs Single Tenant Deployment		
	Single Tenant	Multi-Tenant
Managed Computers	100,000	1,000,000 or more
Deep Security Nodes	1 - 5	1 - 50
Databases	1	1 - 10,000
Database Servers	1 (with or without replication)	1 - 100

Recommendations:

1. Reconnaissance IP List

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

2. Multi-Database Servers

Multi-tenancy relies on using multiple databases in case of MS SQL or multiple users in case of Oracle. To scale further, Deep Security Manager can be connected to multiple database servers and automatically distribute the new tenants across the available set of database servers.

To configure additional databases to use, go to:
Administration > System Settings > Database Servers

3. Use the chargeback feature to monitor tenant usage

Monitoring can help determine the percentage usage of Deep Security Manager by hours of protection. Deep Security Manager records data about Tenant usage. This information is displayed in the **Tenant Protection Activity** widget on the Dashboard, the **Tenant Properties** window's **Statistics** tab, and the Chargeback report.

This information can be customized to determine what attributes are included in the record. It also provides the ability to monitor the usage of the overall system and look for indicators of abnormal activity. For instance, if a single Tenant experiences a spike in **Security Event Activity**, it may be under attack.

4. Tenant pending deletion state

Tenants can be deleted. However, the process is not immediate. It ensures that all the tenant-related jobs are finished before the records are deleted. The longest job runs every week, so the tenant, will be in the pending deletion state for approximately seven (7) days before the database is removed.

5. Multi-tenant options under System Settings

- **Allow Tenants to use the Relays in my "Default Relay Group" (for unassigned Relays):**

It gives the tenants automatic access to relays setup in the primary tenant. This saves the tenants from setting up dedicated relays for security updates.

- **Allow Tenants to use the "Backup" Scheduled Task:**

It 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.

8.2 Environments using Teamed NICs

Windows NIC teaming software creates a new virtual master interface, which adopts the MAC address of the first slave interface. By default, the Windows Agent will bind to all virtual and physical interfaces during installation. As a result, in a teamed NIC environment, the agent will bind with the physical interfaces as well as the virtual interface created by the teaming software. The agent cannot function properly with multiple interfaces having the same MAC address.

1. To function properly in a teamed-NIC environment, the agent must be bound only to the virtual interface created by the teaming software. For more information, refer to the following KB:
<http://esupport.trendmicro.com/solution/en-us/1054496.aspx>
2. Using the agent in a teamed-NICs environment on Windows 2003 requires SP 2 or later, or the installation of the following patch: <http://support.microsoft.com/kb/912222/article>.
3. The Agent's network driver is bound to the network interfaces only at the installation or upgrade period. After installation, it is impossible for the bindings to be automatically adjusted when you add or remove network interfaces to or from a teamed-NIC.

Doing so can lead to network connectivity problems, or to the system not being properly protected. After adding or removing a network interface in a teamed environment where the agent's network driver is installed, you should verify that the driver is only bound to the virtual interface and not bound to any physical adapters.

4. On Solaris systems with multiple interfaces on the same subnet, the operating system may route packets through any of the interfaces. Because of this, any Firewall Stateful Configuration options or Intrusion Prevention Rules should be applied to all interfaces equally.

8.3 Air-Gapped Environments

At least one (1) Deep Security Relay is required in every Deep Security environment. It must be able to download updates from the Trend Micro Update Server so the rest of the Relays, Agents and Appliances connect to that Relay for update distribution.

However, if your environment requires that the Deep Security Relay is not allowed to connect to a relay or update server via Internet, then an alternative method is available to import a package of updates to a Relay for distribution to other Deep Security Software Components.

The following resources provide details on generating an update bundle:

<http://esupport.trendmicro.com/solution/en-US/1060674.aspx>

Another tool is the Trend Micro Update Utility. This tool is a Windows application that provides a mechanism for downloading software component updates from the Trend Micro Active Update and Intelligent Active Update repositories via Internet. This can be used to bundle product updates into a ZIP file, which can then be manually delivered to Deep Security Relays (DSR) in an air-gapped environment.

Please contact Trend Micro Technical Support to request this tool.

To avoid confusion when working in an air-gapped scenario, it is recommended to **disable** the following options under **System Settings > Updates**:

- Allow Agents/Appliances to update from this source if Deep Security Relays are not available
- Agents can update components automatically when not in contact with Deep Security Manager

8.4 Solaris Zones

When working with Solaris Zones, keep in mind that it allows multiple instances of Solaris to run in one shared kernel.

The Deep Security Agent for Solaris is only supported to run with the Global/Root Zone. Refer to the article below for more details:

<http://esupport.trendmicro.com/solution/en-us/1058701.aspx>

8.5 Microsoft Cluster Servers

Cluster servers involve two (2) separate installations of the underlying operating system with shared resources (databases, disks, IP addresses, etc) that get swapped back and forth when the cluster performs a failover.

Deep Security can be configured to protect one node in the cluster or both. Some points to consider in this environment are:

- Ensure that you are installing DSA to a local disk, and not a shared disk.
- If the cluster software uses a network heartbeat with a dedicated network interface card, ensure that no rules are assigned to this interface. You may also create bypass rules that will ensure that the heartbeats aren't inspected.
- Currently, we have encountered some issues when activating/deactivating MS cluster or SQL cluster in the ESXi 5.5 machines. The VMware ESXi 5.1 does not have such issue. To avoid the issue, please install DSA as a workaround.

Note: Installing or uninstalling DSA may cause temporarily disconnection of the cluster due to binding/unbinding the drivers. Please pick up suitable time to do this.

8.6 Microsoft Hyper-V

When deploying Deep Security on a Microsoft Hyper-V environment, the Deep Security Agent should be installed within each guest operating system in each virtual machine (VM). This provides the maximum amount of context and security for each guest.

- Recommendation Scans can be used to determine the applicable set of Intrusion Prevention, Integrity Monitoring and Log Inspection rules required per guest.
- Anti-Malware, Web Reputation, and Firewall policies can also be individually configured per guest using the Agent deployment.

If protection of the Parent Partition (also known as the Management Operating System) is desired, additional steps are required to ensure that network traffic is not inspected twice.

It is recommended to choose one of the following options:

- Do not utilize Intrusion Prevention in the parent partition.
- Utilize Intrusion Prevention in the parent partition, but utilize the Firewall policy assigned to the Agent in the parent partition to bypass incoming and outgoing traffic for the IPs of the VMs being hosted.

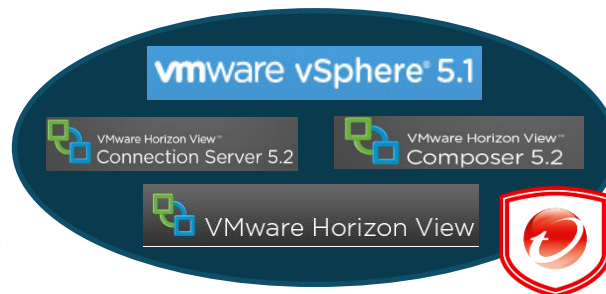
This can be accomplished through the use of two (2) Bypass rules - one for incoming and one for outgoing - that operate on the destination IP range of guests for incoming traffic, and the source IP range of guests for outgoing traffic.

The use of Bypass skips the Intrusion Prevention rule processing, thus preventing duplicate inspection of the traffic in both the parent partition and guest virtual machine.

It is also advised to use Bypass rules, like the second option above, if using a Firewall policy on the parent partition.

8.7 Virtualized Environments (VDI)

VMware Horizon View



1. Install the VMware vShield with the Golden Image

When using either the traditional installation method or Microsoft Deployment Toolkit (MDT), and preparing the Golden Master Image(s), make sure that you install the necessary VMware vShield Endpoint in-guest driver which is a part of the VMware Tools.

2. Persistent and Non-Persistent VMs

Both non-persistent and persistent View desktops need antivirus protection. Agentless protection is recommended for both scenarios. Make sure you install VMware tools in the virtual machine before it is converted into a parent virtual machine for linked clones.

If the Agent-based protection is required, make sure to install an un-activated DSA on the VM before it becomes the parent virtual machine.

3. Deep Security Notifier

Notifier file "ds_notifier.vif" should not be added into exclusion due to infrastructure changes. We do not use VMware VMCI for the Trend Micro Notifier anymore. In case notifier is not working, please make sure you did not add the C:\ProgramData\ds_notifier.vif into the exclusion list.

4. Automating Virtual Machine Activations

DSVA can instantiate and activate Virtual Agents for virtual machines as they are created and assigned automatically a specific policy. Event-based tasks should be created so it can trigger Instant Protection functionality when VMs are added to a virtual environment protected by DSVA.

To configure event-based tasks, go to **Administration > Event-Based Tasks**.

Event-based tasks can use conditions to trigger the action. The conditions use standard regex expressions. To know more about regex usage and to test the expressions configured, you may refer to these sites:

<http://www.regular-expressions.info/> (Regex reference)

<http://regexpal.com/> (Regex expression tester)

5. Note the number of protected VMs

DSM must control the maximum number of protected VMs running on each protected ESXi host. Improper sizing can degrade the DSWA performance. Please refer to [Sizing Considerations](#) section in this document. For additional best practice details on running Anti-Malware protection for VMware View, you may refer to this document:

<http://www.vmware.com/files/pdf/VMware-View-AntiVirusPractices-TN-EN.pdf>

6. Activating Virtual Machine using Event-Based Task

Trend Micro recommends setting a delay time for Event-Based task for activation to ensure a successful execution. Please refer to KB link: <http://esupport.trendmicro.com/solution/en-US/1102764.aspx>

7. Golden image

When using golden image in VDI environment, you need to select the correct OS type to avoid DSM reporting an incapable Anti-Malware.

Citrix XenDesktop

1. Install a deactivated Deep Security Agent on a Master image.

Deep Security Virtual Appliance (Agentless) does not work with a pure Citrix environment (i.e. VMs running on Citrix XenServer).

For these environments, the physical agent-based solution is recommended. Install the Agents in the master image (deactivated) and then perform Agent-based activation in the provisioning process. Use an Event-Based Task to assign the correct policy based on the attributes available (i.e. Computer Name).

DSVA (Agentless) can be used to provide protection for the pooled Citrix VDI desktops if they are running on top of VMware vSphere. VMware tools would also need to be installed within the master image to include the necessary vShield Endpoint driver to use appliance-based protection.

2. Deep Security Agent and the Citrix target device driver

On Citrix PVS 6.0 Environment, if you plan on installing (In-Guest) Deep Security Agent, the Citrix Target device driver may not be able to connect successfully to the Provisioning Server due to a possible conflict.

If you plan on installing Deep Security Agent on a Windows operating system that is connected to a PVS server using disk provisioning, the temporary workaround is to change the tbimdsa driver loading order during system startup from PNP_TDI to NDIS.

To do so, manually change the loading order of tbimdsa driver used by Deep Security Agent.

- Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\tbimdsa
- Add or modify String "Group" value to "NDIS"
- Add or modify DWORD "Start" value to "0"

By changing the Group from "PNP_TDI" to "NDIS" and Start value from "3" to "0", it allows tbimdsa driver to load after Citrix driver has loaded.

- Reboot the machine and the PVS Target Device will be able to connect to the vDisk upon boot-up.

Refer to <http://esupport.trendmicro.com/solution/en-US/1098061.aspx> for more details.

Citrix XenApp

1. Citrix XenApp's API Hooks

Citrix's API hooks can prevent the DSA service from starting. In order to resolve this, the ds_agent.exe must be added into XenApps exclusion list.

<http://support.citrix.com/article/CTX107825>

2. Anti-Malware Exclusion for Citrix

Trend Micro recommends that Citrix files are excluded from scanning by Deep Security. For a more comprehensive list of recommended scan exclusion, refer to following KB link:

<http://esupport.trendmicro.com/solution/en-us/1102554.aspx>

8.8 Private, Public & Hybrid Cloud Environments

Amazon Web Services (AWS)

Deep Security Manager can now be connected to Amazon Web Services to provide instance discovery and collect additional information about the instances. This can be used to automate security (e.g. assigning a policy based on an Amazon Security Group).

Allot a dedicated account for Deep Security. This ensures that you can refine the rights and permissions or revoke the account at any time. It is recommended that you give Deep Security an Access/Secret key with no more than read-only permissions.

vCloud Environment

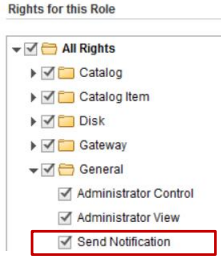
Deep Security Manager can now connect to the vCloud director to discover the machines to be protected. If this is used with a public cloud, it can help with agent management. If vCloud is used within a private or community cloud where Deep Security Manager is deployed, the vCloud support can work together with the vCenter integration to provide agentless protection to vCloud.

vCloud director (vCD) workloads are presented in Deep Security in the following hierarchy:

- vCloud Director Instance
- Virtual Datacenter
- vApp
- Virtual Machine (being the endpoint that can be protected)

This enables the administrator to select virtual machines belonging to certain vDC/vApp's to be protected.

1. Multiple vCD instances can be presented but always ensure the following rules are applied:
 - Ensure all vCenters that vCD used for resources are already configured in the Administrative side of the portal.
 - Present vCD instances at vCD System object. This will allow all workloads to be discovered in vCD.
2. The following vCloud Director settings must be configured correctly:
 - vCD public URL
 - vCD public REST API base URL (System > Administration > Public Addresses)
3. The vCloud organization accounts to be used by DSM to access vCloud must have the "Administrator View" right. This can be verified by checking the user's role properties in vCloud, then go to Rights for this Role > All Rights > General folder.



4. Consider the following settings when adding the vCloud Director Instance:
 - Ensure the name is descriptive.
 - Enter the address of the vCloud Director instance as follows:
vcloud.mycompany.com
 - There is no need to add "http" or "https" in the form field of the address.
 - There is no need to add the organization name at the end of the URL.
5. When importing the vCloud resources into Deep Security Manager, the username must include "@orgName". For example, if the vCloud account's username is kevin and the vCloud Organization you've given the account access to is called CloudOrgOne, then the Deep Security user must enter kevin@CloudOrgOne as their username when importing the vCloud resources.
6. When adding more than one vCloud Director instance, ensure that the corresponding Provider Virtual Datacenter resources have been added to DSM. This includes :
 - All vCenter instances used for Provider Virtual Datacenters
 - All vShield Manager instances used for Provider Virtual Datacenters
7. Public Catalog VMs must have the vShield Driver installed as part of the template configuration before adding the vApp/VM to the Catalog.
8. Configure the vCenter Database to Assign Unique UUIDs to New Virtual Machines:

http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&externalId=2002506&sliceId=2&docTypeID=DT_KB_1_1&dialogID=505128773&stateId=1_0_505140029

Other Useful References:

<http://esupport.trendmicro.com/solution/en-US/1102173.aspx>

<http://esupport.trendmicro.com/solution/en-US/1102253.aspx>

8.9 VMware SRM (Site Recovery Management) environment

In the VMware SRM (Site Recovery Management) environment, both multi-node DSM and separate DSM are supported to provide protections:

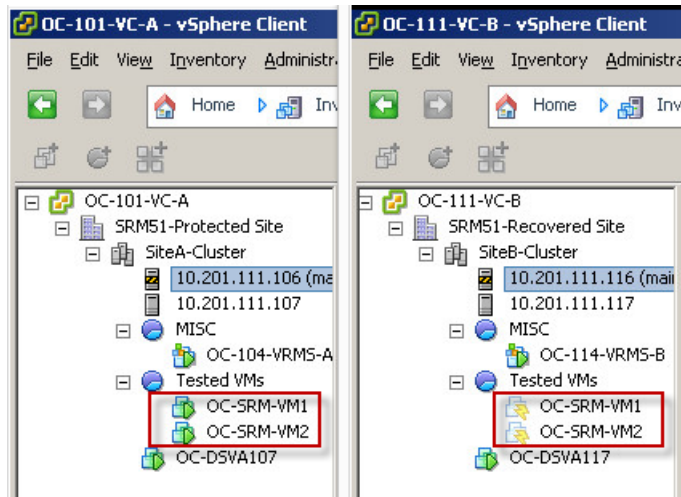
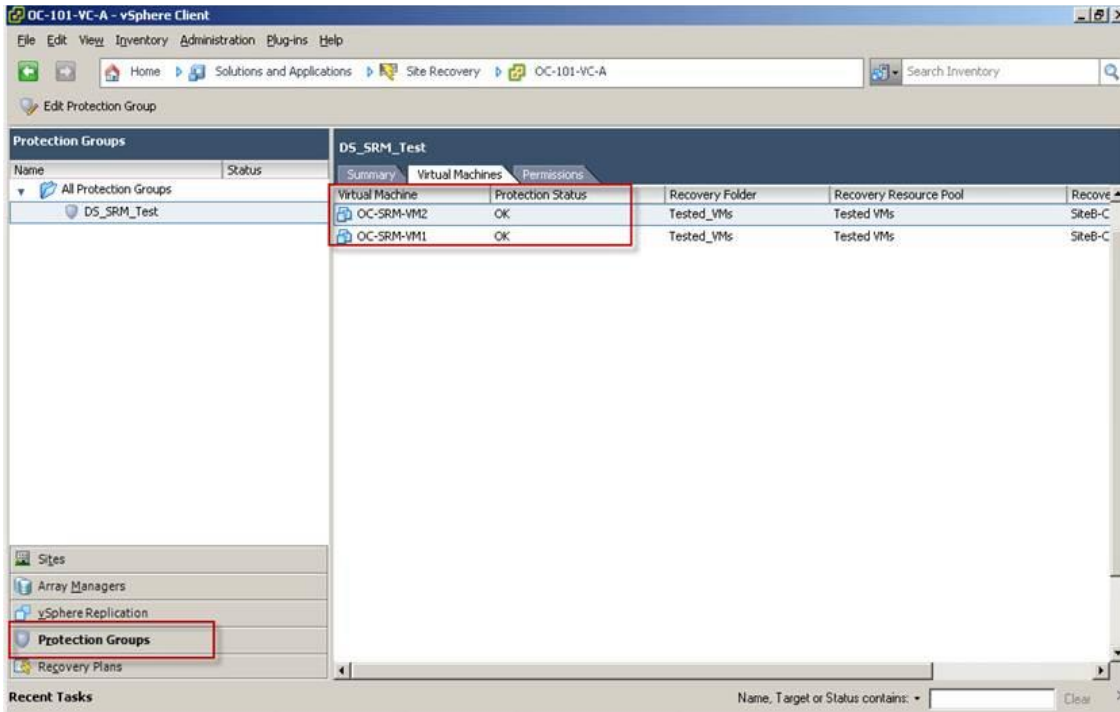
Scenario 1: Multi-node DSM in Protected site-A and Recovery Site-B.

Scenario 2: Separate DSM in Protected site-A and Recovery Site-B.

Scenario 1 and 2, agentless (DSVA) both work fine after a failover to recovered site, and can also work fine after returning back to protected site.

The Agent-based (DSA), can ONLY be managed by one site. Although the VMs cannot be managed after failover to recovery site, the DSA service and function still can work fine. Upon returning back to protected site, the VMs could be managed and work normal.

By design, when the VMs are set up in VMware Site Recovery Protection Groups, the Recovery site's VMs icon will be changed. Please refer to the screenshot below:



On the DSM, not only the Protected site's VMs will be displayed, but the Recovery site's VMs are also shown on the DSM before the recovery. Therefore, we cannot use the **Event-Based Tasks (Computer-Created)** to activate/re-activate the VMs when they failover to Recovery Site.

8.10 SAP

If customers install the DSA prior to "SAP server with Virus Scan Adapter", please disable the Real-Time Scan of DSA before the SAP installation to avoid race condition.

Create a new security profile for SAP server only. Do not use the existing policy plus the SAP function.

8.11 IBM Rational ClearCase

It may result in server freeze if the Deep Security on a Linux has IBM Rational ClearCase installed. Please refer to the IBM's recommendation about running the AV on the server:

<http://www-01.ibm.com/support/docview.wss?uid=swg21149511>

8.12 AM Exclusion for Veeam

Veeam backup fails because the AV is interfering with the operation. Some files and directories need to be excluded. For more information, refer to this link: <http://www.veeam.com/kb1999>