TREND MICRO™

9.5 Deep Security

Administrator's Guide

Advanced Protection for Physical, Virtual, and Cloud Servers

Cloud & Data Center

Complete End User

Cyber Threats

Document version: 1.2
Document number: APEM96331/140306
Release date: Aug 27, 2014
Document generated: Aug 27, 2014 (18:34:01)

Table of Contents

Introduction

Overview

Deep Security provides agentless and agent-based protection for physical, virtual, and cloud-based computers.

Protection includes:

- Anti-Malware
- Web Reputation
- Firewall
- Intrusion Detection and Prevention
- Integrity Monitoring
- Log Inspection

System Requirements

Deep Security Manager

- **Memory:** 8GB, which includes:
  - 4GB heap memory
  - 1.5GB JVM overhead
  - 2GB operating system overhead
- **Disk Space:** 1.5GB (5GB recommended)
- **Operating System:** Windows Server 2012 (64-bit), Windows Server 2012 R2 (64-bit), Windows Server 2008 (64-bit), Windows Server 2008 R2 (64-bit), Windows 2003 Server SP2 (64-bit), Windows 2003 Server R2 (64-bit), Red Hat Linux 5/6 (64-bit)
- **Database:** Oracle 11g, Oracle 11g Express, Oracle 10g, Oracle 10g Express, Microsoft SQL Server 2014, Microsoft SQL Server 2014 Express, Microsoft SQL Server 2012, Microsoft SQL Server 2012 Express, Microsoft SQL Server 2008, Microsoft SQL Server 2008 Express, Microsoft SQL Server 2008 R2, Microsoft SQL Server 2008 R2 Express
- **Web Browser:** Firefox 24+, Internet Explorer 9.x, Internet Explorer 10.x, Internet Explorer 11.x, Chrome 33+, Safari 6+. (Cookies must be enabled in all browsers.)
  - **Monitor:** 1024 x 768 resolution at 256 colors or higher

Note: *These requirements assume that the database is installed on a separate server.*

Deep Security Virtual Appliance

- **Memory:** 4GB
- **Disk Space:** 20GB
- **VMware Environment:** VMware vCenter 5 and ESXi 5

Note: *For specifics about the VMware Environment, see the Installation Guide.*

Note: *The Deep Security Virtual Appliance runs on 64-bit CentOS. Because the Deep Security Virtual Appliance uses the same Protection Module plug-ins as Deep Security Agents, and because the CentOS Agent software is included in the Red Hat Agent software package, importing an update to the 64-bit Red Hat Agent software can lead to a notification that new software is available for the Virtual Appliance.*

Deep Security Agent

- **Memory:**
  - **with Anti-Malware protection:** 512MB
  - **without Anti-Malware protection:** 128MB
- **Disk Space:** 1GB
  - **with Anti-Malware protection:** 1GB
  - **without Anti-Malware protection:** 500MB
  - **with Relay functionality enabled:** 8GB
- **Supported Platforms:** Windows, Linux, Solaris, AIX, HP-UX, CloudLinux, Amazon Linux, Oracle Linux, Ubuntu, SuSE
  - **Relay functionality** supported on 64-bit Windows and Linux Agents

Note: *See the **Supported Platforms and Features** and **Supported Linux Kernels** documents for the currently supported versions of each platform. For the latest available Agent versions, go to **Administration > Updates > Software > Download Center**.*

Note: *The CentOS Agent software is included in the Red Hat Agent software package. To install a Deep Security Agent on CentOS, use the Red Hat Agent installer.*

Note: *Windows Agents running on Windows XP or Windows 2003 will not function in an IPv6 environment.*

Deep Security Notifier

- **Memory:** 1MB
- **Disk Space:** 1MB
- **Supported Platforms:** Windows

The Deep Security Notifier is a Windows notification tray tool. It is installed by default with the Windows agents and Relays. It can installed independently in cases where a Windows VM is being protected agentlessly by a Deep Security Virtual Appliance but the Anti-Malware module must be licensed and enabled on the VM for the Deep Security Notifier to display information.

Product Features

Deep Security provides advanced server security for physical, virtual, and cloud servers. It protects enterprise applications and data from breaches and business disruptions without requiring emergency patching. This comprehensive, centrally managed platform helps you simplify security operations while enabling regulatory compliance and accelerating the ROI of virtualization and cloud projects. The following tightly integrated modules easily expand the platform to ensure server, application, and data security across physical, virtual, and cloud servers, as well as virtual desktops.

Protection Modules

Anti-Malware

Integrates with VMware environments for agentless protection, or provides an agent to defend physical servers and virtual desktops in local mode.

Integrates new VMware vShield Endpoint APIs to provide agentless anti-malware protection for VMware virtual machines with zero in-guest footprint. Helps avoid security brown-outs commonly seen in full system scans and pattern updates. Also provides agent-based anti-malware to protect physical servers, Hyper-V and Xen-based virtual servers, public cloud servers as well as virtual desktops in local mode. Coordinates protection with both agentless and agent-based form factors to provide adaptive security to defend virtual servers as they move between the data center and public cloud.

Web Reputation

Strengthens protection against web threats for servers and virtual desktops.

Integrates with the Trend Micro Smart Protection Network web reputation capabilities to safeguard users and applications by blocking access to malicious urls. Provides same capability in virtual environments in agentless mode through the same virtual appliance that also delivers agentless security technologies for greater security without added footprint.

Integrity Monitoring

Detects and reports malicious and unexpected changes to files and systems registry in real time. Now available in agentless form factor.

Provides administrators with the ability to track both authorized and unauthorized changes made to the instance. The ability to detect unauthorized changes is a critical component in your cloud security strategy as it provides the visibility into changes that could indicate the compromise of an instance.

Intrusion Prevention

Shields known vulnerabilities from unlimited exploits until they can be patched.

Helps achieve timely protection against known and zero-day attacks. Uses vulnerability rules to shield a known vulnerability -- for example those disclosed monthly by Microsoft -- from an unlimited number of exploits. Offers out-of-the-box vulnerability protection for over 100 applications, including database, web, email and FTP servers. Automatically delivers rules that shield newly discovered vulnerabilities within hours, and can be pushed out to thousands of servers in minutes, without a system reboot.

Defends against web application vulnerabilities.

Enables compliance with PCI Requirement 6.6 for the protection of web applications and the data that they process. Defends against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities. Shields vulnerabilities until code fixes can be completed.

Identifies malicious software accessing the network.

Increases visibility into, or control over, applications accessing the network. Identifies malicious software accessing the network and reduces the vulnerability exposure of your servers.

Firewall

Decreases the attack surface of your physical and virtual servers.

Centralizes management of server firewall policy using a bidirectional stateful firewall. Supports virtual machine zoning and prevents denial of service attacks. Provides broad coverage for all IP-based protocols and frame types as well as fine-grained filtering for ports and IP and MAC addresses.

Log Inspection

Provides visibility into important security events buried in log files.

Optimizes the identification of important security events buried in multiple log entries across the data center. Forwards suspicious events to a SIEM system or centralized logging server for correlation, reporting and archiving. Leverages and enhances open-source software available at OSSEC.

Deep Security Components

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

- **Deep Security Manager**, the centralized Web-based management console which administrators use to configure security policy and deploy protection to the enforcement components: the Deep Security Virtual Appliance and the Deep Security Agent.
- **Deep Security Virtual Appliance** is a security virtual machine built for VMware vSphere environments that provides Anti-Malware, Intrusion Prevention, Integrity Monitoring, Firewall, Web Application Protection and Application Control protection.
- **Deep Security Agent** is a security agent deployed directly on a computer which can provide Intrusion Prevention, Firewall, Web Application Protection, Application Control, Integrity Monitoring and Log Inspection protection.
    - **Relay:** The Relay module distributes updates to other Agents and Virtual Appliances. In Deep Security 9.5, Windows and Linux Agents have built-in Relay functionality which can be enabled or disabled. (Earlier versions of the Agents do not have this functionality and Relays are available as standalone install packages. These older versions of the Relay have embedded Agents to provide local protection on the host machine.)
- **Deep Security Notifier:** The Deep Security Notifier is a Windows System Tray application that communicates the state of the Deep Security Agent and Deep Security Relay on local computers.

Deep Security Manager

Deep Security Manager ("the Manager") is a powerful, centralized web-based management system that allows security administrators to create and manage comprehensive security policies and track threats and preventive actions taken in response to them. Deep Security Manager integrates with different aspects of the datacenter including: VMware vCenter, Microsoft Active Directory and has a web services API for integration with datacenter automation environments.

Policies

Policies are policy templates that specify the security rules to be configured and enforced automatically for one or more computers. These compact, manageable rule sets make it simple to provide comprehensive security without the need to manage thousands of rules. Default Policies provide the necessary rules for a wide range of common computer configurations.

Dashboard

The customizable, web-based UI makes it easy to quickly navigate and drill down to specific information. It provides:

- Extensive system, event and computer reporting, with drill-down capabilities
- Graphs of key metrics with trends, with drill-down
- Detailed event logs, with drill-down
- Ability to save multiple personalized dashboard layouts

Built-in Security

Role-based access allows multiple administrators (Users), each with different sets of access and editing rights, to edit and monitor different aspects of the system and receive information appropriate to them. Digital signatures are used to authenticate system components and verify the integrity of rules. Session encryption protects the confidentiality of information exchanged between components.

Deep Security Agent

The Deep Security Agent ("the Agent") is a high performance, small footprint, software component installed on a computer to provide protection.

Deep Security Virtual Appliance

The Deep Security Virtual Appliance ("the Appliance") runs as a VMware virtual machine and protects the other virtual machines on the same ESXi server, each with its own individual security policy.

Deep Security Relay

The Deep Security Relay is a server which relays Deep Security Updates from the Trend Micro global update server to the Deep Security system. By using Relays you can improve performance by distributing the task of delivering updates to the Manager, Appliances, and Agents of your Deep Security installation.

Note: *The Windows and Linux versions of the Deep Security 9.5 Agents have built-in Relay functionality which can be enabled from the* ***Computer Editor*** *window.*

Deep Security Notifier

The Deep Security Notifier is a Windows System Tray application that communicates the state of the Deep Security Agent to client machines. The Notifier displays pop-up user notifications when the Deep Security Agent begins a scan, or blocks malware or access to malicious web pages. The Notifier also provides a console utility that allows the user to view events and configure whether pop ups are displayed. The Notifier has a small footprint on the client machine, requiring less than 1MB of disk space and 1MB of memory.

What's New in Deep Security 9.5

vSphere 5.5 Support

- Security for Software-Defined Data Center NSX
- Support for mixed-model deployments (NSX and non-NSX)

Smarter, Lightweight Agent

- Lightweight installer
- Selective deployment of Protection Modules to Agents based on Security Policy requirements results in smaller Agent footprint
- Automatic support for new Linux Kernels

Trend Micro Control Manager Enhancements

- More dashboard widgets with drill-down capability
- Full Events for Anti-Malware and Web Reputation Service

Linux Support

- New distributions: Oracle Unbreakable
- On-demand Anti-Malware scanning for all distributions
- Real-Time Anti-Malware for Red Hat and SuSE

Improvements to Security and Software Update Management

- Improved visibility into Update status
- Improved accessibilty to Software Updates

User's Guide

Quick Start: System Configuration

This Quickstart Guide describes the initial basic Deep Security system configuration that is required before you can start protecting your computer resources.

To complete basic Deep Security system configuration, you will need to:

1. Make sure you have at least one Relay-enable Agent
2. Configure Deep Security's ability to retrieve Updates from Trend Micro
3. Check that you have a Scheduled Task to perform regular Updates
4. Set up email notification of important events

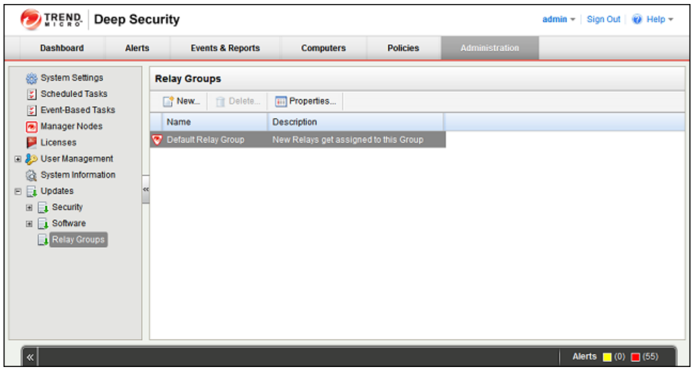
Make sure you have at least one Relay-enabled Agent

The Relay is responsible for retrieving Security Updates from Trend Micro and distributing them to your protected computers, therefore you must have at least one Relay available. See the Installation Guide for instructions if you do not.

Note: *The Windows (64-bit) and Linux (64-bit) versions of the Deep Security 9.5 Agents have built-in Relay functionality which can be enabled from the* ***Computer Editor*** *window.*

Note: *Relays are always organized into Relay Groups, even if it's only the one "Default Relay Group" to which all new Relays are assigned. You can create multiple Relay Groups if you have a large number of computers and want to create a hierarchical Relay structure or if your computers are spread out over large geographical areas. For more information on Relay Groups, see* ***Relay Groups (page 48)****.*

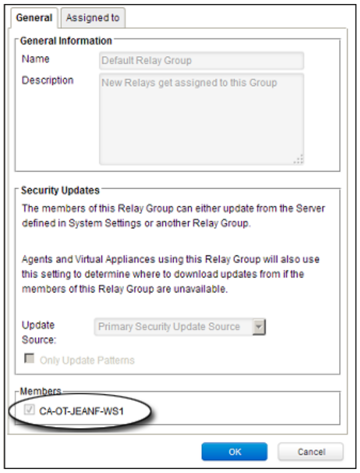
To view your Deep Security Relays, go to **Administration > Updates > Relay Groups**.



Name	Description
Default Relay Group	New Relays get assigned to this Group

This will display your current Relay Groups in the **Relay Groups** window. Usually you will only have the single **Default Relay Group**.

Double-click the Default Relay Group to display its **Relay Group Properties** window:



Name: Default Relay Group

Description: New Relays get assigned to this Group

The members of this Relay Group can either update from the Server defined in System Settings or another Relay Group.

Agents and Virtual Appliances using this Relay Group will also use this setting to determine where to download updates from if the members of this Relay Group are unavailable.

Update Source: Primary Security Update Source

□ Only Update Patterns

☑ CA-OT-JEANF-WS1

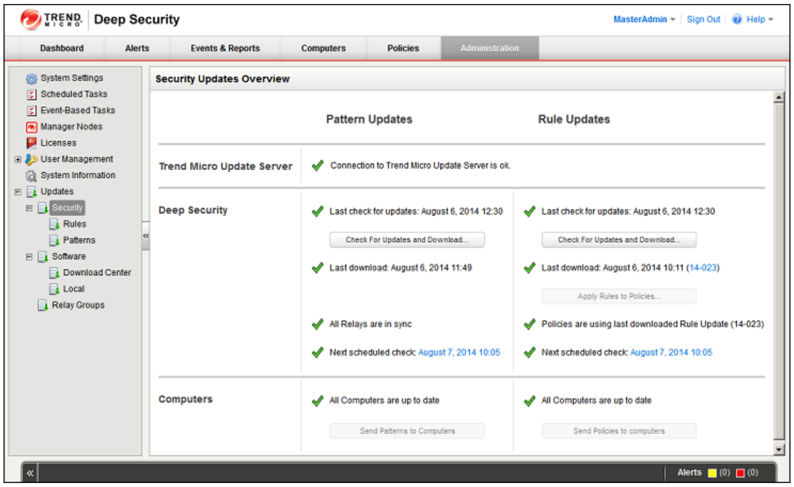
In the Members area of the **Relay Group Properties** window you'll see the Relays that are members of the group.

Note: *If there are no computers in the Members area see* ***Installing and Configuring a Relay-enabled Agent*** *in the Installation Guide.*

Configure Deep Security's ability to retrieve Updates from Trend Micro

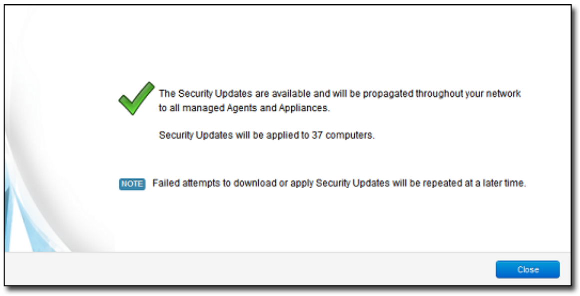
Now that you've confirmed that you have a Relay, you can check that it can retrieve updates from Trend Micro.

Go to the **Administration > Updates > Security** and click the **Check For Updates and Download** button under both **Pattern Updates** and **Rule Updates**.



	Pattern Updates	Rule Updates
Trend Micro Update Server	✓ Connection to Trend Micro Update Server is ok.	
Deep Security	✓ Last check for updates: August 6, 2014 12:30 ✓ Last download: August 6, 2014 11:49 ✓ All Relays are in sync ✓ Next scheduled check: August 7, 2014 10:05	✓ Last check for updates: August 6, 2014 12:30 ✓ Last download: August 6, 2014 10:11 (14-023) ✓ Policies are using last downloaded Rule Update (14-023) ✓ Next scheduled check: August 7, 2014 10:05
Computers	✓ All Computers are up to date	✓ All Computers are up to date

This will display the **Download Patterns** or **Download Rules** Wizard, which contacts the Trend Micro Update Servers, downloads the latest Security Updates, and distributes them to your computers. If the wizard displays a success message at its completion, it means your Relay computer can communicate with the Update servers:



The Security Updates are available and will be propagated throughout your network to all managed Agents and Appliances.

Security Updates will be applied to 37 computers.

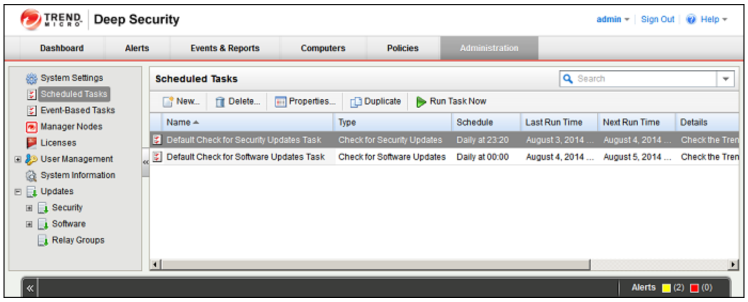
NOTE Failed attempts to download or apply Security Updates will be repeated at a later time.

Note: *If your Relays are unable to update their Components, see* ***Installing and Configuring a Relay-enabled Agent*** *in the Installation Guide.*

Check that you have a Scheduled Task to perform regular Updates

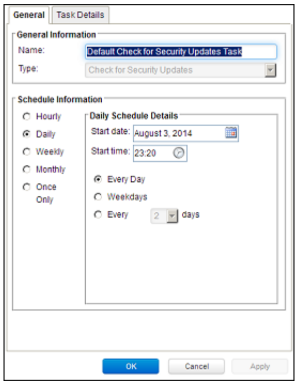
Now that you know your Relay can communicate with the Update servers, you should create a Scheduled Task which will regularly retrieve and distribute security Updates.

Go to **Administration > Scheduled Tasks**. You should see two default scheduled tasks: **Default Check for Security Updates Task** and **Default Check for Software Updates Task**:



Name	Type	Schedule	Last Run Time	Next Run Time	Details
Default Check for Security Updates Task	Check for Security Updates	Daily at 23:20	August 3, 2014 ...	August 4, 2014 ...	Check the Tren
Default Check for Software Updates Task	Check for Software Updates	Daily at 00:00	August 4, 2014 ...	August 5, 2014 ...	Check the Tren

Double-click a Scheduled Task to view its **Properties** window:



General Information

Name: Default Check for Security Updates Task

Type: Check for Security Updates

Schedule Information

○ Hourly
● Daily
○ Weekly
○ Monthly
○ Once Only

Daily Schedule Details

Start date: August 3, 2014

Start time: 23:20

● Every Day
○ Weekdays
○ Every 2 days

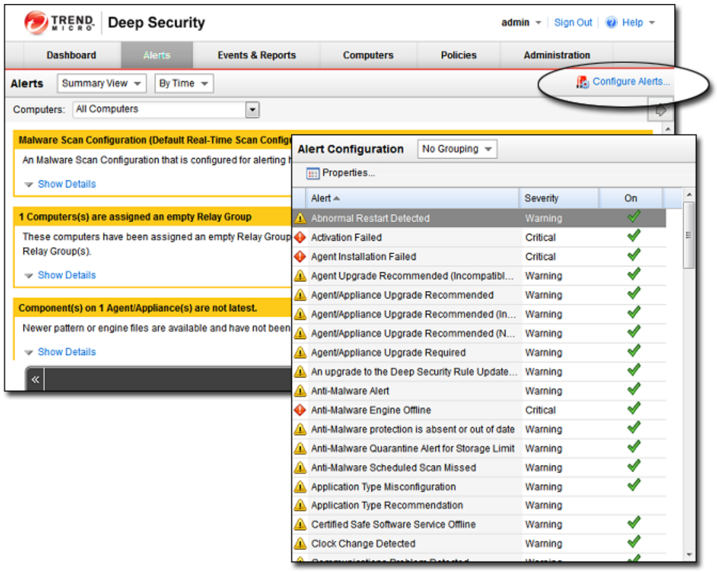
Notice that (in this case) the **Check for Security Updates** Scheduled Task is set to perform a Security Update everyday at 23:20.

Note: *If you don't have a* ***Default Check for Security Updates*** *Scheduled Task in your list, you can create one by clicking on* ***New*** *on the Scheduled Task page menu bar and following the instructions in the* ***New Scheduled Task*** *wizard.*

Set up email notification of important events

Deep Security Alerts are raised when situations occur that require special attention. Alerts can be raised due to security Events such as the detection of malware or an abnormal restart on a protected computer, or they can be system events like the Deep Security Manager running low on disk space. Deep Security can be configured to send email notifications when specific Alerts are raised.

To configure which Alerts will generate an email notification, go to the **Alerts** page and click **Configure Alerts...** to display the list of Deep Security Alerts:



Computers: All Computers

Malware Scan Configuration (Default Real-Time Scan Config

An Malware Scan Configuration that is configured for alerting h

Show Details

1 Computers(s) are assigned an empty Relay Group

These computers have been assigned an empty Relay Group Relay Group(s).

Show Details

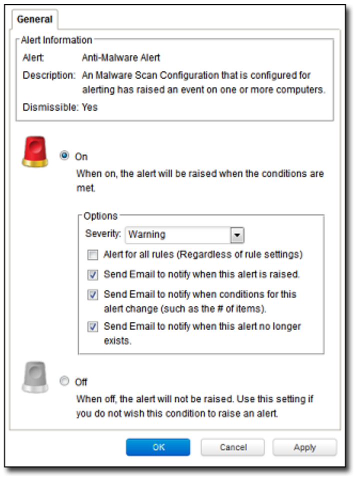
Component(s) on 1 Agent/Appliance(s) are not latest.

Newer pattern or engine files are available and have not been

Show Details

Alert	Severity	On
Abnormal Restart Detected	Warning	✓
Activation Failed	Critical	✓
Agent Installation Failed	Critical	✓
Agent Upgrade Recommended (Incompatibl...	Warning	✓
Agent/Appliance Upgrade Recommended	Warning	✓
Agent/Appliance Upgrade Recommended (In...	Warning	✓
Agent/Appliance Upgrade Recommended (N...	Warning	✓
Agent/Appliance Upgrade Required	Warning	✓
An upgrade to the Deep Security Rule Update...	Warning	✓
Anti-Malware Alert	Warning	✓
Anti-Malware Engine Offline	Critical	✓
Anti-Malware protection is absent or out of date	Warning	✓
Anti-Malware Quarantine Alert for Storage Limit	Warning	✓
Anti-Malware Scheduled Scan Missed	Warning	✓
Application Type Misconfiguration	Warning	✓
Application Type Recommendation	Warning	
Certified Safe Software Service Offline	Warning	✓
Clock Change Detected	Warning	✓

Double-click on an Alert see its **Properties** window where you can you can set the Alert options for email notification:



Alert Information

Alert: Anti-Malware Alert

Description: An Malware Scan Configuration that is configured for alerting has raised an event on one or more computers.

Dismissible: Yes

● On

When on, the alert will be raised when the conditions are met.

Options

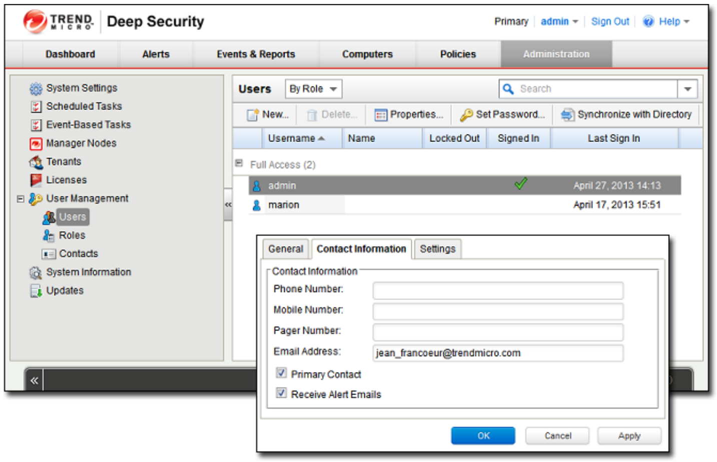
Severity: Warning

- ☐ Alert for all rules (Regardless of rule settings)
- ☑ Send Email to notify when this alert is raised.
- ☑ Send Email to notify when conditions for this alert change (such as the # of items).
- ☑ Send Email to notify when this alert no longer exists.

○ Off

When off, the alert will not be raised. Use this setting if you do not wish this condition to raise an alert.

Now you need to configure your User account to receive the email notifications Deep Security will send out. Go to **Administration > User Management > Users** and double-click on your User account to display its **Properties** window. Go to the **Contact Information** tab and enter an email address and select the **Receive Alert Emails** option:



Username	Name	Locked Out	Signed In	Last Sign In
Full Access (2)				
admin			✓	April 27, 2013 14:13
marion				April 17, 2013 15:51

Contact Information

Phone Number:

Mobile Number:

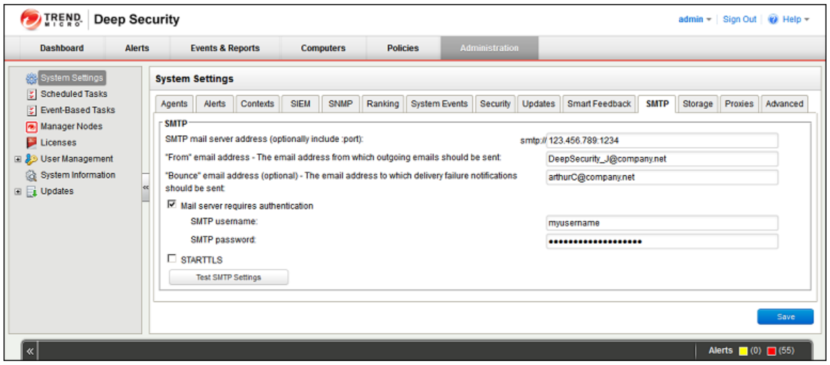
Pager Number:

Email Address: jean_francoeur@trendmicro.com

☑ Primary Contact

☑ Receive Alert Emails

In order for Deep Security to send email notification it has to be able to communicate with an SMTP server (access to an SMTP server is a requirement for email notifications). To connect the Deep Security Manager to your SMTP server, go to the **Administration > System Settings > SMTP** tab:



SMTP

SMTP mail server address (optionally include :port): smtp:// 123.456.789:1234

"From" email address - The email address from which outgoing emails should be sent: DeepSecurity_J@company.net

"Bounce" email address (optional) - The email address to which delivery failure notifications should be sent: arthurC@company.net

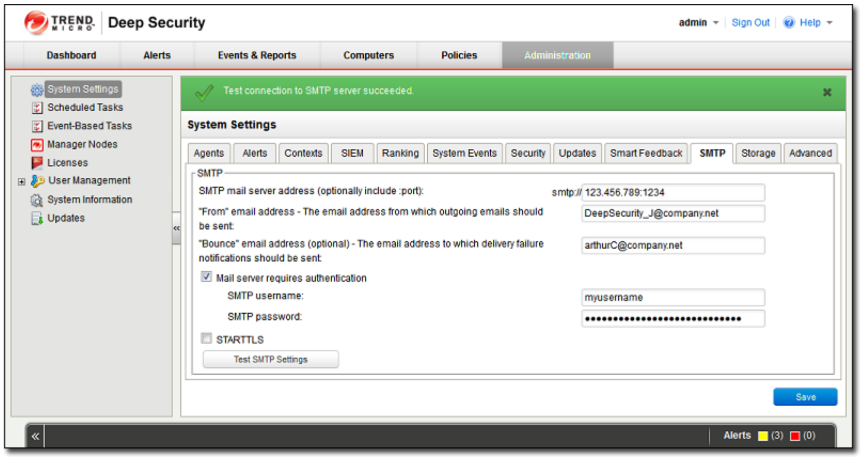
☑ Mail server requires authentication

SMTP username: myusername

SMTP password: ••••••••••••••••••

☐ STARTTLS

Complete the required fields in the **SMTP** area press test SMTP Settings at the bottom of the page when you're done. you should see a **Test connection to SMTP server succeeded** message:



✓ Test connection to SMTP server succeeded.

SMTP

SMTP mail server address (optionally include :port): smtp:// 123.456.789:1234

"From" email address - The email address from which outgoing emails should be sent: DeepSecurity_J@company.net

"Bounce" email address (optional) - The email address to which delivery failure notifications should be sent: arthurC@company.net

☑ Mail server requires authentication

SMTP username: myusername

SMTP password: ••••••••••••••••••••••••••••

☐ STARTTLS

Note: *If you unable to connect with your SMTP server, make sure the Manager can connect with the SMTP server on port 25.*

Basic Configuration is complete

This completes the basic Deep Security system configuration. Deep Security is now configured to regularly contact Trend Micro for security Updates and distribute those Updates on regular basis, and it will send you email notifications when Alerts are raised. Now you need to apply Deep Security protection to your computers. See ***QuickStart: Protecting a Computer (page 21)*** or ***Protecting a Mobile Laptop (page 155)*** for a quick guide to protecting those two kinds of computer resources.

Quick Start: Protecting a Computer

The following describes the steps involved in using Deep Security to protect a Windows Server 2008 computer.

It will involve the following steps:

1. Adding the computer to the Deep Security Manager.
2. Configuring and running a Recommendation Scan
3. Automatically implement scan recommendations
4. Create a Scheduled task to perform regular Recommendation Scans
5. Monitor Activity Using the Deep Security Manager

Note: *We will assume that you have already installed the Deep Security Manager on the computer from which you intend to manage the Deep Security Agents throughout your network. We will also assume that* ***you have imported the Agent software package (.zip) into Deep Security Manager and installed (but not activated) Deep Security Agent on the computer you wish to protect****. And finally, we will assume that you have a Relay-enabled Agent available from which Deep Security can download the latest Security Updates. If any of these requirements are not in place, consult the Installation Guide for instructions to get to this stage.*

Adding the computer to the Deep Security Manager

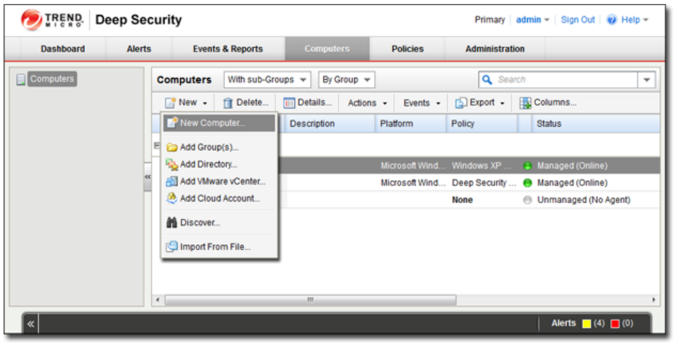
There are several ways of adding computers to the Deep Security Manager's **Computers** page. You can add computers by:

- Adding computers individually from a local network by specifying their IP addresses or hostnames
- Discovering computers on a local network by scanning the network
- Connecting to a Microsoft Active Directory and importing a list of computers
- Connecting to a VMware vCenter and importing a list of computers
- Connecting to computing resources from the following Cloud Provider services:
    - Amazon EC2
    - VMware vCloud

For the purposes of this exercise, we will add a computer from a local network but once a computer is added to the Manager, the protection procedures are the same regardless of where the computer is located.

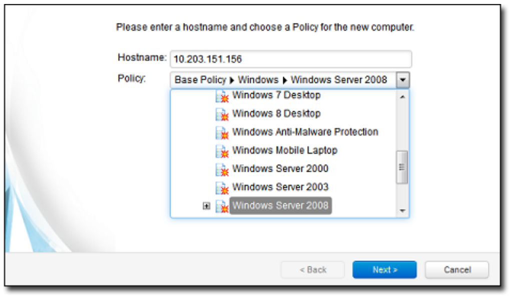
To add a computer from a local network:

1. In the Deep Security Manager console, go to the **Computers** page and click **New** in the toolbar and select **New Computer...** from the drop-down menu.



Description	Platform	Policy	Status
	Microsoft Wind...	Windows XP ...	Managed (Online)
	Microsoft Wind...	Deep Security ...	Managed (Online)
		None	Unmanaged (No Agent)

2. In the **New Computer** wizard, enter the hostname or IP address of the computer and select an appropriate security Policy to apply from the Policy tree in the drop-down menu. (In this case we will select the **Windows Server 2008** Policy.) Click **Next**.

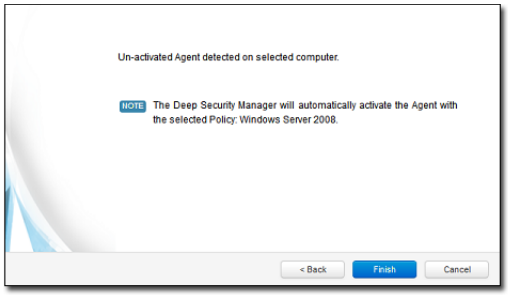


Please enter a hostname and choose a Policy for the new computer.

Hostname: 10.203.151.156

Policy: Base Policy ▸ Windows ▸ Windows Server 2008

3. The wizard will contact the computer, add it to the Computers page, detect the unactivated Agent, activate it, and apply the selected Policy. Click **Finish**.

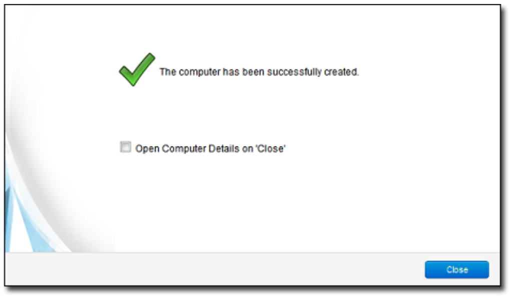


Un-activated Agent detected on selected computer.

NOTE The Deep Security Manager will automatically activate the Agent with the selected Policy: Windows Server 2008.

Note: *An Agent can be configured to automatically initiate its own activation upon installation. For details, see* ***Command-Line Utilities (page 167)****.*

4. When the computer has been added the wizard will display a confirmation message:



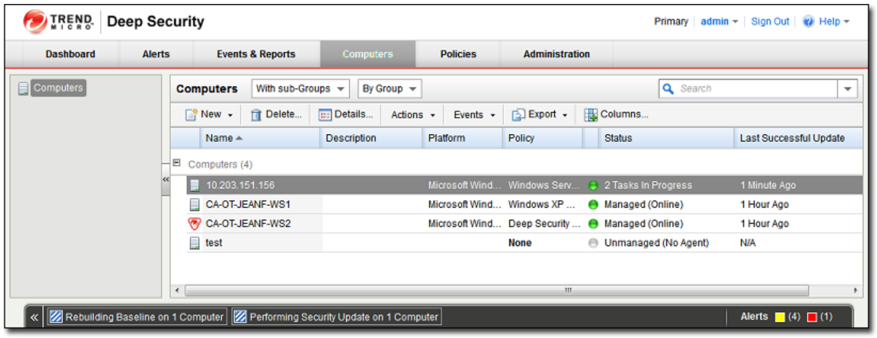
The computer has been successfully created.

□ Open Computer Details on 'Close'

5. Deselect the **Open Computer Details on 'Close'** option and click **Close**.

The computer now appears in the Deep Security Manager's list of managed computers on the **Computers** page.

Deep Security will automatically download the latest Security Updates to the computer after activation. As well, the **Windows Server 2008** Policy that was assigned to the computer has Integrity Monitoring enabled and so it will start to Build an Integrity Monitoring baseline for the computer. You can see activities currently being carried out in the status bar of the Manager window:



Name	Description	Platform	Policy	Status	Last Successful Update
10.203.151.156		Microsoft Wind...	Windows Serv...	2 Tasks In Progress	1 Minute Ago
CA-OT-JEANF-WS1		Microsoft Wind...	Windows XP ...	Managed (Online)	1 Hour Ago
CA-OT-JEANF-WS2		Microsoft Wind...	Deep Security ...	Managed (Online)	1 Hour Ago
test			None	Unmanaged (No Agent)	N/A

Rebuilding Baseline on 1 Computer

Performing Security Update on 1 Computer

Once Deep Security Manager has completed its initial post-activation tasks, the computer's **Status** should display as **Managed (Online)**.

Note: *More information is available for each page in the Deep Security Manager by clicking the **Help** button in the menu bar.*

Configuring and Running a Recommendation Scan

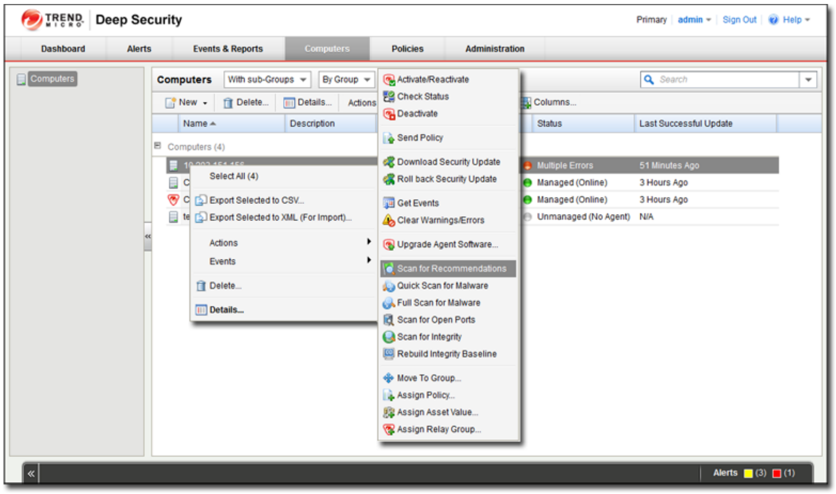
The security Policy that we assigned to the computer is made up of a collection of Rules and settings designed for a computer running the Windows Server 2008 operating system. However, a static Policy can soon fall out of date. This can be because of new software being installed on the computer, new operating system vulnerabilities being discovered for which Trend Micro has created new protection Rules, or even because a previous vulnerability was corrected by an operating system or software service pack. Because of the dynamic nature of the security requirements on a computer, you should regularly run Recommendation Scans which will assess the current state of the computer and compare it against the latest Deep Security protection module updates to see if the current security Policy needs to be updated.

Recommendation Scans make recommendations for the following protection modules:

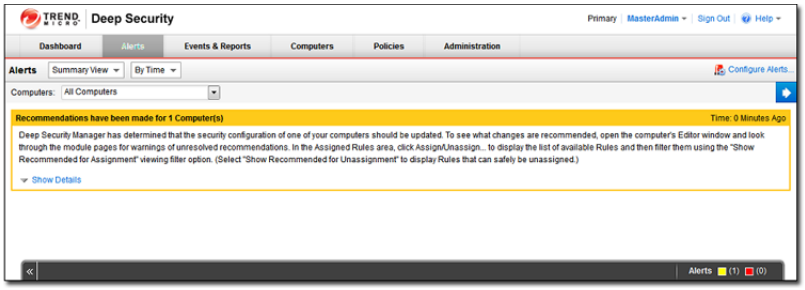
- **Intrusion Prevention**
- **Integrity Monitoring**
- **Log Inspection**

To run a Recommendation Scan on your computer:

1. Go to the Computers page in the main Deep Security Manager console window.
2. Right-click on your computer and select **Actions > Scan for Recommendations**:



During the Recommendation Scan, your computer's Status will display **Scanning for Recommendations**. When the scan is finished, if Deep Security has any recommendations to make, you will see an Alert on the Alerts screen:



Computers: All Computers

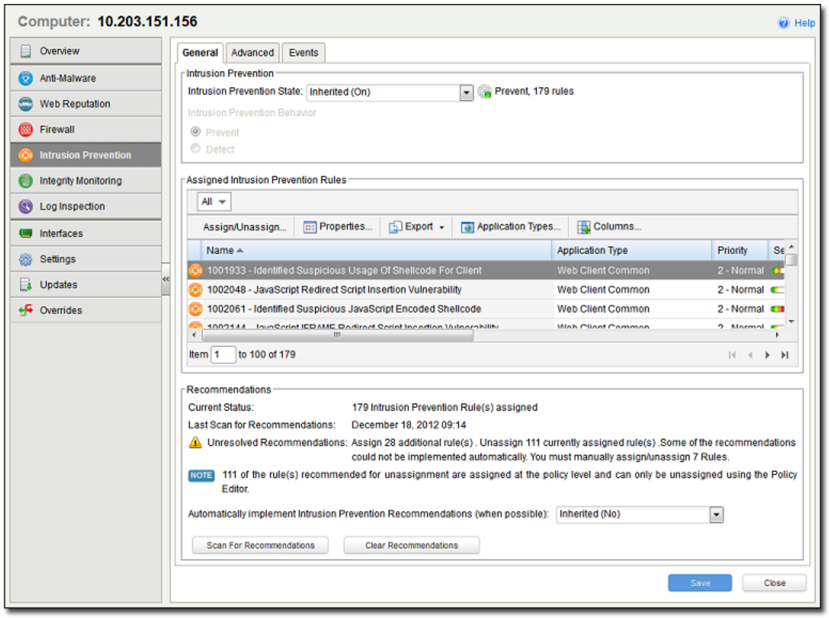
Recommendations have been made for 1 Computer(s) Time: 0 Minutes Ago

Deep Security Manager has determined that the security configuration of one of your computers should be updated. To see what changes are recommended, open the computer's Editor window and look through the module pages for warnings of unresolved recommendations. In the Assigned Rules area, click Assign/Unassign... to display the list of available Rules and then filter them using the "Show Recommended for Assignment" viewing filter option. (Select "Show Recommended for Unassignment" to display Rules that can safely be unassigned.)

To see the results of the Recommendation Scan:

1. Open the computer editor for your computer (**Details...** in the **Computers** page menu bar or from the right-click menu.)
2. In the computer editor window, go to the **Intrusion Prevention** module page.

In the **Recommendations** area of the **General** tab, you'll see the results of the scan:



Intrusion Prevention State: Inherited (On) Prevent, 179 rules

Name	Application Type	Priority
1001933 - Identified Suspicious Usage Of Shellcode For Client	Web Client Common	2 - Normal
1002048 - JavaScript Redirect Script Insertion Vulnerability	Web Client Common	2 - Normal
1002061 - Identified Suspicious JavaScript Encoded Shellcode	Web Client Common	2 - Normal
1002144 - JavaScript IFRAME Redirect Script Insertion Vulnerability	Web Client Common	2 - Normal

Item 1 to 100 of 179

Current Status: 179 Intrusion Prevention Rule(s) assigned

Last Scan for Recommendations: December 18, 2012 09:14

Unresolved Recommendations: Assign 28 additional rule(s) . Unassign 111 currently assigned rule(s) .Some of the recommendations could not be implemented automatically. You must manually assign/unassign 7 Rules.

NOTE 111 of the rule(s) recommended for unassignment are assigned at the policy level and can only be unassigned using the Policy Editor.

Automatically implement Intrusion Prevention Recommendations (when possible): Inherited (No)

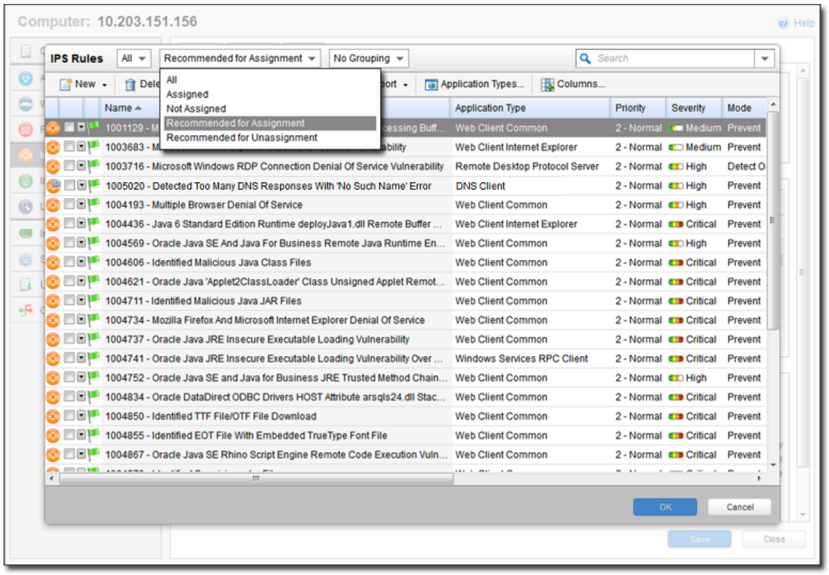
The **Current Status** tells us that there are currently 179 Intrusion Prevention Rules assigned to this computer.

Last Scan for Recommendations tells us that the last scan took place on December 18th, 2012, at 09:14.

Unresolved Recommendations tells us that as a result of the scan, Deep Security recommends assigning an additional 28 Intrusion Prevention Rules and unassigning 111 currently assigned Rules.

The **Note** informs us that 111 of the Rules recommended for unassignment (all of them as it turn out) have been assigned at the Policy level (rather than directly here on the computer level). Rules that have been assigned at a level higher up the Policy tree can only be unassigned in the Policy where they were assigned -- in this case, the Windows Server 2008 Policy. (If we had opened the **Windows Server 2008** Policy editor, we would have seen the same recommendations and we could have unassigned them from there.)

We are also told that 7 of the Rules that are recommended for assignment can't be automatically assigned. Usually these are either Rules that require configuration or Rules that are prone to false positives and whose behavior should be observed in detect-only mode being being enforced in prevent mode. To see which Rules have been recommended for assignment, click **Assign/Unassign...** to display the **IPS Rules** rule assignment modal window. Then select Recommended for Assignment from the second drop-down filter list:



Name ▲	Application Type	Priority	Severity	Mode
1001129 - M … cessing Buff...	Web Client Common	2 - Normal	Medium	Prevent
1003683 - M … ability	Web Client Internet Explorer	2 - Normal	Medium	Prevent
1003716 - Microsoft Windows RDP Connection Denial Of Service Vulnerability	Remote Desktop Protocol Server	2 - Normal	High	Detect O
1005020 - Detected Too Many DNS Responses With 'No Such Name' Error	DNS Client	2 - Normal	High	Prevent
1004193 - Multiple Browser Denial Of Service	Web Client Common	2 - Normal	High	Prevent
1004436 - Java 6 Standard Edition Runtime deployJava1.dll Remote Buffer ...	Web Client Internet Explorer	2 - Normal	Critical	Prevent
1004569 - Oracle Java SE And Java For Business Remote Java Runtime En...	Web Client Common	2 - Normal	High	Prevent
1004606 - Identified Malicious Java Class Files	Web Client Common	2 - Normal	Critical	Prevent
1004621 - Oracle Java 'Applet2ClassLoader' Class Unsigned Applet Remot...	Web Client Common	2 - Normal	Critical	Prevent
1004711 - Identified Malicious Java JAR Files	Web Client Common	2 - Normal	Critical	Prevent
1004734 - Mozilla Firefox And Microsoft Internet Explorer Denial Of Service	Web Client Common	2 - Normal	Critical	Prevent
1004737 - Oracle Java JRE Insecure Executable Loading Vulnerability	Web Client Common	2 - Normal	Critical	Prevent
1004741 - Oracle Java JRE Insecure Executable Loading Vulnerability Over ...	Windows Services RPC Client	2 - Normal	Critical	Prevent
1004752 - Oracle Java SE and Java for Business JRE Trusted Method Chain...	Web Client Common	2 - Normal	High	Prevent
1004834 - Oracle DataDirect ODBC Drivers HOST Attribute arsqls24.dll Stac...	Web Client Common	2 - Normal	Critical	Prevent
1004850 - Identified TTF File/OTF File Download	Web Client Common	2 - Normal	Critical	Prevent
1004855 - Identified EOT File With Embedded TrueType Font File	Web Client Common	2 - Normal	Critical	Prevent
1004867 - Oracle Java SE Rhino Script Engine Remote Code Execution Vuln...	Web Client Common	2 - Normal	Critical	Prevent

Rules that require configuration are identified by an icon with a small configuration badge (⚙). To see the configurable options for a Rule, double-click the Rule to open its **Properties** window (in local editing mode) and go to the **Configuration** tab. To Assign a Rule, select the checkbox next to its name.

To view Rules that are recommended for *unassignment*, filter the list of Rules by selecting **Recommended for Unassignment** from the same drop-down list. To unassign a Rule, deselect the checkbox next to its name.

Note: *Rules that are in effect on a computer because they have been assigned in a Policy higher up the policy tree can't be unassigned locally. The only way to unassign such Rules is to edit the Policy where they were originally assigned and unassign them from there. For more information on this kind of Rule inheritance, see* ***Policies, Inheritance and Overrides (page 257)****.*

Automatically implement scan recommendations

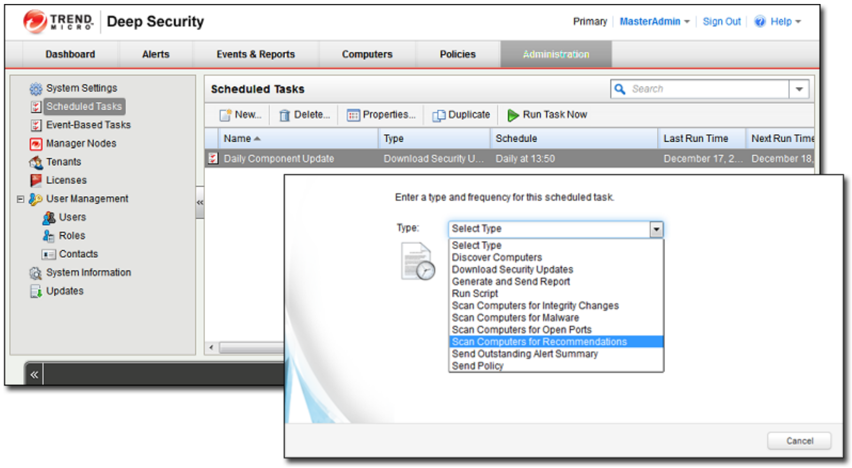
You can configure Deep Security to automatically assign and unassign Rules after a Recommendation Scan. To do so, open the computer or Policy editor and go to the individual protection module pages that support Recommendation Scans (Intrusion, Prevention, Integrity Monitoring, and Log Inspection). In the Recommendation area on the General tab, set **Automatically implement Intrusion Prevention Recommendations (when possible):** to Yes.

Create a Scheduled task to perform regular Recommendation Scans

Performing regular Recommendation Scans ensures that your computers are protected by the latest relevant Rule sets and that those that are no longer required are removed. You can create a Scheduled Task to carry out this task automatically.

To create a Scheduled Task:

1. In the main Deep Security Manager window, go to **Administration > Scheduled Tasks**
2. In the menu bar, click **New** to display the **New Scheduled Task** wizard.



Name ▲	Type	Schedule	Last Run Time	Next Run Time
Daily Component Update	Download Security U...	Daily at 13:50	December 17, 2...	December 18,

Enter a type and frequency for this scheduled task.

3. Select **Scan Computers for Recommendations** as the scan type and select **Weekly** recurrence. Click **Next**.
4. Select a start time, select every 1 week, and select a day of the week. Click **Next**.
5. When specifying which computers to Scan, select the last option (**Computer**) and select the Windows Server 2008 computer we are protecting. Click **Next**.
6. Type a name for the new Scheduled Task. Leave the **Run task on 'Finish'** unchecked (because we just ran a Recommendation Scan). Click **Finish**.

The new Scheduled task now appears in the list of Scheduled Tasks. It will run once a week to scan your computer and make recommendations for you computer. If you have set **Automatically implement Recommendations** for each of the three protection modules that support it, Deep Security will assign and unassign Rules are required. If Rules are identified that require special attention, an Alert will be raised to notify you.

Note: *With Agent-based protection, scheduled tasks use the same time zone as the endpoint operating system. With Agentless protection, scheduled tasks use the same time zone as the Deep Security Virtual Appliance.*

Schedule Regular Security Updates

If you follow the steps described in ***Quick Start: System Configuration (page 15)***, your computer will now be regularly updated with the latest protection from Trend Micro.

Monitor Activity Using the Deep Security Manager

The Dashboard

After the computer has been assigned a Policy and has been running for a while, you will want to review the activity on that computer. The first place to go to review activity is the Dashboard. The Dashboard has many information panels ("widgets") that display different types of information pertaining to the state of the Deep Security Manager and the computers that it is managing.

At the top right of the Dashboard page, click **Add/Remove Widgets** to view the list of widgets available for display.

For now, we will add the following widgets from the **Firewall** section:

- Firewall Activity (Prevented)
- Firewall IP Activity (Prevented)
- Firewall Event History [2x1]

Select the checkbox beside each of the three widgets, and click **OK**. The widgets will appear on the dashboard. (It may take a bit of time to generate the data.)

- The **Firewall Activity (Prevented)** widget displays a list of the most common reasons for packets to be denied (that is, blocked from reaching a computer by the Agent on that computer) along with the number of packets that were denied. Items in this list will be either types of Packet Rejections or Firewall Rules. Each "reason" is a link to the corresponding logs for that denied packet.
- The **Firewall IP Activity (Prevented)** widget displays a list of the most common source IPs of denied packets. Similar to the **Firewall Activity (Prevented)** widget, each source IP is a link to the corresponding logs.
- The **Firewall Event History [2x1]** widget displays a bar graph indicating how many packets were blocked in the last 24 hour period or seven day period (depending on the view selected). Clicking a bar will display the corresponding logs for the period represented by the bar.

Note: *Note the trend indicators next to the numeric values in the **Firewall Activity (Prevented)** and **Firewall IP Activity (Prevented)** widgets. An upward or downward pointing triangle indicates an overall increase or decrease over the specified time period, and a flat line indicates no significant change.*

Logs of Firewall and Intrusion Prevention Events

Now drill-down to the logs corresponding to the top reason for Denied Packets: in the **Firewall Activity (Prevented) widget**, click the first reason for denied packets (in the picture above, the top reason is "Out of Allowed Policy"). This will take you to the **Firewall Events** page.

The **Firewall Events** page will display all Firewall Events where the **Reason** column entry corresponds to the first reason from the **Firewall Activity (Prevented) widget** ("Out of Allowed Policy"). The logs are filtered to display only those events that occurred during the view period of the Dashboard (Last 24 hours or last seven days). Further information about the **Firewall Events** and **Intrusion Prevention Events** page can be found in the help pages for those pages.

Note: *For the meaning of the different packet rejection reasons, see **Firewall Events (page 211)** and **Intrusion Prevention Events (page 209)**.*

Reports

Often, a higher-level view of the log data is desired, where the information is summarized, and presented in a more easily understood format. The **Reports** fill this Role, allowing you to display detailed summaries on computers, Firewall and Intrusion Prevention Event Logs, Events, Alerts, etc. In the **Reports** page, you can select various options for the report to be generated.

We will generate a **Firewall Report**, which displays a record of Firewall Rule and Firewall Stateful Configuration activity over a configurable date range. Select **Firewall Report** from the Report drop-down. Click **Generate** to launch the report in a new window.

By reviewing scheduled reports that have been emailed by the Deep Security Manager to Users, by logging into the system and consulting the dashboard, by performing detailed investigations by drilling-down to specific logs, and by configuring Alerts to notify Users of critical events, you can remain apprised of the health and status of your network.

System

- ***Secure the Deep Security Manager (page 29)*** describes how to protect the Deep Security Manager with an agent.
- ***Communication (page 30)*** describes how the different Deep Security components communicate with each other.
- ***Customize the Dashboard (page 32)*** describes how to create custom dashboard layout for yourself or other Users.
- ***Email Notifications (page 36)*** describes how to configure Deep Security to send email notifications of important Deep Security Events to various users.
- ***Alerts (page 37)*** describes how to configure which events will raise Alerts, what the severity of those Alerts will be, and whether notifications of the Alerts are sent out by email.
- ***Port Scan Settings (page 39)*** describes how to set which port are scanned during one of Deep Security's Port Scans.
- ***Syslog Integration (SIEM) (page 40)*** describes how to configure Deep Security to send Events to a SIEM via Syslog.
- ***Relay Groups (page 48)*** describes how to configure and use Relay Groups to automate the process of keeping your Deep Security system updated with the latest security and software updates from Trend Micro.
- ***Security Updates (page 51)*** describes how to manage Deep Security Security Updates.
- ***Software Updates (page 55)*** describes how to manage Deep Security software updates.
- ***Virtual Appliance Scan Caching (page 56)*** describes how to take advantage of the Deep Security Appliance's scan caching ability which significantly improves the performance of Malware and Integrity scanning on virtual machines.
- ***User Management (page 58)*** describes how to manage Users of Deep Security including how to use role-based access control to restrict the access of Users specific areas of Deep Security and your network.
- ***Database Backup and Recovery (page 63)*** describes how to perform (and automate) a backup of your Deep Security data.

Secure the Deep Security Manager

Protecting the Deep Security Manager with an Agent

Protect Deep Security Manager by installing an Agent on its host computer and apply **the Deep Security Manager** Policy.

Configuring an Agent on the Deep Security Manager's computer

1. Install an Agent on the same computer as the Manager.
2. On the **Computers** page, add the Manager's computer. Do not choose to apply a Policy at this time.
3. Double-click the new computer in the **Computers** page to display its **Details** window and go to **Intrusion Prevention > Advanced > SSL Configurations**.
4. A listing of the SSL Configurations for this computer will be displayed. Click **New** to start the wizard to create a new SSL Configuration.
5. Specify the interface used by the Manager. Click **Next**.
6. On the **Port** page, choose to protect the port used by the Deep Security Manager Web Application GUI over HTTPS. (4119 by default, unless you chose another port during installation. To confirm which port the Manager is using, check the URL you're using to access it.) Click **Next**.
7. Specify whether SSL Intrusion Prevention analysis should take place on all IP addresses for this Computer, or just one. (This feature can be used to set up multiple virtual computers on a single computer.)
8. Next, choose to "Use the SSL Credentials built into the Deep Security Manager". (This option only appears when creating an SSL Configuration for the Manager's computer.) Click **Next**.
9. Finish the wizard and close the **SSL Configuration** page.
10. Back in the computer's **Details** window, apply the **Deep Security Manager Policy**, which includes the Firewall Rules and Intrusion Prevention Rules required for the Deep Security Manager to operate on port 4119.

You have now protected the Manager's computer and are now filtering the traffic (including SSL) to the Manager.

Note: *After configuring the Agent to filter SSL traffic, you may notice that the Deep Security Agent will return several **Renewal Error** events. These are certificate renewal errors caused by the new SSL certificate issued by the Manager computer. You should therefore restart your browser session with the Manager to acquire the new certificate from the Manager computer.*

The **Deep Security Manager** Policy has the basic Firewall Rules assigned to enable remote use of the Manager. Additional Firewall Rules may need to be assigned if the Manager's computer is being used for other purposes. The Policy also includes the Intrusion Prevention Rules in the **Web Server Common** Application Type. Additional Intrusion Prevention Rules can be assigned as desired.

Because the **Web Server Common** Application Type typically filters on the **HTTP** Port List and does not include port 4119, port 4119 is added as an override to the ports setting in the **Intrusion Prevention Rules** page of the Policy's **Details** window.

For more information on SSL data inspection, see ***SSL Data Streams (page 126)***.

Communication

Who Initiates Communication

At the default setting (**Bidirectional**), the Agent/Appliance will initiate the heartbeat but will still listen on the Agent port for Manager connections and the Manager is free to contact the Agent/Appliance in order to perform operations as required.

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

Manager Initiated means that the Manager will initiate all communications. Communication will occur when the Manager performs scheduled updates, performs heartbeat operations (below), and when you choose the **Activate/Reactivate** or **Update Now** options from the Manager interface. If you are isolating the computer from communications initiated by remote sources, you can choose to have the Agent itself periodically check for updates and control heartbeat operations. If this is the case, select **Agent/Appliance Initiated**.

Note: *Communication between the Deep Security Manager and the Agent/Appliance takes place over SSL/TLS using the FIPS recognized symmetric encryption algorithm AES-256 and the hash function SHA-256.*

Note: *The following information is collected by the Manager during a heartbeat: the status of the drivers (on- or off-line), the status of the Agent/Appliance (including clock time), Agent/Appliance logs since the last heartbeat, data to update counters, and a fingerprint of the Agent/Appliance security configuration (used to determine if it is up to date). You can change how often heartbeats occur (whether Agent/Appliance or Manager initiated), and how many missed heartbeats can elapse before an Alert is triggered.*

This setting (like many other settings) can be configured at multiple levels: on all computers to which a Policy has been assigned by configuring it on the Base Policy (the parent Policy of all Policies), by setting it it on a Policy further down the Policy tree along the branch that leads to your computer, or on an individual computer.

To configure Communication Direction in a Policy:

1. Open the Policy Editor (the **Details** window) of the Policy whose communications settings you want to configure.
2. Go to **Settings > Computer > Communication Direction.**
3. In the **Direction of Deep Security Manager to Agent/Appliance communication** drop-down menu, select one of the three options ("Manager Initiated", "Agent/Appliance Initiated", or "Bidirectional"), or choose "Inherited". If you select "Inherited", the Policy will inherit the setting from its parent Policy in the Policy hierarchy. Selecting one of the other options will override the inherited setting.
4. Click **Save** to apply the changes.

To configure Communication Direction on a specific computer:

1. Open the Computer Editor(the **Details** window) of the computer whose communications settings you want to configure.
2. Go to **Settings > Computer > Communication Direction.**
3. In the "Direction of Deep Security Manager to Agent/Appliance communication: "drop-down menu, select one of the three options ("Manager Initiated", "Agent/Appliance Initiated", or "Bidirectional"), or choose "Inherited". If you select "Inherited", the computer will inherit its setting from the Policy that has been applied it. Selecting one of the other options will override the inherited setting.
4. Click **Save** to apply the changes.

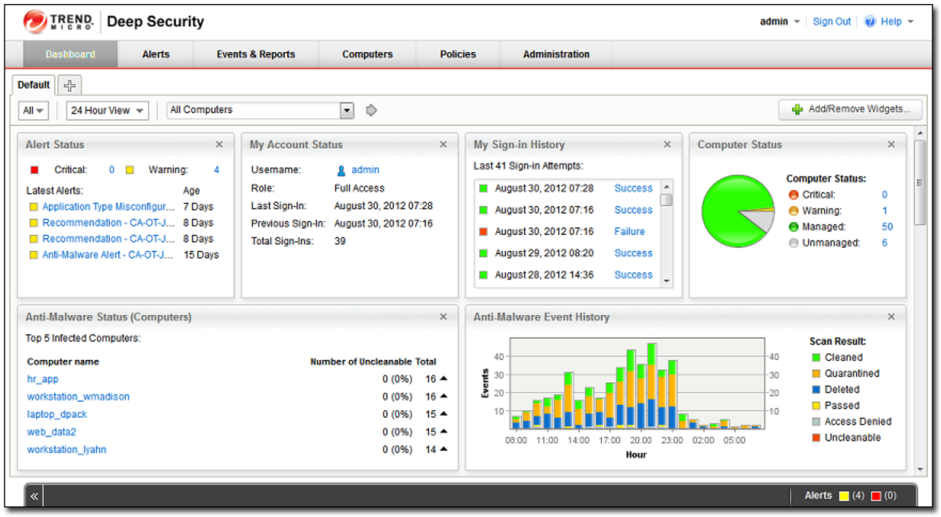
Note: *Agents/Appliances look for the Deep Security Manager on the network by the Manager's hostname. Therefore the Manager's hostname **must** be in your local DNS for Agent/Appliance-initiated or bidirectional communication to work.*

See also:

- ***Policies, Inheritance and Overrides (page 257)***

Customize the Dashboard

The Dashboard is the first page that comes up after you sign in to the Deep Security Manager. Several aspects of the dashboard can be configured and customized, and layouts can be saved and displayed when you sign in. (The dashboard will be displayed as you left it when you logged out, regardless of whether another User has logged in in the meantime and made changes to their layout.)



Alert Status

Critical: 0 Warning: 4

Latest Alerts:	Age
Application Type Misconfigur...	7 Days
Recommendation - CA-OT-J...	8 Days
Recommendation - CA-OT-J...	8 Days
Anti-Malware Alert - CA-OT-J...	15 Days

My Account Status

Username: admin
Role: Full Access
Last Sign-In: August 30, 2012 07:28
Previous Sign-In: August 30, 2012 07:16
Total Sign-Ins: 39

My Sign-in History

Last 41 Sign-in Attempts:

August 30, 2012 07:28	Success
August 30, 2012 07:16	Success
August 30, 2012 07:16	Failure
August 29, 2012 08:20	Success
August 28, 2012 14:36	Success

Computer Status

Computer Status:
Critical: 0
Warning: 1
Managed: 50
Unmanaged: 6

Anti-Malware Status (Computers)

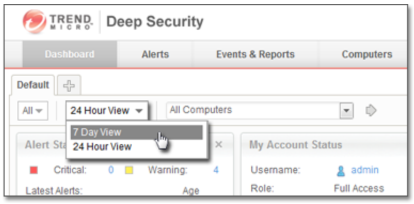
Top 5 Infected Computers:

Computer name	Number of Uncleanable	Total
hr_app	0 (0%)	16 ▲
workstation_wmadison	0 (0%)	16 ▲
laptop_dpack	0 (0%)	15 ▲
web_data2	0 (0%)	15 ▲
workstation_lyahn	0 (0%)	14 ▲

Configurable elements of the Dashboard display are the time period the data is taken from, which computers' or computer groups' data is displayed, which "widgets" are displayed, and the layout of those widgets on the page.

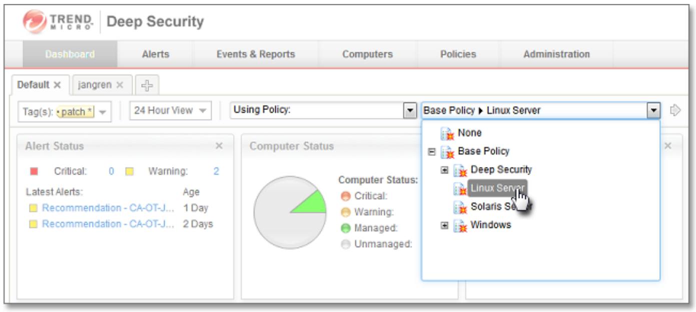
Date/Time Range

The Dashboard displays data from either the last 24 hours, or the last seven days.



Computers and Computer Groups

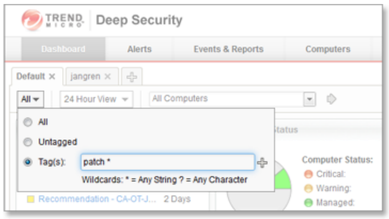
Use the **Computer:** drop-down menu to filter the displayed data to display only data from specific computers. For example, only those using the **Linux Server** security Policy:



Filter by Tags

In Deep Security, a **Tag** is a unit of meta-data that you can apply to an Event in order to create an additional attribute for the Event that is not originally contained within the Event itself. Tags can be used to filter Events in order to simplify the task of Event monitoring and management. A typical use of tagging is to distinguish between Events that require action and those that have been investigated and found to be benign.

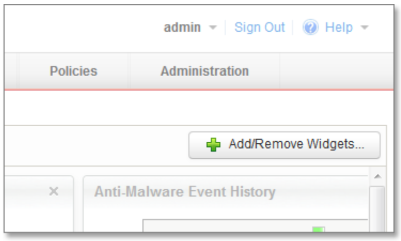
The data displayed in the Dashboard can be filtered by tags:



For more information on tagging see ***Event Tagging (page 133)***.

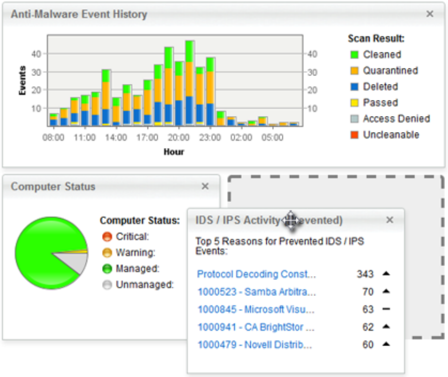
Select Dashboard Widgets

Click the **Add/Remove Widgets...** link to display the widget selection window and choose which widgets to display.



Changing the Layout

The selected widgets can be moved around the dashboard by dragging them by their title bar. Move the widget over an existing one and they will exchange places. (The widget that is about to be displaced will temporarily gray out.)

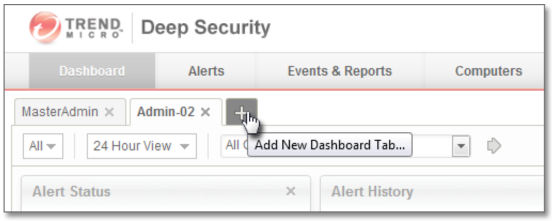


Top 5 Reasons for Prevented IDS / IPS Events:

Protocol Decoding Const...	343	▲
1000523 - Samba Arbitra...	70	▲
1000845 - Microsoft Visu...	63	—
1000941 - CA BrightStor ...	62	▲
1000479 - Novell Distrib...	60	▲

Save and Manage Dashboard Layouts

You can create multiple dashboard layouts and save them as separate tabs. Your Dashboard settings and layouts will not be visible to other Users after you sign out. To create a new Dashboard tab, click the "plus" symbol to the right of the last tab on the Dashboard:



Event Logging and Data Collection

By default, Deep Security Manager collects Events from the Agents/Appliances at every heartbeat. The amount of data being collected depends on the number of computers begin protected, how active your computers are, and the Event recording settings.

System Events

All the Deep Security System Events are listed and can be configured on the **Administration > System Settings > System Events** tab. You can set whether to record the individual Events and whether to forward them to a SIEM system.

Security Events

Each protection module generates Events when Rules are triggered or other configuration conditions are met. Some of this security Event generation is configurable.

The Firewall Stateful Configuration in effect on a computer can be modified to enable or disable TCP, UDP, and ICMP Event logging. To edit the properties of a Stateful firewall Configuration, go to **Policies > Common Objects > Other > Firewall Stateful Configurations**. The logging options are in the **TCP**, **UDP**, and **ICMP** tabs of the Firewall Stateful Configuration's **Properties** window.

The Intrusion Prevention module lets you disable Event logging for individual Rules. To disable Event logging for a Rule, open the Rule's **Properties** window and select **Disable Event Logging** on the **Events** area of the **General** tab.

The Intrusion Prevention module can record the data that causes a Rule to trigger. Because it would be impractical to record all the data every time an individual Rule triggers, Deep Security will only record the data for a Rule the first time it is triggered within a specified period of time (default is five minutes). To configure whether Deep Security will record this data, go to **Policy/Computer Editor > Intrusion Prevention > Advanced > Event Data**. You can configure the length of the period by adjusting the **Period for Log only one packet within period** setting in **Policy/Computer Editor > Settings > Network Engine > Advanced Network Engine Settings.**

The Log Inspection Module can be configured to only record events if a Log Inspection Rule is triggered which contains a condition that exceeds a specified Severity Level. To set the Severity Level at which Log Inspection Events will begin to be recorded, go to **Policy/Computer Editor > Log Inspection > Advanced Severity Clipping**.

Here are some suggestion to help maximize the effectiveness of Event collection:

- Reduce or disable log collection for computers that are not of interest.
- Consider reducing the logging of Firewall Rule activity by disabling some logging options in the Firewall Stateful Configuration **Properties** window. For example, disabling the UDP logging will eliminate the "Unsolicited UDP" log entries.
- For Intrusion Prevention Rules, the best practice is to log only dropped packets. Logging packet modifications may result in a lot of log entries.
- For Intrusion Prevention Rules, only include packet data (an option in the Intrusion Prevention Rule's **Properties** window) when you are interested in examining the source of attacks. Otherwise leaving packet data inclusion on will result in much larger log sizes.

Email Notifications

Deep Security Manager can send emails to specific Users when selected Alerts are triggered. To enable the email system, you must give Deep Security Manager access to an SMTP mail server. You must configure your SMTP settings and select which Alerts will trigger emails to which Users.

Configuring your SMTP Settings

The SMTP configuration panel can be found in **Administration > System Settings > SMTP**.

Type the address of your SMTP mail (with the port if required). Enter a "From" email address from which the emails should be sent. Optionally type a "bounce" address to which delivery failure notifications should be sent if the Alert emails can't be delivered to one or more Users. If your SMTP mail server requires outgoing authentication, type the username and password credentials. Once you've entered the necessary information, use the **Test SMTP Settings** to test the settings.

Configuring which Alerts should generate emails

There are over 30 conditions that trigger Alerts and you may not want all of them to trigger the sending of an email. To configure which Alerts trigger the sending of an email, go to **Administration > System Settings > Alerts**. Click **View Alert Configuration** to display the list of all Alerts. The checkmark next to the Alert indicates whether the Alert is "On" or not. If it is on, it means the Alert will be triggered if the corresponding situation arises, but it does not mean an email will sent out. Double-click an Alert to view its **Alert Configuration** window.

To have an Alert trigger an email, it must be turned "On" and at least one of the "Send Email" checkboxes must be selected.

Setting which Users Receive the Alert Emails

Finally, you have to set which Users receive Alert emails. Go to **Administration > User management > Users**. Double-click a User and select the **Contact Information** tab.

Select the "Receive Email Alerts" checkbox to have this User receive emailed notifications of Alerts.

SIEM, Syslog and SNMP

Both the Agents/Appliances and the Manager can be instructed to forward Events to a SIEM system. The Agent/Appliance will send protection module-related security Event information and the Manager will send System Information.

System Events can be forwarded from the Manager via Syslog or SNMP. To configure the System Event Syslog or SNMP settings, go to the **Administration> System Settings > SIEM** or **Administration> System Settings > SNMP** tabs in the Deep Security Manager.

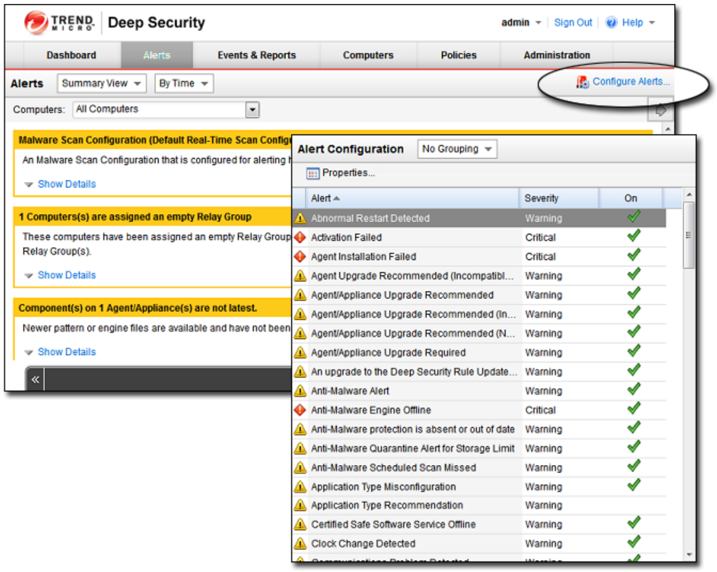
Protection module security Events can be forwarded from the Agents/Appliances via Syslog. To configure the Protection module security Events Syslog settings, go to the **Policy/Computer Editor > Settings > SIEM** tab.

For information on configuring Syslog, see ***Syslog Integration (SIEM) (page 40)***.

Alerts

Generally, Alerts exists to warn of system status anomalies like computers going offline or Rules being out of date, although there are some Alerts for the detection of fingerprinting scans and other security-related events. (For notifications of individual Intrusion Prevention and Firewall Events, consider setting up a Syslog server.)

The complete list of Alerts can be viewed by going to the **Alerts** page and clicking **Configure Alerts...** at the top-right of the page, or going to **Administration > System Settings > Alerts** and clicking **View Alert Configuration...**.



Malware Scan Configuration (Default Real-Time Scan Config

An Malware Scan Configuration that is configured for alerting h

Show Details

1 Computers(s) are assigned an empty Relay Group

These computers have been assigned an empty Relay Group Relay Group(s).

Show Details

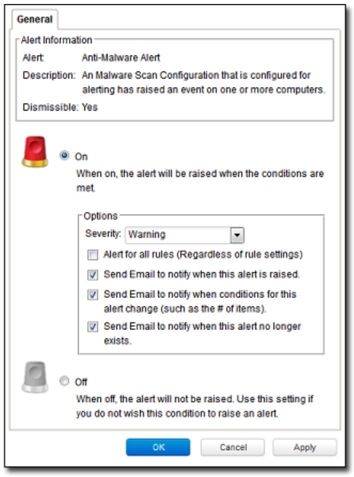
Component(s) on 1 Agent/Appliance(s) are not latest.

Newer pattern or engine files are available and have not been

Show Details

	Alert	Severity	On
⚠	Abnormal Restart Detected	Warning	✓
◆	Activation Failed	Critical	✓
◆	Agent Installation Failed	Critical	✓
⚠	Agent Upgrade Recommended (Incompatibl...	Warning	✓
⚠	Agent/Appliance Upgrade Recommended	Warning	✓
⚠	Agent/Appliance Upgrade Recommended (In...	Warning	✓
⚠	Agent/Appliance Upgrade Recommended (N...	Warning	✓
⚠	Agent/Appliance Upgrade Required	Warning	✓
⚠	An upgrade to the Deep Security Rule Update...	Warning	✓
⚠	Anti-Malware Alert	Warning	✓
◆	Anti-Malware Engine Offline	Critical	✓
⚠	Anti-Malware protection is absent or out of date	Warning	✓
⚠	Anti-Malware Quarantine Alert for Storage Limit	Warning	✓
⚠	Anti-Malware Scheduled Scan Missed	Warning	✓
⚠	Application Type Misconfiguration	Warning	✓
⚠	Application Type Recommendation	Warning	
⚠	Certified Safe Software Service Offline	Warning	✓
⚠	Clock Change Detected	Warning	✓

The actions precipitated by each Alert can be configured by opening the **Properties** window for the Alert. Alerts can be turned on or off and their severity can be switched between Warning and Critical.



Alert Information

Alert: Anti-Malware Alert

Description: An Malware Scan Configuration that is configured for alerting has raised an event on one or more computers.

Dismissible: Yes

● On

When on, the alert will be raised when the conditions are met.

Options

Severity: Warning

☐ Alert for all rules (Regardless of rule settings)

☑ Send Email to notify when this alert is raised.

☑ Send Email to notify when conditions for this alert change (such as the # of items).

☑ Send Email to notify when this alert no longer exists.

○ Off

When off, the alert will not be raised. Use this setting if you do not wish this condition to raise an alert.

Note: *Alerts cannot be configured differently for individual Policies or computers. All configuration changes to an Alert's properties are global.*

You may also want to configure which Users receive email Alerts. Go to **Administration > Users**, double-click an individual User, click the **Contact Information** tab, and select or de-select the **Receive Email Alerts** option.

There is also an option to specify a default email address to which all Alerts notifications will be sent in addition to the Users configured to receive them. This option is found on the **Administration > System Settings > Alerts** tab.

Note: *Make sure you have configured the SMTP settings on the* ***Administration > System Settings > SMTP*** *tab.*

In cases where an Alert condition occurs multiple times on the same computer, the Alert will show the timestamp of the first occurrence of the condition. If the Alert is dismissed and the condition reoccurs, the timestamp of the first reoccurrence will be displayed.

Port Scan Settings

The Deep Security Manager can be instructed to scan a computer for open ports by right-clicking the computer and selecting **Actions > Scan for Open ports**, or by clicking the **Scan for Open Ports** button in the **Firewall** page of the **Computer Editor** window (where the results of the latest scan are displayed).

(Port scans can also be initiated by right-clicking an existing computer on the Manager's **Computers** page and choosing "Scan for Open Ports". Another way to initiate port scans is to create a **Scheduled Task** to regularly carry out port scans on a list of computers.)

By default, the range of ports that are scanned is the range known as the "Common Ports", 1-1024, but you can define a different set of ports to scan.

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

To define a new port range to be scanned:

1. Go to **Policies > Common Objects > Lists > Port Lists** and click **New** in the menu bar. The **New Port List** window will appear.
2. Type a name and description for the new port list and then define the ports in the **Port(s)** text box using the accepted formats. (For example, to scan ports 100, 105, and 110 through 120, you would type "100" on the first line "105" on the second, and "110-120" on the third.) Click **OK**.
3. Now go to **Policy/Computer Editor > Settings > Scanning** and click the "Ports to Scan" drop-down menu. Your newly defined Port List will be one of the choices.

Syslog Integration (SIEM)

Deep Security supports Common Event Format 1.0, a format sponsored by ArcSight (www.arcsight.com). Some Modules support a "Basic Syslog" format; however, these formats are made available for legacy installations and should not be used for new integration projects.

> Note: *Enabling Syslog forwarding in the Deep Security Manager does not affect default Event logging. That is, enabling syslog will not disable the normal Event recording mechanisms.*

Setting up a Syslog on Red Hat Enterprise 6

The following steps describe how to configure rsyslog on Red Hat Enterprise 6 to receive logs from Deep Security Agents/Appliances.

1. Log in as root
2. Execute: `vi /etc/rsyslog.conf`
3. Uncomment the following lines near the top of the `rsyslog.conf` to change them from:

   ```
   #$ModLoad imudp
   #$UDPServerRun 514

   #$ModLoad imtcp
   #$InputTCPServerRun 514
   ```

   to

   ```
   $ModLoad imudp
   $UDPServerRun 514

   $ModLoad imtcp
   $InputTCPServerRun 514
   ```

4. Add the following two lines of text to the end of the `rsyslog.conf`:
   - `#Save Deep Security Manager logs to DSM.log`
   - `Local4.* /var/log/DSM.log`
5. Save the file and exit
6. Create the `/var/log/DSM.log` file by typing `touch /var/log/DSM.log`
7. Set the permissions on the DSM log so that syslog can write to it
8. Save the file and exit
9. Restart syslog: `service rsyslog restart`

When Syslog is functioning you will see logs populated in: `/var/log/DSM.log`

Setting up a Syslog on Red Hat Enterprise 5

The following steps describe how to configure Syslog on Red Hat Enterprise to receive logs from Deep Security Agents/Appliances.

1. Log in as root
2. Execute: `vi /etc/syslog.conf`

3. Add the following two lines of text to the end of the `syslog.conf` :
   - `#Save Deep Security Manager logs to DSM.log`
   - `Local4.* /var/log/DSM.log`
4. Save the file and exit
5. Create the `/var/log/DSM.log` file by typing `touch /var/log/DSM.log`
6. Set the permissions on the DSM log so that syslog can write to it
7. Execute: `vi /etc/sysconfig/syslog`
8. Modify the line " `SYSLOGD_OPTIONS` " and add a " `-r` " to the options
9. Save the file and exit
10. Restart syslog: `/etc/init.d/syslog restart`

When Syslog is functioning you will see logs populated in: `/var/log/DSM.log`

Deep Security Manager Settings

You can configure Deep Security Manager to instruct all managed computers to send logs to the Syslog computer, or you can configure individual computers independently.

To configure the Manager to instruct all managed computers to use Syslog:

1. Go to the **Administration > System Settings > SIEM** tab.
2. In the **System Event Notification (from the Manager)** area, set the **Forward System Events to a remote computer (via Syslog)** option.
3. Type the hostname or the IP address of the Syslog computer.
4. Enter which UDP port to use (usually 514).
5. Select which Syslog facility to use (Local4 from the Red Hat example above.)
6. Select the "Common Event Format 1.0" log format. (The "Basic Syslog" format is listed only for legacy support and should not be used for new integrations.)

Note: *Common Event Format 1.0 is a format sponsored by ArcSight (www.arcsight.com). The specification can be requested through their Web site.*

You have now configured the Deep Security Manager to instruct all existing and new computers to use remote Syslog by default.

There are two options for where the syslog messages are sent from. The first option (Direct Forward) sends the messages in real time directly from the Agents or Virtual Appliances. The second option (Relay via the Manager) sends the syslog messages from the Manager after events are collected on heartbeats. The option to send from the Manager may be desirable if the destination licenses based on the number of sources.

If the syslog messages are sent from the Manager, there are several differences. In order to preserve the original hostname (the source of the event), a new extension ("dvc" or "dvchost") is present. "dvc" is used if the hostname is an IPv4 address; "dvchost" is used for hostnames and IPv6 addresses. Additionally, the extension "TrendMicroDsTags" is used if the events are tagged (This applies only to auto-tagging with run on future, since events are forwarded via syslog only as they are collected by the Manager). The product for logs relayed through the Manager will still read "Deep Security Agent"; however, the product version is the version of the Manager.

All CEF events include dvc=IPv4 Address or dvchost=Hostname (or the IPv6 address) for the purposes of determining the original source of the event. This extension is important for events sent from a Virtual Appliance or the Manager, since in this case the syslog sender of the message is not the originator of the event.

This default setting can be overridden for specific Policies and on individual computers. To override on a computer, find the computer you want to configure, open the **Computer Editor** and go to **Settings** and click the **Notifications** tab. Like many other settings on a computer, you can instruct it to inherit default settings, or override them. To instruct this computer to ignore any inheritable default settings, select the **Forward Events To** option and enter the details for a different syslog server, or to not forward logs at all. Follow the same procedure to override the setting on a Policy.

Parsing Syslog Messages

Base CEF format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

To determine whether the log entry comes from the Deep Security Manager or a Deep Security Agent, look at the "Device Product" field:

Sample Log Entry: Jan 18 11:07:53 dsmhost CEF:0|Trend Micro|**Deep Security Manager**|8.0.1000|600|Administrator Signed In|4|suser=Master...

Note: *Events that occur on a VM being protected by a Virtual Appliance but without an in-guest Agent will still be identified as coming from an "Agent.*

To further determine what kind of rule triggered the event, look at the "Signature ID" and "Name" fields:

Sample Log Entry: Mar 19 15:19:15 chrisds7 CEF:0|Trend Micro|Deep Security Agent|7.0.0.2036|**123**|**Out Of Allowed Policy**|5|cn1=1...

The following "Signature ID" values indicate what kind of event has been triggered:

Signature IDs	Description
10	Custom Intrusion Prevention Rule
20	Log-Only Firewall Rule
21	Deny Firewall Rule
30	Custom Integrity Monitoring Rule
40	Custom Log Inspection Rule
100-299	Out of "Allowed" Policy Firewall Rule and Firewall Stateful Configuration
300-399	SSL Events
500-899	Intrusion Prevention Normalization
1,000,000-1,999,999	Trend Micro Intrusion Prevention Rule
2,000,000-2,999,999	Trend Micro Integrity Rule
3,000,000-3,999,999	Trend Micro Log Inspection Rule
4,000,000-4,999,999	Trend Micro Anti-Malware
5,000,000-5,999,999	Trend Micro Web Reputation

Note: *All the CEF extensions described in the tables below will not necessarily be included in each log entry. As well, they may not be in the order described below. If you are using regular expressions (regex) to parse the entries, make sure your expressions do not depend on each key/value pair to be there or for the key/value pairs to be in a particular order.*

Note: *Syslog messages are limited to 64K bytes by the syslog protocol specification. In rare cases data may be truncated. The Basic Syslog format is limited to 1K bytes.*

Events Originating in Deep Security Manager

System Event Log Format

Base CEF Format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Sample Log Entry: CEF:0|Trend Micro|Deep Security Manager|8.0.1046|600|User Signed In|3|src=10.52.116.160 suser=admin target=admin msg=User signed in from fe80:0:0:0:2d02:9870:beaa:fd41

Extension Field	Name	Description	Examples
src	Source IP Address	Source Deep Security Manager IP Address.	src=10.52.116.23

Extension Field	Name	Description	Examples
suser	Source User	Source Deep Security Manager user account.	suser=MasterAdmin

target	Target entity	The event target entity. The target of the event maybe the administrator account logged into Deep Security Manager, or a Computer.	target=MasterAdmin
			target=server01

msg	Details	Details of the System event. May contain a verbose description of the event.	msg=User password incorrect for username MasterAdmin on an attempt to sign in from 127.0.0.1 msg=A Scan for Recommendations on computer (localhost) has completed...

Events Originating in Deep Security Agent

Firewall Event Log Format

Base CEF format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Sample Log Entry: CEF:0|Trend Micro|Deep Security Agent|8.0.0.995|20|Log for TCP Port 80|0|cn1=1 cn1Label=Host ID dvc=hostname act=Log dmac=00:50:56:F5:7F:47 smac=00:0C:29:EB:35:DE TrendMicroDsFrameType=IP src=192.168.126.150 dst=72.14.204.147 out=1019 cs3=DF 0 cs3Label=Fragmentation Bits proto=TCP spt=49617 dpt=80 cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=1 TrendMicroDsPacketData=AFB...

Extension Field	Name	Description	Examples

act	Action	The action taken by the Firewall rule. Can contain: Log or Deny. If the rule or the network engine is operating in tap mode, the action value will be proceeded by "IDS:".	act=Log
			act=Deny

cn1	Host Identifier	The Agent Computer internal identifier which can be used to uniquely identify the Agent Computer from a given syslog event.	cn1=113
cn1Label	Host ID	The friendly name label for the field cn1.	cn1Label=Host ID
cnt	Repeat Count	The number of times this event was sequentially repeated.	cnt=8

cs2	TCP Flags	(For the TCP protocol only) The raw TCP flag byte followed by the URG, ACK, PSH, RST, SYN and FIN fields may be present if the TCP header was set. If "Relay via Manager" is selected, the output of this extension contains only the flag names.	cs2=0x10 ACK
			cs2=0x14 ACK RST

cs2Label	TCP Flags	The friendly name label for the field cs2.	cs2Label=TCP Flags

cs3	Packet Fragmentation Information	The "DF" field will be present if the IP "Don't Fragment" bit is set. The "MF" field will be present if the "IP More Fragments" bit is set.	cs3=MF
			cs3=DF MF

cs3Label	Fragmentation Bits	The friendly name label for the field cs3.	cs3Label=Fragmentation Bits

cs4	ICMP Type and Code	(For the ICMP protocol only) The ICMP type and code stored in their respective order delimited by a space.	cs4=11 0
			cs4=8 0

cs4Label	ICMP	The friendly name label for the field cs4.	cs4Label=ICMP Type and Code
dmac	Destination MAC Address	Destination computer network interface MAC address.	dmac= 00:0C:29:2F:09:B3

dpt	Destination Port	(For TCP and UDP protocol only) Destination computer connection port.	dpt=80
			dpt=135

dst	Destination IP Address	Destination computer IP Address.	dst=192.168.1.102
			dst=10.30.128.2

in	Inbound Bytes Read	(For inbound connections only) Number of inbound bytes read.	in=137
			in=21

out	Outbound Bytes Read	(For outbound connections only) Number of outbound bytes read.	out=216
			out=13

proto	Transport protocol	Name of the connection transportation protocol used.	proto=tcp
			proto=udp
			proto=icmp

smac	Source MAC Address	Source computer network interface MAC address.	smac= 00:0E:04:2C:02:B3

Extension Field	Name	Description	Examples

spt	Source Port	(For TCP and UDP protocol only) Source computer connection port.	spt=1032
			spt=443

src	Source IP Address	Source computer IP Address.	src=192.168.1.105
			src=10.10.251.231

TrendMicroDsFrameType	Ethernet frame type	Connection Ethernet frame type.	TrendMicroDsFrameType=IP
			TrendMicroDsFrameType=ARP
			TrendMicroDsFrameType=RevARP
			TrendMicroDsFrameType=NetBEUI

TrendMicroDsPacketData	Packet data	(If include packet data is set) A Base64 encoded copy of the packet data. The "equals" character is escaped. E.g. "\=" This extension is not included when the "Relay via the Manager" option is selected.	TrendMicroDsPacketData=AA...BA\=

Intrusion Prevention Event Log Format

Base CEF format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Sample Log Entry: CEF:0|Trend Micro|Deep Security Agent|8.0.0.995|1001111|Test Intrusion Prevention Rule|3|cn1=1 cn1Label=Host ID dvchost=hostname dmac=00:50:56:F5:7F:47 smac=00:0C:29:EB:35:DE TrendMicroDsFrameType=IP src=192.168.126.150 dst=72.14.204.105 out=1093 cs3=DF 0 cs3Label=Fragmentation Bits proto=TCP spt=49786 dpt=80 cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=1 act=IDS:Reset cn3=10 cn3Label=Intrusion Prevention Packet Position cs5=10 cs5Label=Intrusion Prevention Stream Position cs6=8 cs6Label=Intrusion Prevention Flags TrendMicroDsPacketData=R0VUIC9zP3...

Extension Field	Name	Description	Examples
act	Action	The action taken by the Intrusion Prevention rule. Can contain: Block, Reset, or Log. If the rule or the network engine is operating in detect-only mode, the action value will be preceded by "IDS:". (IPS Rules written before Deep Security version 7.5 SP1 could additionally perform Insert, Replace, and Delete actions. These actions are no longer performed. If an older IPS Rule is triggered which still attempts to perform those actions, the Event will indicate that the Rule was applied in detect-only mode.)	act=Block
cn1	Host Identifier	The Agent Computer internal identifier which can be used to uniquely identify the Agent Computer from a given syslog event.	cn1=113
cn1Label	Host ID	The friendly name label for the field cn1.	cn1Label=Host ID
cn3	Intrusion Prevention Packet Position	Position within packet of data that triggered the event.	cn3=37
cn3Label	Intrusion Prevention Packet Position	The friendly name label for the field cn3.	cn3Label=Intrusion Prevention Packet Position
cnt	Repeat Count	The number of times this event was sequentially repeated.	cnt=8
cs1	Intrusion Prevention Filter Note	(Optional) A note field which can contain a short binary or text note associated with the payload file. If the value of the note field is all printable ASCII characters, it will be logged as text with spaces converted to underscores. If it contains binary data, it will be logged using Base-64 encoding.	cs1=Drop_data
cs1Label	Intrusion Prevention Note	The friendly name label for the field cs1.	cs1Label=Intrusion Prevention Note

cs2	TCP Flags	(For the TCP protocol only) The raw TCP flag byte followed by the URG, ACK, PSH, RST, SYN and FIN fields may be present if the TCP header was set.	cs2=0x10 ACK
			cs2=0x14 ACK RST

cs2Label	TCP Flags	The friendly name label for the field cs2.	cs2Label=TCP Flags

cs3	Packet Fragmentation Information	The "DF" field will be present if the IP "Don't Fragment" bit is set. The "MF" field will be present if the "IP Mote Fragments" bit is set.	cs3=MF
			cs3=DF MF

cs3Label	Fragmentation Bits	The friendly name label for the field cs3.	cs3Label=Fragmentation Bits

Extension Field	Name	Description	Examples

cs4	ICMP Type and Code	(For the ICMP protocol only) The ICMP type and code stored in their respective order delimited by a space.	cs4=11 0
			cs4=8 0

cs4Label	ICMP	The friendly name label for the field cs4.	cs4Label=ICMP Type and Code

cs5	Intrusion Prevention Stream Position	Position within stream of data that triggered the event.	cs5=128
			cs5=20

cs5Label	Intrusion Prevention Stream Position	The friendly name label for the field cs5.	cs5Label=Intrusion Prevention Stream Position
cs6	Intrusion Prevention Filter Flags	A combined value that includes the sum of the following flag values: 1 - Data truncated - Data could not be logged. 2 - Log Overflow - Log overflowed after this log. 4 - Suppressed - Logs threshold suppressed after this log. 8 - Have Data - Contains packet data 16 - Reference Data - References previously logged data.	The following example would be a summed combination of 1 (Data truncated) and 8 (Have Data): cs6=9
cs6Label	Intrusion Prevention Flags	The friendly name label for the field cs6.	cs6=Intrusion Prevention Filter Flags
dmac	Destination MAC Address	Destination computer network interface MAC address.	dmac= 00:0C:29:2F:09:B3

dpt	Destination Port	(For TCP and UDP protocol only) Destination computer connection port.	dpt=80
			dpt=135

dst	Destination IP Address	Destination computer IP Address.	dst=192.168.1.102
			dst=10.30.128.2

in	Inbound Bytes Read	(For inbound connections only) Number of inbound bytes read.	in=137
			in=21

out	Outbound Bytes Read	(For outbound connections only) Number of outbound bytes read.	out=216
			out=13

proto	Transport protocol	Name of the connection transportation protocol used.	proto=tcp
			proto=udp
			proto=icmp

Smac	Source MAC Address	Source computer network interface MAC address.	smac= 00:0E:04:2C:02:B3

Spt	Source Port	(For TCP and UDP protocol only) Source computer connection port.	spt=1032
			spt=443

Src	Source IP Address	Source computer IP Address.	src=192.168.1.105
			src=10.10.251.231

TrendMicroDsFrameType	Ethernet frame type	Connection Ethernet frame type.	TrendMicroDsFrameType=IP
			TrendMicroDsFrameType=ARP
			TrendMicroDsFrameType=RevARP
			TrendMicroDsFrameType=NetBEUI

TrendMicroDsPacketData	Packet data	(If include packet data is set) A Base64 encoded copy of the packet data. The "equals" character is escaped. E.g. "\=" This extension is not included when the "Relay via the Manager" option is selected.	TrendMicroDsPacketData=AA...BA\=

Log Inspection Event Format

Base CEF format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Sample Log Entry: CEF:0|Trend Micro|Deep Security Agent|8.0.0.995|3002795|Microsoft Windows Events|8|cn1=1 cn1Label=Host ID dvchost=hostname cs1Label=LI Description cs1=Multiple Windows Logon Failures fname=Security src=127.0.0.1 duser=(no user) shost=WIN-RM6HM42G65V msg=WinEvtLog Security: AUDIT_FAILURE(4625): Microsoft-Windows-Security-Auditing: (no user): no domain: WIN-RM6HM42G65V: An account failed to log on. Subject: ..

Extension Field	Name	Description	Examples
cn1	Host Identifier	The Agent Computer internal identifier which can be used to uniquely identify the Agent Computer from a given syslog event.	cn1=113
cn1Label	Host ID	The friendly name label for the field cn1.	cn1Label=Host ID
cs1	Specific Sub-Rule	The Log Inspection sub-rule which triggered this event.	cs1=Multiple Windows audit failure events
cs1Label	LI Description	The friendly name label for the field cs1.	cs1Label=LI Description

duser	User Information	(If parse-able username exists) The name of the target user initiated the log entry.	duser=(no user)
			duser=NETWORK SERVICE

fname	Target entity	The Log Inspection rule target entity. May contain a file or directory path, registry key, etc.	fname=Application
			fname=C:\Program Files\CMS\logs\server0.log

msg	Details	Details of the Log Inspection event. May contain a verbose description of the detected log event.	msg=WinEvtLog: Application: AUDIT_FAILURE(20187): pgEvent: (no user): no domain: SERVER01: Remote login failure for user 'xyz'
shost	Source Hostname	Source computer Hostname	shost=webserver01.corp.com

src	Source IP Address	Source computer IP Address.	src=192.168.1.105
			src=10.10.251.231

Integrity Monitoring Log Format

Base CEF format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Sample Log Entry: CEF:0|Trend Micro|Deep Security Agent|8.0.0.995|30|New Integrity Monitoring Rule|6|cn1=1 cn1Label=Host ID dvchost=hostname act=updated filePath=c:\\windows\\message.dll msg=lastModified,sha1,size

Note: *The message only appears for "update" actions and includes the properties modified. For a full description, use the option to "Relay via the Manager".*

Extension Field	Name	Description	Examples

act	Action	The action detected by the integrity rule. Can contain: created, updated, detected or renamed.	act=created
			act=deleted

cn1	Host Identifier	The Agent Computer internal identifier which can be used to uniquely identify the Agent Computer from a given syslog event.	cn1=113
cn1Label	Host ID	The friendly name label for the field cn1.	cn1Label=Host ID
filePath	Target Entity	The integrity rule target entity. May contain a file or directory path, registry key, etc.	filePath=C:\WINDOWS\system32\drivers\etc\hosts
msg	Attribute changes	(For "updated" action only) A list of changed attribute names. If "Relay via Manager" is selected, all event action types include a full description.	msg=lastModified,sha1,size
oldfilePath	Old target entity	(For "renamed" action only) The previous integrity rule target entity to capture the rename action from the previous target entity to the new, which is recorded in the filePath field.	oldFilePath=C:\WINDOWS\system32\logfiles\ds_agent.log

Anti-Malware Format

Base CEF format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Sample Log Entry: CEF:0|Trend Micro|Deep Security Agent|8.0.0.995|4000000|Eicar_test_file|6|cn1=1 cn1Label=Host ID dvchost=hostname cn2=205 cn2Label=Quarantine File Size filePath=C:\\Users\\trend\\Desktop\\eicar.txt act=Delete msg=Realtime

Extension Field	Name	Description	Examples
cn1	Host Identifier	The Agent Computer internal identifier which can be used to uniquely identify the Agent Computer from a given syslog event.	cn1=1
cn1Label	Host ID	The friendly name label for the field cn1.	cn1Label=Host ID

Extension Field	Name	Description	Examples
cn2	File Size	The size of the quarantine file. This extension is included only when the "direct forward" from Agent/Appliance is selected.	cn2=100
cn2Label	File Size	The friendly name label for the field cn2.	cn2Label=Quarantine File Size
filepath	Filepath	The location of the target file.	filePath=C:\\virus\\ei1.txt

act	Action	The action carried out by the Anti-malware engine. Possible values are: Deny Access, Quarantine, Delete, Pass, and Clean.	act=Clean
			act=Pass

msg	Message	The type of scan. Possible values are: Realtime, Scheduled, and Manual.	msg=Realtime
			msg=Scheduled

fsize	Filesize	The size of the target file in bytes.	fsize=120

Web Reputation Format

Base CEF format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Sample Log Entry: CEF:0|Trend Micro|Deep Security Agent|8.0.0.995|5000000|WebReputation|5|cn1=1 cn1Label=Host ID dvchost=hostname request=site.com msg=Blocked By Admin

Extension Field	Name	Description	Examples
cn1	Host Identifier	The Agent Computer internal identifier which can be used to uniquely identify the Agent Computer from a given syslog event.	cn1=1
cn1Label	Host ID	The friendly name label for the field cn1.	cn1Label=Host ID
request	Request	The URL of the request.	request=site.com

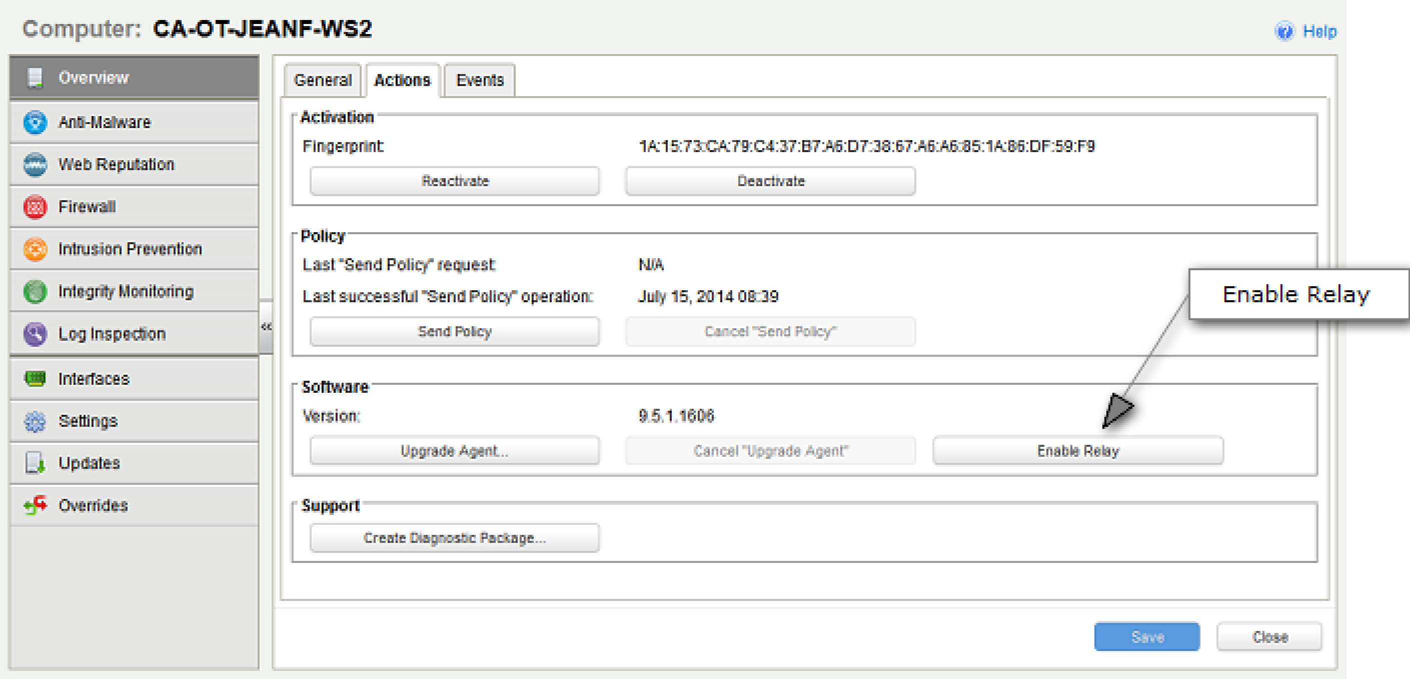
msg	Message	The type of action. Possible values are: Safe, Suspicious, Highly Suspicious, Dangerous, Blocked By Admin, Untested.	msg=Safe
			msg=Suspicious

See also:

- ***Policies, Inheritance and Overrides (page 257)***

Relay Groups

A Relay is a module within a Deep Security Agent that is responsible for the download and distribution of Security and Software updates. The Manager instructs the Relays to get the latest updates and when new updates are available, and Agents and Appliances are automatically directed to pull their updates from the Relays. The Relay module is available on 64-bit Windows and Linux Agents only. It is turned off by default. To enable the Relay module in an Agent, open the **Computer Editor** window of a computer running an activated 64-bit Windows or Linux Agent and go to **Overview > Actions > Software** and click **Enable Relay**.



Computer: CA-OT-JEANF-WS2

Activation

Fingerprint: 1A:15:73:CA:79:C4:37:B7:A6:D7:38:67:A6:A6:85:1A:86:DF:59:F9

Policy

Last "Send Policy" request: N/A

Last successful "Send Policy" operation: July 15, 2014 08:39

Software

Version: 9.5.1.1606

Support

Relays are organized into Relay Groups. Newly enabled Relays are assigned to the **Default Relay Group**. Agents/Appliances retrieve updates from the Default Relay Group unless configured otherwise. Trend Micro recommends that Agents on computers in a particular geographic region or office be configured to download updates from a Relay Group in the same region.

A Relay Group may contain as few as a single member Relay. However to improve performance and redundancy, a Relay Group can be configured to contain more than one member Relay. In order to distribute load and fault impact, Relays in a group are not prioritized - each Agent/Appliance assigned to a Relay Group automatically chooses a member Relay at random to connect to. When the Agent/Appliance attempts to download updates, if the initial Relay fails to respond, then the Agent/Appliance randomly selects another member Relay from the Group to update from. Since the list is shuffled by each Agent/Appliance, they each contact the Relays in a different order.

Note: *A Relay can obtain security updates from another Relay Group, but not from another Relay (even if they are both part of the same Relay Group). A Relay must obtain updates from another Relay Group further up the hierarchy or another configured security update source.*

Note that when a Relay is busy with an update to an Agent/Appliance, it will reject new connections from other Agents/Appliances.

Relay Groups may be arranged in hierarchies to optimize bandwidth and provide further redundancy. Although there must always be at least one Relay Group in your environment that downloads Security Updates from the Trend Micro Update Server, a Relay Group can alternatively download updates from another Relay Group. If all contact with an assigned Relay Group fails, the Agent/Appliance will switch to the parent Relay Group. From then on, the Agent/Appliance will attempt to contact a member Relay from the parent Relay Group to obtain updates.

Note: *Relays always retrieve Updates from the next Group up the Relay Group Hierarchy or from the Trend Micro Update Servers. They never retrieve Updates from other Relays in the same Relay Group.*

If configured to do so, Agents/Appliances can pull updates directly from the Trend Micro Update source if they are unable to contact any Relays.

Create Relay Groups

1. After installing and activating your Relays, from **Administration > Update > Relay Groups**.
2. Click **New**, and use the **Relay Groups** wizard to: create and name your Relay Group, select the Relays that are members of this group.
3. For the primary Relay Group, in **Download Updates From:** select **Update Source**. This setting will download updates from the Update source URL configured in the **Relays** section on the **Administration > System Settings > Updates** tab.
4. Repeat step 2 to create more Relay Groups. To create a hierarchy, in **Download Updates From:**, select the source for your new Relay Group to be an existing Relay Group.

Note: *Relays not yet configured into any Relay Group are automatically configured as members of the "Default Relay Group".*

Newly activated Relays will be automatically notified by the Manager to update their Security Update content.

Assign Agents/Appliances to Relay Groups

1. From the **Computers** page, right click the selected Computer and select **Actions > Assign Relay Group**. Select the Relay Group to use from the drop-down list, or from the **Computer Details window**, use **Download Updates From:** to select the Relay Group.
2. To assign multiple computers, from the **Computers** page, shift-click or ctr-click on selected Computers in the list. Select **Actions > Assign Relay Group**. Select the Relay Group that you want all the selected computers to use from the drop-down list.

   Note: *When selecting multiple computers, the action **Assign Relay Group** will only be available for selection if this action is available for all computers you selected.*

3. To review all the Relay Group assignments, from **Administration > System Settings > Updates**, click the **View Relay Groups...** button. For each Relay Group in the list, right-click and select **Properties**. Go to the **Assigned to** tab to review the list of Agents/Appliances assigned to this Relay Group. (To quickly change the assignment for an Agent/Appliance, clicking the link on the **Assigned to** list opens the **Computer Details** page for that Agent/Appliance, from where you can select another Relay Group assignment).

Note: *Agents/Appliances not yet assigned to a specific Relay Group are automatically assigned to the "Default Relay Group".*

When Relay Groups are modified, the configuration is automatically updated on computers that are already assigned to them (including child Relay Groups).

You can also create an Event-Based Task which will automatically assign a Relay Group to computers after they have been added to the Manager's **Computers** page. See **Event-Based Tasks** in the Deep Security Manager Interface Guide or the online help for more information.

Updating Anti-Malware Patterns Only

In some circumstances, you may wish to only apply Anti-Malware pattern updates, and exclude Anti-Malware engine updates. To do so,

1. Go to **Administration > Updates > Relay Groups**.
2. Double-click on a Relay Group to open its **Properties** window.
3. In the **Updates** area of the **Relay Group Properties** tab, select **Only Update Patterns**. Click **OK**.

Note: *Because Relays operate in Groups, this option can only be set on Relays Groups, and not on individual Relays.*

Note: *If your Relays Groups are organized in a hierarchical structure and one of your Relay Groups has this setting enabled, Relay Groups below it will not receive or distribute Engine patterns either, whether or not the setting is checked for that Group.*

Note: *If you enable this option, the* ***Administration > Updates > Security Updates*** *tab may indicate that some of your computers are "Out-of-Date". This is because the Manager makes an assessment by comparing the state of the updates on a computer with a master manifest list.*

Initiate Security Updates

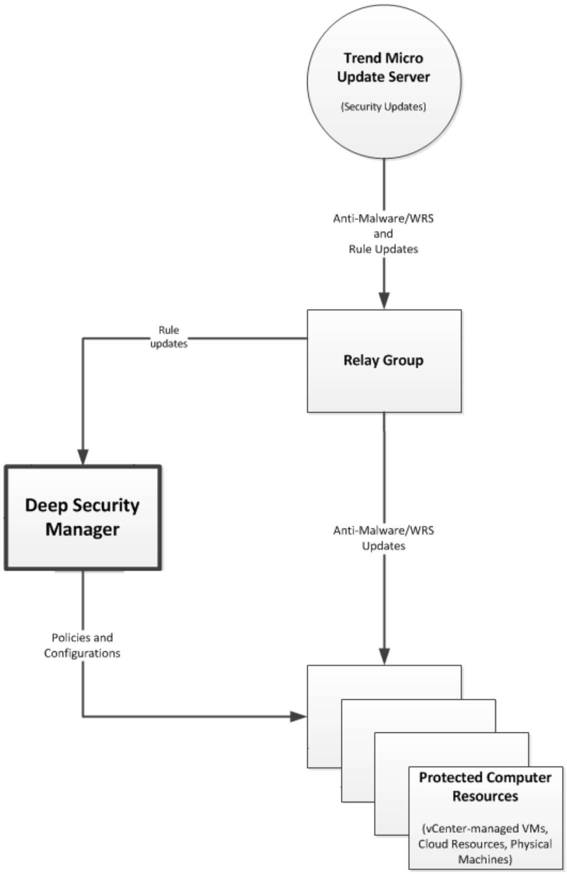
For a system-wide update, go to **Administration > Updates > Security**, and click the **Check For Updates and Download...** button.

To perform Security Updates on specific Agents/Appliances, select the Agent/Appliance from the list of computers on the **Computers** page, then right-click and select **Actions > Download Security Update**.

To schedule a regular **Check For Security Updates** task , go to **Administration > Scheduled Tasks**, and create a new **Scheduled Task** of the **Check For Security Updates** type.

Security Updates

Deep Security periodically needs to be updated with the latest Security and Software Updates. The update packages are retrieved from Trend Micro in the form of **Security Updates**. Deep Security **Relays**, organized into **Relay Groups** (also managed and configured by the Deep Security Manager) are used to retrieve Security Updates from Trend Micro and distribute them to the Agents and Appliances:


Trend Micro Update Server
(Security Updates)
Anti-Malware/WRS and Rule Updates
Relay Group
Rule updates
Deep Security Manager
Anti-Malware/WRS Updates
Policies and Configurations
Protected Computer Resources
(vCenter-managed VMs, Cloud Resources, Physical Machines)

Security Updates

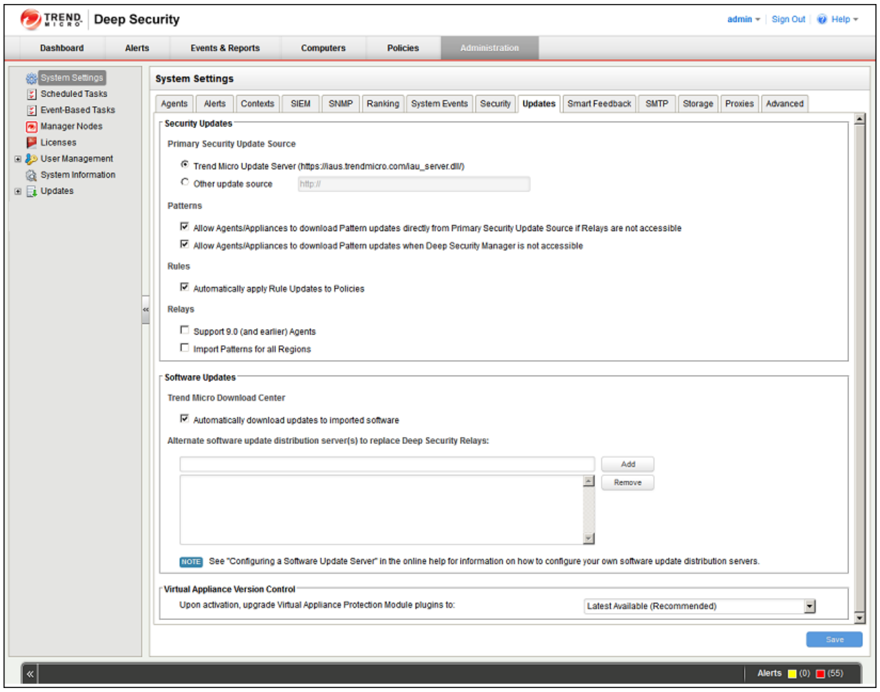
Note: *Before configuring Security Updates, you must have installed and activated your Agents and Appliances and your Deep Security Relays. Installation instructions for all Deep Security software are in the* ***Deep Security Installation Guide****.*

To configure Security Updates, you will need to:

1. Configure your Security Update source
2. Organize your Relays into Relay Groups
3. Assign Relay Groups to your Agents/Appliances
4. Special Case: Configure Updates on a Relay in an Air-Gapped Environment

Configure your Security Update Source

To view your current Update source settings, go to **Administration > System Settings > Updates:**



System Settings

Security Updates

Primary Security Update Source

● Trend Micro Update Server (https://iaus.trendmicro.com/iau_server.dll/)

○ Other update source http://

Patterns

☑ Allow Agents/Appliances to download Pattern updates directly from Primary Security Update Source if Relays are not accessible

☑ Allow Agents/Appliances to download Pattern updates when Deep Security Manager is not accessible

Rules

☑ Automatically apply Rule Updates to Policies

Relays

□ Support 9.0 (and earlier) Agents

□ Import Patterns for all Regions

Software Updates

Trend Micro Download Center

☑ Automatically download updates to imported software

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

NOTE See "Configuring a Software Update Server" in the online help for information on how to configure your own software update distribution servers.

Virtual Appliance Version Control

Upon activation, upgrade Virtual Appliance Protection Module plugins to: Latest Available (Recommended)

Note: *Alerts are raised if a Pattern Update has been downloaded from Trend Micro and available for more than an hour but computers have yet to be updated.*

Security Updates

In the **Security Updates** area, set your Update source. By default this will be the **Trend Micro Update Server** accessed over the Internet. Unless your support provider has told you to do otherwise, leave the setting as is.

You may have Agents installed on roaming computers that are not always in contact with a Deep Security Manager or a Deep Security Relay. To allow Agents to use the Update source specified above when their Relay Group is not available, select the **Allow Agents/Appliances to download Pattern updates directly from Primary Security Update Source if Relays are not accessible** option. To allow Agents to update (either from a Relay or the Update server) when not in contact with a Deep Security Manager, select **Allow Agents/Appliances to download Pattern updates when Deep Security Manager is not accessible**. (You may want to uncheck this option on computers where you do not want to risk a potentially problematic Security Update when the computer is not in contact with a Manager and therefore possibly far away from any support services.)

Automatically apply Rule Updates to Policies: Trend Micro will occasionally issue an update to an existing Deep Security Rule. This setting determines whether updated Rules get sent to computers during a Security Update.

Updates to existing Rules are either improvements to the efficiency of the Rule or bug fixes. So although it's a good a idea to test new Rules (either in detect-only mode or in a test environment) before deploying them to a production environment, automatically applying updates to existing Rules is a safe option.

Note: *Alerts are raised if a Rule Update has been downloaded from Trend Micro and available for more than thirty minutes but computers have yet to be updated.*

Proxy Servers

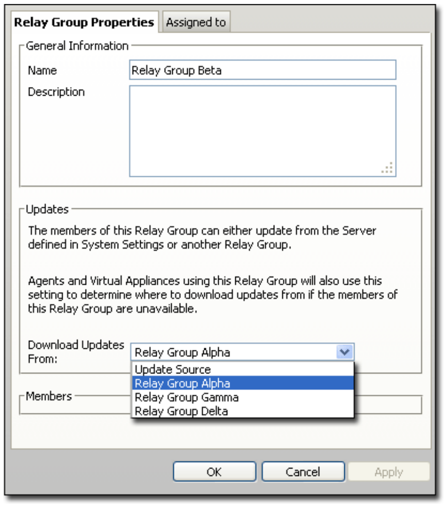
If your Relays must connect to a proxy to access the Internet (and Trend Micro Update Servers), you can define the proxies in the **Proxy Servers** area on the **Administration > System Settings > Proxies** tab.

Organize your Relays into Relay Groups

A Deep Security installation requires at least one Deep Security Relay. Relays are organized into Relays Groups (even if there is only one Relay in the group.) As soon as you activate a Relay with the Manager, it is added to a Group called **Default Relay Group.** This Relay Group will always be there as a catch-all for new Relays. Once activated, you can move your new Relay from one Relay Group to another.

To view your current Relay Groups or to create new Relay Groups, go to **Administration > Updates > Relay Groups**.

The Update Source for a Relay is assigned at the Group level. By default, a Relay Group is configured to get its updates from the Update source designated on the **Administration > System Settings > Updates** tab. However, a Relay Group can be configured to get its updates from another Relay Group, creating a hierarchy of Relay Groups.



Name: Relay Group Beta

The members of this Relay Group can either update from the Server defined in System Settings or another Relay Group.

Agents and Virtual Appliances using this Relay Group will also use this setting to determine where to download updates from if the members of this Relay Group are unavailable.

Download Updates From: Relay Group Alpha

Note: *A Relay can obtain security updates from another Relay Group, but not from another Relay (even if they are both part of the same Relay Group). A Relay must obtain updates from another Relay Group further up the hierarchy or another configured security update source.*

For more information on Relay Groups, see ***Relay Groups (page 48)*** in the User's Guide.

Assign Relay Groups to your Agents/Appliances

Once your Relay Groups are established and configured to connect with an Update Source, you can assign the Relay Groups to your Agents and Appliances.

To assign a Relay Group to an Agent/Appliance, go to the **Computers** page, right-click on the computer and select **Actions > Assign Relay Group...**. The list of available Relay Groups will appear and you can select from it.

Special Case: Configure Updates on a Relay in an Air-Gapped Environment

In a typical environment, at least one Deep Security Relay is configured and able to download Updates from the Trend Micro Update Server and the rest of the Relays or 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 the Internet, then an alternative method is available to import a package of Updates to a Relay for distribution to other Deep Security Software Components.

Using a Relay to generate an Updates package

Use a Deep Security Relay that is able to download the latest updates from the Trend Micro Update Server.

To create a Relay Updates bundle, at the command prompt on the Relay, enter:

```
dsa_control -b
```

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

Importing Updates to the Air-Gapped Relay

Copy the .zip file to the installation directory of the Deep Security Relay on which you want to import the Updates.

When a Security Update Download is initiated from the Deep Security Manager (either scheduled or manual), if any Deep Security Relay is unable to get the update from the configured Update Source location, it will automatically check for the presence of a Relay Updates .zip file in its installation directory. If it finds the zipped Updates package, the Relay will extract and import the Updates.

Note: *Remember to remove the Updates .zip file after the Updates have been successfully imported to the Relay.*

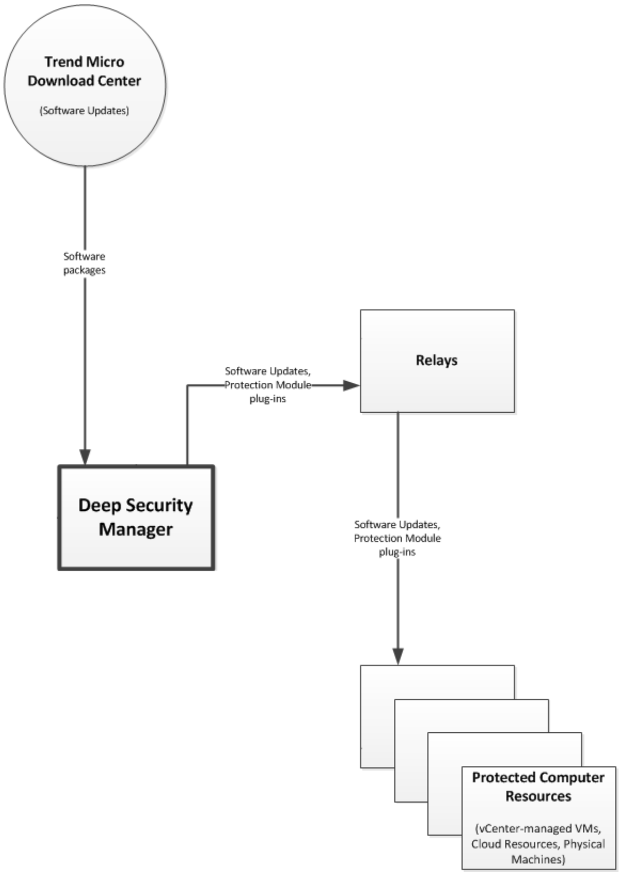
Configuring an Update Source for an Air-Gapped Relay

Air-gapped Relays will still try to contact an Update server to check for Updates. To avoid Update failure Alerts, set the Relay to use itself as an Update source:

1. In the Deep Security Manager, go to **Administration > Update > Relay Groups**.
2. Double-click the name of the Relay Group.
3. In the **Security Updates** area, select "Other Update Source" and enter https://localhost:4122
4. Click **OK**.

Software Updates

Deep Security Software Updates are managed and distributed by the Deep Security Manager. The Manager periodically connects to Trend Micro Update Servers to check for available Software Updates. If it determines that updates are available, it will raise an Alert to that effect. You will use the Deep Security Manager to download and distribute Software Updates:


Trend Micro Download Center
(Software Updates)
Software packages
Deep Security Manager
Software Updates, Protection Module plug-ins
Relays
Software Updates, Protection Module plug-ins
Protected Computer Resources
(vCenter-managed VMs, Cloud Resources, Physical Machines)

When you receive an Alert that new software is available, you have to import the software into the Deep Security Manager.

To import software into the Deep Security Manager:

1. Go to **Administration > Updates > Software**.
2. Check the Trend Micro Download Center section of the page to see whether there are any new software updates available. If no new updates are available, the section will say "All imported software is up to date". If updates are available, select the packages that you want and then click **Import**. You can select multiple packages by pressing Shift or Ctrl when clicking.
3. When a green checkmark appears in the **Imported** column, the package has been downloaded into Deep Security Manager. The package will also appear on **Administration** > **Updates** > **Local**.
4. After a period of time, the Relays will replicate the packages.

Once the software is imported into the Deep Security Manager, you can upgrade the Deep Security Agents, Appliances, and Relays:

- To upgrade only certain Agents, right-click the Agents on the Computers page and select **Actions > Upgrade Agent/Appliance/Relay** software.
- To upgrade all Agents at once, go to **Administration** > **Updates** > **Software** and then click **Upgrade Agent/Appliance Software**.

Virtual Appliance Scan Caching

Introduction

Scan Caching is used by the Virtual Appliance to maximize the efficiency of Malware and Integrity Monitoring Scans of virtual machines. Scan Caching improves the efficiency of on-demand scans by eliminating the unnecessary scanning of identical content across multiple VMs in large VMware deployments. A Scan Cache contains lists of files and other scan targets that have been scanned by a Deep Security protection module. If a scan target on a virtual machine is determined to be identical to a target that has already been scanned, the Virtual Appliance will not scan the target a second time. Attributes used to determine whether entities are identical are creation time, modification time, file size, and file name. In the case of Real-time Scan Caching, Deep Security will read partial content of files to determine if two files are identical. There is an option setting to use a file's Update Sequence Number (USN, Windows only) but its use should be limited to cloned virtual machines.

Scan Caching benefits **Integrity Monitoring** by sharing Integrity Monitoring scan results among cloned or similar virtual machines.

Scan Caching benefits **Manual (on-demand) Malware Scans** of cloned or similar virtual machines by increasing the speed up subsequent scans.

Scan Caching benefits **Real-Time Malware Scanning** by speeding up boot process scans and application access scans on cloned or similar virtual machines.

These improvements in efficiency further improve overall scan performance by allowing the Virtual Appliance to perform concurrent scans of multiple virtual machines at the same time.

Scan Cache Configurations

A Scan Cache Configuration is a collection of settings that determines Expiry Time, the use of Update Sequence Numbers (USNs), files to exclude, and files to include.

Note: *Virtual machines that use the same Scan Cache Configuration also share the same Scan Cache.*

You can see the list of existing Scan Cache Configurations by going **Administration > System Settings > Advanced > Scan Cache Configurations** and clicking the **View Scan Cache Configurations...** button. Deep Security comes with several preconfigured default Scan Cache Configurations. These are implemented automatically by the Virtual Appliance depending the properties of the virtual machines being protected and the types of scan being performed.

Expiry Time determines the lifetime of individual entries in a Scan Cache. The default recommended settings are one day for Manual (on-demand) Malware Scans, 15 mins for Real-Time Malware Scans, and one day for Integrity Monitoring Scans.

Use USN (Windows only) specifies whether to make use of Windows NTFS Update Sequence Numbers, which is a 64-bit number used to record changes to an individual file. This option should only be set for cloned VMs.

Files Included and **Files Excluded** are regular expression patterns and lists of files to be included in or excluded from the Scan Cache. Files to be scanned are matched against the include list first.

Individual files and folders can be identified by name or you can use wildcards ("*****" and "**?**") to refer to multiple files and/or locations with a single expression. (Use "*****" to represent any zero or more characters, and use question mark "**?**" to represent any single character.)

Note: *The include and exclude lists only determine whether the scan of the file will take advantage of Scan Caching. The lists will not prevent a file from being scanned in the traditional way.*

Malware Scan Cache Configuration

To select which Scan Cache Configuration is used by a virtual machine, open the Policy or Computer Editor and go to **Anti-Malware > Advanced > VM Scan Cache**. You can select which Scan Cache Configuration is used for Real-Time Malware Scans and which Scan Cache Configuration is used for Manual Scans.

Integrity Monitoring Scan Cache Configuration

To select which Scan Cache Configuration is used by a virtual machine, open the Policy or Computer Editor and go to **Integrity Monitoring > Advanced > VM Scan Cache**.

Scan Cache Settings

Scan Cache Settings are not included in a Scan Cache Configuration because they determine how the Virtual Appliance manages Scan Caches rather than how Scan Caching is carried out. Scan Cache settings are controlled at the Policy level. You can find the Scan cache settings by opening a Policy Editor and going to the **Settings > Scanning > Virtual Appliance Scans** area.

Max Concurrent Scans determines the number of scans that the Virtual Appliance will perform at the same time. The recommended number is five. If you increase this 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.

Max On-Demand Malware Scan Cache Entries determines, for Manual or Scheduled Malware Scans, the maximum number of records that identify and describe a file or other type of scannable content to keep. One million entries will use approximately 100MB of memory.

Max Malware Real-Time Scan Cache Entries determines, for Real-Time Malware Scans, the maximum number of records that identify and describe a file or other type of scannable content to keep. One million entries will use approximately 100MB of memory.

Max Integrity Monitoring Scan Cache Entries determines, for Integrity Monitoring, the maximum number of entities included in the baseline data for Integrity Monitoring. Two hundred thousand entities will use approximately 100MB of memory.

When should you change the default configuration or settings?

Scan caching is designed to avoid scanning identical files twice. Deep Security does not examine the entire contents of all files to determine if files are identical. Although when configured to do so, Deep Security can check the USN value of a file, and during Real-time Scans it will read partial content of files, it generally examines file attributes to determine if files are identical. It would be difficult but not impossible for some malware to make changes to a file and then restore those files attributes to what they were before the file was modified.

Deep Security limits this potential vulnerability by establishing short default cache expiry times. To strengthen the security you can use shorter expiry times on cache and you can use USN but doing so may reduce the performance benefit and/or you may need a bigger cache setting. For the strongest security for VMs that you want to keep separate and never share scan results you can create dedicated policies for these VMs kind of like keeping them in separate zones. This might be appropriate if you have different departments or organizations sharing the same infrastructure. (This is automatically enforced for different Tenants.)

If you have a very large number of VMs per host (for example, a VDI environment) then you should monitor your disk I/O and CPU usage during scanning. If scanning is taking too long then you may need to increase the size of the cache or adjust the Scan Cache Settings to obtain the required performance. If you need to increase cache size you may need to adjust Virtual Appliance system memory accordingly.

User Management

Deep Security has **Users**, **Roles**, and **Contacts** which are found under **Administration > User Management**.

A **User** is a Deep Security account holder who can sign in to the Deep Security Manager with a unique username and password. Users are assigned a **Role** which is a collection of permissions to view data and perform operations within Deep Security Manager. **Contacts** do not have a User account and cannot sign in to Deep Security Manager but they can be designated as the recipients of email notifications and scheduled Reports.

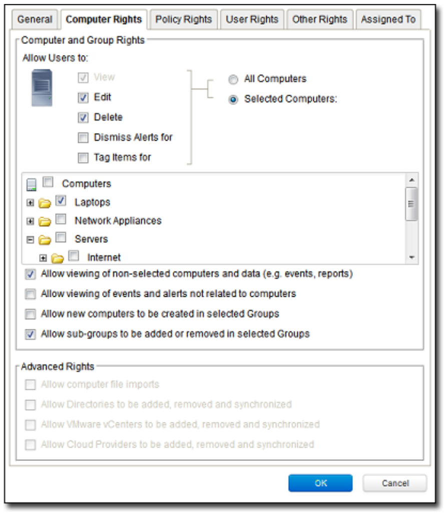
> Note: *Although Contacts cannot sign in to Deep Security Manager, they are assigned Roles that define the scope of the information that is sent to them. For example, three Contacts may each be listed as the recipients of a weekly Summary Report but the contents of the three Reports could be entirely different for each Contact depending on the computers that their Roles give them "View" permissions on.*

Role-Based Access Rights and Editing Privileges

Access rights and editing privileges are attached to Roles and not to Users. To change the access rights and editing privileges of an individual User, the User must be assigned a different Role, or the Role itself must be edited.

Role-Based Access to Computers and Policies

The access Roles have to computers and Policies can be restricted to subsets of computers and Policies. This can be controlled at a fairly granular level. For example, Users can be permitted to view all existing computers, but only permitted to modify those in a particular Group. To edit a Role, go to **Administration > User Management > Roles** and double-click a Role (or click the **New...** button) to display the **Roles Properties** window.



Computer and Group Rights

Allow Users to:

☑ View
☑ Edit
☑ Delete
☐ Dismiss Alerts for
☐ Tag Items for

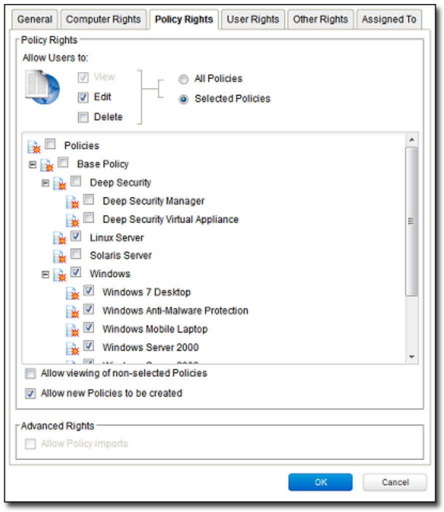
○ All Computers
● Selected Computers:

☐ Computers
☑ Laptops
☐ Network Appliances
☐ Servers
☐ Internet

☑ Allow viewing of non-selected computers and data (e.g. events, reports)
☐ Allow viewing of events and alerts not related to computers
☐ Allow new computers to be created in selected Groups
☑ Allow sub-groups to be added or removed in selected Groups

Advanced Rights

☐ Allow computer file imports
☐ Allow Directories to be added, removed and synchronized
☐ Allow VMware vCenters to be added, removed and synchronized
☐ Allow Cloud Providers to be added, removed and synchronized



Policy Rights

Allow Users to:

- ☑ View
- ☑ Edit
- □ Delete

- ○ All Policies
- ● Selected Policies

- □ Policies
  - □ Base Policy
    - □ Deep Security
      - □ Deep Security Manager
      - □ Deep Security Virtual Appliance
    - ☑ Linux Server
    - □ Solaris Server
    - ☑ Windows
      - ☑ Windows 7 Desktop
      - ☑ Windows Anti-Malware Protection
      - ☑ Windows Mobile Laptop
      - ☑ Windows Server 2000

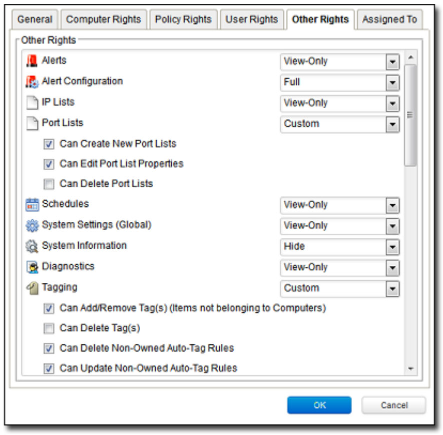
- □ Allow viewing of non-selected Policies
- ☑ Allow new Policies to be created

Advanced Rights

- □ Allow Policy imports

Role-Based Editing Privileges

Within those access restrictions, Roles can have limitations placed on their editing privileges.

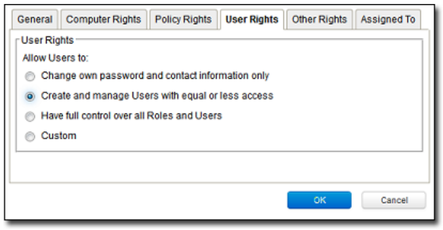


Other Rights

- Alerts: View-Only
- Alert Configuration: Full
- IP Lists: View-Only
- Port Lists: Custom
  - ☑ Can Create New Port Lists
  - ☑ Can Edit Port List Properties
  - □ Can Delete Port Lists
- Schedules: View-Only
- System Settings (Global): View-Only
- System Information: Hide
- Diagnostics: View-Only
- Tagging: Custom
  - ☑ Can Add/Remove Tag(s) (Items not belonging to Computers)
  - □ Can Delete Tag(s)
  - ☑ Can Delete Non-Owned Auto-Tag Rules
  - ☑ Can Update Non-Owned Auto-Tag Rules

User rights

A Role can give Users delegated rights over other Users. That is, the Users with that Role can create and modify the properties of Users only with equal or less access than themselves.



User Rights

Allow Users to:

- ○ Change own password and contact information only
- ● Create and manage Users with equal or less access
- ○ Have full control over all Roles and Users
- ○ Custom

Default Settings for Full Access, Auditor, and New Roles

The following table identifies the default rights settings for the **Full Access** Role and the **Auditor** Role. Also listed are the rights settings that are in place when creating a new Role by clicking **New** in the toolbar on the **Roles** page.

RIGHTS	**SETTINGS BY ROLE**		
General	**Full Access Role**	**Auditor Role**	**New Role Defaults**
Access to DSM User Interface	Allowed	Allowed	Allowed
Access to Web Service API	Allowed	Allowed	Not allowed
Computer Rights	Full Access Role	Auditor Role	New Role Defaults
View	Allowed, All Computers	Allowed, All Computers	Allowed, All Computers
Edit	Allowed, All Computers	Not allowed, All Computers	Not allowed, All Computers
Delete	Allowed, All Computers	Not allowed, All Computers	Not allowed, All Computers
Dismiss Alerts for	Allowed, All Computers	Not allowed, All Computers	Not allowed, All Computers
Tag Items for	Allowed, All Computers	Not allowed, All Computers	Not allowed, All Computers
View non-selected computers and data (e.g. events, reports)	Allowed	Allowed	Allowed, All Computers
View events and Alerts not related to computers	Allowed	Allowed	Allowed, All Computers
Create new computers in selected groups	Allowed	Not allowed	Not allowed
Add or remove sub-groups in selected groups	Allowed	Not Allowed	Not allowed
Import computer files	Allowed	Not allowed	Not allowed
Add, remove, and synchronize Directories	Allowed	Not allowed	Not allowed
Add, remove, and synchronize VMware vCenters	Allowed	Not allowed	Not allowed
Policy Rights	Full Access Role	Auditor Role	New Role Defaults
View	Allowed, All Policies	Allowed, All Policies	Allowed, All Policies
Edit	Allowed, All Policies	Not allowed, All Policies	Not allowed, All Policies
Delete	Allowed, All Policies	Not allowed, All Policies	Not allowed, All Policies
View non-selected Policies	Allowed	Allowed	Allowed
Create new Policies	Allowed	Not allowed	Not allowed
Import Policies	Allowed	Not allowed	Not allowed
User Rights (See note on User rights below)	Full Access Role	Auditor Role	New Role Defaults
View Users	Allowed	Allowed	Not allowed
Create Users	Allowed	Not allowed	Not allowed
Edit User Properties	Allowed	Not allowed	Not allowed
Delete Users	Allowed	Not allowed	Not allowed
View Roles	Allowed	Allowed	Not allowed
Create Roles	Allowed	Not allowed	Not allowed
Edit Role Properties	Allowed	Not allowed	Not allowed
Delete Roles	Allowed	Not allowed	Not allowed
Delegate Authority	Allowed	Not allowed	Not allowed
Other Rights	Full Access Role	Auditor Role	New Role Defaults
Alerts	Full (Can Dismiss Global Alerts)	View-Only	View-Only
Alert Configuration	Full (Can Edit Alert Configurations)	View-Only	View-Only
Malware Scan Configuration	Full (Can Create, Edit, Delete Malware Scan Configuration)	View-Only	View-Only
Quarantined File	Full (Can Delete, Download Quarantined File)	View-Only	View-Only
Firewall Rules	Full (Can Create, Edit, Delete Firewall Rules)	View-Only	View-Only
Firewall Stateful Configurations	Full (Can Create, Edit, Delete Firewall Stateful Configurations)	View-Only	View-Only
Intrusion Prevention Rules	Full (Can Create, Edit, Delete)	View-Only	View-Only
Application Types	Full (Can Create, Edit, Delete)	View-Only	View-Only
Integrity Monitoring Rules	Full (Can Create, Edit, Delete)	View-Only	View-Only
Log Inspection Rules	Full (Can Create, Edit, Delete)	View-Only	View-Only
Log Inspection Decoders	Full (Can Create, Edit, Delete)	View-Only	View-Only

RIGHTS	**SETTINGS BY ROLE**		
Directory Lists	Full (Can Create, Edit, Delete)	View-Only	View-Only
Files Lists	Full (Can Create, Edit, Delete)	View-Only	View-Only
Files Extension Lists	Full (Can Create, Edit, Delete)	View-Only	View-Only
IP Lists	Full (Can Create, Edit, Delete)	View-Only	View-Only
MAC Lists	Full (Can Create, Edit, Delete)	View-Only	View-Only
Port Lists	Full (Can Create, Edit, Delete)	View-Only	View-Only
Contexts	Full (Can Create, Edit, Delete)	View-Only	View-Only
Schedules	Full (Can Create, Edit, Delete)	View-Only	View-Only
System Settings (Global)	Full (Can View, Edit System Settings (Global))	View-Only	Hide
System Information	Full (Can View System Information, Can Edit and Decommission Manager Nodes, Can Manage System Extensions)	View-Only	Hide
Diagnostics	Full (Can Create Diagnostic Packages)	View-Only	View-Only
Tagging (Advanced)	Full (Can Tag (Items not belonging to Computers), Can Delete Tags, Can Update Non-Owned Auto-Tag Rules, Can Run Non-Owned Auto-Tag Rules, Can Delete Non-Owned Auto-Tag Rules)	View-Only	View-Only
Tasks	Full (Can View, Add, Edit, Delete Tasks, Execute Tasks)	View-Only	Hide
Contacts	Full (Can View, Create, Edit, Delete Contacts)	View-Only	Hide
Licenses	Full (Can View, Change License)	View-Only	Hide
Updates	Full (Can Add, Edit, Delete Software; Can View Update For Components; Can Download, Import, Apply Update Components; Can Delete Deep Security Rule Updates)	View-Only	Hide
Asset Values	Full (Can Create, Edit, Delete Asset Values)	View-Only	View-Only
Certificates	Full (Can Create, Delete SSL Certificates)	View-Only	View-Only
Update Relay Lists	Full (Can Create, Edit, Delete Relay Lists)	View-Only	View-Only

Note on User Rights

The **User Rights** area on the **User Rights** tab of the **Role Properties window** has three general User rights options (**Change own password and contact information only**, **Create and manage users with equal or less access**, and **Have full control over all Roles and users**) and a **Custom** option.

The custom settings corresponding to the **Change own password and contact information only** option are listed in the following table:

Custom settings corresponding to "Change own password and contact information only" option	
Users	
Can View Users	Not allowed
Can Create New Users	Not allowed
Can Edit User Properties (User can always edit select properties of own account)	Not allowed
Can Delete Users	Not allowed
Roles	
Can View Roles	Not allowed

Custom settings corresponding to "Change own password and contact information only" option	
Can Create New Roles	Not allowed
Can Edit Role Properties (Warning: conferring this right will let users with this Role edit their own rights)	Not allowed
Can Delete Roles	Not allowed
Delegate Authority	
Can only manipulate users with equal or lesser rights	Not allowed

The custom settings corresponding to the **Create and manage users with equal or less access** option are listed in the following table:

Custom settings corresponding to "Create and manage users with equal or less access" option	
Users	
Can View Users	Allowed
Can Create New Users	Allowed
Can Edit User Properties (User can always edit select properties of own account)	Allowed
Can Delete Users	Allowed
Roles	
Can View Roles	Not allowed
Can Create New Roles	Not allowed
Can Edit Role Properties (Warning: conferring this right will let users with this Role edit their own rights)	Not allowed
Can Delete Roles	Not allowed
Delegate Authority	
Can only manipulate users with equal or lesser rights	Allowed

The custom settings corresponding to the **Have full control over all Roles and users** option are listed in the following table:

Custom settings corresponding to "Have full control over all Roles and users" option	
Users	
Can View Users	Allowed
Can Create New Users	Allowed
Can Edit User Properties (User can always edit select properties of own account)	Allowed
Can Delete Users	Allowed
Roles	
Can View Roles	Allowed
Can Create New Roles	Allowed
Can Edit Role Properties (Warning: conferring this right will let users with this Role edit their own rights)	Allowed
Can Delete Roles	Allowed
Delegate Authority	
Can only manipulate users with equal or lesser rights	N/A

Database Backup and Recovery

Backup

Database backups are for restoring your Deep Security system in the event of a catastrophic failure, or for transferring your Deep Security Manager to another computer.

Note: *The Deep Security Manager cannot initiate a backup of an Oracle database. To backup your Oracle database consult your Oracle documentation.*

Internal Database or MS SQL Server Database

Database backups can carried out using the **Scheduled Tasks** interface. Go to the **Administration > Scheduled Tasks** page. Click **New** and select "New Scheduled Task" to display the **New Scheduled Task** wizard. Give a name to this task and choose "Backup" from the drop-down list. The next page will prompt you for how often you want this task carried out and when. To carry out a one-time-only backup, choose "Once Only" and enter a time (5 minutes from now, for example). The next page will prompt you for a location to store the backup files. Click through to the end of the wizard to finish. A complete backup shouldn't take more than a minute or so to complete.

A "date-named" folder will be created in the backup location you specified. If you are using the Deep Security Manager's embedded Apache Derby database (which is intended for test purposes), a folder structure will be created beneath it that maps to the folders in the Deep Security Manager's install directory. To restore this database, shut down the "Trend Micro Deep Security Manager" service (using the Services Microsoft Management Console), copy the backup folders into the corresponding folders of the install directory, and restart Deep Security Manager.

If you are using a SQL Server database, a SQL Server database backup file named **[timestamp].dsmbackup** will be written to the backup folder specified in the Scheduled Task. (For instructions on how to restore a SQL Server database refer to your SQL Server documentation.)

Restore

Note: *The Deep Security Manager cannot backup or restore an Oracle database. To backup or restore your Oracle database consult your Oracle documentation.*

Database Only

1. Stop the Deep Security Manager service
2. Restore the database (Must be a database from the same version number of the Manager)
3. Start the service
4. Verify contents restored
5. Update all of the computers to ensure they have the proper configuration

Both Deep Security Manager and Database

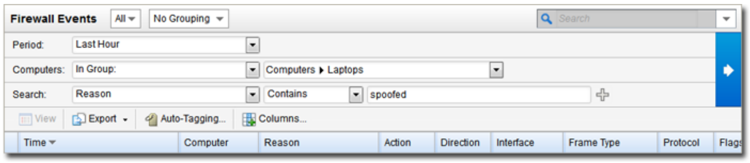
- Remove any remnants of the lost/corrupted Manager and database
- Install a fresh Deep Security Manager using a fresh/empty database
- Stop the Deep Security Manager service

- Restore the database over the freshly installed one, must be the same database name (Must be a database from the same version number of the Manager)
- Start the Deep Security Manager service
- Verify contents restored
- Update all of the computers to ensure they have the proper configuration

Export

You can export various Deep Security objects in XML or CSV format:

- **Events:** Go to one of the Events pages and use the Advanced Search options to filter the Event data. For example, you could search for all **Firewall Events** for computers in the **Computers > Laptops** computer group that were logged within the **Last Hour** (the Period bar) whose **Reason** column **Contained** the word "**spoofed**" (the Search bar).



Period: Last Hour

Computers: In Group: Computers ▸ Laptops

Search: Reason Contains spoofed

  Press the submit button (with the right-facing arrow) to execute the "query". Then press **Export** to export the filtered data in CSV format. (You can export all the displayed entries or just selected/highlighted data.) (The exporting of logs in this format is primarily for integration with third-party reporting tools.)

- **Computer Lists:** computer Lists can be exported in XML or CSV format from the **Computers** page. You may want to do this if you find you are managing too many computers from a single Deep Security Manager and are planning to set up a second Manager to manage a collection of computers. Exporting a list of selected computers will save you the trouble of re-discovering all the computers again and arranging them into groups.

  Note: *Policy, Firewall Rule, and Intrusion Prevention Rule settings will not be included. You will have to export your Firewall Rules, Intrusion Prevention Rules, Firewall Stateful Configurations, and Policies as well and then reapply them to your computers.*

- **Policies:** Policies are exported in XML format from the **Policies** page.

  Note: *When you export a selected Policy to XML, any child Policies the Policy may have are included in the exported package. The export package contains all the actual objects associated with the policy except: Intrusion Prevention Rules, Log Inspection Rules, Integrity Monitoring Rules, and Application Types.*

- **Firewall Rules:** Firewall Rules can be exported to an XML or CSV file using the same searching/filtering techniques as above.
- **Firewall Stateful Configurations:** Firewall Stateful Configurations can be exported to an XML or CSV file using the same searching/filtering techniques as above.
- **Intrusion Prevention Rules:** Intrusion Prevention Rules can be exported to an XML or CSV file using the same searching/filtering techniques as above.
- **Integrity Monitoring Rules:** Integrity Monitoring Rules can be exported to an XML or CSV file using the same searching/filtering techniques as above.
- **Log Inspection Rules:** Log Inspection Rules can be exported to an XML or CSV file using the same searching/filtering techniques as above.
- **Other Common Objects :** All the reusable components Common Objects can be exported to an XML or CSV file the same way.

When exporting to CSV, only displayed column data is included. (Use the **Columns...** tool to change which data is displayed.) Grouping is ignored so the data may not be in same order as on the screen.

Importing

To import each of the individual objects into Deep Security, choose "Import From File" from the drop-down list next to the **New** button in the toolbar of the objects' respective pages.

Adding Computers

To protect computers with Deep Security, they must first be added to the **Computers** list in the Deep Security Manager. New computers can be added to your Computers List by:

- ***Importing computers from a local network (page 67)*** If you are protecting computers on a locally accessible network you can add them individually by supplying their IP address or hostname or you can perform a Discovery operation to search for all computers visible to the Deep Security Manager.
- ***Importing a Directory (page 69)*** You can import a Microsoft Active Directory or any other LDAP-based directory service.
- ***Importing computers from a VMware vCenter (page 73)*** You can import a VMware vCenter and provide the hosted VMs with Agent-based or Agentless protection.
- ***Importing computers from a Cloud Provider (page 75)*** You can import virtual machines being hosted on VMware vCloud or Amazon EC2 infrastructures.
- ***Using a deployment script (page 79)*** If you are going to be adding/protecting a large number of computers you may want to automate the process of installing and activating Agents. You can use the Deep Security Manager's deployment script generator to generate scripts you can run on your computers which will install the Agents and optionally perform subsequent tasks like activation and Policy assignment. The scripts are also useful as a starting template to create your own customized scripts to execute various additional available commands.

Local Network

Agent-Initiated Activation

If the Deep Security Manager is hosted outside of your local network and cannot initiate communication with the computers on your network, you will need to instruct the computers to perform Agent-initiated activation. With Agent-initiated activation, you must install the Deep Security Agent on the computer and then run a set of command-line instructions which tell the Agent to communicate with the Deep Security Manager. During the communication, the Deep Security Manager activates the Agent and can be further instructed to perform a number of other actions such as assigning a security Policy, making the computer a member of a computer Group, and so on.

If you are going to add a large number of computers to the Deep Security Manager at one time, you can use the command-line instructions to create scripts to automate the process. For more information on Agent-initiated activation, scripting, and command line options, see ***Command-Line Utilities (page 167)***.

Entering the IP Address or Hostname Directly

You can manually add an individual computer.

To manually add a computer:

1. Go to the **Computers** page and click **New** in the toolbar to display the **New Computer** wizard.
2. Enter the new computer's IP address or hostname.
3. Select a Policy to assign to it from the drop-down list.
4. Select a Relay Group from which the new computer will download Security Updates.
5. Click **Next** to begin the search for the computer.

If the computer is detected and an Agent is installed and running on that computer, the computer will be added to your computer List and the Agent will be activated.

Note: *"Activating" an Agent means that the Manager communicates with the Agent sending it a unique "fingerprint". The Agent will then use this fingerprint to uniquely identify the Deep Security Manager and will not accept instructions from any other Managers that might try to contact it.*

If a Policy has been assigned to the computer, the Policy will be deployed to the Agent and the computer will be protected with all the rules and configurations that make up the Policy. The Agent will communicate with the Relay Group assigned to and download the latest Security Update.

Note: *By default, the Security Updates delivered by Relay Groups include new malware patterns and updates to the detection engines. If you don't want to update the Deep Security detection software on your computers, you can configure specific Relay Groups to only deliver pattern updates. For more information on configuring Relay Groups and Updates, see **Relay Groups (page 48)**.*

If the computer is detected but no Deep Security Agent is present, you will be told that the computer can still be added to your computer list but that you still have to install an Agent on the computer. Once you install an Agent on the computer, you will have to find the computer in your computer List, right-click it, and choose "Activate/Reactivate" from the context menu.

If the computer is not detected (not visible to the Manager), you will be told that you can still add the computer but that when it becomes visible to the Manager you will have to activate it as above.

Performing a Discovery Operation

A discovery operation scans the network for visible computers. To initiate a discovery operation, click **Discover...** in the toolbar on the **Computers** page. The **Discover Computers** dialog will appear.

You are provided several options to restrict the scope of the scan. You can choose to perform a port scan of each discovered computer. Use this option carefully as it can take a lot of time if you are discovering/scanning a large number of computers.

When discovering computers you can specify a computer group to which they should be added. Depending on how you have chosen to organize your computer groups, it may be convenient to create a computer group called "Newly Discovered Computers", or "Newly Discovered Computers on Network Segment X" if you will be scanning multiple network segments. You can then move your discovered computers to other computer groups based on their properties and activate them.

During discovery, the Manager searches the network for any visible computers. When a computer is found, the Manager attempts to detect whether an Agent is present. When discovery is complete, the Manager displays all the computers it has detected and displays their status in the **Status** column. After discovery operations, a computer can be in one of the following states:

- **Discovered (No Agent):** The computer has been detected but no Agent is present. The computer may also be in this state if an Agent is installed but has been previously activated and is configured for Agent initiated communications. In this case, you will have to deactivate and then reactivate the Agent. ("No Agent" will also be reported if the Agent is installed but not running.)
- **Discovered (Activation Required):** The Agent is installed and listening, and has been activated, but is not yet being managed by the Manager. This state indicates that this Manager was at one point managing the Agent, but the Agent's public certificate is no longer in the Manager's database. This may be the case if the if the computer was removed from the Manager and then discovered again. To begin managing the Agent on this computer, right-click the computer and select "Activate/Reactivate". Once reactivated, the **Status** will change to "Online".
- **Discovered (Deactivation Required):** The Agent is installed and listening, but it has already been activated by another Manager. In this case the Agent must be deactivated (reset) prior to activation by this Manager. Deactivating an Agent must be done using the Manager that originally activated it or it can be reset directly on the computer. To deactivate the Agent from the Manager, right-click the computer and choose **Actions > Deactivate**.

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

Active Directory

Deep Security Manager supports the discovery of computers using Microsoft Active Directory. Computers are imported to the Deep Security Manager and are grouped and displayed according to the structure of the Active Directory.

To import a Microsoft Active Directory:

1. Right-click **Computers** in the navigation panel and select **Add Directory...**
2. Type a name and description for your imported directory (it doesn't have to match that of the Active Directory), the IP and port of the Active Directory server, and finally your access method and credentials.

   Note: *You must include your domain name with your username in the* ***User Name*** *field.*

   Click **Next** to continue.
3. The second page of the **New Directory** wizard asks for schema details. (The default values can be left.)

   Note: *The* ***Details*** *window of each computer in the Deep Security Manager has a "Description" field. To use an attribute of the "Computer" object class from your Active Directory to populate the "Description" field, type the attribute name in the* ***Computer Description Attribute*** *text box.*

   Set the **Create a Scheduled Task to Synchronize this Directory** checkbox if you want to automatically keep this structure in the Deep Security Manager synchronized with your Active Directory Server. If this checkbox is selected, the **Scheduled Task** wizard will appear when you are finished adding the directory. (You can set this up later using the **Scheduled Tasks** wizard: **Administration > Scheduled Tasks**.) Click **Next** to continue.
4. When the Manager is finished importing your directory, you will be shown a list of computers that were added. Click **Finish**.

The directory structure now appears under **Computers** in the navigation panel.

Additional Active Directory Options

Right-clicking an Active Directory structure gives you the following options that are not available for ordinary computer groups listed under **Computers**.

- **Remove Directory**
- **Synchronize Now**

Remove Directory

When you remove a directory from the Deep Security Manager, you have the following options:

- **Remove directory and all subordinate computers/groups from DSM:** removes all traces of the directory.
- **Remove directory, but retain computer data and computer group hierarchy:** turns the imported directory structure into identically organized regular computer groups, no longer linked with the Active Directory server.
- **Remove directory, retain computer data, but flatten hierarchy:** removes links to the Active Directory server, discards directory structure, and places all the computers into the same computer group.

Synchronize Now

Synchronizes the directory structure in the Deep Security Manager with the Active Directory Server.

You can automate this procedure as a **Scheduled Task**.

Deep Security can leverage Active Directory information for computer discovery and User account and Contact creation.

Port Requirements

Depending on the nature of Active Directory integration, the following ports may be required:

- Port 389: Used for non-SSL based access methods
- Port 636: Used for SSL-based access methods

Note: *To use SSL-based access methods, the Active Directory server must have SSL enabled, which is often not the default condition.*

Server Certificate Usage

Computer discovery can use both SSL-based and clear text methods, while users and contacts are restricted to non-anonymous SSL methods. The latter restriction ensures that user account and usage is protected. SSL-based access methods will only work with SSL-enabled Active Directory servers, so users and contacts can only be imported from suitably configured servers.

SSL-enabled Active Directory servers must have a server certificate installed. This may either be self-signed, or created by a third-party certificate authority.

To verify the presence of a certificate, open the Internet Information Services (IIS) Manager on the Active Directory server, and select **Server Certificates**.

Filtering Active Directory Objects

When importing Active Directory objects, search filters are available to manage the objects that will be returned. By default the wizard will only show groups. You can add additional parameters to the filter to further refine the selections. For additional information about search filter syntax, refer to http://msdn.microsoft.com/en-us/library/aa746475(v=vs.85).aspx

Importing Users and Contacts

Deep Security can import user account information from Active Directory and create corresponding Deep Security Users or Contacts. This offers the following advantages:

- Users can use their network passwords as defined in Active Directory.
- Administrators can centrally disable accounts from within Active Directory.
- Maintenance of contact information is simplified (e.g., email, phone numbers, etc.) by leveraging information already in Active Directory.

Both Users and Contacts can be imported from Active Directory. Users have configuration rights on the Deep Security Manager. Contacts can only receive Deep Security Manager notifications. The synchronization wizard allows you to choose which Active Directory objects to import as users and which to import as contacts.

Note: *To successfully import an Active Directory user account into Deep Security as a Deep Security User or Contact, the Active Directory user account must have a* ***userPrincipalName*** *attribute value. (The* ***userPrincipalName*** *attribute corresponds to an Active Directory account holder's "User logon name".)*

To import Users or Contacts:

1. In the navigation panel, click on **Administration > User management > Users** or **Administration > User Management** and go to the **Users** or **Contacts** screen.

2. Click **Synchronize with Directory**. If this is the first time User or Contact information is imported, the wizard displays the server information page. (For information about how to set the options on this page, see the section above on importing computers.) Otherwise, the Synchronize with Directory wizard is displayed.
3. Select the appropriate access options and provide logon credentials. Click **Next**.
4. On the **Select Groups to Synchronize** page, select which Active Directory objects to import as either **Users** or **Contacts**. Unselected objects will not be imported.
5. On the **Select Options for New users/Contacts** page, define the default User Roles given to imported accounts. Choose the Role with the least access rights to avoid inadvertently giving individuals inappropriate privileges. Click **Next**.
6. After synchronization, the wizard generates a report, indicating the number of objects imported. Click **Finish**.

Once imported, these accounts can be differentiated from organic Deep Security accounts by the inability to change General Information for the account.

Keeping Active Directory Objects Synchronized

Once imported, Active Directory objects must be continually synchronized with their Active Directory servers to reflect the latest updates for these objects. This ensures, for example, that Computers that have been deleted in Active Directory are also deleted in Deep Security Manager. To keep the Active Directory objects that have been imported to the Deep Security Manager synchronized with Active Directory, it is essential to set up a scheduled task that synchronizes Directory data. Both the user/contact and host importation wizards include the option to create these scheduled tasks.

It is also possible to create this task using the Scheduled Task wizard. On-demand synchronization can be performed using the **Synchronize Now** option for hosts and **Synchronize with Directory** button for users and contacts.

Removing an Active Directory from Deep Security Manager

You can remove a Deep Security Manager-Active Directory integration for both computer discovery and users and contacts.

Removing Active Directory from the Computers List

When a Directory is removed from the Computers list, you are presented with the following options:

- Remove Directory and all subordinate computers/groups from Deep Security Manager: All host records will be removed from the Computer list
- Remove Directory but retain computer data and group hierarchy: The existing Active Directory structure will be retained, but this will no longer be synchronized with Active Directory. Since the structure is unaffected, User and Role access to folders and hosts will be retained
- Remove Directory, retain computer data, but flatten hierarchy: Host records will be stripped of their original hierarchy, but will all be stored in a group named after the former Directory. User and Role access to the Directory will be transferred to the group, thus maintaining access to all of the hosts.

To remove a directory:

1. On the Computers page, right-click the Directory, and select **Remove Directory**.
2. Select a removal option in the Remove Directory dialog box.
3. Confirm the action in the dialog box that follows. This completes directory removal.

Removing Active Directory Users and Contacts

Unlike Directory removal, which provides an option to retain certain types of information, removal of users and contacts deletes all of these records. This action, therefore, cannot be performed while logged on to the Deep Security Manager console with an imported user account. Doing so will result in an error.

To remove users and contacts:

1. On either the Users or Contacts page, click **Synchronize with Directory**.
2. Select **Discontinue Synchronization** then click **OK**. The wizard displays a summary page of the changes that will be made.
3. Click **Finish**.

VMware vCenter

Agent-based or Agentless Protection of VMs

Deep Security can protect virtual machines using only the Virtual Appliance, or you can use the Coordinated Approach and use both the Virtual Appliance and an Agent to protect the computer.

The Virtual Appliance and the Coordinated Approach using Deep Security Agents

The Virtual Appliance

The Deep Security Virtual Appliance provides Anti-Malware, Firewall, Intrusion Detection/Prevention, Application Control, Web Application, and Integrity Monitoring protection to Virtual Machines without requiring the presence of an in-guest Agent. The Virtual Appliance uses VMware's VMsafe-NET API to intercept network traffic at the hypervisor in a vSphere environment. Security policies are applied per virtual machine. The Virtual Appliance provides some distinct security advantages over scenarios with an in-guest Agent:

- The Appliance is isolated from the guest. The guest can operate with only the minimum required software being installed.
- Short-lived and reverted machines for which administrator time may not have been allocated for installing security software can be easily and quickly protected.
- Virtual machines and other Appliances whose operating systems are not directly accessible can be protected, even those machines being managed by other administrators.

The Deep Security Virtual Appliance simplifies deployment. There is no need to remotely install Agent software on the virtual machine. Connectivity to the virtual machine from Deep Security is not required.

Coordinated Protection

Using the Virtual Appliance to protect virtual machines doesn't preclude the use of Deep Security Agents for virtual machines on the same host. When coordinated protection is implemented on virtual machines, the Virtual Appliance automatically provides back up protection if the if the Agent ever goes offline.

This coordinated approach provides the following benefits:

- Recommendation Scans can be run on the virtual machines.
- Provides mobility to the virtual machines. They can be moved between data centers or cloud providers and the protection moves with them.
- Performance improvement. While the Deep Security Agent is active on the virtual machine, the Virtual Appliance automatically passes traffic through to the Agent.
- Allows you to implement the additional Integrity Monitoring and Log Inspection modules on the virtual machine by using the Deep Security Agent to provide the protection.

For the Coordinated Approach to be implemented for a particular protection module, both the Agent and the Appliance have to implement that protection. The following table shows the Deep Security protection modules that can make use of the Coordinated Approach:

	Supported by Appliance	**Supported by Agent**	**Coordinated Approach Available**
Anti-Malware	Yes	Yes	Yes
Web Reputation	Yes	Yes	Yes
Firewall	Yes	Yes	Yes
Intrusion Prevention	Yes	Yes	Yes
Integrity Monitoring	Yes	Yes	Yes

	Supported by Appliance	Supported by Agent	Coordinated Approach Available
Log Inspection	No	Yes	No

Note: *Some features are not available on all platforms. For a complete detailed list of supported features by platform, see the* ***Supported Features and Platforms*** *guide.*

Adding a VMware vCenter

To add a VMware vCenter to the list of managed computers:

1. Click **Computers** > **New** > **Add VMware vCenter**.
2. In the **Add VMware vCenter** wizard that appears, provide the server address (IP or hostname) and port, a name and description, and the username and password for the ESXiServer. Click **Next**.
3. Enter the vShield Manager or NSX Manager Server Address, Username and Password. Click **Next**.
4. If prompted, accept the vShield Manager or NSX Manager SSL certificate and the vCenter certificate.
5. The wizard will display the details of the vCenter being added. Click **Finish** and then **Close** to close the wizard.

Note: *Real-time synchronization will be maintained with this VMware vCenter to keep the information displayed in the Deep Security Manager up-to-date (number of VMs, their status, etc.).*

The VMware vCenter is now displayed among your other computers on the **Computers** page.

Now that your virtual machines are listed in the Deep Security Manager, you can protect them with locally installed Deep Security Agents, or you can provide Agentless protection by installing a Deep Security Virtual Appliance. For information on providing Agentless protection with a Deep Security Virtual Appliance, please consult the Deep Security Installation Guide.

Cloud Account

Deep Security supports Agent-based protection of computing resources from the following Cloud Provider services:

- **Amazon EC2**
- **VMware vCloud**
- **Microsoft Azure**

Once you have imported the resources from the Cloud Provider account into the Deep Security Manager, the computers in the account are managed like any computer on a local network.

To import cloud resources into their Deep Security Manager, Deep Security Users must first have an account with which to access the cloud provider service resources. For each Deep Security User who will import a cloud account into the Deep Security Manager, Trend Micro Recommends creating dedicated account for that Deep Security Manager to access the cloud resources. That is, Users should have one account to access and control the virtual machines themselves, and a separate account for their Deep Security Manager to connect to those resources.

Note: *Having a dedicated account for Deep Security ensures that you can refine the rights and revoke this account at any time. It is recommended to give Deep Security a Access/Secret key with read-only rights at all times.*

Note: *The Deep Security manager only requires read-only access to import the cloud resources and mange their security.*

Creating an Amazon Web Services account for the Deep Security Manager

To create an Amazon Web Services account for access by a Deep Security Manager:

1. Log in to your Amazon Web Services Console.
2. Go to **IAM (Identity and Access Management)**.
3. In the left navigation pane, click on **Users**.
4. Click **Create New Users** to open the **Create User** dialog window.
5. Enter a username and select the **Generate an access key for each User** option.
6. Record the generated **User Security Credentials** (Access Key and Secret Key) and close the dialog window.
7. Back on the Users page, select the User and then click on the **Permissions** tab at the bottom of the page.
8. Click on **Attach User Policy** at the bottom of the window to display the **Manage User Permissions** dialog window.
9. Select the **Policy Generator** option.
10. Click the **Select** button to edit the permissions you will grant to the new User.
11. Select **Effect: Allow**.
12. Select **AWS Service: Amazon EC2.**
13. Select the following **Actions:**
    - **DescribeImages**
    - **DescribeInstances**
    - **DescribeTags**
14. Leave the **Amazon Resource Name** as it is.
15. Click **Add Statement**.
16. Click **Continue** to generate the permission policy.
17. Click **Apply Policy** to apply the policy to the user account.

The Amazon Web Services account is now ready for access by a Deep Security Manager.

> Note: *To import the Amazon AWS resources into the Deep Security Manager, the User will be prompted for the **Region** the resources are hosted in. (If resources are hosted in multiple regions, the User will have to add the resources independently for each region), the **Access Key Id** , and the **Secret Access Key** .*

Importing Computers from a Amazon Web Services account

To import Amazon Web Services cloud resources:

1. In the Deep Security Manager, go to the **Computers** section, right-click **Computers** in the navigation panel and select **Add Cloud Account...** to display the **Add Cloud Account** wizard.
2. Select **Amazon** as the Cloud Provider Type.
3. Select the **Region** the cloud resources are hosted in. (If resources are hosted in multiple regions, you will have to add the resources independently for each region.)
4. Enter a **Name** and **Description** of the resources you are adding. (These are only used for display purposes in the Deep Security Manager.)
5. Enter the **Access Key Id** and **Secret Access Key** provided to you by your AWS administrator. Click **Next** .
6. Deep Security Manager will verify the connection to the cloud resources and display a summary of the import action. Click **Finish** .
7. Upon successfully importing the Cloud Provider resources, the wizard will display the results of the action.

The Amazon AWS resources now appear in the Deep Security Manager under their own branch under **Computers** in the navigation panel.

Creating a VMware vCloud Organization account for the Deep Security Manager

To create a VMware vCloud Organization account for access by a Deep Security Manager:

1. Log in to VMware vCloud Director.
2. On the **System** tab, go to **Manage And Monitor**.
3. In the left navigation pane, click **Organizations**.
4. Double-click the Organization you wish to give the Deep Security User access to.
5. On the **Organizations** tab, click **Administration**.
6. In the left navigation pane, go to **Members > Users**.
7. Click the " plus " sign to create a new User.
8. Enter the new User's credentials and other information, and select **Organization Administrator** as the User's **Role**.

   > Note: ***Organization Administrator** a simple pre-defined Role you can assign to the new user account, but the only privilege required by the account is **All Rights > General > Administrator View** and you should consider creating a new vCloud role with just this permission. For more detailed information on preparing vCloud resources for Deep Security integration, see the Installation Guide.*

9. Click **OK** to close the new User's properties window.

The vCloud account is now ready for access by a Deep Security Manager.

> Note: *To import the VMware vCloud resources into the Deep Security Manager, Users will be prompted for the **Address** of the vCloud, their **User name** , and their **Password** .*
>
> *The **User name** must include "@orgName". For example if the vCloud account's username is **kevin** and the vCloud Organization you've given the account access to is called **CloudOrgOne**, then the Deep Security User must enter **kevin@CloudOrgOne** as their username when importing the vCloud resources.*

*(For a vCloud administrator view, use **@system**.)*

Importing Computers from a VMware vCloud Organization Account

To import VMware vCloud Organization resources:

1. In the Deep Security Manager, go to the **Computers** section, right-click **Computers** in the navigation panel and select **Add Cloud Account...** to display the **Add Cloud Account** wizard.
2. Select **vCloud** as the Cloud Provider Type.
3. Enter a **Name** and **Description** of the resources you are adding. (These are only used for display purposes in the Deep Security Manager.)
4. Enter the vCloud **Address**. (The hostname of the vCloud Director host machine.)
5. Enter your **User name** and **Password**.

   Note: *Your **User name** must be in the form **username@vcloudorganization**.*

6. Click **Next**.
7. Deep Security Manager will verify the connection to the cloud resources and display a summary of the import action. Click **Finish**.

The VMware vCloud resources now appear in the Deep Security Manager under their own branch under **Computers** in the navigation panel.

Importing Computers from a VMware vCloud Hybrid Services (vCHS) Virtual Data Center

To import a VMware vCloud Hybrid Services (vCHS) data center:

1. In the Deep Security Manager, go to the **Computers** section, right-click **Computers** in the navigation panel and select **Add Cloud Account...** to display the **Add Cloud Account** wizard.
2. Select **vCloud** as the Cloud Provider Type.
3. Enter a **Name** and **Description** of the vCHS virtual data center you are adding. (These are only used for display purposes in the Deep Security Manager.)
4. Enter the **Address** of the vCHS virtual data center.

   Note: ***To determine the address of the vCHS virtual data center:***

   1. *Log in to your vCHS portal.*
   2. *On the **Dashboard** tab, click on the data center you want to import into Deep Security. This will display the **Virtual Data Center Details** information page.*
   3. *In the Related Links section of the **Virtual Data Center Details** page, click on **vCloud Director API URL**. This will display the full URL of the vCloud Director API.*
   4. *Use the hostname only (not the full URL) as the Address of the vCHS virtual data center that you are importing into Deep Security.*

5. Enter your **User name** and **Password**.

   Note: *Your **User name** must be in the form **username@virtualdatacenterid**.*

6. Click **Next** .
7. Deep Security Manager will verify the connection to the virtual data center and display a summary of the import action. Click **Finish**.

The VMware vCloud Hybrid Services data center now appears in the Deep Security Manager under its own branch under **Computers** in the navigation panel.

Microsoft Azure

Deep Security Agents can be installed on machine instances running in the Microsoft Azure cloud through the VM Extension option on the Azure portal. Alternatively, Deep Security Agent deployment scripts can be created with the Deep Security Deployment Script Generator to install Deep Security Agents in a Microsoft Azure environment. (See ***Deployment Scripts (page 79)***.)

Managing a Cloud Account

To implement Deep Security protection on your Cloud computers, you must install an Agent and assign a Policy to the computer like any other computers on a network. See the Installation Guide for instructions on installing Deep Security Agents on your computers. Computers running in a Cloud Provider infrastructure are managed by Deep Security no differently than any other computers using Agent-based protection.

If synchronization is enabled, the list of Cloud Provider account instances is updated every ten minutes. To enable or disable regular synchronization, open the Cloud Provider account **Properties** window by right-clicking on the Cloud Provider account in the navigation panel and then go to the **General** tab. (You can determine your own synchronization schedules by automating this procedure as a **Scheduled Task** in the **Administration** section.)

Removing a Cloud Account

Removing a Cloud Provider account from Deep Security Manager permanently removes the account from the Deep Security database. Your account with your Cloud Provider is unaffected and any Deep Security Agents that were installed on the instances will still be installed, running, and providing protection (although they will no longer receive Security Updates.) If you decide to re-import computers from the Cloud Provider Account, the Deep Security Agents will download the latest Security Updates at the next scheduled opportunity.

To remove a Cloud Provider account from Deep Security Manager:

1. Go to the **Computers** page, right-click on the Cloud Provider account in the navigation panel, and select **Remove Cloud Account...** .
2. Confirm that you want to remove the account.
3. The account is removed from the Deep Security Manager.

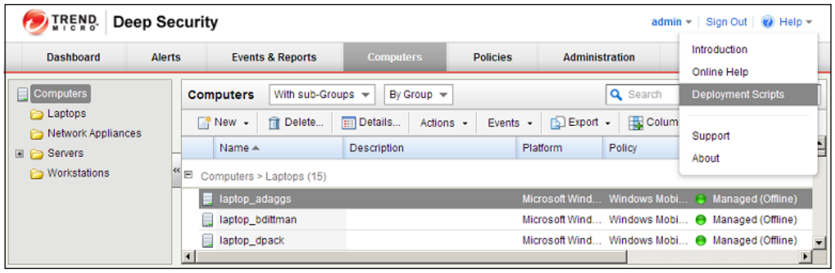
Deployment Scripts

Adding a computer to your list of protected resources in Deep Security and implementing protection is a multi-step process. Almost all of these steps can be performed from the command line on the computer and can therefore be scripted. The Deep Security Manager contains a deployment script writing assistant which can be accessed from the Manager's Help menu.

Note: *Agent-initiated Activation must be enabled before Deployment Scripts can be generated.* ***Got Administration > System Settings > Agents*** *and select* ***Allow Agent-Initiated Activation.***

To generate a deployment script:

1. Start the Deployment Script generator by selecting **Deployment Scripts** from the Deep Security Manager's Help menu (at the top right of the Deep Security Manager window).



Computers > Laptops (15)

Name	Description	Platform	Policy	
laptop_adaggs		Microsoft Wind...	Windows Mobi...	Managed (Offline)
laptop_bdittman		Microsoft Wind...	Windows Mobi...	Managed (Offline)
laptop_dpack		Microsoft Wind...	Windows Mobi...	Managed (Offline)

2. Select the platform to which you are deploying the software. (Platforms listed in the drop-down menu will correspond to the software that you have imported into the Deep Security Manager from the Trend Micro Download Center. For information on importing Deep Security Software, see **Administration > Updates** in the Deep Security Manager Interface Guide or the online help.)
3. Select **Activate the Agent Automatically**. (Agents must be activated by the Deep Security Manager before a protection Policy can be implemented.)
4. Select the Policy you wish to implement on the computer (optional)
5. Select the Computer Group (optional)
6. Select the Relay Group (optional)

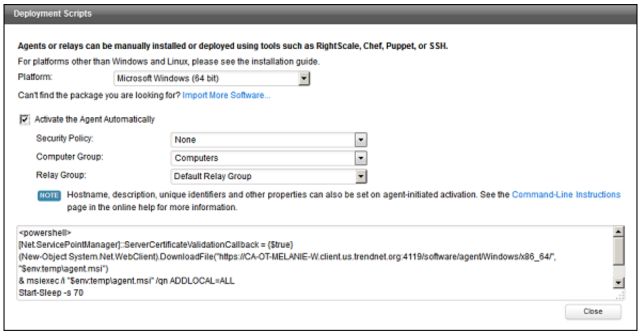
As you make the above selections, the Deployment Script Generator will generate a script which you can import into your deployment tool of choice.

If you are using Amazon Web Services and deploying new EC2 or VPC instances, copy the generated script and paste it into the **User Data** field. This will let you launch existing Amazon Machine Images (AMI's) and automatically install and activate the Agent at startup. The new instances must be able to access the URLs specified in the generated deployment script. This means that your Deep Security Manager must be either Internet-facing, connected to AWS via VPN/Direct Link, or that your Deep Security Manager be deployed on Amazon Web Services as well.

When copying the deployment script into the **User Data** field for a **Linux** deployment, copy the deployment script as-is into the "User Data" field and CloudInit will execute the script as sudo. (If there are failures they will be noted in /var/log/cloud-init.log.)

Note: *The deployment scripts generated by Deep Security Manager for Windows Agent deployments require Windows Powershell version 2.0 or later.*

Note: *The* ***User Data*** *field is also used with other services like CloudFormation. For more information, see:* *http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cloudformation-waitcondition-article.html*



Agents or relays can be manually installed or deployed using tools such as RightScale, Chef, Puppet, or SSH.

For platforms other than Windows and Linux, please see the installation guide.

Platform: Microsoft Windows (64 bit)

Can't find the package you are looking for? Import More Software...

☑ Activate the Agent Automatically

Security Policy: None

Computer Group: Computers

Relay Group: Default Relay Group

NOTE Hostname, description, unique identifiers and other properties can also be set on agent-initiated activation. See the Command-Line Instructions page in the online help for more information.

```
<powershell>
[Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}
(New-Object System.Net.WebClient).DownloadFile("https://CA-OT-MELANIE-W.client.us.trendnet.org:4119/software/agent/Windows/x86_64/",
"$env:temp\agent.msi")
& msiexec /i "$env:temp\agent.msi" /qn ADDLOCAL=ALL
Start-Sleep -s 70
```

Note: *If you do not intend to enable Anti-Malware protection on your computers, you may want to prevent the installation of the Anti-Malware engine entirely. To do so, delete the string "ADDLOCAL=ALL" from the deployment script.*

Deploying Protection

- **Agent-based Protection:** The Deep Security Agent provides protection on a physical or virtual machine. This small software component is deployed on the computer and implements the security Policy you have applied to it.
- **Agent-less Protection:** The Deep Security Virtual Appliance provides protection for VMware vSphere virtual machines without the need to install a Deep Security Agent on them. The Virtual Appliance is installed on the same ESXi that hosts the VMs.
- **Applying Policies:** Whether you are protecting your computers with Agents or with a Virtual Appliance, you will assign security Policies to them which are a defined set of rules, configurations, permissions, and schedules. Policies can be created and saved for use on multiple machines. Policies are created in a hierarchical structure so that a parent Policy can be used as a template for the creation of child Policies that have been fine-tuned for use on individual machines that have specific requirements.

Agent-Based Protection

Manual Deployment

You can manually install any of the Deep Security Agents on your computers by running the appropriate install package on the computer. Agent install packages can be downloaded from the Trend Micro Download Center at http://downloadcenter.trendmicro.com. See the Installation Guide for instructions on installing the individual Agent packages.

Once an Agent is installed, you will have to add the computer to your list of managed computers and manually activate the Agent. For information on adding computers, see ***Adding Computers (page 66)***.

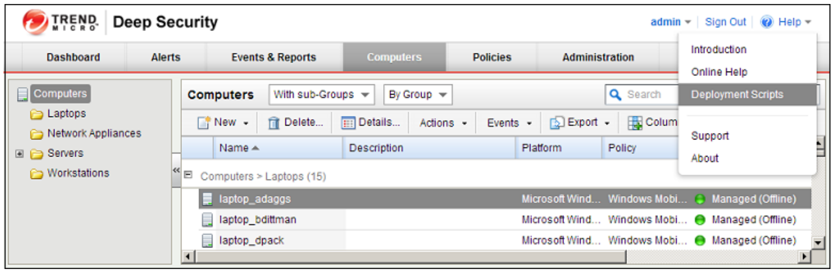
Deployment Scripts

Adding a computer to your list of protected resources in Deep Security and implementing protection is a multi-step process. Almost all of these steps can be performed from the command line on the computer and can therefore be scripted. The Deep Security Manager contains a deployment script writing assistant which can be accessed from the Manager's Help menu.

To generate a deployment script:

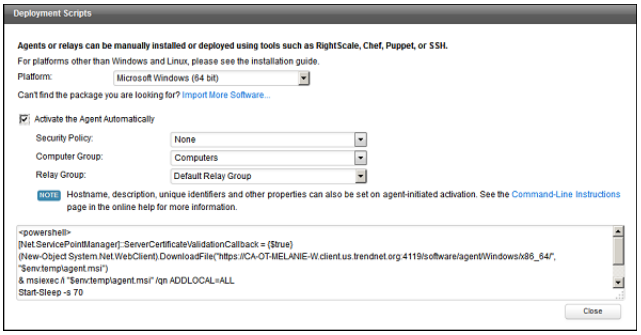
1. Start the Deployment Script Generator by clicking **Deployment Scripts** in the Deep Security Manager's Help menu at the top right of the page.
2. Select whether you are deploying an Agent or a Relay.
3. Select the platform to which you are deploying the software. (Platforms listed in the drop-down menu will correspond to the software that you have imported into the Deep Security Manager from the Trend Micro Download Center. For information on importing Deep Security Software, see **Administration > Updates** in the Deep Security Manager Interface Guide or the online help.)
4. Select **Activate the Agent Automatically**. (Agents must be activated by the Deep Security Manager before a protection Policy can be implemented.)
5. Select the Policy you wish to implement on the computer.
6. Select the computer Group
7. Select the Relay Group

As you make the above selections, the Deployment Script Generator will generate a script which you can import into your systems management software.



Computers > Laptops (15)

Name	Description	Platform	Policy	
laptop_adaggs		Microsoft Wind...	Windows Mobi...	Managed (Offline)
laptop_bdittman		Microsoft Wind...	Windows Mobi...	Managed (Offline)
laptop_dpack		Microsoft Wind...	Windows Mobi...	Managed (Offline)



Agents or relays can be manually installed or deployed using tools such as RightScale, Chef, Puppet, or SSH.

For platforms other than Windows and Linux, please see the installation guide.

Platform: Microsoft Windows (64 bit)

Can't find the package you are looking for? Import More Software...

☑ Activate the Agent Automatically

Security Policy: None

Computer Group: Computers

Relay Group: Default Relay Group

NOTE Hostname, description, unique identifiers and other properties can also be set on agent-initiated activation. See the Command-Line Instructions page in the online help for more information.

```
<powershell>
[Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}
(New-Object System.Net.WebClient).DownloadFile("https://CA-OT-MELANIE-W.client.us.trendnet.org:4119/software/agent/Windows/x86_64/",
"$env:temp\agent.msi")
& msiexec /i "$env:temp\agent.msi" /qn ADDLOCAL=ALL
Start-Sleep -s 70
```

Agentless Protection

The Deep Security Virtual Appliance provides protection to virtual machines (VMs) in a VMware vSphere environment without requiring the presence of an in-guest Deep Security Agent. Virtual machines are managed as though they had an Agent installed.

The Virtual Appliance provides some distinct security advantages over scenarios with an in-guest Agent:

- The Appliance is isolated from the guest. The guest can operate with only the minimum required software being installed.
- Short-lived and reverted machines for which administrator time may not have been allocated for installing security software can easily and quickly be protected.
- Virtual machines and other Appliances whose operating systems are not directly accessible can be protected, even those machines being managed by other administrators.
- The Deep Security Virtual Appliance is easier to deploy. There is no need to remotely install Agent software on the virtual machine. Even connectivity to the virtual machine is not required.

As well, using the Virtual Appliance allows you to protect guests running operating systems not directly supported by Deep Security Agents.

Using the Virtual Appliance to protect virtual machines doesn't preclude the use of Deep Security Agents on those virtual machines. This Coordinated Protection provides the following benefits:

- Allows you to implement the additional Integrity Monitoring and Log Inspection modules on the virtual machine.
- Provides mobility to the virtual machines. They can be moved between data centers or Cloud Providers and the protection moves with them.
- Performance improvement. While the Deep Security Agent is active on the virtual machine, the Virtual Appliance automatically passes traffic through to the Agent.

VMware Environment for Anti-Malware Protection

VMware

The VMware vCenter manages the ESXi hypervisors which host the guest VMs that are to be protected.

For detailed instructions on how to setup the VMware environment including system requirements, installation steps and configuration, refer to the **Deep Security 9.5 Installation Guide (vShield)** or the **Deep Security 9.5 Installation Guide (NSX)**.

Deep Security

The Deep Security Manager coordinates the protection being provided to each guest virtual machine. This is done through the Deep Security Virtual Appliance which uses the VMware Endpoint API to apply the protection to the virtual machines. The Deep Security Filter driver controls network traffic in and out of the guest virtual machines.

Note: *The vShield Manager and the Deep Security Manager must not be installed on the same ESXi that is hosting the guest virtual machines being protected.*

Implementing Deep Security protection in a VMware environment involves:

1. Adding vCenter to the DSM's list of Managed Computers
2. Preparing ESXi for Deep Security Virtual Appliance Deployment (by deploying the Deep Security Filter Driver)
3. Installing and activating the Deep Security Virtual Appliance
4. Installing the Deep Security Notifier on Windows virtual machines to be protected (optional)

5. Applying Deep Security protection to the virtual machines
6. Optionally, installing Deep Security Agents on the virtual machines to implement Coordinated Protection

For detailed instructions for all installation and configuration steps, refer to the **Deep Security 9.5 Installation Guide (vShield)** or the **Deep Security 9.5 Installation Guide (NSX)**.

Protection Modules

Describes configuration of the Deep Security protection modules.

- The ***Anti-Malware (page 87)*** module protects your computers from viruses, trojans, spyware and other software that is intended to harm your computer or perform operations without your consent.
- The ***Web Reputatio (page 91)***n module protects against web threats by blocking access to malicious URLs. Deep Security uses Trend Micro's Web security databases from Smart Protection Network sources to check the reputation of Web sites that users are attempting to access. The Web site's reputation is correlated with the specific Web reputation policy enforced on the computer. Depending on the Web Reputation Security Level being enforced, Deep Security will either block or allow access to the URL.
- The ***Firewall (page 93)*** is a bidirectional, stateful firewall that is responsible for making sure that packets originating from unauthorized sources do not reach the applications on its host.
- The ***Intrusion Prevention (page 104)*** module protects computers from being exploited by attacks against known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities. It shields vulnerabilities until code fixes can be completed. It identifies malicious software accessing the network and increases visibility into, or control over, applications accessing the network.
- The ***Integrity Monitoring (page 106)*** module allows you to monitor specific areas on a computer for changes. Deep Security has the ability to monitor installed software, running services, processes, files, directories, listening ports, registry keys, and registry values. It functions by performing a baseline scan of the areas on the computer specified in the assigned rules and then periodically rescanning those areas to look for changes. The Deep Security Manager ships with predefined Integrity Monitoring Rules and new Integrity Monitoring Rules are provided in Security Updates.
- The ***Log Inspection (page 107)*** module allows you to monitor the logs and events generated by the operating systems and applications running on the computers. Log Inspection Rules can be assigned directly to computers or can be made part of a Security Profile. Like Integrity Monitoring Events, Log Inspection events can be configured to generate alerts in the Deep Security Manager.

Anti-Malware

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

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

Note: *A newly installed Deep Security Agent cannot provide Anti-Malware protection until it has contacted an update server to download Anti-Malware patterns and updates. Ensure that your Deep Security Agents can communicate with a Deep Security Relay or the Trend Micro Update Server after installation.*

Malware Types

Anti-Malware protects against all kinds of file-based threats, including the following.

Viruses (File Infectors)

Viruses are able to infect normal files by inserting malicious code. Typically, whenever an infected file is opened, the malicious code automatically runs and delivers a payload in addition to infecting other files. Below are some of the more common types of viruses:

- **COM and EXE infectors** infect DOS and Windows executable files, which typically have COM and EXE extensions.
- **Macro viruses** infect Microsoft Office files by inserting malicious macros.
- **Boot sector viruses** infect the section of hard disk drives that contain operating system startup instructions

Anti-Malware uses different technologies to identify and clean infected files. The most traditional method is to detect the actual malicious code that is used to infect files and strip infected files of this code. Other methods include regulating changes to infectable files or backing up such files whenever suspicious modifications are applied to them.

Trojans and Other Non-Infectors

Non-infectors are malware files that do not have the ability to infect other files. This large set includes the following malware types:

- **Trojans:** non-infecting executable malware files that do not have backdoor or worm capabilities.
- **Backdoors:** malicious applications that allow unauthorized remote users to access infected systems. Backdoors are known to connect to communication servers through open ports.
- **Worms:** malware programs that can propagate from system to system are generally referred to as "worms". Worms are known to propagate by taking advantage of social engineering through attractively packaged email messages, instant messages, or shared files. They are also known to copy themselves to accessible network shares and spread to other computers by exploiting vulnerabilities.
- **Network viruses:** worms that are memory-only or packet-only programs (not file-based). Anti-Malware is unable to detect or remove network viruses**.**
- **Rootkits:** file-based malware that manipulate calls to operating system components. Applications, including monitoring and security software, need to make such calls for very basic functions, such as listing files or identifying running processes. By manipulating these calls, rootkits are able to hide their presence or the presence of other malware.

Spyware/Grayware

Spyware/grayware comprises applications and components that collect information to be transmitted to a separate system or collected by another application. Spyware/grayware detections, although exhibiting potentially malicious behavior, may include applications used for legitimate purposes such as remote monitoring. Spyware/grayware applications that are inherently malicious, including those that are distributed through known malware channels, are typically detected as other Trojans.

Spyware/grayware applications are typically categorized as:

- **Spyware:** software installed on a computer to collect and transmit personal information.
- **Dialers:** malicious dialers are designed to connect through premium-rate numbers causing unexpected charges. Some dialers also transmit personal information and download malicious software.
- **Hacking tools:** programs or sets of programs designed to assist unauthorized access to computer systems.
- **Adware (advertising-supported software):** any software package that automatically plays, displays, or downloads advertising material.
- **Cookies:** text files stored by a Web browser. Cookies contain website-related data such as authentication information and site preferences. Cookies are not executable and cannot be infected; however, they can be used as spyware. Even cookies sent from legitimate websites can be used for malicious purposes.
- **Keyloggers:** software that logs user keystrokes to steal passwords and other private information. Some keyloggers transmit logs to remote systems.

What Is Grayware?

Although they exhibit what can be intrusive behavior, some spyware-like applications are considered legitimate. For example, some commercially available remote control and monitoring applications can track and collect system events and then send information about these events to another system. System administrators and other users may find themselves installing these legitimate applications. These applications are called "grayware".

To provide protection against the illegitimate use of grayware, Anti-Malware detects grayware but provides an option to "approve" detected applications and allow them to run.

Packers

Packers are compressed and/or encrypted executable programs. To evade detection, malware authors often pack existing malware under several layers of compression and encryption. <Malware protection> checks executable files for compression patterns associated with malware.

Probable Malware

Files detected as probable malware are typically unknown malware components. By default, these detections are logged and files are anonymously sent back to Trend Micro for analysis.

Other Threats

"Other Threats" includes malware not categorized under any of the malware types. This category includes joke programs, which display false notifications or manipulate screen behavior but are generally harmless.

Types of Malware Scans

Deep Security performs three kinds of Malware Scans:

- **Full Scan**
- **Quick Scan**
- **Real-Time Scan**

A **Full Scan** runs a full system scan on all processes and files on computer. Full Scans can be run at scheduled times by creating a Scheduled Task for the purpose, or manually (on-demand).

A **Quick Scan** only scans a computer's critical system areas for currently active threats. A Quick Scan will look for currently active malware but it will not perform deep file scans to look for dormant or stored infected files. On larger drives it is significantly faster than a Full Scan. Quick Scan is only available on-demand. You cannot schedule a Quick Scan as part of a Scheduled Task.

Real-Time Scanning is the ongoing monitoring of running processes and I/O events.

Basic Configuration

To enable Anti-Malware functionality on a computer:

1. In the Policy/Computer editor, go to **Anti-Malware > General**
2. Select **On** , and then click Save

Advanced Configuration

Modifying Malware Scan Configuration

The scope of Malware Scans can be controlled by editing the **Malware Scan Configuration** that is in effect on a computer. The **Malware Scan Configuration** determines which files and directories are included or excluded during a scan and which actions are taken if malware is detected on a computer (for example, clean, quarantine, or delete). There are two types of Malware Scan Configurations:

- **Manual/Scheduled Scan Configurations**
- **Real-Time Scan Configurations**

Manual Scan Configurations or **Scheduled Scan Configurations** are for Full And Quick Scans. **Real-Time Scan Configurations** are for Real-Time Scanning.

Deep Security comes with preconfigured default Malware Scan Configurations for each type of scan. These default Malware Scan Configurations are used in Deep Security's preconfigured security Policies.

The following table lists the objects scanned during each type of scan and the sequence in which they are scanned.

Targets	Full Scan	Quick Scan
Drivers	1	1
Trojan	2	2
Process Image	3	3
Memory	4	4
Boot Sector	5	-
Files	6	5
Spyware	7	6

Smart Scan

Smart Scan references threat signatures that are stored on Trend Micro servers. When Smart Scan is enabled, Deep Security first scans for security risks locally. If Deep Security cannot assess the risk of the file during the scan, try to connect to a local Smart Scan Server. If no local Smart Scan Server is detected, they will attempt to connect to the Trend Micro Global Smart Scan Server.

Smart Scan provides the following features and benefits:

- Reduces the overall time it takes to deliver protection against emerging threats
- Reduces network bandwidth consumed during pattern updates. The bulk of pattern definition updates only needs to be delivered to the cloud and not to many computers
- Reduces the cost and overhead associated with corporate-wide pattern deployments
- Lowers kernel memory consumption on computers. Consumption increases minimally over time
- Provides fast, real-time security status lookup capabilities in the cloud

To turn Smart Scan on or off, go to **Policy/Computer Editor > Anti-Malware > Smart Protection**.

NSX Security Tags

Deep Security can apply **NSX Security Tags** to protected VMs upon detecting a malware threat. NSX Security Tags are part of the VMware vSphere NSX environment and are not to be confused with Deep Security Event Tags. For more information on NSX Security Tags, consult your VMware documentation. For more information on Deep Security Event Tagging, see ***Event Tagging (page 133)***.

To configure the application of NSX Security Tags, go to **Computer/Policy Editor > Anti-Malware > Advanced > NSX Security Tagging**.

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

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

Web Reputation

The Web Reputation module protects against web threats by blocking access to malicious URLs. Deep Security uses Trend Micro's Web security databases from Smart Protection Network sources to check the reputation of Web sites that users are attempting to access. The Web site's reputation is correlated with the specific Web reputation policy enforced on the computer. Depending on the Web Reputation Security Level being enforced, Deep Security will either block or allow access to the URL.

Basic Configuration

To enable Web Reputation functionality on a computer:

1. In the Policy/Computer editor, go to **Web Reputation > General**
2. Select **On** , and then click Save

Inline vs. Tap Mode

Web Reputation uses the Deep Security Network Engine which can operate in one of two modes:

- **Inline:** Live packet streams pass directly through the Deep Security network engine. All rules, therefore are applied to the network traffic before they proceed up the protocol stack
- **Tap Mode:** Live packet streams are replicated and diverted from the main stream.

In Tap Mode, the live stream is not modified. All operations are performed on the replicated stream. When in Tap Mode, Deep Security offers no protection beyond providing a record of Events.

To switch between Inline and Tap mode, open a Policy or Computer Editor and go to **Settings > Network Engine > Network Engine Mode**.

Smart Protection Server

The Web Reputation module relies on databases maintained on the Trend Micro Smart Protection Network. Deep Security will either connect to a locally installed Smart Protection Server or it will connect to the Global smart Protection Service. To configure the connection to the Smart Protection Network, go to the **Policy/Computer Editor > Web Reputation > Smart Protection** tab.

Security Levels

Web addresses that are known to be or are suspected of being malicious are assigned a **risk level** of

- **Suspicious**: Associated with spam or possibly compromised
- **Highly suspicious**: Suspected to be fraudulent or possible sources of threats
- **Dangerous**: Verified to be fraudulent or known sources of threats

You can enforce the one of the following Security Levels:

- **High:** Blocks sites that are assessed as:
  - Dangerous
  - Highly Suspicious
  - Suspicious
- **Medium:** Blocks only sites that are assessed as:

    - Dangerous
    - Highly Suspicious

- **Low:** Blocks only sites that are assessed as:
    - Dangerous

Note: *The security levels determine whether Deep Security will allow or block access to a URL. For example, if you set the security level to Low, Deep Security will only block URLs that are known to be Web threats. As you set the security level higher, the Web threat detection rate improves but the possibility of false positives also increases.*

You can also choose to block URLs that have not been tested by Trend Micro.

To enforce a Security Level, go to the **Policy/Computer Editor > Web Reputation > General** tab.

Exceptions

You can override the block/allow behavior dictated by the Smart Protection Network's assessments with your lists of URLs that you want to block or allow. To create these block/allow exception lists, go to the **Policy/Computer Editor > Web Reputation > Exceptions** tab.

Firewall

The Deep Security firewall is a bidirectional, stateful firewall that is responsible for making sure that packets originating from unauthorized sources do not reach the applications on its host.

Basic configuration

To enable Firewall functionality on a computer:

1. In the Policy/Computer editor, go to **Firewall > General**
2. Select **On** , and then click Save

Inline vs. Tap Mode

The Firewall module uses the Deep Security Network Engine which can operate in one of two modes:

- **Inline:** Live packet streams pass directly through the Deep Security network engine. All rules, therefore are applied to the network traffic before they proceed up the protocol stack
- **Tap Mode:** Live packet streams are replicated and diverted from the main stream.

In Tap Mode, the live stream is not modified. All operations are performed on the replicated stream. When in Tap Mode, Deep Security offers no protection beyond providing a record of Events.

To switch between Inline and Tap mode, open a Policy or Computer Editor and go to **Settings > Network Engine > Network Engine Mode**.

Firewall Rule Properties

Packet Source and Packet Destination

The Firewall can use the following criteria to determine traffic source and destination:

- **IP address**
- **MAC address**
- **Port**

IP Address

The following options are available for defining IP addresses:

- **Any:** No address is specified so any host can be either a source or destination
- **Single IP:**A specific machine is identified using its IP address.
- **Masked IP:** This applies the rule to all machines that share the same subnet mask
- **Range:** This applies the rule to all machines that fall within a specific range of IP addresses
- **IP(s):** Use this when applying a rule to several machines that do not have consecutive IP addresses.
- **IP List:** This uses a Component list, particularly one for IP addresses, to define hosts.

MAC Address

The following options are available for defining MAC addresses:

- **Any:** No MAC address was specified, so the rule applies to all addresses
- **Single MAC:** Rule applies to a specific MAC address
- **MAC(s):** Rule applies to the MAC addresses specified here
- **MAC List:** Rule applies to MAC addresses in a MAC list

Port

The following options are available for defining Port addresses:

- **Any:** Rule applies to a single port
- **Port(s):** Rule applies to multiple ports written here
- **Port List:** Rule applies to a port list

Transport Protocols

If the rule is meant for the Internet Protocol (IP) frame type, the protocol field is enabled, and administrators will be asked to specify the transport protocol that will be analyzed. The protocol options available are:

- **Any** (the Firewall will not discriminate based on protocol)
- **ICMP**
- **ICMPV6**
- **IGMP**
- **GGP**
- **TCP**
- **PUP**
- **UDP**
- **IDP**
- **ND**
- **RAW**
- **TCP+UDP**
- **Othe**r (for which you must provide a protocol number)

Direction

The Deep Security firewall is a bidirectional firewall. Therefore it is able to enforce rules on traffic originating from the network to the Deep Security host, referred to as **incoming**, and traffic from the host to the network, referred to as **outgoing**.

Note: *Firewall rules only apply to a single direction; therefore Firewall Rules for specific types of traffic often come in pairs.*

TCP Header Flags

When dealing with TCP traffic, administrators can choose the TCP flags to which rules apply. If the rule does not apply to all flags, administrators can choose from the following:

- **Any Flags**
- **URG**
- **ACK**
- **PSH**
- **RST**
- **SYN**
- **FIN**

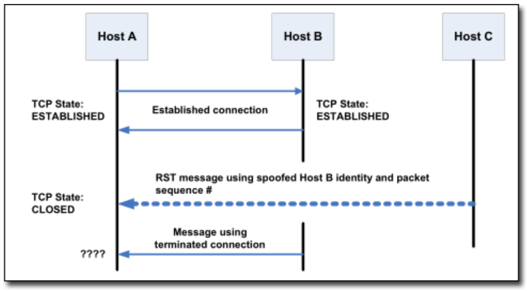
There are a number of ways these flags can be used in different attacks. Only a selection will be discussed here.

The URG flag indicates that the packet is urgent and must be processed before all others, while the PSH flag sets the TCP stack to flush its buffers and send all information up to the application. Both flags can be used in a type port scan called the Xmas scan which is typically a FIN packet with the URG and PSH flags enabled. This scan gets its name from the alternating bits turned on and off in the flags byte (00101001), much like the lights of a Christmas tree.

When an unprotected machine receives packets related to a Xmas scan, the following happens:

Condition	Response
Closed Port	Returns an RST packet
Open Port	No response, exposing existence of the open port

The RST, or RESET, flag abruptly terminates TCP connections. As described above, among its legitimate uses is to terminate connects to closed ports indicating an impossible or disallowed connection. However, the RST flag can also be used as part of an RESET attack, designed to disrupt existing sessions. The following diagram illustrates a situation where an attack, Host C, was able to calculate the TCP sequence number that Host A expected from a packet from Host B, thereby spoofing Host A into believing that Host B had sent it a RST packet. The end result is a denial of service attack:



Frame Types

The term "frame" refers to Ethernet frames, and the available protocols specify the data that the frame carries.

Internet Protocol (IP), Address Resolution Protocol (ARP), and Reverse Address Resolution Protocol (RARP) are the most commonly carried protocols on contemporary Ethernet networks but by selecting "Other" from the drop-down list you can specify any other frame type by its "frame number".

Firewall Rule Actions

Firewall Rules can take the following actions:

- **Allow:** Explicitly allows traffic that matches the rule to pass, and then implicitly denies everything else.
- **Bypass:** Allows traffic to bypass both firewall and Intrusion Prevention analysis. Use this setting only for media-intensive protocols. Only the port, direction, and protocol can be set with this action.
- **Deny:** Explicitly blocks traffic that matches the rule.
- **Force Allow:** Forcibly allows traffic that would otherwise be denied by other rules.

  Note: *Traffic permitted by a **Force Allow** Rule will still be subject to analysis by the Intrusion Prevention module.*

- **Log only:** Traffic will be only be logged. No other action will be taken.

More about "Allow" Rules

Allow rules have two functions:

1. Permit traffic that is explicitly allowed.
2. Implicitly deny all other traffic.

Note: *Traffic that is not explicitly allowed by an **Allow** rule is dropped, and gets recorded as an **Out of "allowed" Policy** Firewall Event.*

Commonly applied **Allow** rules include:

- **ARP**: Permits incoming Address Resolution Protocol (ARP) traffic .
- **Allow solicited TCP/UDP replies**: Ensures that the host computer is able to receive replies to its own TCP and UDP messages. This works in conjunction with TCP and UDP stateful configuration.
- **Allow solicited ICMP replies**: Ensures that the host computer is able to receive replies to its own ICMP messages. This works in conjunction with ICMP stateful configuration.

More about "Bypass" Rules

The **Bypass** rule is designed for media-intensive protocols where filtering by the Firewall or Intrusion Prevention modules is neither required nor desired. **Bypass** rules have the following noteworthy characteristics:

A packet that matches the conditions of a **Bypass** rule:

- is not subject to conditions of Stateful Configuration settings.
- bypasses *both Firewall and Intrusion Prevention analysis*.

Since stateful inspection is not applied to bypassed traffic, bypassing traffic in one direction does not automatically bypass the response in the other direction. Because of this bypass rules should always be created and applied in pairs, one rule for incoming traffic and another for outgoing.

Note: *Bypass Rules Events are not recorded. This is not a configurable behavior.*

If the Deep Security Manager uses a remote database that is protected by a Deep Security Agent, Intrusion Prevention-related false alarms may occur when the Deep Security Manager saves Intrusion Prevention rules to the database. The contents of the rules themselves could be misidentified as an attack. One of two workarounds for this is to create a Bypass rule for traffic from the Deep Security Manager to the database host.

Default Bypass Rule for Deep Security Manager Traffic

The Deep Security Manager automatically implements a **Priority 4 Bypass Rule** that opens incoming TCP traffic at port 4118 on host computers running Deep Security Agent. Priority 4 ensures that this Rule is applied before any Deny rule, and Bypass guarantees that the traffic is never impaired.

This rule, however, accepts traffic from any IP address and any MAC address. To harden the DSA at this port, you can create an alternative, more restrictive, Bypass Rule for this port. The Agent will actually disable the default Manager traffic rule in favor of the new custom rule provided it has the following characteristics:

- **Priority:** 4 - Highest
- **Packet direction:** Incoming
- **Frame type:** IP
- **Protocol:** TCP
- **Packet Destination Port:** 4118

The custom rule must use the above parameters to replace the default rule. Ideally, the IP address or MAC address of the actual Manager should be used as the packet source for the rule.

More about "Force Allow" Rules

The Force Allow option excludes a sub-set of traffic that could otherwise have been covered by a deny action. Its relationship to other actions is illustrated below. Force allow has the same effect as a Bypass rule. However, unlike Bypass, traffic that passes the firewall because of this action is still subject to inspection by the Intrusion Prevention module. The Force allow action is particularly useful for making sure that essential network services are able to communicate with the DSA computer. Among the default Force allow rules that are commonly enabled in real-life are:

- Allow
- Deny
- Force Allow

Note: *When using multiple Manager machines in a multi-node arrangement, it may be useful to define an IP list for these machines and then using this list for the custom Manager traffic rule*

Firewall Rule Sequence

Packets arriving at a computer get processed first by Firewall Rules, then the Firewall Stateful Configuration conditions, and finally by the Intrusion Prevention Rules.

This is the order in which Firewall Rules are applied (incoming and outgoing):

1. Firewall Rules with priority **4 (highest)**
   1. **Bypass**
   2. **Log Only** (**Log Only** rules can only be assigned a priority of **4 (highest)**)
   3. **Force Allow**
   4. **Deny**
2. Firewall Rules with priority **3 (high)**
   1. **Bypass**
   2. **Force Allow**
   3. **Deny**

3. Firewall Rules with priority **2 (normal)**
    1. **Bypass**
    2. **Force Allow**
    3. **Deny**
4. Firewall Rules with priority **1 (low)**
    1. **Bypass**
    2. **Force Allow**
    3. **Deny**
5. Firewall Rules with priority **0 (lowest)**
    1. **Bypass**
    2. **Force Allow**
    3. **Deny**
    4. **Allow** (Note that an **Allow** rule can only be assigned a priority of **0 (lowest)**)

Note: If you have no ***Allow*** *rules in effect on a computer, all traffic is permitted unless it is specifically blocked by a* ***Deny*** *rule. Once you create a single* ***Allow*** *rule, all other traffic is blocked unless it meets the conditions of the* ***Allow*** *rule. There is one exception to this: ICMPv6 traffic is always permitted unless it is specifically blocked by a* ***Deny*** *rule.*

Within the same priority context, a **Deny** rule will override an **Allow** rule, and a **Force Allow** rule will override a **Deny** rule. By using the rule priorities system, a higher priority **Deny** rule can be made to override a lower priority **Force Allow** rule.

Consider the example of a DNS server policy that makes use of a **Force Allow** rule to allow all incoming DNS queries over TCP/UDP port 53. Creating a **Deny** rule with a higher priority than the **Force Allow** rule lets you specify a particular range of IP addresses that must be prohibited from accessing the same public server.

Priority-based rule sets allow you set the order in which the rules are applied. If a **Deny** rule is set with the highest priority, and there are no **Force Allow** rules with the same priority, then any packet matching the **Deny** rule is automatically dropped and the remaining rules are ignored. Conversely, if a **Force Allow** rule with the highest priority flag set exists, any incoming packets matching the **Force Allow** rule will be automatically allowed through without being checked against any other rules.

A Note on Logging

Bypass Rules will never generate an Event. This is not configurable.

Log-only rules will only generate an Event if the packet in question is not subsequently stopped by either:

- a **Deny** rule, or
- an **Allow** rule that excludes it.

If the packet is stopped by one of those two rules, those rules will generate the Event and not the **Log-only** rule. If no subsequent rules stop the packet, the **Log-only** rule will generate an Event.

How Firewall Rules work together

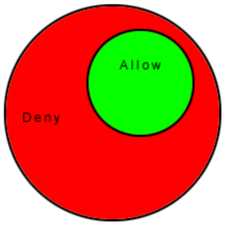
Deep Security Firewall Rules have both a rule action and a rule priority. Used in conjunction, these two properties allow you to create very flexible and powerful rule-sets. Unlike rule-sets used by other firewalls, which may require that the rules be defined in the order in which they should be run, Deep Security Firewall Rules are run in a deterministic order based on the rule action and the rule priority, which is independent of the order in which they are defined or assigned.

Rule Action

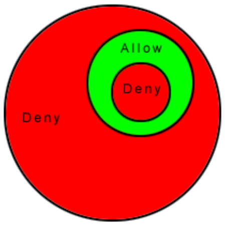
Each rule can have one of four actions.

1. **Bypass:** if a packet matches a **bypass** rule, it is passed through both the firewall *and the Intrusion Prevention Engine* regardless of any other rule (at the same priority level).
2. **Log Only:** if a packet matches a **log only** rule it is passed and the event is logged.
3. **Force Allow:** if a packet matches a **force allow** rule it is passed regardless of any other rules (at the same priority level).
4. **Deny:** if a packet matches a **deny** rule it is dropped.
5. **Allow:** if a packet matches an **allow** rule, it is passed. Any traffic not matching one of the **allow** rules is denied.

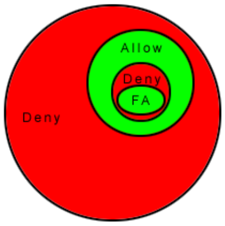
Implementing an ALLOW rule will cause all other traffic not specifically covered by the Allow rule to be denied:



A DENY rule can be implemented over an ALLOW to block specific types of traffic:



A FORCE ALLOW rule can be placed over the denied traffic to allow certain exceptions to pass through:



Rule Priority

Rule actions of type **deny** and **force allow** can be defined at any one of 5 priorities to allow further refinement of the permitted traffic defined by the set of **allow** rules. Rules are run in priority order from highest (Priority 4) to lowest (Priority 0). Within a specific priority level the rules are processed in order based on the rule action (force allow, deny, allow, log only).

The priority context allows a User to successively refine traffic controls using **deny**/**force allow** combinations to achieve a greater flexibility. Within the same priority context an **allow** rule can be negated with a **deny** rule, and a **deny** rule can be negated by a **force allow** rule.

Note: *Rule Actions of type **allow** run only at priority 0 while rule actions of type **log only** run only at priority 4.*

Putting Rule Action and Priority together

Rules are run in priority order from highest (Priority 4) to lowest (Priority 0). Within a specific priority level the rules are processed in order based on the rule action. The order in which rules of equal priority are processed is as follows:

- Bypass
- Log Only
- Force Allow
- Deny
- Allow

Note: *Remember that Rule Actions of type **allow** run only at priority 0 while rule actions of type **log only** run only at priority 4.*

Note: *It is important to remember that if you have a **force allow** rule and a **deny** rule at the same priority the **force allow** rule takes precedence over the **deny** rule and therefore traffic matching the **force allow** rule will be permitted.*

Stateful Filtering

When a Stateful Configuration is in effect on a computer, packets are analyzed within the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions. In the case of stateless protocols (e.g. UDP and ICMP) a pseudo-stateful mechanism is implemented based on historical traffic analysis.

Note: *Saved Stateful Configurations are found in the Deep Security Manager in **Policies > Common Objects > firewall Stateful Configurations**. They are applied to computers in the Policy or Computer editor by going to **Policy/Computer Editor > Firewall > General > Firewall Stateful Configurations**.*

A packet is passed through the stateful routine if it is explicitly allowed via static rules.

- The packet is examined if it belongs to an existing connection by checking the connection table for matching end points
- The TCP header is examined for correctness (e.g. sequence numbers, flag combination)

Once enabled, the stateful engine is applied to all traffic traversing the interface.

UDP pseudo-stateful inspection, by default, rejects any incoming "unsolicited" UDP packets. If a computer is running a UDP server, a **force allow** rule must be included in the policy to permit access to that service. For example, if UDP stateful inspection is enabled on a DNS server, a **force allow** rule permitting UDP traffic to port 53 is required.

ICMP pseudo-stateful inspection, by default, rejects any incoming unsolicited ICMP request-reply and error type packets. A **force allow** must be explicitly defined for any unsolicited ICMP packet to be allowed. All other ICMP (non request-reply or error type) packets are dropped unless explicitly allowed with static rules.

Putting it all together to design a Firewall Policy

Generally speaking, there are two approaches when defining a firewall policy for a computer:

- **Prohibitive:** That which is not expressly allowed is prohibited. Prohibitive policies can be created by using a combination of **allow** rules to describe allowed traffic and **deny** rules to further restrict permitted traffic.

- **Permissive:** That which is not expressly prohibited is allowed. Permissive policies can be created through the exclusive used of **deny** rules to describe the traffic that should be dropped.

In general, prohibitive policies are preferred and permissive policies should be avoided.

Force allow rules should only be used in conjunction with **allow** and **deny** rules to allow a subset of traffic that has been prohibited by the **allow** and **deny** rules. **Force allow** rules are also required to allow unsolicited ICMP and UDP traffic when ICMP and UDP stateful are enabled.

Example

Take the example of how a simple firewall policy can be created for a Web server.

1. First enable stateful inspection for TCP, UDP, and ICMP using a global Firewall Stateful Configuration with these options enabled.
2. Add a Firewall Rule to allow TCP and UDP replies to requests originated on the workstation. To do this create an incoming **allow** rule with the protocol set to "TCP + UDP" and select the **Not** checkbox and the **Syn** checkbox under **Specific Flags**. At this point the policy only allows TCP and UDP packets that are replies to requests initiated by a user on the workstation. For example, in conjunction with the stateful analysis options enabled in step 1, this rule allows a user on this computer to perform DNS lookups (via UDP) and to browse the Web via HTTP (TCP).
3. Add a Firewall Rule to allow ICMP replies to requests originated on the workstation. To do this, create an incoming **allow** rule with the protocol set to "ICMP" and select the **Any Flags** checkbox. This means that a user on this computer can ping other workstations and receive a reply but other users will not be able to ping this computer.
4. Add a Firewall Rule to allow incoming TCP traffic to port 80 and 443 with the **Syn** checkbox checked in the **Specific Flags** section. This means that external users can access a Web server on this computer.

At this point we have a basic firewall policy that allows solicited TCP, UDP and ICMP replies and external access to the Web server on this computer all other incoming traffic is denied.

For an example of how **deny** and **force allow** rule actions can be used to further refine this Policy consider how we may want to restrict traffic from other computers in the network. For example, we may want to allow access to the Web server on this computer to internal users but deny access from any computers that are in the DMZ. This can be done by adding a **deny** rule to prohibit access from servers in the DMZ IP range.

5. Next we add a **deny** rule for incoming TCP traffic with source IP 10.0.0.0/24 which is the IP range assigned to computers in the DMZ. This rule denies any traffic from computers in the DMZ to this computer.

We may, however, want to refine this policy further to allow incoming traffic from the mail server which resides in the DMZ.

6. To do this we use a **force allow** for incoming TCP traffic from source IP 10.0.0.100. This **force allow** overrides the **deny** rule we created in the previous step to permit traffic from this one computer in the DMZ.

Important things to remember

- All traffic is first checked against Firewall Rules before being analyzed by the stateful inspection engine. If the traffic clears the Firewall Rules, the traffic is then analyzed by the stateful inspection engine (provided stateful inspection is enabled in the Firewall Stateful Configuration).
- **Allow** rules are prohibitive. Anything not specified in the **allow** rules is automatically dropped. This includes traffic of other frame types so you need to remember to include rules to allow other types of required traffic. For example, don't forget to include a rule to allow ARP traffic if static ARP tables are not in use.
- If UDP stateful inspection is enabled a **force allow** rule must be used to allow unsolicited UDP traffic. For example, if UDP stateful is enabled on a DNS server then a **force allow** for port 53 is required to allow the server to accept incoming DNS requests.
- If ICMP stateful inspection is enabled a **force allow** rule must be used to allow unsolicited ICMP traffic. For example, if you wish to allow outside ping requests a **force allow** rule for ICMP type 3 (Echo Request) is required.
- A **force allow** acts as a trump card only within the same priority context.
- If you do not have a DNS or WINS server configured (which is common in test environments) a **force allow incoming UDP port 137** rule may be required for NetBios.

Note: *When troubleshooting a new firewall policy the first thing you should do is check the Firewall Rule logs on the Agent/Appliance. The Firewall Rule logs contain all the information you need to determine what traffic is being denied so that you can further refine your policy as required.*

Bypass Rule

There is a special type of Firewall Rule called a Bypass Rule. It is designed for media intensive protocols where filtering may not be desired. You create a Bypass Rule by selecting "bypass" as the rule's "Action" when creating a new Firewall Rule.

The "Bypass" action on Firewall Rules differs from a Force Allow rule in the following ways:

- Packets matching Bypass will not be processed by Intrusion Prevention Rules
- Unlike Force Allow, Bypass will not automatically allow the responses on a TCP connection when Firewall Stateful Configuration is on (See below for more information)
- Some Bypass rules are optimized, in that traffic will flow as efficiently as if our Agent/Appliance was not there (See below for more information)

Note: ***Important:*** *When a Bypass Firewall Rule is sent to an Agent older than version 5.0, it will be treated as a Force Allow, which will not skip Intrusion Prevention Rule processing.*

Using Bypass when Firewall Stateful Configuration is On

If you plan to use a Bypass Rule to skip Intrusion Prevention Rule processing on incoming traffic to TCP destination port N and Firewall Stateful Configuration is set to perform stateful inspection on TCP, you *must* create a matching outgoing rule for *source* port N to allow the TCP responses. (This is not required for Force Allow rules because force-allowed traffic is still processed by the stateful engine.)

All Bypass rules are unidirectional. Explicit rules are required for each direction of traffic.

Optimization

The Bypass Rule is designed to allow matching traffic through at the fastest possible rate. Maximum throughput can be achieved with (all) the following settings:

- **Priority**: Highest
- **Frame Type**: IP
- **Protocol**: TCP, UDP, or other IP protocol. (Do not use the "Any" option.)
- **Source and Destination IP and MAC**: all "Any"
- If the protocol is TCP or UDP and the traffic direction is "incoming", the Destination Ports must be one or more specified ports (not "Any"), and the Source Ports must be "Any".
- If the protocol is TCP or UDP and the traffic direction is "outgoing", the Source Ports must be one or more specified ports (Not "Any"), and the Destination Ports must be "Any".
- **Schedule**: None.

Logging

Packets that match the bypass rule will not be logged. This is not a configurable option.

Intrusion Prevention

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

Intrusion Prevention prevents attacks by detecting malicious instructions in network traffic and dropping relevant packets.

Intrusion Prevention can be used for the following functions:

- **Virtual patching:** Intrusion Prevention rules can drop traffic designed to leverage unpatched vulnerabilities in certain applications or the operating system itself. This protects the host while awaiting the application of the relevant patches.
- **Protocol hygiene:** this detects and blocks traffic with malicious instructions
- **Application control:** this control can be used to block traffic associated with specific applications like Skype or file-sharing utilities

Basic configuration

To enable Intrusion Prevention functionality on a computer:

1. In the Policy/Computer editor, go to **Intrusion Prevention > General**
2. Select **On** , and then click Save

Inline vs. Tap Mode

The Intrusion Prevention module uses the Deep Security Network Engine which can operate in one of two modes:

- **Inline:** Live packet streams pass directly through the Deep Security network engine. All rules, therefore are applied to the network traffic before they proceed up the protocol stack
- **Tap Mode:** Live packet streams are replicated and diverted from the main stream.

In Tap Mode, the live stream is not modified. All operations are performed on the replicated stream. When in Tap Mode, Deep Security offers no protection beyond providing a record of Events.

To switch between Inline and Tap mode, open a Policy or Computer Editor and go to **Settings > Network Engine > Network Engine Mode**.

Prevent vs Detect

There are two additional options that are available if Deep Security Network Engine is in **Inline** mode:

- **Prevent:** Intrusion Prevention rules are applied to traffic and related log events are generated
- **Detect:** Intrusion Prevention rules are still triggered and Events are generated but traffic is not affected. You should always test new Intrusion Prevention settings and rules in Detect mode to make sure that possible false positives will not interrupt service on your computers. Once you are satisfied that no false positives are being triggered (by monitoring Intrusion Prevention Events for a period of time), you can switch over to Prevent mode.

Individual Intrusion Prevention Rules can be applied in detect-only or prevent mode as well. When applying any new Intrusion Prevention Rule, it's a good idea to run it for a period of time detect-only mode to make sure it won't interfere with legitimate traffic. Some Rules issued by Trend Micro are set to detect-only by default. For example, mail client Intrusion Prevention Rules are generally detect-only since they will block the download of all subsequent mail. Some Rules only trigger if a condition occurs a large number times, or a certain number of times over a certain period and so the individual condition shouldn't be prevented but an alerts is raised if the condition recurs. And some Rules are simply susceptible to false positives. These Rules will be shipped in detect-only mode by default and it is up to you to determine if you wish to switch them to prevent mode after having observed that no false positives are being triggered.

Integrity Monitoring

Integrity Monitoring allows you to monitor specific areas on a computer for changes. Deep Security has the ability to monitor installed software, running services, processes, files, directories, listening ports, registry keys, and registry values. It functions by performing a baseline scan of the areas on the computer specified in the assigned rules and then periodically rescanning those areas to look for changes. The Deep Security Manager ships with predefined Integrity Monitoring Rules and new Integrity Monitoring Rules are provided in Security Updates.

Recommendation Scans will recommend Integrity Monitoring Rules for a computer.

The typical procedure for enabling Integrity Monitoring on a computer is to:

1. Turn on Integrity Monitoring (either globally or on a specific computer)
2. Run a Recommendation Scan on the computer
3. Apply the recommended Integrity Monitoring Rules
4. Optionally, apply any Integrity Monitoring Rules you may have written yourself for the computer
5. Build a Baseline for the computer by opening the computer's **Details** window, going to the **Integrity Monitoring** page, and clicking "Rebuild Baseline".
6. Periodically scan for changes (either manually or by creating a Scheduled Task)

Basic configuration

To enable Integrity Monitoring functionality on a computer:

1. In the Policy/Computer editor, go to **Integrity Monitoring > General**
2. Select **On** , and then click Save

Use the main **Integrity Monitoring** page to turn Integrity Monitoring on or off and to set whether Integrity Monitoring Rules that are recommended after a Recommendation Scan are automatically applied.

- **On:** Scheduled Integrity Monitoring Scans. Integrity Monitoring scans can be scheduled just like other Deep Security operations. Changes to the Entities monitored since the last scan will be identified and an Event will be recorded.

  Note: *Multiple changes to monitored entities between scans will not be tracked, only the last change will be detected. To detect and report multiple changes to an entity's state , consider increasing the frequency of scheduled scans (i.e. daily instead of weekly for example) or select Real Time Integrity Monitoring for entities that change frequently.*

- **Off:** On Demand Integrity Monitoring Scans. Integrity Monitoring scans for changes can also be initiated by the Administrator and would function similar to scheduled Integrity Monitoring scans.
- **Real Time:** Real Time Integrity Monitoring. Real Time Integrity Monitoring provides the ability to monitor Entity changes in real time and raise Integrity Monitoring events when changes are detected. Events are forwarded in real time via syslog to the SIEM or when the next heartbeat communication (configurable) to the Deep Security Manager occurs.

The **Integrity Monitoring** page in a computer's **Details** window has extra options that apply to the specific computer only. On it you can initiate a scan for changes or rebuild the baseline data for the computer. You can also initiate a Recommendation Scan or clear existing Recommendations.

For information on writing custom Integrity Monitoring Rules, see the documentation for the **Integrity Monitoring Rules** page and ***Integrity Monitoring Rules Language (page 218)*** in the **Reference** section.

Log Inspection

The OSSEC Log Inspection Engine is integrated into Deep Security and gives you the ability to inspect the logs and events generated by the operating systems and applications running on the computers. Log Inspection Rules can be assigned directly to computers or can be made part of a Security Profile. Like Integrity Monitoring Events, Log Inspection events can be configured to generate alerts in the Deep Security Manager.

Note: *Some Log Inspection Rules written by Trend Micro require local configuration to function properly. If you assign one of these Rules to your computers or one of these Rules gets assigned automatically, an Alert will be raised to notify you that configuration is required.*

Basic Configuration

To enable Log Inspection functionality on a computer:

1. In the Policy/Computer editor, go to **Log Inspection > General**
2. Select **On** , and then click **Save**

Recommendation Scans

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

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

Advanced topics

For more information on Log Inspection, see ***Examining a Log Inspection Rule (page 108)***.

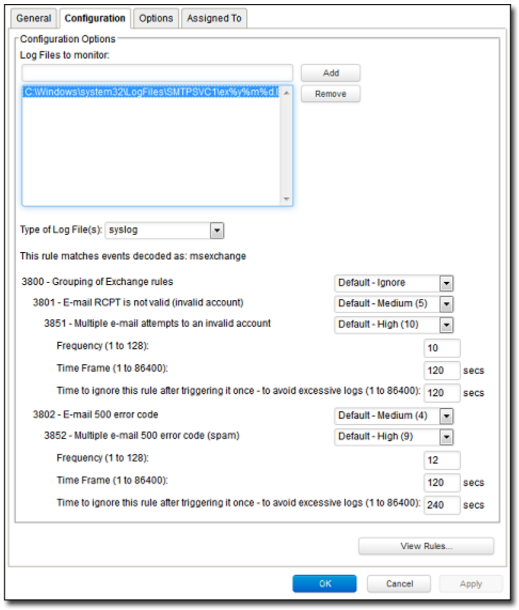
Examining a Log Inspection Rule

The Log Inspection feature in Deep Security enables real-time analysis of 3rd party log files. The Log Inspection Rules and Decoders provide a framework to parse, analyze, rank and correlate events across a wide variety of systems. As with Intrusion Prevention and Integrity Monitoring, Log Inspection content is delivered in the form of Rules included in a Security Update. These Rules provide a high level means of selecting the applications and logs to be analyzed.

Log Inspection Rules are found in the Deep Security Manager at **Policies > Common Objects > Rules > Log Inspection Rules**.

Log Inspection Rule Structure and the Event Matching Process

This screen shot displays the contents of the **Configuration** tab of the Properties window of the "Microsoft Exchange" Log Inspection Rule:



Configuration Options

Log Files to monitor:

C:\Windows\system32\LogFiles\SMTPSVC1\ex%y%m%d.l

Type of Log File(s): syslog

This rule matches events decoded as: msexchange

3800 - Grouping of Exchange rules	Default - Ignore
3801 - E-mail RCPT is not valid (invalid account)	Default - Medium (5)
3851 - Multiple e-mail attempts to an invalid account	Default - High (10)
Frequency (1 to 128):	10
Time Frame (1 to 86400):	120 secs
Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400):	120 secs
3802 - E-mail 500 error code	Default - Medium (4)
3852 - Multiple e-mail 500 error code (spam)	Default - High (9)
Frequency (1 to 128):	12
Time Frame (1 to 86400):	120 secs
Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400):	240 secs

Here is the structure of the Rule:

```
3800 - Grouping of Exchange Rules - Ignore
3801 - Email rcpt is not valid (invalid account) - Medium (4)
3851 - Multiple email attempts to an invalid account - High (9)
Frequency - 10
Time Frame - 120
Ignore - 120
3802 - Email 500 error code - Medium (4)
3852 - Email 500 error code (spam) - High (9)
Frequency - 12
Time Frame - 120
Ignore - 240
```

The Log Inspection engine will apply Log Events to this structure and see if a match occurs. Let's say that an Exchange event occurs, and this event is an email receipt to an invalid account. The event will match line 3800 (because it is an Exchange event). The event will then be applied to line 3800's sub-rules: 3801 and 3802.

If there is no further match, this "cascade" of matches will stop at 3800. Because 3800 has a severity level of "Ignore", no Log Inspection Event would be recorded.

However, an email receipt to an invalid account does match one of 3800's sub-rules: sub-rule 3801. Sub-rule 3801 has a severity level of "Medium(4)". If the matching stopped here, a Log Inspection Event with a severity level of "Medium(4)" would be recorded.

But there is still another sub-rule to be applied to the event: sub-rule 3851. Sub-rule 3851 with its three attributes will match if the same event has occurred 10 times within the last 120 seconds. If so, a Log Inspection Event with a severity "High(9)" is recorded. (The "Ignore" attribute tells sub-rule 3851 to ignore individual events that match sub-rule 3801 for the next 120 seconds. This is useful for reducing "noise".)

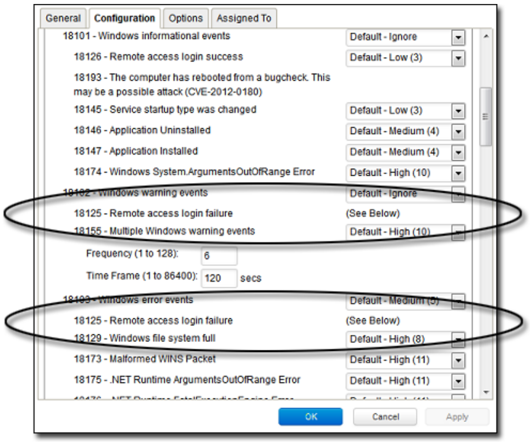
Assuming the parameters of sub-rule 3851 have been matched, a Log Inspection Event with Severity "High(9)" is now recorded.

Looking at the Options tab of the Microsoft Exchange Rule, we see that Deep Security Manager will raise an Alert if any sub-rules with a severity level of "Medium(4)" have been matched. Since this is the case in our example, the Alert will be raised (if "Alert when this rule logs an event" is selected).

Duplicate Sub-rules

Some Log Inspection Rules have duplicate sub-rules. To see an example, open the "Microsoft Windows Events" rule and click on the **Configuration** tab. Note that sub-rule 18125 (Remote access login failure) appears under sub-rules 18102 and 18103. Also note that in both cases sub-rule 18125 does not have a severity value, it only says "See Below".

Instead of being listed twice, Rule 18125 is listed once at the bottom of the **Configuration** page:



18101 - Windows informational events	Default - Ignore
18126 - Remote access login success	Default - Low (3)
18193 - The computer has rebooted from a bugcheck. This may be a possible attack (CVE-2012-0180)	
18145 - Service startup type was changed	Default - Low (3)
18146 - Application Uninstalled	Default - Medium (4)
18147 - Application Installed	Default - Medium (4)
18174 - Windows System.ArgumentsOutOfRange Error	Default - High (10)
18102 - Windows warning events	Default - Ignore
18125 - Remote access login failure	(See Below)
18155 - Multiple Windows warning events	Default - High (10)
Frequency (1 to 128):	6
Time Frame (1 to 86400):	120 secs
18103 - Windows error events	Default - Medium (5)
18125 - Remote access login failure	(See Below)
18129 - Windows file system full	Default - High (8)
18173 - Malformed WINS Packet	Default - High (11)
18175 - .NET Runtime ArgumentsOutOfRange Error	Default - High (11)

Creating Log Inspection Rules

The Deep Security Log Inspection module lets you collect and analyze operating system and application logs to identify important security events buried in thousands of log entries. These events can be sent to a security information and event management (SIEM) system, or centralized logging server for correlation, reporting, and archiving. All events are also securely collected centrally at Deep Security Manager.

The Deep Security Log Inspection module lets you:

- Meet PCI DSS Log Monitoring requirements.
- Detect suspicious behavior.
- Collect events across heterogeneous environments containing different operating systems and diverse applications.
- View events such as error and informational events (disk full, service start/shutdown, etc.).
- Create and maintain audit trails of administrator activity (administrator login/logout, account lockout, policy change, etc.).

Deep Security Log Inspection automates the collection of important security events in a number of ways:

- **Recommendation Scan:** A Recommendation Scan will recommend Log Inspection rules for the server being scanned (i.e. Windows Log Inspection rules vs. Unix Log Inspection rules, etc.).
- **Default Log Inspection Rules:** Deep Security ships with many pre-defined rules covering a wide variety of operating systems and applications.
- **Auto-Tagging:** Log Inspection events are "auto-tagged" based upon their grouping in the log file structure. This simplifies and automates the processing of Log Inspection Events within Deep Security Manager.

Note: *The Log Inspection module monitors specified log files in real time and reacts to changes to the files as they occur. It is important to remember that if the Agent is turned off for a period of time and then turned back on, changes to the log files will not be detected by the Log Inspection module. (Unlike the Integrity Monitoring module which builds a baseline, and then periodically scans specified files and system components and compares them to the baseline.)*

Although Deep Security ships with Log Inspection Rules for many common operating systems and applications, you also have the option to create your own custom Rules. To create a custom Rule, you can either use the "Basic Rule" template, or you can write your new Rule in XML. This article will describe the Log Inspection Rule language and provide an example of a custom written rule. For a description of the properties of existing Log Inspection Rules, see the documentation for the **Log Inspection Rules** in the Deep Security Manager Interface Guide or the online help as well as ***Examining a Log Inspection Rule (page 108)*** in the **Reference** section.

The Log Inspection Process

Decoders

A Log Inspection Rule consists of a list of files to monitor for changes and a set of conditions to be met for the Rule to trigger. When the Log Inspection engine detects a change in a monitored log file, the change is parsed by a decoder. Decoders parse the raw log entry into the following fields:

- **log:** the message section of the event
- **full_log:** the entire event
- **location:** where the log came from
- **hostname:** hostname of the vent source
- **program_name:** Program name. This is taken from the syslog header of the event
- **srcip:** the source IP address within the event
- **dstip:** the destination IP address within the event

- **srcport:** the source port within the event
- **dstport:** the destination port within the event
- **protocol:** the protocol within the event
- **action:** the action taken within the event
- **srcuser:** the originating user within the event
- **dstuser:** the destination user within the event
- **id:** any ID decoded as the ID from the event
- **status:** the decoded status within the event
- **command:** the command being called within the event
- **url:** the URL within the event
- **data:** any additional data extracted from the event
- **systemname:** the system name within the event

Rules examine this decoded data looking for information that matches the conditions defined in the Rule.

If the matches are at a sufficiently high severity level, any of the following actions can be taken:

- An Alert can be raised. (Configurable on the **Options** tab of the Log Inspection Rule's **Properties** window.)
- The Event can be written to syslog. (Configurable in the **System Event Notification** area on **Administration > System Settings > SIEM** tab.)
- The Event can sent to the Deep Security Manager. (Configurable in the **Log Inspection Event Forwarding** area on the **Policy/ Computer Editor > Settings > SIEM** tab.)

Log Inspection Rules

The Log Inspection engine applies Log Inspection Rules to a computer's log entries to determine if any of those entries warrant the generation of a Log Inspection Event.

A single Log Inspection Rule can contain multiple subrules. These subrules can be of two types: atomic or composite. An atomic rule evaluates a single event and a composite rule examines multiple events and can evaluate frequency, repetition, and correlation between events.

Atomic Rules

Groups

Each rule, or grouping of rules, must be defined within a **<group></group>** element. The attribute name must contain the rules you want to be a part of this group. In the following example we have indicated that our group contains the syslog and sshd rules:

```
<group name="syslog,sshd,">
</group>
```

Note: *Notice the trailing comma in the group name. Trailing commas are required if you intend to use the **<if_group></if_group>** tag to conditionally append another sub-rule to this one.*

Note: *When a set of Log Inspection Rules are sent to an Agent, the Log Inspection engine on the Agent takes the XML data from each assigned rule and assembles it into what becomes essentially a single long Log Inspection Rule. Some group definitions are common to all Log Inspection Rules written by Trend Micro. For this reason Trend Micro has included a rule called "Default Rules Configuration" which defines these groups and which always gets assigned along with any other Trend Micro rules. (If you select a rule for assignment and haven't also selected the "Default Rules Configuration" rule, a notice will appear informing you that the rule will be assigned automatically.) If you create your own Log Inspection Rule and assign it to a Computer without assigning any*

Trend Micro-written rules, you must either copy the content of the "Default Rules Configuration" rule into your new rule, or also select the "Default Rules Configuration" rule for assignment to the Computer.

Rules, ID, and Level

A group can contain as many rules as you require. The rules are defined using the **<rule></rule>** element and must have at least two attributes, the **id** and the **level**. The **id** is a unique identifier for that signature and the **level** is the severity of the Alert. In the following example, we have created two rules, each with a different rule id and level:

```
<group name="syslog,sshd,">
 <rule id="100120" level="5">
 </rule>
 <rule id="100121" level="6">
 </rule>
</group>
```

Note: *Custom rules must have ID values between 100,000 to 119,999.*

You can define additional subgroups within the parent group using the **<group></group>** tag. This subgroup can reference any of the groups listed in the following table:

Group Type	Group Name	Description
Reconnaissance	connection_attempt web_scan recon	Connection attempt Web scan Generic scan
Authentication Control	authentication_success authentication_failed invalid_login login_denied authentication_failures adduser account_changed	Success Failure Invalid Login Denied Multiple Failures User account added User Account changed or removed
Attack/Misuse	automatic_attack exploit_attempt invalid_access spam multiple_spam sql_injection attack virus	Worm (nontargeted attack) Exploit pattern Invalid access Spam Multiple spam messages SQL injection Generic attack Virus detected
Access Control	access_denied access_allowed unknown_resource firewall_drop multiple_drops client_misconfig client_error	Access denied Access allowed Access to nonexistent resource Firewall drop Multiple firewall drops Client misconfiguration Client error
Network Control	new_host ip_spoof	New host detected Possible ARP spoofing
System Monitor	service_start system_error system_shutdown logs_cleared invalid_request promisc policy_changed config_changed	Service start System error Shutdown Logs cleared Invalid request Interface switched to promiscuous mode Policy changed Configuration changed

Group Type	Group Name	Description
	low_diskspace	Low disk space
	time_changed	Time changed

Note: *If event auto-tagging is enabled, the event will be labeled with the group name. Log Inspection Rules provided by Trend Micro make use of a translation table that changes the group to a more user-friendly version. So, for example, "login_denied" would appear as "Login Denied". Custom rules will be listed by their group name as it appears in the rule.*

Description

Include a **<description></description>** tag. The description text will appear in the event if the rule is triggered.

```
<group name="syslog,sshd,">
 <rule id="100120" level="5">
 <group>authentication_success</group>
 <description>SSHD testing authentication success</description>
 </rule>
 <rule id="100121" level="6">
 <description>SSHD rule testing 2</description>
 </rule>
</group>
```

Decoded As

The **<decoded_as></decoded_as>** tag instructs the Log Inspection engine to only apply the rule if the specified decoder has decoded the log.

```
<rule id="100123" level="5">
 <decoded_as>sshd</decoded_as>
 <description>Logging every decoded sshd message</description>
</rule>
```

Note: *To view the available decoders, go to **Log Inspection > Log Inspection Decoders**. Right-click on **1002791-Default Log Decoders** and select **Properties...**. Go the **Configuration** tab and click **View Decoders...**.*

Match

To look for a specific string in a log, use the **<match></match>**. Here is a Linux sshd failed password log:

```
 Jan 1 12:34:56 linux_server sshd[1231]: Failed password for invalid user jsmith from 192.168.1.123 port 1799
```

Use the **<match></match>** tag to search for the "password failed" string.

```
<rule id="100124" level="5">
 <decoded_as>sshd</decoded_as>
 <match>^Failed password</match>
 <description>Failed SSHD password attempt</description>
</rule>
```

Note: *Notice the regex caret ("^") indicating the beginning of a string. Although "Failed password" does not appear at the beginning of the log, the Log Inspection decoder will have broken up the log into sections. (See "Decoders", above.) One of those sections is "log" which is the message part of the log (as opposed to "full_log" which is the log in its entirety.)*

The following table lists supported regex syntax:

Regex Syntax	Description
\w	A-Z, a-z, 0-9 single letters and numerals

Regex Syntax	Description
\d	0-9 single numerals
\s	single space
\t	single tab
\p	()*+,-.:;<=>?[]
\W	not \w
\D	not \d
\S	not \s
\.	anything
+	match one or more of any of the above (for example, \w+, \d+)
*	match zero or more of any of the above (for example, \w*, \d*)
^	indicates the beginning of a string (^somestring)
$	specify the end of a string (somestring$)
|	indicate an "OR" between multiple strings

Conditional Statements

Rule evaluation can be conditional upon other rules having been evaluated as true. The **<if_sid></if_sid>** tag instructs the Log Inspection engine to only evaluate this subrule if the rule identified in the tag has evaluated as true. The following example shows three rules: 100123, 100124, and 100125. Rules 100124 and 100125 have been modified to be children of the 100123 rule using the **<if_sid></if_sid>** tag:

```
<group name="syslog,sshd,">
 <rule id="100123" level="2">
 <decoded_as>sshd</decoded_as>
 <description>Logging every decoded sshd message</description>
 </rule>
 <rule id="100124" level="7">
 <if_sid>100123</if_sid>
 <match>^Failed password</match>
 <group>authentication_failure</group>
 <description>Failed SSHD password attempt</description>
 </rule>
 <rule id="100125" level="3">
 <if_sid>100123</if_sid>
 <match>^Accepted password</match>
 <group>authentication_success</group>
 <description>Successful SSHD password attempt</description>
 </rule>
</group>
```

Hierarchy of Evaluation

The **<if_sid></if_sid>** tag essentially creates a hierarchical set of rules. That is, by including an **<if_sid></if_sid>** tag in a rule, the rule becomes a child of the rule referenced by the **<if_sid></if_sid>** tag. Before applying any rules to a log, the Log Inspection engine assesses the **<if_sid></if_sid>** tags and builds a hierarchy of parent/child rules.

Note: *The hierarchical parent/child structure can be used to improve the efficiency of your rules. If a parent rule does not evaluate as true, the Log Inspection engine will ignore the children of that parent.*

Note: *Although the **<if_sid></if_sid>** tag can be used to refer to subrules within an entirely different Log Inspection Rule, you should avoid doing this because it makes the rule very difficult to review at a later time.*

The list of available atomic rule conditional options is shown in the following table:

Tag	Description	Notes
match	A pattern	Any string to match against the event (log).

Tag	Description	Notes
regex	A regular expression	Any regular expression to match against the event(log).
decoded_as	A string	Any prematched string.
srcip	A source IP address	Any IP address that is decoded as the source IP address. Use "!" to negate the IP address.
dstip	A destination IP address	Any IP address that is decoded as the destination IP address. Use "!" to negate the IP address.
srcport	A source port	Any source port (match format).
dstport	A destination port	Any destination port (match format).
user	A username	Any username that is decoded as a username.
program_name	A program name	Any program name that is decoded from the syslog process name.
hostname	A system hostname	Any hostname that is decoded as a syslog hostname.
time	A time range in the format hh:mm - hh:mm or hh:mm am - hh:mm pm	The time range that the event must fall within for the rule to trigger.
weekday	A weekday (sunday, monday, tuesday, etc.)	Day of the week that the event must fall on for the rule to trigger.
id	An ID	Any ID that is decoded from the event.
url	A URL	Any URL that is decoded from the event.

Use the **<if_sid>100125</if_sid>** tag to make this rule depend on the 100125 rule. This rule will be checked only for sshd messages that already matched the successful login rule.

```
<rule id="100127" level="10">
 <if_sid>100125</if_sid>
 <time>6 pm - 8:30 am</time>
 <description>Login outside business hours.</description>
 <group>policy_violation</group>
</rule>
```

Restrictions on the Size of the Log Entry

The following example takes the previous example and adds the **maxsize** attribute which tells the Log Inspection engine to only evaluate rules that are less than the maxsize number of characters:

```
<rule id="100127" level="10" maxsize="2000">
 <if_sid>100125</if_sid>
 <time>6 pm - 8:30 am</time>
 <description>Login outside business hours.</description>
 <group>policy_violation</group>
</rule>
```

The following table lists possible atomic rule tree-based options:

Tag	Description	Notes
if_sid	A rule ID	Adds this rule as a child rule of the rules that match the specified signature ID.
if_group	A group ID	Adds this rule as a child rule of the rules that match the specified group.
if_level	A rule level	Adds this rule as a child rule of the rules that match the specified severity level.
description	A string	A description of the rule.
info	A string	Extra information about the rule.
cve	A CVE number	Any Common Vulnerabilities and Exposures (CVE) number that you would like associated with the rule.
options	alert_by_email no_email_alert no_log	Additional rule options to indicate if the Alert should generate an e-mail, alert_by_email, should not generate an email, no_email_alert, or should not log anything at all, no_log.

Composite Rules

Atomic rules examine single log entries. To correlate multiple entries, you must use composite rules. Composite rules are supposed to match the current log with those already received. Composite rules require two additional options: the **frequency** option specifies how many times an event/pattern must occur before the rule generates an Alert, and the **timeframe** option tells the Log Inspection engine how far back, in seconds, it should look for previous logs. All composite rules have the following structure:

```
<rule id="100130" level="10" frequency="x" timeframe="y">
</rule>
```

For example, you could create a composite rule that creates a higher severity Alert after five failed passwords within a period of 10 minutes. Using the **<if_matched_sid></if_matched_sid>** tag you can indicate which rule needs to be seen within the desired frequency and timeframe for your new rule to create an Alert. In the following example, the **frequency** attribute is set to trigger when five instances of the event are seen and the **timeframe** attribute is set to specify the time window as 600 seconds.

The **<if_matched_sid></if_matched_sid>** tag is used to define which other rule the composite rule will watch:

```
<rule id="100130" level="10" frequency="5" timeframe="600">
 <if_matched_sid>100124</if_matched_sid>
 <description>5 Failed passwords within 10 minutes</description>
</rule>
```

There are several additional tags that you can use to create more granular composite rules. These rules, as shown in the following table, allow you to specify that certain parts of the event must be the same. This allows you to tune your composite rules and reduce false positives:

Tag	Description
same_source_ip	Specifies that the source IP address must be the same.
same_dest_ip	Specifies that the destination IP address must be the same.
same_dst_port	Specifies that the destination port must be the same.
same_location	Specifies that the location (hostname or agent name) must be the same.
same_user	Specifies that the decoded username must be the same.
same_id	Specifies that the decoded id must be the same.

If you wanted your composite rule to Alert on every authentication failure, instead of a specific rule ID, you could replace the **<if_matched_sid></if_matched_sid>** tag with the **<if_matched_ group></if_matched_ group>** tag. This allows you to specify a category, such as **authentication_ failure**, to search for authentication failures across your entire infrastructure.

```
<rule id="100130" level="10" frequency="5" timeframe="600">
 <if_matched_group>authentication_failure</if_matched_group>
 <same_source_ip />
 <description>5 Failed passwords within 10 minutes</description>
</rule>
```

In addition to **<if_matched_sid></if_matched_sid>** and **<if_matched_group></if_matched_ group>** tags, you can also use the **<if_matched_regex></if_matched_regex>** tag to specify a regular expression to search through logs as they are received.

```
<rule id="100130" level="10" frequency="5" timeframe="600">
 <if_matched_regex>^Failed password</if_matched_regex>
 <same_source_ip />
 <description>5 Failed passwords within 10 minutes</description>
</rule>
```

Real World Examples

Deep Security includes many default Log Inspection rules for dozens of common and popular applications. Through Security Updates, new rules are added regularly. In spite of the growing list of applications supported by Log Inspection rules, you may find the need to create a custom rule for an unsupported or custom application.

In this section we will walk through the creation of a custom CMS (Content Management System) hosted on the Microsoft Windows Server IIS .Net platform with a Microsoft SQL Database as the data repository.

The first step is to identify the following application logging attributes:

1. Where does the application log to?

2. Which Log Inspection decoder can be used to decode the log file?
3. What is the general format of a log file message?

For our custom CMS example the answers are as follows:

1. Windows Event Viewer
2. Windows Event Log (eventlog)
3. Windows Event Log Format with the following core attributes:
    - Source: CMS
    - Category: None
    - Event: <Application Event ID>

The second step is to identify the categories of log events by application feature, and then organize the categories into a hierarchy of cascading groups for inspection. Not all inspected groups need to raise events; a match can be used as a conditional statement. For each group, identify the log format attributes which the rule can use as matching criteria. This can be performed in a reverse manner by inspecting all application logs for patterns and natural groupings of log events.

For example, the CMS application supports the following functional features which we will create log inspection rules for:

- CMS Application Log (Source: CMS)
    - Authentication (Event: 100 to 119)
        - User Login successful (Event: 100)
        - User Login unsuccessful (Event: 101)
        - Administrator Login successful (Event: 105)
        - Administrator Login unsuccessful (Event: 106)
    - General Errors (Type: Error)
        - Database error (Event: 200 to 205)
        - Runtime error (Event: 206-249)
    - Application Audit (Type: Information)
        - Content
            - New content added (Event: 450 to 459)
            - Existing content modified (Event: 460 to 469)
            - Existing content deleted (Event: 470 to 479)
        - Administration
            - User
                - New User created (Event: 445 to 446)
                - Existing User deleted (Event: 447 to 449)

This structure will provide you with a good basis for rule creation. Now to create a new Log Inspection rule in Deep Security Manager.

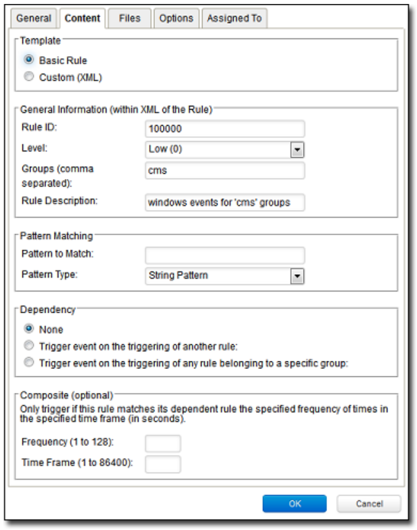
To create the new CMS Log Inspection Rule:

1. In the Deep Security Manager, go to **Policies > Common Objects > Rules > Log Inspection Rules** and click **New** to display the **New Log Inspection Rule Properties** window.
2. Give the new rule a Name and a Description, and then click the **Content** tab.
3. The quickest way to create a new custom rule is to start with a basic rule template. Select the **Basic Rule** radio button.
4. The **Rule ID** field will be automatically populated with an unused ID number between 100,000 and 199,000, the IDs reserved for custom rules.

5. Set the **Level** setting to **Low (0)**.

6. Give the rule an appropriate Group name. In this case, "cms".

7. Provide a short rule description.



Template
● Basic Rule
○ Custom (XML)

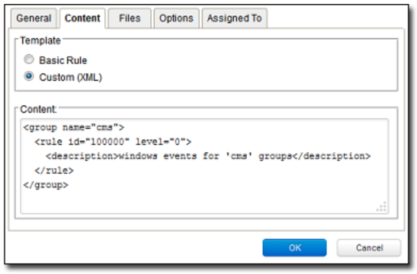
General Information (within XML of the Rule)
Rule ID: 100000
Level: Low (0)
Groups (comma separated): cms
Rule Description: windows events for 'cms' groups

Pattern Matching
Pattern to Match:
Pattern Type: String Pattern

Dependency
● None
○ Trigger event on the triggering of another rule:
○ Trigger event on the triggering of any rule belonging to a specific group:

Composite (optional)
Only trigger if this rule matches its dependent rule the specified frequency of times in the specified time frame (in seconds).
Frequency (1 to 128):
Time Frame (1 to 86400):

8. Now select the **Custom (XML)** option. The information you have entered will be used to generate the XML for your rule.

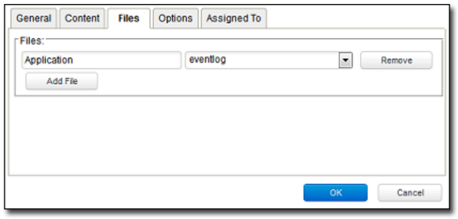


Template
○ Basic Rule
● Custom (XML)

Content:

```
<group name="cms">
  <rule id="100000" level="0">
    <description>windows events for 'cms' groups</description>
  </rule>
</group>
```

9. Next, click the **Files** tab and click the **Add File** button to add any application log files and log types which the rule will be applied to. In this case, "Application", and "eventlog" as the file type.



Files:
Application eventlog

Note: ***Eventlog*** *is a unique file type in Deep Security because the location and filename of the log files don't have to be specified. Instead, it is sufficient to type the log name as it is displayed in the Windows Event Viewer. Other log names for the eventlog file type might be "Security", "System", "Internet Explorer", or any other section listed in the Windows Event Viewer. Other file types will require the log file's location and filename. (C/C++ strftime() conversion specifiers are available for matching on filenames. See the table below for a list of some of the more useful ones.)*

10. Click **OK** to save the basic rule.

11. Working with the basic rule Custom (XML) created, we can begin adding new rules to the group based on the log groupings identified previously. We will set the base rule criteria to the initial rule. In the following example, the CMS base rule has identified Windows Event Logs with a Source attribute of "CMS":

```
<group name="cms">
 <rule id="100000" level="0">
 <category>windows</category>
 <extra_data>^CMS</extra_data>
 <description>Windows events from source 'CMS' group messages.</description>
 </rule>
```

12. Now we build up subsequent rules from the identified log groups. The following example identifies the authentication and login success and failure and logs by Event IDs.

```
<rule id="100001" level="0">
 <if_sid>100000</if_sid>
 <id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id>
 <group>authentication</group>
 <description>CMS Authentication event.</description>
 </rule>

 <rule id="100002" level="0">
 <if_group>authentication</if_group>
 <id>100</id>
 <description>CMS User Login success event.</description>
 </rule>

 <rule id="100003" level="4">
 <if_group>authentication</if_group>
 <id>101</id>
 <group>authentication_failure</group>
 <description>CMS User Login failure event.</description>
 </rule>

 <rule id="100004" level="0">
 <if_group>authentication</if_group>
 <id>105</id>
 <description>CMS Administrator Login success event.</description>
 </rule>

 <rule id="100005" level="4">
 <if_group>authentication</if_group>
 <id>106</id>
 <group>authentication_failure</group>
 <description>CMS Administrator Login failure event.</description>
 </rule>
```

13. Now we add any composite or correlation rules using the established rules. The follow example shows a high severity composite rule which is applies to instances where the repeated login failures have occurred 5 times within a 10 second time period:

```
 <rule id="100006" level="10" frequency="5" timeframe="10">
 <if_matched_group>authentication_failure</if_matched_group>
 <description>CMS Repeated Authentication Login failure event.</description>
 </rule>
```

14. Review all rules for appropriate severity levels. For example, error logs should have a severity of level 5 or higher. Informational rules would have a lower severity.

15. Finally, open the newly created rule, click the **Configuration** tab and copy your custom rule XML into the rule field. Click **Apply** or **OK** to save the change.

Once the rule is assigned to a Policy or computer, the Log Inspection engine should begin inspecting the designated log file immediately.

The complete Custom CMS Log Inspection Rule:

```
<group name="cms">

 <rule id="100000" level="0">
 <category>windows</category>
 <extra_data>^CMS</extra_data>
 <description>Windows events from source 'CMS' group messages.</description>
 </rule>

 <rule id="100001" level="0">
 <if_sid>100000</if_sid>
 <id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id>
 <group>authentication</group>
 <description>CMS Authentication event.</description>
 </rule>

 <rule id="100002" level="0">
 <if_group>authentication</if_group>
 <id>100</id>
 <description>CMS User Login success event.</description>
 </rule>

 <rule id="100003" level="4">
 <if_group>authentication</if_group>
 <id>101</id>
 <group>authentication_failure</group>
 <description>CMS User Login failure event.</description>
 </rule>

 <rule id="100004" level="0">
 <if_group>authentication</if_group>
 <id>105</id>
 <description>CMS Administrator Login success event.</description>
 </rule>

 <rule id="100005" level="4">
 <if_group>authentication</if_group>
 <id>106</id>
 <group>authentication_failure</group>
 <description>CMS Administrator Login failure event.</description>
 </rule>

 <rule id="100006" level="10" frequency="5" timeframe="10">
 <if_matched_group>authentication_failure</if_matched_group>
 <description>CMS Repeated Authentication Login failure event.</description>
 </rule>

 <rule id="100007" level="5">
 <if_sid>100000</if_sid>
 <status>^ERROR</status>
 <description>CMS General error event.</description>
 <group>cms_error</group>
 </rule>

 <rule id="100008" level="10">
 <if_group>cms_error</if_group>
 <id>^200|^201|^202|^203|^204|^205</id>
 <description>CMS Database error event.</description>
 </rule>

 <rule id="100009" level="10">
 <if_group>cms_error</if_group>
 <id>^206|^207|^208|^209|^230|^231|^232|^233|^234|^235|^236|^237|^238|^239^|240|^241|^242|^243|^244|^245|^246|
 <description>CMS Runtime error event.</description>
 </rule>

 <rule id="100010" level="0">
 <if_sid>100000</if_sid>
 <status>^INFORMATION</status>
 <description>CMS General informational event.</description>
 <group>cms_information</group>
 </rule>

 <rule id="100011" level="5">
 <if_group>cms_information</if_group>
 <id>^450|^451|^452|^453|^454|^455|^456|^457|^458|^459</id>
 <description>CMS New Content added event.</description>
 </rule>

 <rule id="100012" level="5">
 <if_group>cms_information</if_group>
 <id>^460|^461|^462|^463|^464|^465|^466|^467|^468|^469</id>
 <description>CMS Existing Content modified event.</description>
 </rule>

 <rule id="100013" level="5">
 <if_group>cms_information</if_group>
 <id>^470|^471|^472|^473|^474|^475|^476|^477|^478|^479</id>
 <description>CMS Existing Content deleted event.</description>
 </rule>

 <rule id="100014" level="5">
 <if_group>cms_information</if_group>
 <id>^445|^446</id>
 <description>CMS User created event.</description>
 </rule>

 <rule id="100015" level="5">
 <if_group>cms_information</if_group>
 <id>^447|449</id>
 <description>CMS User deleted event.</description>
 </rule>

</group>
```

Log Inspection Rule Severity Levels and their Recommended Use

Level	Description	Notes
Level 0	Ignored, no action taken	Primarily used to avoid false positives. These rules are scanned before all the others and include events with no security relevance.
Level 1	no predefined use	
Level 2	System low priority notification	System notification or status messages that have no security relevance.
Level 3	Successful/ authorized events	Successful login attempts, firewall allow events, etc.

Level	Description	Notes
Level 4	System low priority errors	Errors related to bad configurations or unused devices/applications. They have no security relevance and are usually caused by default installations or software testing.
Level 5	User-generated errors	Missed passwords, denied actions, etc. These messages typically have no security relevance.
Level 6	Low relevance attacks	Indicate a worm or a virus that provide no threat to the system such as a Windows worm attacking a Linux server. They also include frequently triggered IDS events and common error events.
Level 7	no predefined use	
Level 8	no predefined use	
Level 9	Error from invalid source	Include attempts to login as an unknown user or from an invalid source. The message might have security relevance especially if repeated. They also include errors regarding the **admin** or **root** account.
Level 10	Multiple user generated errors	Include multiple bad passwords, multiple failed logins, etc. They might indicate an attack, or it might be just that a user forgot his or her credentials.
Level 11	no predefined use	
Level 12	High-importance event	Include error or warning messages from the system, kernel, etc. They might indicate an attack against a specific application.
Level 13	Unusual error (high importance)	Common attack patterns such as a buffer overflow attempt, a larger than normal syslog message, or a larger than normal URL string.
Level 14	High importance security event	Typically the result of the correlation of multiple attack rules and indicative of an attack.
Level 15	Attack Successful	Very small chance of false positive. Immediate attention is necessary.

strftime() Conversion Specifiers

Specifier	Description
%a	Abbreviated weekday name (e.g., Thu)
%A	Full weekday name (e.g., Thursday)
%b	Abbreviated month name (e.g., Aug)
%B	Full month name (e.g., August)
%c	Date and time representation (e.g., Thu Sep 22 12:23:45 2007)
%d	Day of the month (01 - 31) (e.g., 20)
%H	Hour in 24 h format (00 - 23) (e.g., 13)
%I	Hour in 12 h format (01 - 12) (e.g., 02)
%j	Day of the year (001 - 366) (e.g., 235)
%m	Month as a decimal number (01 - 12) (e.g., 02)
%M	Minute (00 - 59) (e.g., 12)
%p	AM or PM designation (e.g., AM)
%S	Second (00 - 61) (e.g., 55)
%U	Week number with the first Sunday as the first day of week one (00 - 53) (e.g., 52)
%w	Weekday as a decimal number with Sunday as 0 (0 - 6) (e.g., 2)
%W	Week number with the first Monday as the first day of week one (00 - 53) (e.g., 21)
%x	Date representation (e.g., 02/24/79)
%X	Time representation (e.g., 04:12:51)
%y	Year, last two digits (00 - 99) (e.g., 76)
%Y	Year (e.g., 2008)
%Z	Time zone name or abbreviation (e.g., EST)
%%	A % sign (e.g., %)

More information can be found at the following Web sites:

www.php.net/strftime
www.cplusplus.com/reference/clibrary/ctime/strftime.html

Recommendation Scans

Deep Security can run Recommendation Scans on computers to identify known vulnerabilities. The operation scans the operating system but also installed applications. Based on what is detected, Deep Security will recommend security Rules that should be applied.

During a Recommendation Scan, Deep Security Agents scan:

- the operating system
- installed applications
- the Windows registry
- open ports
- the directory listing
- the file system
- running processes and services
- users

Note: *For large deployments, Trend Micro recommends managing Recommendations at the Policy level. That is, all computers that are to be scanned should already have a Policy assigned to them. This way, you can make all your rule assignments from a single source (the Policy) rather than having to manage individual rules on individual computers.*

Recommendation Scans can be initiated manually or you can create a Scheduled Task to periodically run scans on specified computers.

Limitations

On Linux, the Recommendation Scan engine may have trouble detecting applications that have been installed with kernel or software libraries not supported by the application being installed. Applications installed using standard package managers will not be a problem.

The Deep Security Virtual Appliance can perform Agentless Recommendation Scans on virtual machines but only on Windows VMs and is limited to scanning:

- the operating system
- installed applications
- the Windows registry
- the file system

Running Recommendation Scans

To launch a Recommendation Scan manually:

1. In the Deep Security Manager, go to the **Computers** page.
2. Select the computer or computers you want to scan.
3. Right-click the selection and choose **Actions > Scan for Recommendations**.

To create a Recommendation Scan Scheduled Task:

1. In the Deep Security Manager, go to the **Administration > Scheduled Tasks** page.
2. Click **New** on the toolbar and select "New Scheduled Task" to display the **New Scheduled Task** wizard.
3. Select "Scan Computers for Recommendations" from the **Type** menu and select how often you want the scan to occur. Click **Next**.

4. The next page will let you be more specific about the scan frequency, depending on your choice in step 3. Make your selection and click **Next**.
5. Now select which computer(s) will be scanned and click **Next**.

> *Note:* *As usual, for large deployments it's best to perform all actions through Policies.*

6. Finally, give a name to your new Scheduled Task, select whether or not to "Run Task on 'Finish'", click **Finish**.

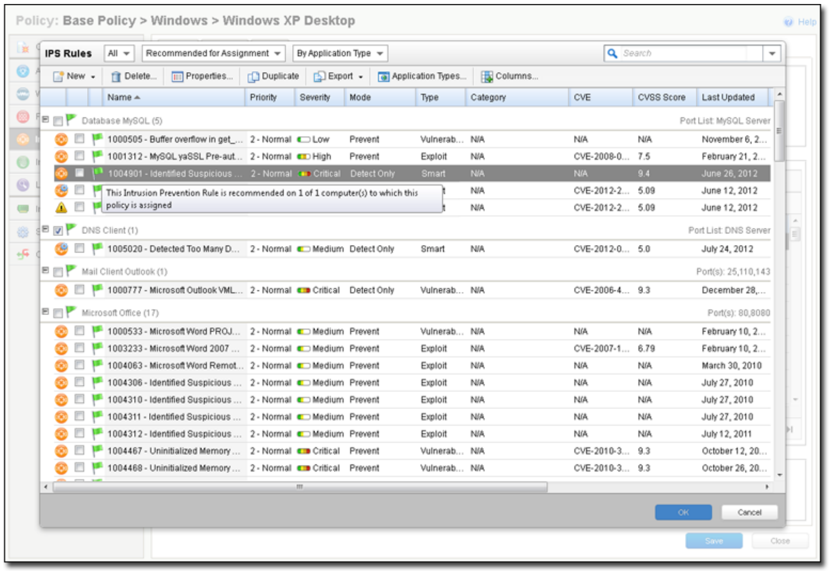
Managing Recommendation Scan Results

Deep Security can be configured to automatically implement Recommendation Scan results when it is appropriate to do so. Not all recommendations can be implemented automatically. The exceptions are:

- Rules that require configuration before they can be applied.
- Rules that have been automatically assigned or unassigned based on a previous Recommendation Scan but which a User has overridden. For example, if Deep Security automatically assigns a Rule and you subsequently unassign it, the Rule will not get reassigned after the next Recommendation Scan.
- Rules that have been assigned at a higher level in the policy hierarchy cannot be unassigned at a lower level. A Rule assigned to a computer at the Policy level must be unassigned at the Policy level.
- Rules that Trend Micro has issued but which may pose a risk of producing false positives. (This will be addressed in the Rule description.)

The results of the latest Recommendation Scan are displayed on the **General** tab of the protection module in the **Policy/Computer Editor**.

Once a Recommendation Scan is complete, open the Policy that is assigned to the computers you have just scanned. Navigate to **Intrusion Prevention > General**. Click **Assign/Unassign**... to open the rule Assignment window. Sort the rules "By Application Type", and select "Show Recommended for Assignment" from the display filter menu:



Policy: Base Policy > Windows > Windows XP Desktop

IPS Rules | All | Recommended for Assignment | By Application Type

Name ▲	Priority	Severity	Mode	Type	Category	CVE	CVSS Score	Last Updated
Database MySQL (5)								Port List: MySQL Server
1000505 - Buffer overflow in get_...	2 - Normal	Low	Prevent	Vulnerab...	N/A	N/A	N/A	November 6, 2...
1001312 - MySQL yaSSL Pre-aut...	2 - Normal	High	Prevent	Exploit	N/A	CVE-2008-0...	7.5	February 21, 2...
1004901 - Identified Suspicious ...	2 - Normal	Critical	Detect Only	Smart	N/A	N/A	9.4	June 26, 2012
				t	N/A	CVE-2012-2...	5.09	June 12, 2012
				t	N/A	CVE-2012-2...	5.09	June 12, 2012
DNS Client (1)								Port List: DNS Server
1005020 - Detected Too Many D...	2 - Normal	Medium	Detect Only	Smart	N/A	CVE-2012-0...	5.0	July 24, 2012
Mail Client Outlook (1)								Port(s): 25,110,143
1000777 - Microsoft Outlook VML...	2 - Normal	Critical	Detect Only	Vulnerab...	N/A	CVE-2006-4...	9.3	December 28,...
Microsoft Office (17)								Port(s): 80,8080
1000533 - Microsoft Word PROJ...	2 - Normal	Medium	Prevent	Vulnerab...	N/A	N/A	N/A	February 10, 2...
1003233 - Microsoft Word 2007 ...	2 - Normal	Medium	Prevent	Exploit	N/A	CVE-2007-1...	6.79	February 10, 2...
1004063 - Microsoft Word Remot...	2 - Normal	Medium	Prevent	Exploit	N/A	N/A	N/A	March 30, 2010
1004306 - Identified Suspicious ...	2 - Normal	Medium	Prevent	Exploit	N/A	N/A	N/A	July 27, 2010
1004310 - Identified Suspicious ...	2 - Normal	Medium	Prevent	Exploit	N/A	N/A	N/A	July 27, 2010
1004311 - Identified Suspicious ...	2 - Normal	Medium	Prevent	Exploit	N/A	N/A	N/A	July 27, 2010
1004312 - Identified Suspicious ...	2 - Normal	Medium	Prevent	Exploit	N/A	N/A	N/A	July 12, 2011
1004467 - Uninitialized Memory ...	2 - Normal	Critical	Prevent	Vulnerab...	N/A	CVE-2010-3...	9.3	October 12, 20...
1004468 - Uninitialized Memory ...	2 - Normal	Critical	Prevent	Vulnerab...	N/A	CVE-2010-3...	9.3	October 26, 20...

This Intrusion Prevention Rule is recommended on 1 of 1 computer(s) to which this policy is assigned

All the recommendations made for all the computers included in the Policy will be listed.

> *Note:* *There are two kinds of green flags. Full flags ( ) and partial flags( ). Recommended Rules always have a full flag. Application Types may have a full or partial flag. If the flag is full, it signifies that all the Rules that are part of this Application Type have been recommended for assignment. If the flag is partial, it signifies that only some of the Rules that are part of this Application Type have been recommended.*

Also notice the tool tip in the screen shot above. It reads: "This Intrusion Prevention Rule is recommended on 1 of 1 computer(s) to which this Policy is assigned." Trend Micro recommends assigning all the recommended Rules to all the computers covered by the Policy. This may mean that some Rules are assigned to computers on which they are not required. However, the minimal effect on performance is outweighed by the ease of management that results from working through Policies.

Remember that a Recommendation Scan will make recommendations for Intrusion Prevention Rules, Log Inspection Rules, and Integrity Monitoring Rules.

Once a Recommendation Scan has run, Alerts will be raised on the all computers for which recommendations have been made.

Note: *The results of a Recommendation Scan can also include recommendations to unassign rules. This can occur if applications are uninstalled, if security patches from a manufacturer are applied, or if unnecessary rules have been applied manually. To view rules that are recommended for unassignment, select "Show Recommended for Unassignment" from the display filter menu.*

Configuring Recommended Rules

Some Rules require configuration before they can be applied. For example, some Log Inspection Rules require that you specify the location of the log files to be inspected for change. If this is the case, an Alert will be raised on the Computer on which the recommendation has been made. The text of the Alert will contain the information required to configure the rule.

SSL Data Streams

The Intrusion Prevention module supports filtering of SSL traffic. The SSL dialog allows the User to create SSL Configurations for a given credential-port pair on one or more interfaces. Credentials can be imported in **PKCS#12** or **PEM** format, and Windows computers have the option of using **CryptoAPI** directly.

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

Configuring SSL Data Stream Filtering on a computer

Start the SSL Configuration Wizard

Open the **Details** window of the computer you wish to configure, go to **Intrusion Prevention > Advanced > SSL Configurations**, and click on **View SSL Configurations...** to display the **SSL Computer Configurations** window. Click **New** to display the first page of the **SSL Configuration** wizard.

1. Select Interface(s)

Specify whether this configuration will apply to all interfaces on this computer or just one.

2. Select Port(s)

Either enter the (comma-separated) ports you want this configuration to apply to, or select a Port List.

Note: *You will also have to change the port settings on the computer's **Details** window. (See below.)*

3. IP Selection

Specify whether SSL Intrusion Prevention analysis should take place on all IP addresses for this computer, or just one. (This feature can be used to set up multiple virtual computers on a single computer.)

4. Specify Source of Credentials

Specify whether you will provide the credentials file yourself, or whether the credentials are already on the computer.

5. Specify Type of Credentials

If you have chosen to provide the credentials now, enter their type, location, and pass phrase (if required).

If you've indicated that the credentials are on the computer, specify the type of credentials to look for.

6. Provide Credential Details

If you are using PEM or PKCS#12 credential formats stored on the computer, identify the location of the credential file and the file's pass phrase (if required).

If you are using Windows CryptoAPI credentials, choose the credentials from the list of credentials found on the computer.

7. Name and Describe this Configuration

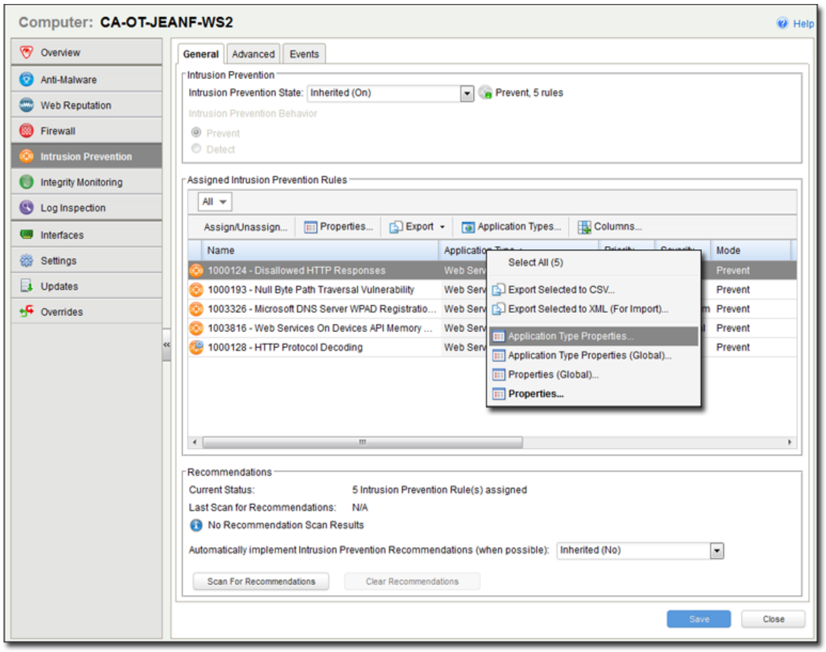
Give a name to and provide a description of this SSL configuration.

8. Look Over the Summary and Close the SSL Configuration Wizard

Read the summary of the configuration operation and click **Finish** to close the wizard.

Change Port Settings in the computer Details window to Monitor SSL Ports.

Finally, you need to ensure that the Agent is performing the appropriate Intrusion Prevention Filtering on the SSL-enabled port(s). Go to **Intrusion Prevention Rules** in the computer's **Details** window to see the list of Intrusion Prevention Rules being applied on this computer. Sort the rules by Application Type. Scroll down the list to find the Application Type(s) running on this computer (in this example, we will use "Web Server Common").



Computer: CA-OT-JEANF-WS2

Intrusion Prevention

Intrusion Prevention State: Inherited (On) Prevent, 5 rules

Intrusion Prevention Behavior

● Prevent

○ Detect

Assigned Intrusion Prevention Rules

Name	Application Type	Mode
1000124 - Disallowed HTTP Responses	Web Serv	Prevent
1000193 - Null Byte Path Traversal Vulnerability	Web Serv	Prevent
1003326 - Microsoft DNS Server WPAD Registratio...	Web Serv	Prevent
1003816 - Web Services On Devices API Memory ...	Web Serv	Prevent
1000128 - HTTP Protocol Decoding	Web Serv	Prevent

Recommendations

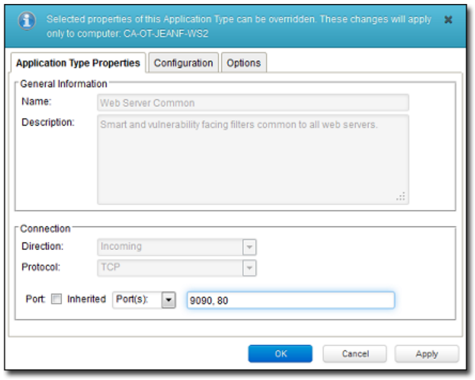
Current Status: 5 Intrusion Prevention Rule(s) assigned

Last Scan for Recommendations: N/A

No Recommendation Scan Results

Automatically implement Intrusion Prevention Recommendations (when possible): Inherited (No)

Right-click the "Web Server Common" Application Type heading and choose **Application Type Properties...** (not **Application Type Properties (Global)...**). This will display the Application Type's **Properties** window (in *local* edit mode).



Selected properties of this Application Type can be overridden. These changes will apply only to computer: CA-OT-JEANF-WS2

General Information

Name: Web Server Common

Description: Smart and vulnerability facing filters common to all web servers.

Connection

Direction: Incoming

Protocol: TCP

Port ☐ Inherited Port(s): 9090, 80

Instead of using the inherited "HTTP" Port List, we will override it to include the port we defined during the SSL Configuration setup (port 9090 in this case) as well as port 80. Enter ports 9090 and 80 as comma-separated values and click **OK** to close the dialog. (Since you selected **Application Type Properties...**, the changes you made will only be applied to this computer. The "Web Server Common" Application Type will remain unchanged on other computers.)

This computer is now configured for filtering SSL encrypted data streams.

Additional Notes

Note: *The Deep Security Agents do not support Diffie-Hellman ciphers on Apache servers. For instructions on how to disable DH ciphers on an Apache Web server, see* ***Disabling Diffie-Hellman in Apache (page 179)****.*

Events, Alerts, and Reports

Events

Deep Security will record security Events when a protection module Rule or condition is triggered, and System Events when administrative or system-related Events occur (like a User signing in or Agent software being upgraded.) Events can occur many times on a daily basis and do not necessarily require individual attention.

Most Events that take place on a computer are sent to the Deep Security Manager during the next heartbeat operation except the following which will be sent right away if ***Communication (page 30)*** settings allow Relays/Agents/Appliances to initiate communication:

- Smart Scan Server is offline
- Smart Scan Server is back online
- Integrity Monitoring scan is complete
- Integrity Monitoring baseline created
- Unrecognized elements in an Integrity Monitoring Rule
- Elements of an Integrity Monitoring Rule are unsupported on the local platform
- Abnormal restart detected
- Low disk space warning
- Log Inspection offline
- Log Inspection back online
- Reconnaissance scan detected (if the setting is enabled in **Policy/Computer Editor > Firewall > Reconnaissance**

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

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

From the main page you can:

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

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

- **Add Tag(s)** to this event (See ***Event Tagging (page 133)***.)
- **Remove Tag(s)** from this event.
- View the **Computer Details window** of the computer that generated the log entry.

View Event Properties

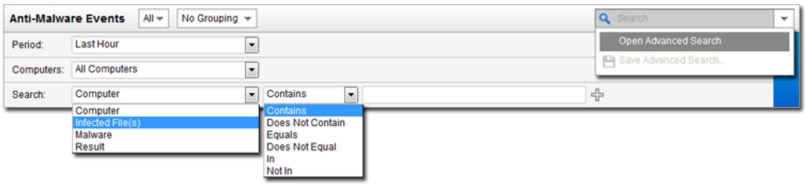
Double-clicking an event (or selecting **View** from the context menu) displays the **Properties** window for that entry which displays all the information about the event on one page. The **Tags** tab displays tags that have been attached to this Event. For More information on Event tagging, see **Policies > Common Objects > Other > Tags**, and ***Event Tagging (page 133)***.

Filter the List and/or Search for an Event

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

The **Period** toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The **Computers** toolbar lets you organize the display of event log entries by computer groups or computer Policies.



Period: Last Hour

Computers: All Computers

Search: Computer Contains

Advanced Search functions (searches are not case sensitive):

- **Contains:** The entry in the selected column contains the search string
- **Does Not Contain:** The entry in the selected column does not contain the search string
- **Equals:** The entry in the selected column exactly matches the search string
- **Does Not Equal:** The entry in the selected column does not exactly match the search string
- **In:** The entry in the selected column exactly matches one of the comma-separated search string entries
- **Not In:** The entry in the selected column does not exactly match any of the comma-separated search string entries

Pressing the "plus" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the submit button (at the right of the toolbars with the right-arrow on it).

Export

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

Auto-Tagging...

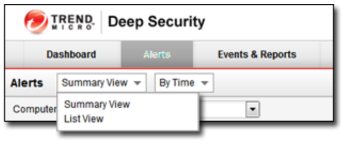
Clicking **Auto-Tagging...** displays a list of existing Auto-Tagging Rules. (See ***Event Tagging (page 133)***.)

Alerts

Alerts are created when an unusual situation arises that requires a user's attention (like a User-issued command failing, or a hard disk running out of storage space). There is a pre-defined list of Alerts. Additionally, protection module Rules can be configured to generate Alerts if they are triggered.

If you connect Deep Security to an SMTP server, you can have email notifications sent to Users when specific Alerts are raised.

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



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

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

Alerts that can't be dismissed (like "Relay Update Service Not Available") will be dismissed automatically when the condition no longer exists.

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

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

Reports

Deep Security Manager produces reports in PDF or RTF formats. Most of the reports generated by the **Reports** page have configurable parameters such as date range or reporting by computer group. Parameter options will be disabled for reports to which they don't apply.

Single Report

Report

The various reports can be output to PDF or RTF format.

Tag Filter

When you select a report that contains event data, you have the option to filter the report data using Event Tags. Select **All** for all events, **Untagged** for only untagged events, or select **Tag(s)** and specify one or more tags to include only those events with your selected tag(s).

Time Filter

You can set the time filter for any period for which records exist. This is useful for security audits.

Time filter options:

- **Last 24 Hours:** Includes events from the past 24 hours, starting and ending at the top of the hour.
- **Last 7 Days:** Includes events from the past week. Weeks start and end at midnight (00:00).
- **Previous Month:** Includes events from the last full calendar month, starting and ending at midnight (00:00). For example, if you select this option on November 15, you will receive a report for events that occurred between midnight October 1 to midnight November 1.
- **Custom Range:** Enables you to specify your own date and time range for the report.

Note: *Reports use data stored in counters. Counters are data aggregated periodically from Events. Counter data is aggregated on an hourly basis for the most recent three days. Data older than three days is stored in counters that are aggregated on a daily basis. For this reason, the time period covered by reports for the last three days can be specified at an hourlyi level of granularity, but beyond three days, the time period can only be specified on a daily level of granularity.*

Computer Filter

Set the computers whose data will be included in the report.

Encryption

Reports can be protected with the password of the currently signed in User or with a new password for this report only.

Note: *To generate a report on specific computers from multiple computer groups, create a User who has viewing rights only to the computers in question and then either create a Scheduled Task to regularly generate an "All Computers" report for that User or sign in as that User and run an "All Computers" report. Only the computers to which that User has viewing rights will be included in the report.*

Recurring Reports

Recurring Reports are simply Scheduled Tasks that periodically generate and distribute Reports to any number of Users and Contacts. For more information on Scheduled Tasks, go to **Administration > Scheduled Tasks**.

Event Tagging

Deep Security enables you to create tags that you can use to identify and sort events. For example, you might use tags to separate events that are benign from those that require further investigation. You can use tags to create customized dashboards and reports.

Although you can use event tagging for a variety of purposes, it was designed to ease the burden of event management. After you have analyzed an event and determined that it is benign, you can look through the Event logs of the computer (and any other similarly configured and tasked computers) to find similar events and apply the same label to them, eliminating the need to analyze each event individually.

Note: *Tags do not alter the data in the events themselves, nor do they allow users to delete events. They are simply extra attributes provided by the Manager.*

These are the ways that you can perform tagging:

- **Manual Tagging** can be done on an ad-hoc basis.
- **Auto-Tagging** lets you use an existing event as the model for auto-tagging similar events on the same or other computers. You define the parameters for "similarity" by selecting which event attributes have to match the model event attributes for a tag to be applied.
- **Trusted Source Tagging** lets you auto-tag Integrity Monitoring events based on their similarity to known-good events from a trusted source.

Note: *An important difference between standard tagging and Trusted Source tagging is that "Run on Existing Events Now" can only be done with standard event tagging.*

Manual Tagging

To tag manually tag an event:

1. In the **Events** list, right-click the event (or select multiple events and right-click) and select **Add Tag(s)...**.
2. Type a name for the tag. (Deep Security Manager will suggest matching names of existing tags as you type.)
3. Select **The Selected [Event Type] Event**. Click **Next**.
4. Enter some optional comments and click **Finish**.

Looking at the Events list, you can see that the event has now been tagged.

Auto-Tagging

Deep Security Manager enables you to define rules that apply the same tag to similar events automatically. To view existing saved auto-tagging rules, click **Auto-Tagging...** in the menu bar on any **Events** page. You can run saved rules manually from this page.

To create an auto-tagging rule:

1. In the **Events** list, right-click a representative event and select **Add tag(s)...**.
2. Type a name for the tag. (Deep Security Manager will suggest matching names of existing tags as you type.)
3. Select **Also apply to selected and similar [Event Type] Events** and click **Next**.
4. Select the computers where you want to auto-tagging events and click **Next**.
5. Select which attributes will be examined to determine whether events are similar. For the most part, the attribute options are the same as the information displayed in the columns of the **Events** list pages (Source IP, Reason, Severity, etc.). When you have selected which attributes to include in the event selection process, click **Next**.

6. On the next page, specify when events should be tagged. If you select **Existing [Event Type] Events**, you can choose whether to apply the auto-tagging rule immediately, or have it run in the background at a lower priority. Select **Future [Event Type] Events** to apply the auto-tagging rule to events that will happen in the future. You can also save the auto-tagging rule. You can access saved rules later by clicking **Auto-Tagging...** in the menu bar of the **Events** page. Click **Next**.
7. Review the summary of your auto-tagging rule and click **Finish**.

Looking at the Events list, you can see that your original event and all similar events have been tagged.

Note: *Event tagging only occurs after events have been retrieved from the Agents/Appliances to the Deep Security Manager's database.*

Once an auto-tagging Rule is created, you can assign it a **Precedence** value. If the auto-tagging rule has been configured to run on future events, the rule's precedence determines the order in which all auto-tagging rules are applied to incoming events. For example, you can have a rule with a precedence value of "1" that tags all "User Signed In" events as "suspicious", and a rule with a precedence value of "2" that removes the "suspicious" tag from all "User Signed In" events where the Target (User) is you. The precedence "1" rule will run first and apply the "suspicious" tag to all "User Signed In" events. The precedence "2" rule will run afterwards and remove the "suspicious" tag from all "User Signed In" events where the User was you. This will result in a "suspicious" tag being applied to all future "User Signed In" events where the User is not you.

To set the precedence for an auto-tagging rule:

1. In the **Events** list, click **Auto-Tagging...** to display a list of saved auto-tagging rules.
2. Right-click an auto-tagging rule and select **View**.
3. Select a **Precedence** for the rule.

Trusted Source Tagging

Note: *Trusted Source Event Tagging can only be used with events generated by the Integrity Monitoring protection module.*

The Integrity Monitoring module allows you to monitor system components and associated attributes on a computer for changes. ("Changes" include creation and deletion as well as edits.) Among the components that you can monitor for changes are files, directories, groups, installed software, listening ports, processes, registry keys, and so on.

Trusted Source Event Tagging is designed to reduce the number of events that need to be analyzed by automatically identifying events associated with authorized changes.

In addition to auto-tagging similar events, the Integrity Monitoring module allows you to tag events based on their similarity to events and data found on **Trusted Sources**. A Trusted Source can be either:

1. A **Local Trusted Computer**,
2. The **Trend Micro Certified Safe Software Service**, or
3. A **Trusted Common Baseline**, which is a set of file states collected from a group of computers.

Local Trusted Computer

A Trusted Computer is a computer that will be used as a "model" computer that you know will only generate benign or harmless events. A "target" computer is a computer that you are monitoring for unauthorized or unexpected changes. The auto-tagging rule examines events on target computers and compares them to events from the trusted computer. If any events match, they are tagged with the tag defined in the auto-tagging rule.

You can establish auto-tagging rules that compare events on protected computers to events on a Trusted Computer. For example, a planned rollout of a patch can be applied to the Trusted Computer. The events associated with the application of the patch can be tagged as "Patch X". Similar events raised on other systems can be auto-tagged and identified as acceptable changes and filtered out to reduce the number of events that need to be evaluated.

How does Deep Security determine whether an event on a target computer matches an event on a Trusted Source computer?

Integrity Monitoring events contain information about transitions from one state to another. In other words, events contain *before* and *after* information. When comparing events, the auto-tagging engine will look for matching before and after states; if the two events share the same before and after states, the events are judged to be a match and a tag is applied to the second event. This also applies to creation and deletion events.

> *Note:* *Remember that when using a Trusted Computer for Trusted Source Event Tagging, the events being tagged are events generated by Deep Security Integrity Monitoring Rules. This means that the Integrity Monitoring Rules that are generating events on the target computer must also be running on the Trusted Source computer.*

> *Note:* *Trusted Source computers must be scanned first.*

> *Note:* *Utilities that regularly make modifications to the content of files on a system (prelinking on Linux, for example) can interfere with Trusted Source Event Tagging.*

To tag events based on a Local Trusted Computer:

1. Make sure the Trusted Computer is free of malware by running a full Anti-Malware scan.
2. Make sure the computer(s) on which you want to auto-tag events are running the same (or some of the same) Integrity Monitoring Rules as the Trusted Source Computer.
3. In Deep Security Manager, go to **Events & Reports > Integrity Monitoring Events** and click **Auto-Tagging...** in the toolbar.
4. In the **Auto-Tag Rules (Integrity Monitoring Events)** window, click **New Trusted Source...** to display the **Tag Wizard**.
5. Select **Local Trusted Computer** and click **Next**.
6. From the drop-down list, select the computer that will be the Trusted Source and click **Next**.
7. Specify one or more tags to apply to events on target computers when they match events on this Trusted Source computer. Click **Next**.

   > *Note:* *You can enter the text for a new tag or select from a list of existing tags.*

8. Identify the target computers whose events will be matched to those of the Trusted Source. Click **Next**.
9. Optionally, give the rule a name and click **Finish**.

Certified Safe Software Service

The Certified Safe Software Service is a whitelist of known-good file signatures maintained by Trend Micro. This type of Trusted Source tagging will monitor target computers for file-related Integrity Monitoring events. When an event has been recorded, the file's signature (after the change) is compared to Trend Micro's list of known good file signatures. If a match is found, the event is tagged.

To tag events based on the Trend Micro Certified Safe Software Service:

1. In Deep Security Manager, go to **Events & Reports > Integrity Monitoring Events** and click **Auto-Tagging...** in the toolbar.
2. In the **Auto-Tag Rules (Integrity Monitoring Events)** window, click **New Trusted Source...** to display the **Tag Wizard**.
3. Select **Certified Safe Software Service** and click **Next**.
4. Specify one or more tags to apply to events on target computers when they match the Certified Safe Software Service. Click **Next**.
5. Identify the target computers whose events will be matched to the Certified Safe Software Service. Click **Next**.
6. Optionally, give the rule a name and click **Finish**.

Trusted Common Baseline

The Trusted Common Baseline method compares events within a group of computers. A group of computers is identified and a common baseline is generated based on the files and system states targeted by the Integrity Monitoring Rules in effect on the computers in the group. When an Integrity Monitoring event occurs on a computer within the group, the signature of the file after the change is compared to the common baseline. If the file's new signature has a match elsewhere in the common baseline, a tag is applied to the event. In Trusted Computer method, the before and after states of an Integrity Monitoring event are compared, but in the Trusted Common Baseline method, only the after state is compared.

Note: *This method relies on all the computers in the common group being secure and free of malware. A full Anti-Malware scan should be run on all the computers in the group before the common baseline is generated.*

Note: *When an Integrity Monitoring baseline is generated for a computer, Deep Security will first check if that computer is part of a Trusted Common baseline group. If it is, it will include the computer's baseline data in the Trusted Common Baseline for that group. For this reason, the Trusted Common Baseline Auto-Tagging Rule must be in place before any Integrity Monitoring Rules have been applied to the computers in the common baseline group.*

To tag events based on a Trusted Common Baseline:

1. Make sure all the computers that will be in the group that will make up the Trusted Common Baseline are free of malware by running a full Anti-Malware scan on them.
2. In Deep Security Manager, go to **Events & Reports > Integrity Monitoring Events** and click **Auto-Tagging...** in the toolbar.
3. In the **Auto-Tag Rules (Integrity Monitoring Events)** window, click **New Trusted Source...** to display the **Tag Wizard**.
4. Select **Trusted Common Baseline** and click **Next**.
5. Specify one or more tags to apply to events when they have a match in the Trusted Common Baseline and click **Next**.
6. Identify the computers to include in the group used to generate the Trusted Common baseline. Click **Next**.
7. Optionally, give this rule a name and click **Finish**.

Deep Security Notifier

The Deep Security Notifier is a Windows System Tray application that communicates the state of the Deep Security Agent and Deep Security Relay to client machines. The Notifier displays popup user notifications when the Deep Security Agent begins a scan, or blocks malware or access to malicious web pages. The Notifier also provides a console utility that allows the user to view events and configure whether popups are displayed. The Notifier has a small footprint on the client machine, requiring less than 1MB of disk space and 1MB of memory. When the Notifier is running the Notifier icon ( ) appears in the system tray.

The Notifier is automatically installed by default with the Deep Security Relay and Deep Security Agent on Windows computers. Use the **Administration > Updates > Software > Local** page to import the latest version for distribution and upgrades.

Note: *On computers running a Deep Security Relay, the Notifier displays the components that are being distributed to Agents/Appliances, not which components are in effect on the local computer.*

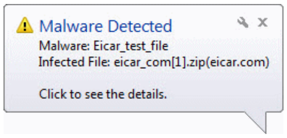
A standalone version of the Notifier can be downloaded and installed on Virtual Machines that are receiving Agentless protection from a Deep Security Virtual Appliance. See the Installation Guide for installation instructions.

Note: *On VMs protected by a Virtual Appliance, the Anti-Malware module must be licensed and enabled on the VM for the Deep Security Notifier to display information.*

How the Notifier Works

When the Deep Security Manager initiates an Anti-Malware or Integrity Monitoring scan, a notification is sent to the Notifier that the scan will begin. This causes a popup window to be displayed, notifying the user that a scan is starting. When malware is detected or a malicious site is blocked, the Deep Security Agent sends a message to the Notifier, which displays a popup message in the system tray.

If malware is detected, the Notifier displays a message in a system tray popup similar to the following:



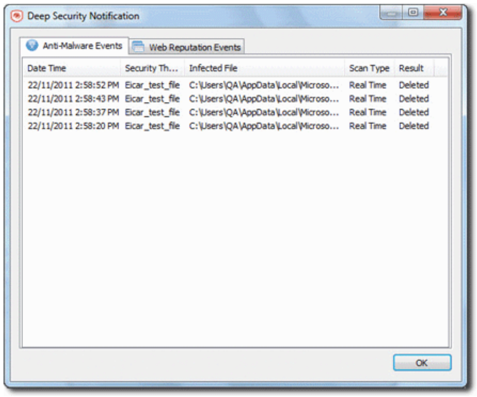
Malware Detected

Malware: Eicar_test_file

Infected File: eicar_com[1].zip(eicar.com)

Click to see the details.

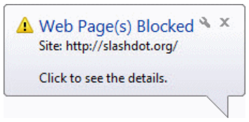
If the user clicks on the message, a dialog box with detailed information about Anti-Malware Events is displayed:



Deep Security Notification

Date Time	Security Th...	Infected File	Scan Type	Result
22/11/2011 2:58:52 PM	Eicar_test_file	C:\Users\QA\AppData\Local\Microso...	Real Time	Deleted
22/11/2011 2:58:43 PM	Eicar_test_file	C:\Users\QA\AppData\Local\Microso...	Real Time	Deleted
22/11/2011 2:58:37 PM	Eicar_test_file	C:\Users\QA\AppData\Local\Microso...	Real Time	Deleted
22/11/2011 2:58:20 PM	Eicar_test_file	C:\Users\QA\AppData\Local\Microso...	Real Time	Deleted

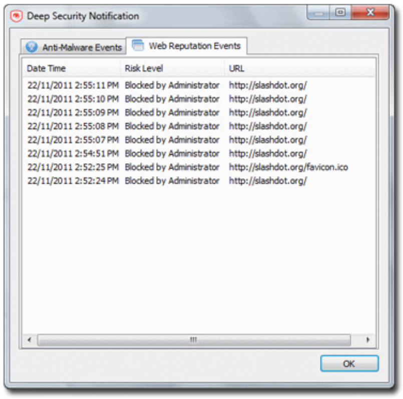
When a malicious web page is blocked, the Notifier displays a message in a system tray popup similar to the following:



Site: http://slashdot.org/

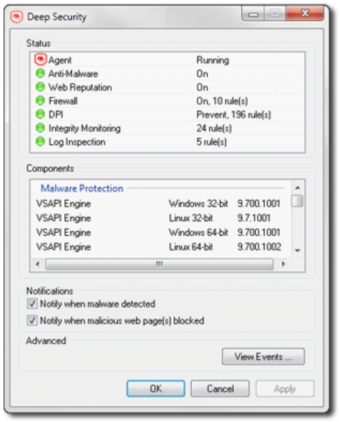
Click to see the details.

If the user clicks on the message, a dialog box with detailed information about Web Reputation Events is displayed:



Date Time	Risk Level	URL
22/11/2011 2:55:11 PM	Blocked by Administrator	http://slashdot.org/
22/11/2011 2:55:10 PM	Blocked by Administrator	http://slashdot.org/
22/11/2011 2:55:09 PM	Blocked by Administrator	http://slashdot.org/
22/11/2011 2:55:08 PM	Blocked by Administrator	http://slashdot.org/
22/11/2011 2:55:07 PM	Blocked by Administrator	http://slashdot.org/
22/11/2011 2:54:51 PM	Blocked by Administrator	http://slashdot.org/
22/11/2011 2:52:25 PM	Blocked by Administrator	http://slashdot.org/favicon.ico
22/11/2011 2:52:24 PM	Blocked by Administrator	http://slashdot.org/

The Notifier also provides a console utility for viewing the current protection status and component information, including pattern versions. The console utility allows the user to turn on and off the popup notifications and access detailed event information.



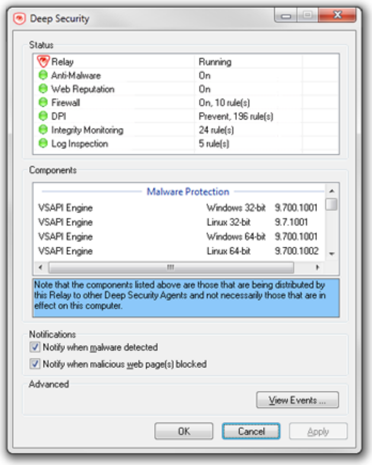
Agent	Running
Anti-Malware	On
Web Reputation	On
Firewall	On, 10 rule(s)
DPI	Prevent, 196 rule(s)
Integrity Monitoring	24 rule(s)
Log Inspection	5 rule(s)

VSAPI Engine	Windows 32-bit	9.700.1001
VSAPI Engine	Linux 32-bit	9.7.1001
VSAPI Engine	Windows 64-bit	9.700.1001
VSAPI Engine	Linux 64-bit	9.700.1002

☑ Notify when malware detected

☑ Notify when malicious web page(s) blocked

Note: *When the notifier is running on a computer hosting Deep Security Relay, the Notifier's display shows the components being distributed by the Relay and not the components that in effect on the computer.*



Status

Relay	Running
Anti-Malware	On
Web Reputation	On
Firewall	On, 10 rule(s)
DPI	Prevent, 196 rule(s)
Integrity Monitoring	24 rule(s)
Log Inspection	5 rule(s)

Components

Malware Protection

VSAPI Engine	Windows 32-bit	9.700.1001
VSAPI Engine	Linux 32-bit	9.7.1001
VSAPI Engine	Windows 64-bit	9.700.1001
VSAPI Engine	Linux 64-bit	9.700.1002

Note that the components listed above are those that are being distributed by this Relay to other Deep Security Agents and not necessarily those that are in effect on this computer.

Notifications

☑ Notify when malware detected

☑ Notify when malicious web page(s) blocked

Advanced

Disabling Protection

The Notifier does not allow protection to be disabled from the client machine. Protection can be disabled only by using the command line from the Deep Security Agent.

Multi-Tenancy

Purpose and Requirements

Multi-Tenancy lets you create multiple distinct management environments using a single Deep Security Manager and database server installation. It fully isolates the settings, Policies, and Events for each Tenant and makes use of a number of additional infrastructure scaling options.

Multi-Tenancy was designed to provide segmentation for business units within an organization and facilitate testing in staging environments prior to full production deployments. It also allows the provision of Deep Security to customers within a service model.

Note: *Role-Based Access Control instead of Multi-Tenancy may still be preferable for Managed Security Service Providers (MSSPs) because of the central control and reporting it offers.*

The requirements for Deep Security Multi-Tenancy are:

- Deep Security Manager 9 or higher
- Oracle Database or Microsoft SQL Server
- The necessary database account privileges for database create/delete operations. (See ***Multi-Tenancy (Advanced) (page 149)***)
- Multi-Tenant Activation Code

Optional but recommended:

- Multi-node Manager (more than one Deep Security Manager node pointed to the same database for scalability)
- SMTP server

Architecture

Multi-Tenancy in Deep Security Manager operates similarly to a hypervisor. Multiple Tenants exist within the same Deep Security Manager installation but their data is highly isolated. All Manager Nodes process GUI, Heartbeat or Job requests for any Tenant. For the background processing, each Tenant is assigned a Manager Node that takes care of job queuing, maintenance and other background tasks. The assigned Manager node is automatically rebalanced when manager nodes are added or taken offline. The majority of each Tenant's data is stored in a separated database. This database may co-exist on the same database server as other Tenants, or it can be isolated onto its own database server. In all cases, some data only exists in the primary database (the one Deep Security Manager was installed with). When multiple database servers are available, Tenants are created on the database with the least amount of load.

	Single Tenant	**Multi-Tenant**
Managed computers	100,000	1,000,000 or more
Deep Security Manager Nodes	1-5	1-50
Databases	1	1-10,000
Database Servers	1 (With or without replication)	1-100

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

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

- **Data destruction:** Deleting a Tenant removes all traces of that Tenant's data (Supported in the product)
- **Backup:** Each Tenant's data can be subject to different backup policies. This may be useful for something like tenancy being used for staging and production where the staging environment requires less stringent backups. (Backups are the responsibility of the administrator setting up Deep Security Manager.)

- **Balancing:** The potential for future re-balancing to maintain an even load on all database servers

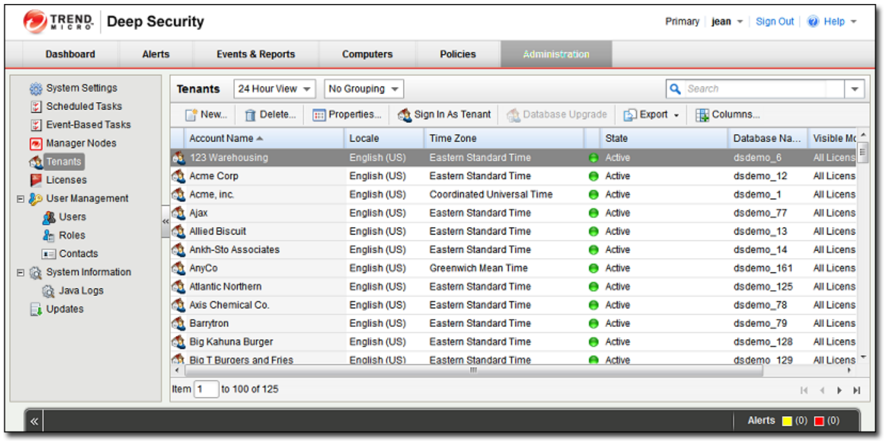
Enabling Multi-Tenancy

To enable Multi-Tenancy:

1. In the Deep Security Manager, go to **Administration > System Settings > Advanced** and click **Enable Multi-Tenancy** in the **Multi-Tenant Options** area to display the **Multi-Tenant Configuration** wizard.
2. Enter the Activation Code provided by your sales representative and click **Next**.
3. Choose the license mode you wish to implement:
   - **Inherit Licensing from Primary Tenant:** Gives all Tenants the same licenses that you (the Primary Tenant) have. This option is recommended if you are using Multi-Tenancy testing in a staging environment, or if you intend to set up Tenancies for separate departments within the same business.
   - **Per Tenant Licensing:** This mode is recommended when Deep Security is being offered as a service. Configured this way, you provide a license at the moment that you create a Tenant account (using the API) or the Tenants themselves enter a license when they sign in for the first time.
4. Click **Next** to finish enabling Multi-Tenancy in your Deep Security Manager.

Managing Tenants

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



Account Name	Locale	Time Zone	State	Database Na...	Visible Mc
123 Warehousing	English (US)	Eastern Standard Time	Active	dsdemo_6	All Licens
Acme Corp	English (US)	Eastern Standard Time	Active	dsdemo_12	All Licens
Acme, inc.	English (US)	Coordinated Universal Time	Active	dsdemo_1	All Licens
Ajax	English (US)	Eastern Standard Time	Active	dsdemo_77	All Licens
Allied Biscuit	English (US)	Eastern Standard Time	Active	dsdemo_13	All Licens
Ankh-Sto Associates	English (US)	Eastern Standard Time	Active	dsdemo_14	All Licens
AnyCo	English (US)	Greenwich Mean Time	Active	dsdemo_161	All Licens
Atlantic Northern	English (US)	Eastern Standard Time	Active	dsdemo_125	All Licens
Axis Chemical Co.	English (US)	Eastern Standard Time	Active	dsdemo_78	All Licens
Barrytron	English (US)	Eastern Standard Time	Active	dsdemo_79	All Licens
Big Kahuna Burger	English (US)	Eastern Standard Time	Active	dsdemo_128	All Licens
Big T Burgers and Fries	English (US)	Eastern Standard Time	Active	dsdemo_129	All Licens

Creating Tenants

To create a new Tenant:

1. Go to the **Administration > Tenants** page and click **New** to display the **New Tenant** wizard.
2. Enter a Tenant Account Name. The account name can be any name except "Primary" which is reserved for the Primary Tenant.
3. Enter an Email Address. The email address is required in order to have a contact point per Tenant. It is also used for two of the three different user account generation methods in the next step.
4. Select the Locale. The Locale determines the language of the Deep Security Manager user interface for that Tenant.
5. Select a Time Zone. All Tenant-related Events will be shown to the Tenant Users in the time zone of the Tenant account.

6. If your Deep Security installation is using more than one database, you will have the option to let Deep Security automatically select a database server on which to store the new Tenant account ("Automatic -- No Preference") or you can specify a particular server.

   Note: *Database servers that are no longer accepting new Tenants will not be included in the drop-down list. The options will not appear if you only have a single database.*

   When you have made your selection, click **Next** to continue.

7. Enter a Username for the first User of the new Tenant account.
8. Select one of the three password options:
   - **No Email:** The Tenancy's first User's username and password are defined here and no emails are sent.
   - **Email Confirmation Link:** You set the Tenancy's first User's password. However the account is not active until the User clicks a confirmation link he will receive by email.
   - **Email Generated Password:** This allows you to generate a Tenant without specifying the password. This is most applicable when manually creating accounts for users where you do not need access.

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

9. Click **Next** to finish with the wizard and create the Tenant. It may take from 30 seconds to four minutes to create the new Tenant database and populate it with data and sample Policies.

Examples of messages sent to Tenants

Email Confirmation Link: Account Confirmation Request

```
Welcome to Deep Security! To begin using your account, click the following confirmation URL. You can
then access the console using your chosen password.
Account Name: AnyCo
Username: admin
Click the following URL to activate your account:
https://managername:4119/SignIn.screen?confirmation=1A16EC7A-D84F-
D451-05F6-706095B6F646&tenantAccount=AnyCo&username=admin
```

Email Generated Password

First email : Account and Username Notification

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

Account Name: AnyCo
Username: admin
You can access the Deep Security management console using the following URL:
https://managername:4119/SignIn.screen?tenantAccount=AnyCo&username=admin
```

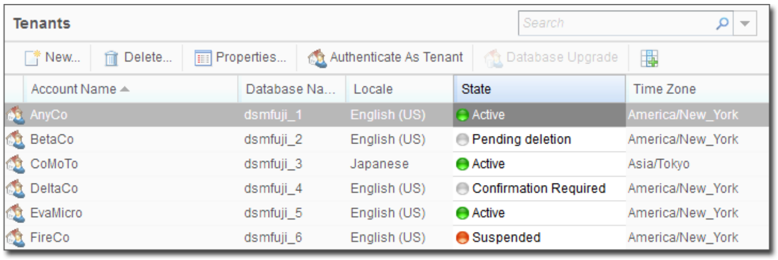
Second email: Password Notification

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

```
Password: z3IgRUQ0jaFi
```

Managing Tenants

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



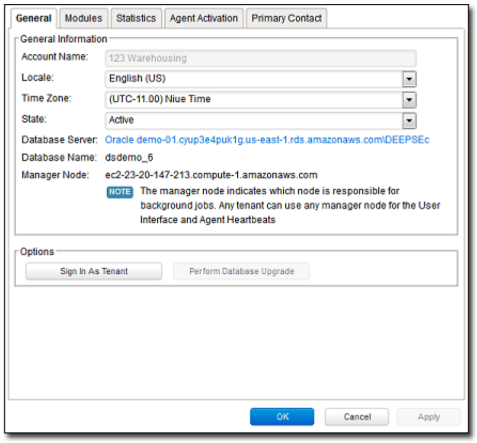
Account Name	Database Na...	Locale	State	Time Zone
AnyCo	dsmfuji_1	English (US)	Active	America/New_York
BetaCo	dsmfuji_2	English (US)	Pending deletion	America/New_York
CoMoTo	dsmfuji_3	Japanese	Active	Asia/Tokyo
DeltaCo	dsmfuji_4	English (US)	Confirmation Required	America/New_York
EvaMicro	dsmfuji_5	English (US)	Active	America/New_York
FireCo	dsmfuji_6	English (US)	Suspended	America/New_York

- **Created:** In the progress of being created but not yet active
- **Confirmation Required:** Created but the activation link in the confirmation email sent to the Tenant User has not yet be clicked. (You can manually override this state.)
- **Active:** Fully online and managed
- **Suspended:** No longer accepting sign ins.
- **Pending Deletion:** Tenants can be deleted, however the process is not immediate. The Tenant will be in the pending deletion state for approximately 7 days before the database is removed.
- **Database Upgrade Failed:** For Tenants that failed the upgrade path. The Database Upgrade button can be used to resolve this situation

Tenant Properties

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

General



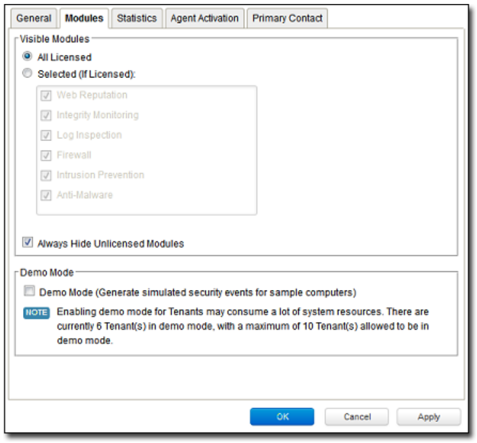
Account Name: 123 Warehousing
Locale: English (US)
Time Zone: (UTC-11.00) Niue Time
State: Active
Database Server: Oracle demo-01.cyup3e4puk1g.us-east-1.rds.amazonaws.com\DEEPSEc
Database Name: dsdemo_6
Manager Node: ec2-23-20-147-213.compute-1.amazonaws.com

NOTE The manager node indicates which node is responsible for background jobs. Any tenant can use any manager node for the User Interface and Agent Heartbeats

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

The Database Name indicates the name of the database used by this Tenancy. The server the database is running on can be accessed via the hyperlink.

Modules



Visible Modules

● All Licensed

○ Selected (If Licensed):

☑ Web Reputation
☑ Integrity Monitoring
☑ Log Inspection
☑ Firewall
☑ Intrusion Prevention
☑ Anti-Malware

☑ Always Hide Unlicensed Modules

Demo Mode

□ Demo Mode (Generate simulated security events for sample computers)

NOTE Enabling demo mode for Tenants may consume a lot of system resources. There are currently 6 Tenant(s) in demo mode, with a maximum of 10 Tenant(s) allowed to be in demo mode.

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

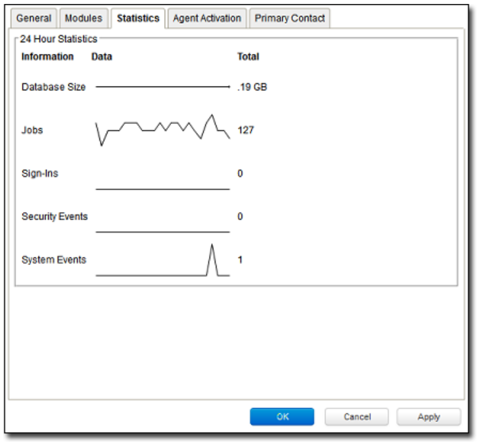
If you select **Inherit License from Primary Tenant**, all features that you (the Primary Tenant) are licensed for will be visible to all Tenants. The selected visibility can be used to tune which modules are visible for which Tenants.

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

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

*Demo Mode is **not** intended to be used in a production environment!*

Statistics

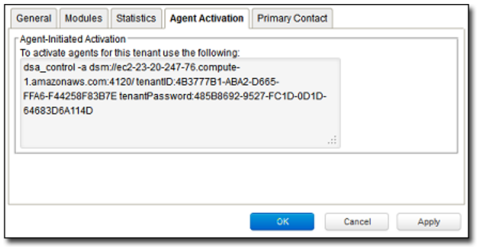


24 Hour Statistics

Information	Data	Total
Database Size		.19 GB
Jobs		127
Sign-Ins		0
Security Events		0
System Events		1

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

Agent Activation



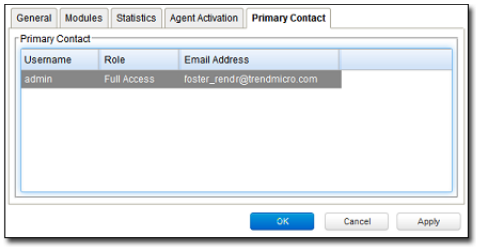
Agent-Initiated Activation

To activate agents for this tenant use the following:

```
dsa_control -a dsm://ec2-23-20-247-76.compute-
1.amazonaws.com:4120/ tenantID:4B3777B1-ABA2-D665-
FFA6-F44258F83B7E tenantPassword:485B8692-9527-FC1D-0D1D-
64683D6A114D
```

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

Primary Contact



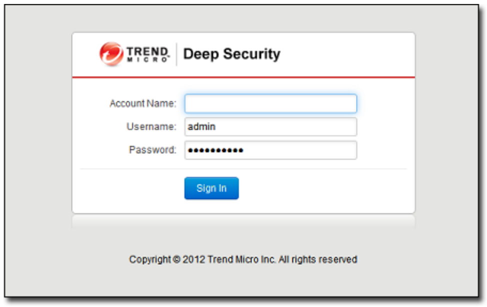
Primary Contact

Username	Role	Email Address
admin	Full Access	foster_rendr@trendmicro.com

The Tenant Account User's View of Deep Security

The Tenant "User experience"

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



Account Name:

Username: admin

Password: ••••••••••

Copyright © 2012 Trend Micro Inc. All rights reserved

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

Note:	*When you (as the Primary Tenant) log in, leave the Account name blank or use "Primary".*

When Tenants log in, they have a very similar environment to a fresh install of Deep Security Manager. Some features in the UI are not available to Tenant Users. The following areas are hidden for Tenants:

- Manager Nodes Widget
- Multi-Tenant Widgets
- Administration > System Information
- Administration > Licenses (If Inherit option selected)
- Administration > Manager Nodes
- Administration > Tenants
- Administration > System Settings:
    - Tenant Tab
    - Security Tab > Sign In Message
    - Updates Tab > Setting for Allowing Tenants to use Relays from the Primary Tenant
    - Advanced Tab > Load Balancers
    - Advanced Tab > Pluggable Section
- Some of the help content not applicable to Tenants
- Some reports not applicable to Tenants
- Other features based on the Multi-Tenant Options (discussed later)
- Some Alert Types will also be hidden from Tenants:
    - Heartbeat Server Failed
    - Low Disk Space
    - Manager Offline
    - Manager Time Out Of Sync
    - Newer Version of Deep Security Manager available
    - Number of Computers Exceeds Database Limit
    - And when inherited licensing is enabled any of the license-related alerts

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

For more information on what is and is not available to Tenant Users, see **Administration > System Settings > Tenants** in the Deep Security Manager Interface Guide or the online help.

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

Agent-Initiated Activation

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

Note: *Unlike Agent-initiated activation for the Primary Tenant, a password and Tenant ID are required to invoke the activation for Tenant Users.*

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

```
dsa_control     -a     dsm://manageraddress:4120/     "tenantID:7156CF5A-D130-29F4-5FE1-8AFD12E0EC02"
"tenantPassword:98785384-3966-B729-1418-3E2A7197D0D5"
```

Tenant Diagnostics

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

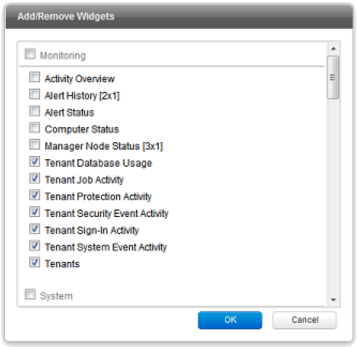
Usage Monitoring

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

This chargeback (or viewback) information can be customized to determine what attributes are included in the record. This configuration is designed to accommodate various charging models that may be required in service provider environments. For enterprises, this may be useful to determine the usage by each business unit.

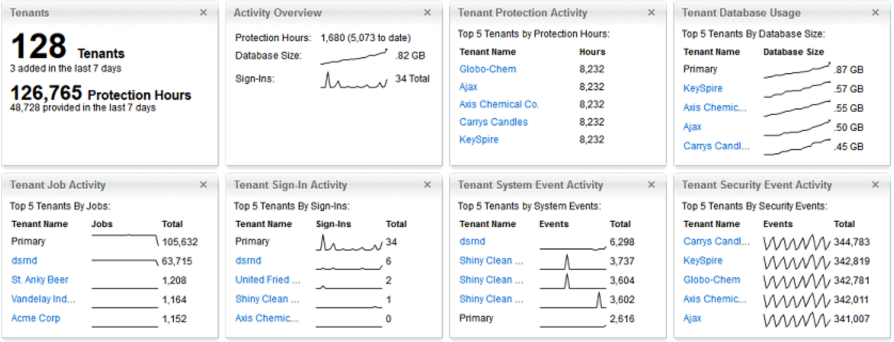
Multi-Tenant Dashboard/Reporting

When Multi-Tenancy is enabled, Primary Tenant Users have access to additional Dashboard widgets for monitoring Tenant activity:



- ☐ Monitoring
  - ☐ Activity Overview
  - ☐ Alert History [2x1]
  - ☐ Alert Status
  - ☐ Computer Status
  - ☐ Manager Node Status [3x1]
  - ☑ Tenant Database Usage
  - ☑ Tenant Job Activity
  - ☑ Tenant Protection Activity
  - ☑ Tenant Security Event Activity
  - ☑ Tenant Sign-In Activity
  - ☑ Tenant System Event Activity
  - ☑ Tenants
- ☐ System

Some examples of Tenant-related widgets:



Tenants

128 Tenants
3 added in the last 7 days

126,765 Protection Hours
48,728 provided in the last 7 days

Activity Overview

Protection Hours: 1,680 (5,073 to date)
Database Size: .82 GB
Sign-Ins: 34 Total

Tenant Protection Activity

Top 5 Tenants by Protection Hours:

Tenant Name	Hours
Globo-Chem	8,232
Ajax	8,232
Axis Chemical Co.	8,232
Carrys Candles	8,232
KeySpire	8,232

Tenant Database Usage

Top 5 Tenants By Database Size:

Tenant Name	Database Size
Primary	.87 GB
KeySpire	.57 GB
Axis Chemic...	.55 GB
Ajax	.50 GB
Carrys Candl...	.45 GB

Tenant Job Activity

Top 5 Tenants By Jobs:

Tenant Name	Jobs	Total
Primary		105,632
dsrnd		63,715
St. Anky Beer		1,208
Vandelay Ind...		1,164
Acme Corp		1,152

Tenant Sign-In Activity

Top 5 Tenants By Sign-Ins:

Tenant Name	Sign-Ins	Total
Primary		34
dsrnd		6
United Fried ...		2
Shiny Clean ...		1
Axis Chemic...		0

Tenant System Event Activity

Top 5 Tenants by System Events:

Tenant Name	Events	Total
dsrnd		6,298
Shiny Clean ...		3,737
Shiny Clean ...		3,604
Shiny Clean ...		3,602
Primary		2,616

Tenant Security Event Activity

Top 5 Tenants By Security Events:

Tenant Name	Events	Total
Carrys Candl...		344,783
KeySpire		342,819
Globo-Chem		342,781
Axis Chemic...		342,011
Ajax		341,007

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

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

More information is available in the **Chargeback** report (in the **Events & Reports** section). This report details protection hours, the current database sizes, and the number of computers (activated and non-activated) for each Tenant.

Multi-Tenancy (Advanced)

Configuring Database User Accounts

Note:

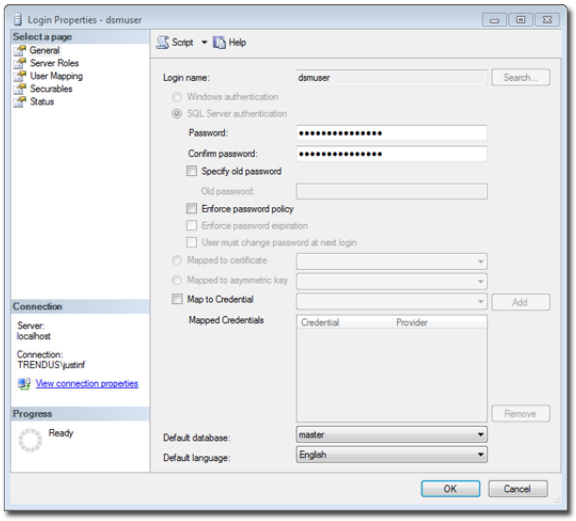
SQL Server and Oracle use different terms for database concepts described below.

	SQL Server	***Oracle***
Process where multiple Tenants execute	*Database Server*	*Database*
One Tenant's set of data	*Database*	*Tablespace/User*

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

SQL Server

Since Multi-Tenancy requires the ability for the software to create databases, the **dbcreator** role is required on SQL Server. For example:



Login name: dsmuser

○ Windows authentication

● SQL Server authentication

Password: •••••••••••••••

Confirm password: •••••••••••••••

□ Specify old password

Old password:

□ Enforce password policy

□ Enforce password expiration

□ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential

Mapped Credentials

Default database: master

Default language: English

Connection

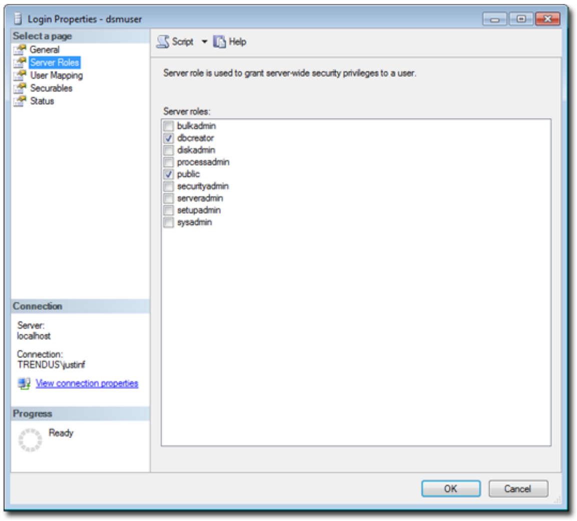
Server: localhost

Connection: TRENDUS\justinf

Progress

Ready

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



Server role is used to grant server-wide security privileges to a user.

Server roles:

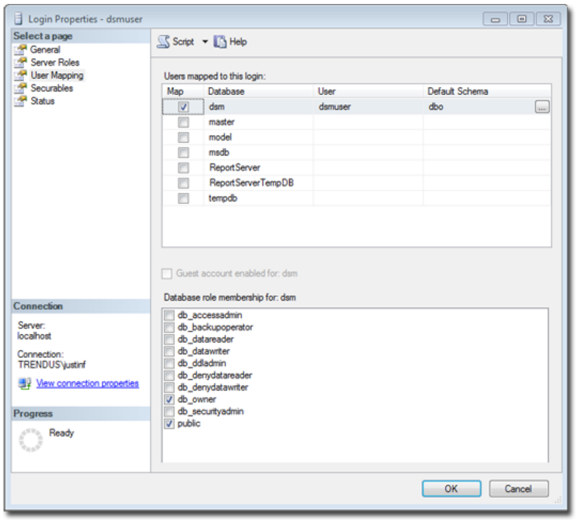
- □ bulkadmin
- ☑ dbcreator
- □ diskadmin
- □ processadmin
- ☑ public
- □ securityadmin
- □ serveradmin
- □ setupadmin
- □ sysadmin

Server:
localhost

Connection:
TRENDUS\justinf

Ready

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



Users mapped to this login:

Map	Database	User	Default Schema
☑	dsm	dsmuser	dbo
□	master		
□	model		
□	msdb		
□	ReportServer		
□	ReportServerTempDB		
□	tempdb		

□ Guest account enabled for: dsm

Database role membership for: dsm

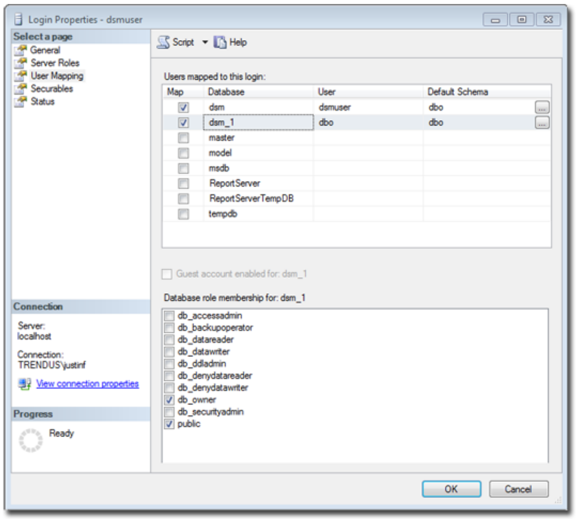
- □ db_accessadmin
- □ db_backupoperator
- □ db_datareader
- □ db_datawriter
- □ db_ddladmin
- □ db_denydatareader
- □ db_denydatawriter
- ☑ db_owner
- □ db_securityadmin
- ☑ public

Server:
localhost

Connection:
TRENDUS\justinf

Ready

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



Login Properties - dsmuser

Users mapped to this login:

Map	Database	User	Default Schema
☑	dsm	dsmuser	dbo
☑	dsm_1	dbo	dbo
□	master		
□	model		
□	msdb		
□	ReportServer		
□	ReportServerTempDB		
□	tempdb		

□ Guest account enabled for: dsm_1

Database role membership for: dsm_1

□ db_accessadmin
□ db_backupoperator
□ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter
☑ db_owner
□ db_securityadmin
☑ public

Connection

Server:
localhost

Connection:
TRENDUS\justinf

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

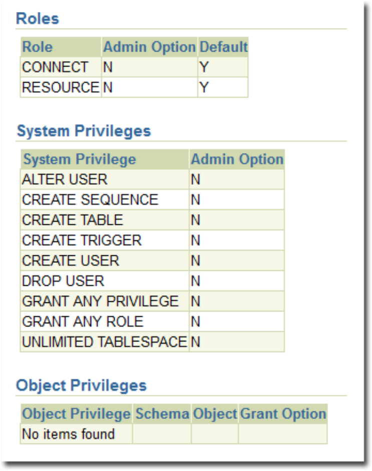
Oracle

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

Note: *Although Oracle allows special characters in database object names if they are surrounded by quotes, Deep Security does not support special characters in database object names. This page on Oracle's web site describes the allowed characters in non-quoted names: http://docs.oracle.com/cd/E14072_01/server.112/e10592/sql_elements008.htm#i27570*

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

If Multi-Tenancy is enabled, the following Oracle permissions must be assigned:



Roles

Role	Admin Option	Default
CONNECT	N	Y
RESOURCE	N	Y

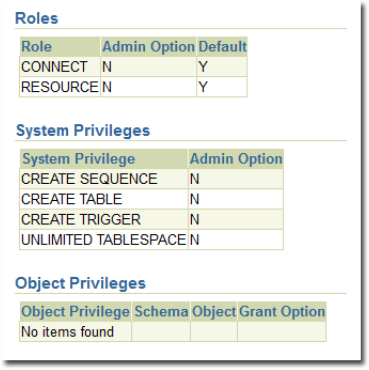
System Privileges

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

Object Privileges

Object Privilege	Schema	Object	Grant Option
No items found			

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



Roles

Role	Admin Option	Default
CONNECT	N	Y
RESOURCE	N	Y

System Privileges

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

Object Privileges

Object Privilege	Schema	Object	Grant Option
No items found			

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

APIs

Deep Security Manager includes a number of REST APIs for:

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

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

For additional information on the REST APIs please see the REST API documentation.

Upgrade

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

The primary Tenant is upgraded first, followed by the Tenants in parallel (5 at a time). Once the installer finishes, the same installer package should be executed on the rest of the Manager nodes.

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

Supporting Tenants

In certain cases, a Primary Tenant may require access to a Tenant's user interface. The Tenants list and Tenant properties pages provide an option to "Authenticate As" a given Tenant, granting them immediate read-only access.

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

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

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

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

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

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

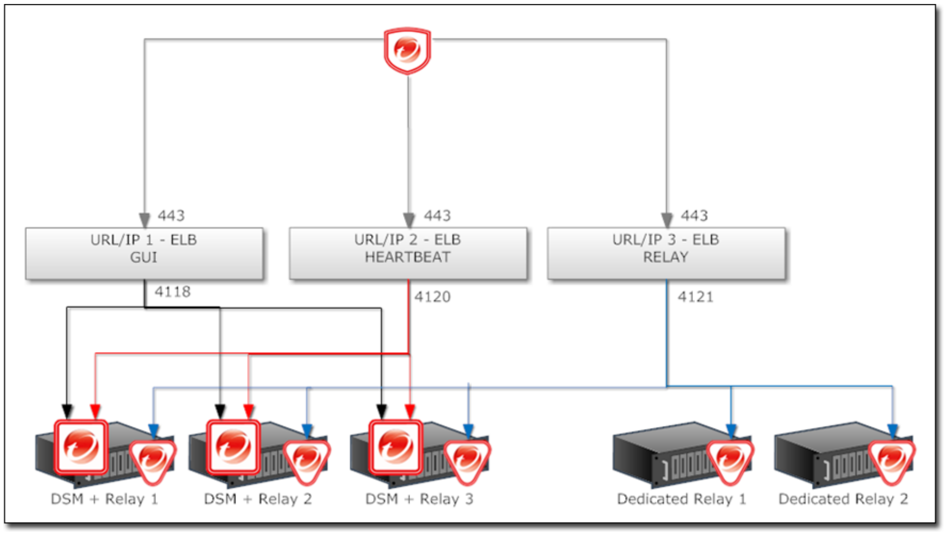
to direct the setting change or other command line action at a specific Tenant. If omitted, the action is on the primary Tenant.

Load Balancers

By default, multi-node Manager provides the address of all Manager nodes to all agents and virtual appliances. The agents and virtual appliances use the list of addresses to randomly select a node to contact and continue to try the rest of the list until no nodes can be reached (or are all busy). If it can't reach any nodes, it waits until the next heartbeat and tries again. This works very well in environments where the number of Manager nodes is fixed and avoids having to configure a load balancer in front of the Manager nodes for availability and scalability.

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

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



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

Multi-Tenant with Deep Security Virtual Appliance

If Deep Security is being deployed in a VMware environment, it is possible to configure the vCenter and vShield connector in the Primary Tenant and the vCloud connector in Tenants. If this is configured properly, the Primary Tenant sees the ESXi servers, Deep Security Virtual Appliances and other infrastructure components while Tenants only see the VMs that belong to them in the vCloud environment. They can further activate these VMs without deploying any agent technology.

To enable this type of environment, you must go to **Administration** > **System Settings** > **Agents** and select the **Allow Appliance protection of vCloud VMs** checkbox.

For more information on vCloud integration, see the Installation Guide.

Technical Details

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

Tenant creation takes between 30 seconds and four minutes due to the creation of the schema and the population of the initial data. This ensures each new Tenant has the most up to date configuration and removes the burden of managing database templates, especially between multiple database servers.

Protecting a Mobile Laptop

The following describes the steps involved in using Deep Security to protect a mobile laptop. It will involve the following steps:

1. Adding Computers to the Manager
    1. Adding individual computers
    2. Performing a Discovery Operation on your network
    3. Importing computers from a Microsoft Active Directory
2. Create a new Policy for a Windows laptop
    1. Creating and naming the new Policy
    2. Setting which interfaces to monitor
    3. Setting the network engine to Inline Mode
    4. Assigning Firewall Rules (including some with Location Awareness) and enabling Firewall Stateful Configuration
    5. Assigning Intrusion Prevention Rules
    6. Assigning Log Inspection Rules
    7. Assigning Integrity Monitoring Rules
3. Applying the Policy to the computer
4. Monitoring Activity using the Manager

We will assume that you have already installed the Manager on the computer from which you intend to manage the Deep Security Agents throughout your network. We will also assume that **you have installed (but not activated) Deep Security Agents on the mobile laptops you wish to protect**. If you have not done so, consult the installation instructions for the steps to get to this stage.

Adding computers to the Manager

You can add computers to the Deep Security **Computers** page by:

1. Adding computers individually by specifying their IP addresses or hostnames
2. Discovering computers by scanning the network
3. Connecting to a Microsoft Active Directory and importing a list of computers
4. Connecting to a VMware vCenter and importing a list of computers (not covered in this section because we are dealing with mobile laptops.)

Adding computers individually by specifying their IP addresses or hostnames

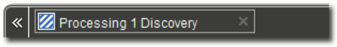
To add an individual computer by specifying its IP address or hostname, go to the **Computers** page and click **New** in the toolbar.

Type the hostname or IP address of the new computer in the **Hostname** text box. The **New Computer** wizard also lets you specify a Policy which it will apply to the new computer if it finds the computer and determines that an unactivated Agent is present. (For now, don't select a Policy.) When you click **Next**, the wizard will find the computer and activate the Agent. When Agent activation has completed, the wizard will give you the option of opening the **Computer Editor** window (the Details window) which lets you configure many the Agent's settings. Skip the **Details** window for now.

Adding computers by scanning the network (Discovery)

To discover computers by scanning the network:

1. Go to the **Computers** page.
2. Click **Discover...** in the toolbar to display the **Discover Computers** dialog.
3. Type a range of IP addresses you want to scan for computers. If you wish, you can enter a masked IP address to do the same thing.
4. Select **Automatically resolve IPs to hostnames** to instruct the Manager to automatically resolve hostnames as it performs the discovery.
5. You have the option to add discovered computers to a computer group you have created. For now, leave the **Add Discovered Computers to Group** drop-down list choice set to "Computers".
6. Finally, clear the **Automatically perform a port scan of discovered computers** checkbox. (Port scanning detects which ports are open on the discovered computers.)
7. Click **OK**. The dialog box will disappear and "Discovery in progress..." will appear in the Manager's status bar at the bottom of your browser. (The discovery process can be cancelled by clicking the "X".)

   Processing 1 Discovery

   In a few minutes, all visible computers on the network will have been detected and the Manager will have identified those with Deep Security Agents installed. These Agents now need to be activated.

8. Activate the Agents by right-clicking an Agent (or multiple selected Agents), and select "Activate/Reactivate" from the shortcut menu. Once the Agents are activated, their status light will turn green and "Managed (Online)" will appear in the status column.

Importing Computers from a Microsoft Active Directory

Computers imported from an Active Directory are treated the same as any other computers in the **Computers** page.

To import computers from a Microsoft Active Directory:

1. Click the down arrow next to "New" in the **Computers** page toolbar and select **Add Directory....** to start the **Add Directory** wizard.

   Note: *Synchronization of computers from other LDAP-based directories may be possible but would require some customization. For assistance contact your support provider.*

2. Type the Active Directory server name, a name and description for your imported directory as it will appear in the Manager (it doesn't have to match that of the Active Directory), the IP and port of the Active Directory server, and finally your access method and credentials. Click **Next**.

   Note: *You must include your domain name with your username in the **User Name** field.*

3. If you select SSL or TLS as the Access method, the wizard will ask you to accept a security certificate. You can view the certificate accepted by the Deep Security Manager by going to **Administration > System Settings > Security** and clicking "View Certificate List..." in the Trusted Certificates area. Click **Next**.
4. The second page of the **New Directory** wizard asks for schema details. (Leave the default values). Click **Finish**.
5. The next page will tell you if there were any errors. Click **Next**.
6. The final page will let you create a Scheduled Task to regularly synchronize the Manager's **Computers** page with the Active Directory. Leave option this cleared for now. Click **Close**.

The directory structure now appears under **Computers** in the navigation panel.

Additional Active Directory Options

Right-clicking an Active Directory structure gives you the following options that are not available for ordinary computer groups listed under **Computers**.

1. Remove Directory
2. Synchronize Now

Remove Directory

When you remove a directory from the Deep Security Manager, you have the following options:

- **Remove directory and all subordinate computers/groups from DSM:** removes all traces of the directory.
- **Remove directory, but retain computer data and computer group hierarchy:** turns the imported directory structure into identically organized regular computer groups, no longer linked with the Active Directory server.
- **Remove directory, retain computer data, but flatten hierarchy:** removes links to the Active Directory server, discards directory structure, and places all the computers into the same computer group.

Synchronize Now

Synchronizes the directory structure in the Deep Security Manager with the Active Directory Server. (Remember that you can automate this procedure as a **Scheduled Task**.)

Now that the Agents are active, they can be assigned Firewall Rules and Intrusion Prevention Rules. Although all the individual security objects can be assigned individually to an Agent, it is convenient to group common security objects into a Policy and then assign the Policy to one or more Agents.

Note: *More information is available for each page in the Deep Security Manager by clicking the **Help** button in the menu bar.*

Activating the Agents on Computers

Agents need to be "activated" by the Manager before Policies and rules can be assigned to them. The activation process includes the exchange of unique fingerprints between the Agent and the Manager. This ensures that only this Deep Security Manager (or one of its nodes) can send instructions to the Agent.

Note: *An Agent can be configured to automatically initiate its own activation upon installation. For details, see **Command-Line Utilities (page 167)**.*

To manually activate an Agent on a computer, right-click one or more selected computers and select **Actions > Activate/Reactivate**.

Create a Policy for a Windows laptop

Now that the Agents are activated, it's time to assign some rules to protect the computer. Although you can assign rules directly to a computer, it's more useful to create a Policy which contains these rules and which can then be assigned to multiple computers.

Creating the Policy will involve the following steps:

1. Creating and naming the new Policy
2. Setting which interfaces to monitor
3. Setting the network engine to Inline Mode
4. Assigning Firewall Rules (including some with location awareness) and enable Stateful Inspection
5. Assigning Intrusion Prevention Rules
6. Assigning Integrity Monitoring Rules
7. Assigning Log Inspection Rules

8. Assigning the Policy to the computer

Creating and naming the New Policy

To create and name the new Policy:

1. Go to the **Policies** section, click on Policies in the navigation panel on the left to go to the **Policies** page.
2. Click **New** in the toolbar to display the **New Policy** wizard.
3. Name the new Policy "My New Laptop Policy" and select **Base Policy** from the **Inherit from:** menu. Click **Next.**
4. The next page asks if you would like to base the Policy on an existing computer's current configuration. If you were to select **Yes**, you would be asked to pick an existing managed computer and the wizard would take all the configuration information from that computer and create a new Policy based on it. This can be useful if, for instance, you have fine-tuned the security configuration of an existing computer over a period of time and now wish to create a Policy based on it so that you can apply it to other functionally identical computers. For now, select **No** and click **Next**.
5. The last page confirms that the new Policy has been created. Select the **Open Policy Details on 'Close'** option and click **Close**.

Setting which interfaces to monitor

To set which interfaces to monitor:

1. Because you set the **Open Policy Details on 'Close'** option, the new Policy editor window is displayed.
2. The laptops to which this Policy will be assigned are equipped with two network interfaces (a local area connection and a wireless connection) and we intend to tune the security configuration to take into account which interface is being used. Click **Interface Types** in the navigation panel and select the **Rules can apply to specific interfaces** option. Enter names for the interfaces and strings (with optional wildcards) which the Agent will use to match to interface names on the computer: "LAN Connection" and "Local Area Connection *", and "Wireless" and "Wireless Network Connection *" in the first two Interface Type areas. Click **Save** at the bottom right of the page.

Setting the network engine to Inline Mode

The Agent's network engine can operate Inline or in Tap Mode. When operating Inline, the live packet stream passes through the network engine. Stateful tables are maintained, Firewall Rules are applied and traffic normalization is carried out so that Intrusion Prevention Rules can be applied to payload content. When operating in Tap Mode, the live packet stream is cloned and diverted from the main stream. In Tap Mode, the live packet stream is not modified; all operations are carried out on the cloned stream.

For now, we will configure our Policy to direct the engine to operate Inline.

To set the network engine to Inline Mode:

1. Still in the My New Laptop Policy editor, go to **Settings** and click on the **Network Engine** tab.
2. Set the Network Engine Mode to **Inline**. By default, the setting should already be set to "Inherited (Inline)" since the **Base** policy default mode is **Inline** and your new Policy inherits its settings from there.

Assigning Firewall Rules (including some with location awareness) and turn on Stateful Inspection

To assign Firewall Rules:

1. Click **Firewall** in the navigation panel and in the **Firewall** area of the **General** tab, select **On** from the **Firewall State** drop-down menu.

> Note: *Selecting "Inherit" will cause this setting on this Policy to be inherited from its parent Policy. This setting in the parent Policy may already be "On" but for now you will enforce the setting at the level of this Policy regardless of any parent Policy settings. For information on Inheritance, see **Policies, Inheritance and Overrides (page 257)**.*

2. Now we will assign some Firewall Rules and Firewall Stateful Configuration rules to this Policy. Click **Firewall Rules** to display the list of available predefined Firewall Rules. (You can create your own Firewall Rules, but for this exercise we will select from the list of existing ones.) Select the following set of Firewall Rules to allow basic communication:
   - Allow Solicited ICMP replies
   - Allow solicited TCP/UDP replies
   - Domain Client (UDP)
   - ARP
   - Wireless Authentication
   - Windows File Sharing (This is a force-allow rule to permit incoming Windows File Sharing traffic.)

   Notice the gray down-arrow next to the Firewall Rule checkboxes. These appear if you have defined multiple interfaces in the previous step. They allow you to specify whether the Firewall Rule will apply to all interfaces on the computer or just to interfaces that you specify. Leave these at the default setting for now. Click the **Save** button.

We assigned a Firewall Rule that permitted Windows File Sharing. Windows File Sharing is a very useful feature in Windows but it has had some security issues. It would better to restrict this ability to when the laptop is in a secure office environment and forbid it when the laptop is out of the office. We will apply Location Awareness to the Firewall Rule when used with this Policy to implement this policy.

To implement location awareness:

1. In the **My New Laptop Policy** Policy editor, go to **Firewall > General > Assigned Firewall Rules**, right-click the Windows File Sharing Firewall Rule and select **Properties...**. This will display the **Properties** window for the Firewall Rule (but the changes we make to it will only apply to the Firewall Rule when it is applied as part this new Policy).
2. In the **Properties** window, click the **Options** tab.
3. In the **Rule Context** area, select **New...** from the drop-down list. This displays the **New Context** Properties window. We will create a Rule Context that will only allow the Firewall Rule to be active when the laptop has local access to its Domain Controller. (That is, when the laptop is in the office.)
4. Name the new Rule Context "In the Office". In the **Options** area, set the **Perform check for Domain Controller connectivity** option and select **Local** below it. Then click **Ok**.
5. Click **OK** in the Windows File Sharing Firewall Rule **Properties** window.

Now the Windows File Sharing Firewall Rule will only be in effect when the laptop has local access to its Windows Domain Controller. The Windows File Sharing Firewall Rule is now displayed in bold letters in the Policy **Details** window. This indicates that the Firewall Rule has had its properties edited for this Policy only.

> Note: *Location Awareness is also available for Intrusion Prevention Rules.*

The final step in the Firewall section is to enable Stateful inspection.

To enable Stateful Inspection:

1. Still in the **My New Laptop Policy** Policy editor window, go to **Firewall > General > Firewall Stateful Configurations**.
2. For the **Global (All Interfaces)** setting, select **Enable Stateful Inspection**.
3. Click **Save** to finish.

Assigning Intrusion Prevention Rules

To assign Intrusion Prevention rules to the Policy:

1. Still in the **My New Laptop Policy** editor window, click **Intrusion Prevention** in the navigation panel.
2. On the General tab, in the **Intrusion Prevention** area, set the **Intrusion Prevention State** to **On**.

Note: *Intrusion Prevention can be set to either Prevent or Detect mode when the Network Engine is operating Inline (as opposed to Tap Mode). Detect mode is useful if you are trying out a new set of Intrusion Prevention Rules and do not want to risk dropping traffic before you are sure the new rules are working properly. In Detect Mode, traffic that would normally be dropped will generate events but will be allowed to pass. Set Intrusion Prevention to "On".*

Note: *Note the* ***Recommendations*** *area. The Deep Security Agent can be instructed to run a Recommendation Scan. (On the Manager's* ***Computers*** *page, right-click a computer and select* ***Actions > Scan for Recommendations.****) The Recommendation engine will scan the computer for applications and make Intrusion Prevention Rule recommendations based on what it finds. The results of the Recommendation Scan can be viewed in the computer editor window by going to* ***Intrusion Prevention > Intrusion Prevention Rules > Assign/Unassign...*** *and selecting* ***Recommended for Assignment*** *from the second drop-down filter menu.*

3. For now, leave the **Recommendations** > **Automatically implement Intrusion Prevention Recommendations (when possible):** option set to **Inherited (No)**.
4. In the Assigned Intrusion Prevention rules area, click **Assign/Unassign...** to open the rule assignment window.
5. Intrusion Prevention Rules are organized by Application Type. Application Types are a useful way of grouping Intrusion Prevention Rules; they have only three properties: communication direction, protocol, and ports. For our new laptop Policy, assign the following Application Types:
   - Mail Client Outlook
   - Mail Client Windows
   - Malware
   - Malware Web
   - Microsoft Office
   - Web Client Common
   - Web Client Internet Explorer
   - Web Client Mozilla Firefox
   - Windows Services RPC Client
   - Windows Services RPC Server

Note: *Make sure the first two drop-down filter menus are showing* ***All*** *and that the third sorting filter menu is sorting* ***By Application Type****. It's easier to page through the Application Types if you right-click in the Rules list and select* ***Collapse All****. There are many Application Types (and Intrusion Prevention Rules), so you will have to have to use the pagination controls at the bottom right of the page to find them all, or use the search feature at the top right of the page. Select an Application Type by putting a check next to the Application Type name.*

Note: *Some Intrusion Prevention Rules are dependent on others. If you assign a rule that requires another rule to also be assigned (which has not yet been assigned) a popup window will appear letting you assign the required rule.*

Note: *When assigning any kinds of Rules to a computer, do not let yourself be tempted to be "extra secure" and assign all available rules to your computer. The Rules are designed for a variety of operating systems, applications, vulnerabilities and may not be applicable to your computer. The traffic filtering engine would just be wasting CPU time looking for patterns that will never appear. Be selective when securing your computers!*

6. Click **OK** and then **Save** to assign the Application Types to the Policy.

Assigning Integrity Monitoring Rules

To assign Integrity Monitoring Rules to the Policy:

1. Still in the **My New Laptop Policy** editor window, click **Integrity Monitoring** in the navigation panel.
2. On the **General** tab, set **Integrity Monitoring State** to **On**.
3. Set **Automatically implement Integrity Monitoring Recommendations (when possible):** to **No**.
4. Now click **Assign/Unassign...** in the **Assigned Integrity Monitoring Rules** area.
5. In the Search box at the top right of the page type the word "Windows" and press Enter. All the rules that apply to Microsoft Windows will be displayed in the rules list. Right-click one of the rules and choose "Select All", then right-click again and choose "Assign Rule(s)". This will assign all the rules that came up in the search result to the Policy.

Assigning Log Inspection Rules

To assign Log Inspection Rules to the Policy:

1. Still in the **My New Laptop Policy** editor window, click **Log Inspection** in the navigation panel.
2. Deselect **Inherit** and set Log Inspection to **On**.
3. Set **Automatically implement Log Inspection Rule Recommendations (when possible):** to **No**.
4. Now click **Assign/Unassign...** in the **Assigned Log Inspection Rules** area.
5. Select the "1002792 - Default Rules Configuration" Rule (required for all other Log Inspection Rules to work), and the "1002795 - Microsoft Windows Events" rule. (This will log events any time Windows auditing functionality registers an event on the laptop.)
6. Click **Ok** and then **Save** to apply the rules to the Policy.

We are now finished editing the new Policy. You can now close the My New Policy **Details** window.

Edit the Domain Controller(s) IP List

Finally, since the new Policy includes three Firewall Rules that use the "Domain Controller(s)" IP List, we will have to edit that IP List to include the IP addresses of the local Windows Domain Controller.

To edit the Domain Controllers IP list:

1. In the main window of the Deep Security Manager console, go to the **Policies > Common Objects > IP Lists**.
2. Double-click the **Domain Controller(s)** IP List to display its **Properties** window.
3. Type the IP(s) of your domain controller(s).
4. Click **OK**.

Apply the Policy to a Computer

Now we can apply the Policy to the computer.

To apply the Policy to the computer:

1. Go to the **Computers** page.
2. Right-click the computer to which you will assign the Policy and select **Actions > Assign Policy...**.
3. Choose "My New Laptop Policy" from the drop-down list in the **Assign Policy** dialog box.
4. click **OK**

After clicking **OK**, the Manager will send the Policy to the Agent. The computer **Status** column and the Manager's status bar will display messages that the Agent is being updated.

Once the Agent on the computer has been updated, the **Status** column will read "Managed (Online)".

Configure SMTP Settings

Configuring the Deep Security Manager's SMTP settings allows email Alerts to be sent out to Users.

To configure SMTP settings:

1. Go to **Administration > System Settings** and click the **SMTP** tab.
2. Type the configuration information and click the **Test SMTP Settings** to confirm Deep Security Manager can communicate with the mail server.
3. Go to the **Alerts** tab.
4. In the **Alert Event Forwarding (From the Manager)** section, type the default email address to which you want notifications sent.
5. Click **Save**.

Note: *Whether a User gets emailed Alerts can be configured on that User's **Properties** window (**Administration > User Management > Users**). Whether a particular Alert generates emailed notifications can be configured on that Alert's **Properties** window.*

Monitor Activity Using the Deep Security Manager

The Dashboard

After the computer has been assigned a Policy and has been running for a while, you will want to review the activity on that computer. The first place to go to review activity is the Dashboard. The Dashboard has many information panels ("widgets") that display different types of information pertaining to the state of the Deep Security Manager and the computers that it is managing.

At the top right of the Dashboard page, click **Add/Remove Widgets** to view the list of widgets available for display.

For now, we will add the following widgets from the **Firewall** section:

- Firewall Computer Activity (Prevented)
- Firewall Event History [2x1]
- Firewall IP Activity (Prevented)

Select the checkbox beside each of the three widgets, and click **OK**. The widgets will appear on the dashboard. (It may take a bit of time to generate the data.)

- The **Firewall Computer Activity (Prevented)** widget displays a list of the most common reasons for packets to be denied (that is, blocked from reaching a computer by the Agent on that computer) along with the number of packets that were denied. Items in this list will be either types of Packet Rejections or Firewall Rules. Each "reason" is a link to the corresponding logs for that denied packet.
- The **Firewall Event History [2x1]** widget displays a bar graph indicating how many packets were blocked in the last 24 hour period or seven day period (depending on the view selected). Clicking a bar will display the corresponding logs for the period represented by the bar.
- The **Firewall IP Activity (Prevented)** widget displays a list of the most common source IPs of denied packets. Similar to the **Firewall Activity (Prevented)** widget, each source IP is a link to the corresponding logs.

Note: *Note the trend indicators next to the numeric values in the **Firewall Computer Activity (Prevented)** and **Firewall IP Activity (Prevented)** widgets. An upward or downward pointing triangle indicates an overall increase or decrease over the specified time period, and a flat line indicates no significant change.*

Logs of Firewall and Intrusion Prevention Events

Now drill-down to the logs corresponding to the top reason for Denied Packets: in the **Firewall Activity (Prevented) widget**, click the first reason for denied packets (in the picture above, the top reason is "Out of Allowed Policy"). This will take you to the **Firewall Events** page.

The **Firewall Events** page will display all Firewall Events where the **Reason** column entry corresponds to the first reason from the **Firewall Activity (Prevented) widget** ("Out of Allowed Policy"). The logs are filtered to display only those events that occurred during the view period of the Dashboard (Last 24 hours or last seven days). Further information about the **Firewall Events** and **Intrusion Prevention Events** page can be found in the help pages for those pages.

Note: *For the meaning of the different packet rejection reasons, see **Firewall Events (page 211)** and **Intrusion Prevention Events (page 209)**.*

Reports

Often, a higher-level view of the log data is desired, where the information is summarized, and presented in a more easily understood format. The **Reports** fill this Role, allowing you to display detailed summaries on computers, Firewall and Intrusion Prevention Event Logs, Events, Alerts, etc. In the **Reports** page, you can select various options for the report to be generated.

We will generate a **Firewall Report**, which displays a record of Firewall Rule and Firewall Stateful Configuration activity over a configurable date range. Select **Firewall Report** from the Report drop-down. Click **Generate** to launch the report in a new window.

By reviewing scheduled reports that have been emailed by the Deep Security Manager to Users, by logging into the system and consulting the dashboard, by performing detailed investigations by drilling-down to specific logs, and by configuring Alerts to notify Users of critical events, you can remain apprised of the health and status of your network.

See also:

- ***Policies, Inheritance and Overrides (page 257)***

Reference

Advanced Logging Policy Modes

To reduce the number of events being logged, the Deep Security Manager can be configured to operate in one of several **Advanced Logging Policy** modes. These modes are set in the Policy and Computer Editors on the **Settings > Network Engine > Advanced Network Engine Settings** area.

The following table lists the types of Events are ignored in four of the more complex Advanced Logging Policy modes:

Mode	Ignored Events
Stateful and Normalization Suppression	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Unsolicited UDP Unsolicited ICMP Out Of Allowed Policy Dropped Retransmit
Stateful, Normalization, and Frag Suppression	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Unsolicited UDP Unsolicited ICMP Out Of Allowed Policy CE Flags Invalid IP Invalid IP Datagram Length Fragmented Invalid Fragment Offset First Fragment Too Small Fragment Out Of Bounds Fragment Offset Too Small IPv6 Packet Max Incoming Connections Max Outgoing Connections Max SYN Sent License Expired IP Version Unknown Invalid Packet Info Maximum ACK Retransmit Packet on Closed Connection Dropped Retransmit
Stateful, Frag, and Verifier Suppression	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Unsolicited UDP Unsolicited ICMP Out Of Allowed Policy CE Flags Invalid IP Invalid IP Datagram Length Fragmented Invalid Fragment Offset First Fragment Too Small Fragment Out Of Bounds Fragment Offset Too Small IPv6 Packet

Mode	Ignored Events
	Max Incoming Connections Max Outgoing Connections Max SYN Sent License Expired IP Version Unknown Invalid Packet Info Invalid Data Offset No IP Header Unreadable Ethernet Header Undefined Same Source and Destination IP Invalid TCP Header Length Unreadable Protocol Header Unreadable IPv4 Header Unknown IP Version Maximum ACK Retransmit Packet on Closed Connection Dropped Retransmit
Tap Mode	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Maximum ACK Retransmit Packet on Closed Connection Dropped Retransmit

Command-Line Utilities

Deep Security Agent (also applies to the Agents in 9.0 and earlier Deep Security Relays)

dsa_control

Usage

dsa_control [-a <str>] [-b] [-c <str>] [-d] [-g <str>] [-s <num>] [-m] [-p <str>] [-r] [-R <str>] [-t <num>] [--buildBaseline] [--scanForChanges] [Additional keyword:value data to send to Manager during activation/heartbeat...]

- **-a <str>, --activate=<str>** Activate agent with Manager at specified URL. URL format must be 'dsm://hostOrIp:port/' where port is the Manager's heartbeat port (default 4120).
- **-b, --bundle** Create update bundle.
- **-c <str>, --cert=<str>** Identify the certificate file.
- **-d, --diag** Generate an agent diagnostic package.
- **-g <str>, --agent=<str>** Agent URL. Defaults to 'https://localhost:4118/'
- **-m, --heartbeat** Ask the Agent to contact the Manager now.
- **-p <str>, --passwd=<str>** Authentication password.
- **-r, --reset** Reset agent configuration.
- **-R <str>, --restore=<str>** Restore quarantined file.
- **-s <num>, --selfprotect=<num>** enable self-protection on the Agent by preventing local end-users from uninstalling, stopping, or otherwise controlling the Agent. Command-line instructions must include the authentication password when self-protection is enabled. (1: enable, 0: disable)

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

- **-t <num>, --retries=<num>** If dsa_control cannot contact the Deep Security Agent service to carry out accompanying instructions, this parameter instructs dsa_control to retry <num> number of times. There is a one second pause between retries.
- **--buildBaseline** Build baseline for Integrity Monitoring
- **--scanForChanges** Scan for changes for Integrity Monitoring

Agent-Initiated Activation ("dsa_control -a")

An Agent installed on a computer needs to be activated before the Manager can assign Rules and Policies to protect the computer. The activation process includes the exchange of unique fingerprints between the Agent and the Manager. This ensures that only one Deep Security Manager (or one of its Manager Nodes) can send instructions to and communicate with the Agent.

You can manually activate an Agent from the Deep Security Manager by right-clicking on the computer in the Computers screen and selecting **Actions > Activate/Reactivate**.

Deep Security Agents can initiate the activation process using a locally-run command-line tool. This is useful when a large number of computers will be added to a Deep Security installation and you want to write a script to automate the activation process.

*Note: For Agent-Initiated Activation to work, the **Allow Agent-Initiated Activation** option must be enabled on the **Administration > System Settings > Agents** tab.*

The minimum activation instruction contains the activation command and the Manager's URL (including the port number):

```
dsa_control -a dsm://[managerurl]:[port]/
```

where:

- **-a** is the command to activate the Agent , and
- **dsm://managerurl:4120/** is the parameter that points the Agent to the Deep Security Manager. ("managerurl" is the URL of the Deep Security Manager, and "4120" is the default Agent-to-Manager communication port.)

The Manager URL is the only required parameter for the activation command. Additional parameters are also available (see the table of available parameters below). They must be entered as key:value pairs (with a colon as a separator). There is no limit to the number of key:value pairs you can enter but the key:value pairs must be separated from each other by a space. For example:

```
dsa_control -a dsm://sec-op-john-doe-3:4120/ hostname:ABCwebserver12 "description:Long Description With Spaces"
```

(Quotation marks are only required if your value includes spaces or special characters.)

Agent-Initiated Activation Over a Private Network Via Proxy

Agents on a private network can perform agent-initiated communication with a Deep Security Manager through a proxy server. Use the following command-line options to instruct the Agent to communicate with the Deep Security Manager through a proxy server:

Syntax	**Notes**
`dsa_control -x "dsm_proxy://<proxyURL>/"`	Sets the address of the proxy server which the Agent uses to communicate with the Manager.
`dsa_control -x ""`	Clears the proxy server address.
`dsa_control -u "<username:password>"`	Sets the proxy username and password.
`dsa_control -u ""`	Clears the proxy username and password.
Examples	
`dsa_control.exe -x "dsm_proxy://172.21.3.184:808/"`	Proxy uses IPv4.
`dsa_control.exe -x "dsm_proxy://winsrv2k3-0:808/"`	Proxy uses hostname.
`dsa_control.exe -x "dsm_proxy://[fe80::340a:7671:64e7:14cc]:808/"`	Proxy uses IPv6.
`dsa_control.exe -u "root:Passw0rd!"`	Proxy authentication is "root" and password is "Passw0rd!" (basic authentication only, digest and NTLM are not supported).

When used in the context of Agent-initiated activation, the proxy commands must be issued first, followed by the Agent-initiated activation commands. The following example shows a complete sequence for setting a proxy address, setting proxy credentials, and activating the Agent:

```
dsa_control.exe -x "dsm_proxy://172.21.3.184:808/"
dsa_control.exe -u "root:Passw0rd!"
dsa_control -a "dsm://seg-dsm-1:4120/"
Required Setting in Deep Security Manager
```

The Deep Security Manager must be configured to allow the Agent to specify its own hostname. To enable the setting:

1. Go to **Administration > System Settings > Agents > Agent-Initiated Activation**
2. Select **Allow Agent-Initiated Activation**
3. Select **Allow Agent to specify hostname**.
4. Click **Save.**

To turn on Deep Security Agent debug tracing in Windows:

1. Create a file named `ds_agent.ini` under `%WINDOWS%`

2. In that file, add the line: `Trace=*`
3. Restart the `ds_agent` service.

Agent-Initiated Heartbeat ("dsa_control -m")

The Agent-Initiated heartbeat command will instruct the Agent to perform an immediate heartbeat operation to the Deep Security Manager. Although this may be useful on its own, like the activation command above, the heartbeat command can be used to pass along a further set of parameters to the Deep Security Manager.

The following table lists the parameters that are available to the activation and heartbeat commands. Note that some parameters can only be used with either the activation or heartbeat exclusively.

Key	**Description**	**Examples**	**Can be performed during Activation**	**Can be performed after activation during Heartbeat**	**Value Format**	**Notes**
description	Sets **description** value.	"description:Extra information about the host"	yes	yes	string	Maximum length 2000 characters.
displayname	Sets **displayname** value. (Shown in parentheses next to the hostname.)	"displayname:the_name"	yes	yes	string	Maximum length 2000 characters.
externalid	Sets the **externalid** value	"externalid:xyz123"	yes	yes	integer	This value can used to uniquely identify an Agent. The value can be accessed using the SOAP Web Service API.
group	Sets the computers page **Group** the computer belongs in.	"group:Zone A/Webservers"	yes	yes	string	Maximum length 254 characters per group name per hierarchy level. The forward slash ("/") indicates a group hierarchy. The **group** parameter can read or create a hierarchy of groups. This parameter can only be used to add computers to standard groups under the main "Computers" root branch. It cannot be used to add computers to groups belonging to Directories (MS Active Directory), VMware vCenters, or Cloud Provider accounts.
groupid		"groupid:33"	yes	yes	integer	
hostname		"hostname:ABWebServer1"	yes	no	string	Maximum length 254 characters. The hostname can specify an IP address, hostname or FQDN that is best used to contact the computer in the **Computers** list in Deep Security Manager.
policy		"policy:Policy Name"	yes	yes	string	Maximum length 254 characters. The Policy name is a case-insensitive match to the Policy list. If the Policy is not found, no Policy will be assigned. A policy assigned by an Event-based Task will override a Policy assigned during Agent-Initiated Activation.
policyid		"policyid:12"	yes	yes	integer	
relaygroup	Links the computer to a	"relaygroup:Custom Relay Group"	yes	yes	string	Maximum length 254 characters.

Key	Description	Examples	Can be performed during Activation	Can be performed after activation during Heartbeat	Value Format	Notes
	specific Relay Group.					The Relay Group name is a case-insensitive match to existing Relay Group names. If the Relay Group is not found the Default Relay Group will be used. This does not affect Relay Groups assigned during Event-based tasks. Use either this option or Event-based tasks, not both.
relaygroupid		"relaygroupid:123"	yes	yes	integer	
tenantID and **tenantPassword**		"tenantID:12651ADC-D4D5" and "tenantPassword:8601626D-56EE"	yes	yes	string	If using Agent-Initiated Activation as a Tenant, both **tenantID** and **tenantPassword** are required. The **tenantID** and **tenantPassword** can be obtained from the deployment script generation tool.
RecommendationScan	Initiate a Recommendation Scan on the computer.	"RecommendationScan:true"	no	yes	boolean	
RebuildBaseline	Rebuilds the Integrity Monitoring baseline on the computer.	"RebuildBaselline:true"	no	yes	boolean	

dsa_query

The dsa_query tool provides the following information :

- License-status of each component
- Scan progress
- Version information of Security Update components

Usage

dsa_query [-c <str>] [-p <str>] [-r <str]

- -p,--passwd <string>: authentication password. Required when agent self-protection is enabled.

> Note: *For some query-commands, authentication can be bypassed directly, in such case, password is not required.*

- -c,--cmd <string>: execute query-command against ds_agent. The following commands are supported:
    - "GetHostInfo": to query which identity is returned to the Deep Security during a heartbeat
    - "GetAgentStatus": to query which protection modules are enabled and other miscellaneous information
    - "GetComponentInfo": query version information of Anti-Malware patterns and engines
- -r,--raw <string>: returns the same query-command information as "-c" but in raw data format for third party software interpretation.

pattern: wildchar pattern to filter result, optional.

These keys are organized in nested namespace because the response from ds_agent are formed in XML-format. If users's key mapped to an leaf-node, we would return string-value directly. In other cases, we would return xml-formatted result, contains all information under that matched node.

Example:
dsa_query -c "GetComponentInfo" -r "au" "AM*"

Deep Security Manager

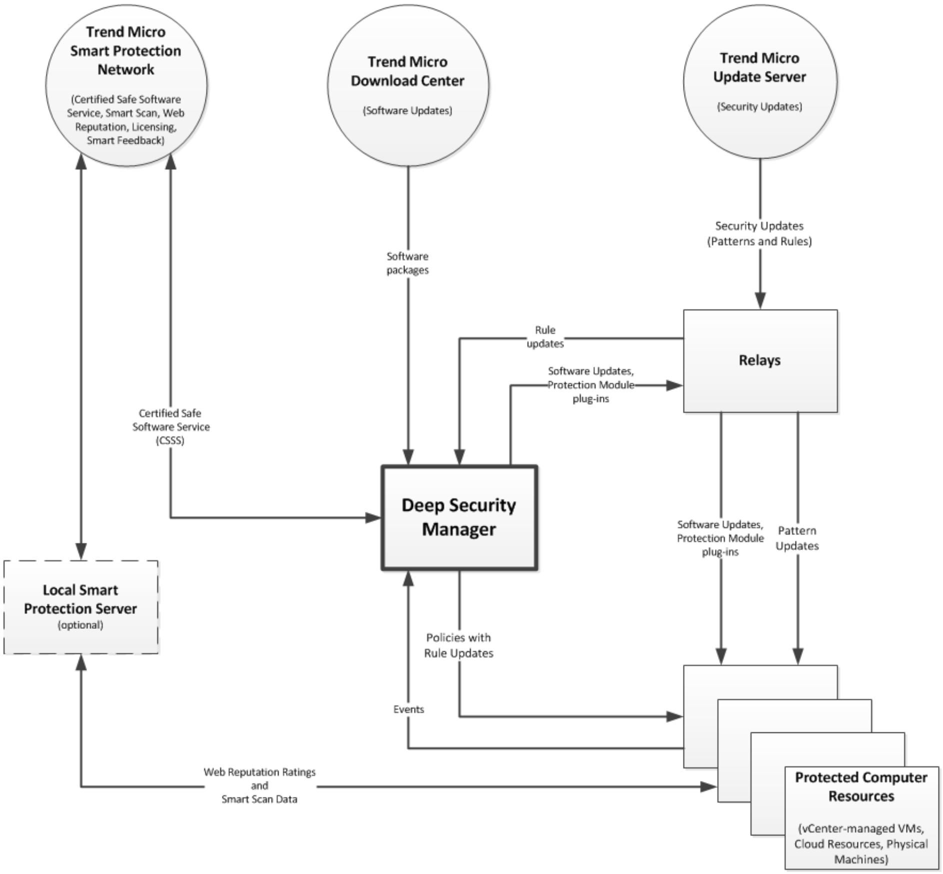
dsm_c

Usage

dsm_c -action actionname

Action Name	Description	Usage with Parameters (if any)
changesetting	Change a setting	dsm_c -action changesetting -name NAME -value VALUE [-computerid COMPUTERID] [-computername COMPUTERNAME] [-policyid POLICYID] [-policyname POLICYNAME] [-tenantname TENANTNAME]
viewsetting	View a setting value	dsm_c -action viewsetting -name NAME [-computerid COMPUTERID] [-computername COMPUTERNAME] [-policyid POLICYID] [-policyname POLICYNAME] [-tenantname TENANTNAME]
createinsertstatements	Create insert statements (for export to a different database)	dsm_c -action createinsertstatements [-file FILEPATH] [-generateDDL] [-databaseType sqlserver|oracle] [-maxresultfromdb count] [-tenantname TENANTNAME]
diagnostic	Create a diagnostic package for the system	dsm_c -action diagnostic
fullaccess	Give an administrator the full access role	dsm_c -action fullaccess -username USERNAME [-tenantname TENANTNAME]
reindexhelp	Reindex help system	dsm_c -action reindexhelp
resetcounters	Reset counter tables (resets back to an empty state	dsm_c -action resetcounters [-tenantname TENANTNAME]
resetevents	Reset the events tables (resets back to an empty state)	dsm_c -action resetevents -type all|am|wrs|fw|dpi|im|li [-tenantname TENANTNAME]
setports	Set Deep Security Manager port(s)	dsm_c -action setports [-managerPort port] [-heartbeatPort port]
trustdirectorycert	Trust the certificate of a directory	dsm_c -action trustdirectorycert -directoryaddress DIRECTORYADDRESS -directoryport DIRECTORYPORT [-username USERNAME] [-password PASSWORD] [-tenantname TENANTNAME]
unlockout	Unlock a User account	dsm_c -action unlockout -username USERNAME [-newpassword NEWPASSWORD] [-tenantname TENANTNAME]

Connection Diagram


Trend Micro Smart Protection Network
(Certified Safe Software Service, Smart Scan, Web Reputation, Licensing, Smart Feedback)
Trend Micro Download Center
(Software Updates)
Trend Micro Update Server
(Security Updates)
Software packages
Security Updates (Patterns and Rules)
Rule updates
Software Updates, Protection Module plug-ins
Relays
Certified Safe Software Service (CSSS)
Deep Security Manager
Software Updates, Protection Module plug-ins
Pattern Updates
Local Smart Protection Server
(optional)
Policies with Rule Updates
Events
Web Reputation Ratings and Smart Scan Data
Protected Computer Resources
(vCenter-managed VMs, Cloud Resources, Physical Machines)

Computer and Agent Status

The **status** column of the Deep Security Manager's **Computers** page displays the current state of the computer and its Agent/Appliance. The status column will usually display the state of the computer on the network followed by the state (in parentheses) of the Agent or Appliance providing protection, if one is present. If the computer or Agent/Appliance is in an error state, that state will also be displayed in the **status** column. When operations are in progress, the status of the operation will appear in the **status** column.

The following three tables list possible status and error messages that may appear in the status column of the **Computers** page.

Note: *In addition to the values below, the status column may also display System or Agent Events. For a list of the Events, see **Agent/Appliance Events (page 205)** and **System Events (page 189)** in the Reference section.*

Computer States

Computer State	Description	Notes
Discovered	Computer has been added to the Computers List via the Discovery process.	
Unmanaged	Unmanaged by this Deep Security Manager, unactivated, and can't be communicated with until activated.	
Managed	An Agent is present and activated with no pending operations or errors.	
Updating	The Agent/Appliance is being updated with a combination of new configuration settings and Security Updates.	
Update Pending (Schedule)	The Agent/Appliance will be updated with a combination of new configuration settings and Security Updates once the computer's access schedule permits.	
Update Pending (Heartbeat)	An update will be performed at the next heartbeat.	
Update Pending (Offline)	The Manager cannot currently communicate with the Agent/Appliance. An update is ready to be applied once the Agent/Appliance comes back online.	
Scanning for Open Ports	The Manager is scanning the Computer for open ports.	
Activating	The Manager is activating the Agent/Appliance.	
Activating (Delayed)	The activation of the Agent/Appliance is delayed by the amount of time specified in the relevant event-based task.	
Activated	The Agent/Appliance is activated.	
Deactivating	The Manager is deactivating the Agent/Appliance. This means that the Agent/Appliance is available for activation and management by another Deep Security Manager.	
Deactivate Pending (Heartbeat)	A deactivate instruction will be sent from the Manager during the next heartbeat.	
Locked	The computer is in a locked state. While in in a locked state the Manager will not communicate with the Agent/Appliance or generate any computer-related Alerts. Existing computer Alerts are not affected.	
Multiple Errors	Multiple errors have occurred on this computer. See the computer's system events for details.	
Multiple Warnings	Multiple warnings are in effect on this computer. See the computer's system events for details.	
Upgrading Agent	The Agent software on this computer is in the process of being upgraded to a newer version.	
Scanning for Recommendations	A Recommendation Scan is underway.	
Scan for Recommendations Pending (Schedule)	A Recommendation Scan will be initiated once the computer's Access Schedule permits.	
Scan for Recommendations Pending (Heartbeat)	The Manager will initiate a Recommendation Scan at the next heartbeat.	
Scan for Recommendations Pending (Offline)	The Agent/Appliance is currently offline. The Manager will initiate a Recommendation Scan when communication is reestablished.	
Integrity Scan Pending	An instruction to start an Integrity Scan is queued to be sent.	
Integrity Scan In Progress	An Integrity Scan is currently in progress.	
Integrity Scan Pending (Offline)	The Agent/Appliance is currently offline. The Manager will initiate an Integrity Scan when communication is reestablished.	
Baseline Rebuild Pending	An instruction to rebuild a system baseline for Integrity Monitoring is queued to be sent.	
Baseline Rebuild In Progress	The Integrity Monitoring engine is currently rebuilding a system baseline.	
Baseline Rebuild Pending (Offline)	The Agent/Appliance is currently offline. The Integrity Monitoring engine will rebuild a system baseline when communication between the Manager and this computer is reestablished.	
Checking Status	The agent state is being checked.	
Getting Events	The Manager is retrieving Events from the Agent/Appliance.	

Computer State	Description	Notes
Prepared	The ESXi has been prepared for the installation of the Virtual Appliance. (The Filter Driver has been installed.)	ESXi
Unprepared	The ESXi has not been prepared for the installation of the Virtual Appliance. (The Filter Driver has been installed.)	ESXi
Filter Driver Offline	The Filter Driver on the ESXi is offline.	ESXi
Upgrade Recommended	A newer version of the Agent or Appliance is available. An software upgrade is recommended.	
Malware Manual Scan Pending	The instruction to perform a manually-initiated Malware Scan has not yet been sent.	
Malware Manual Scan Queued	The instruction to perform a manually-initiated Malware Scan is queued.	
Malware Manual Scan In Progress	A manually-initiated manually-initiated Malware Scan is in progress.	
Malware Manual Scan Paused	A manually-initiated manually-initiatedMalware Scan has been paused.	
Malware Manual Scan Cancellation Pending	The instruction to cancel a manually-initiated Malware Scan is queued to be sent.	
Malware Manual Scan Cancellation In Progress	The instruction to cancel a manually-initiated Malware Scan has been sent.	
Malware Manual Scan Cancellation Pending (Offline)	The Appliance is offline. The instruction to cancel a manually-initiated Malware Scan will be sent when communication is reestablished.	
Malware Scheduled Scan Pending	The instruction to cancel a scheduled Malware Scan has not yet been sent.	
Malware Scheduled Scan Queued	The instruction to cancel a scheduled Malware Scan is queued.	
Malware Scheduled Scan In Progress	A scheduled Malware Scan is in progress.	
Malware Scheduled Scan Paused	A scheduled Malware Scan has been paused.	
Malware Scheduled Scan Cancellation Pending	The instruction to cancel a scheduled Malware Scan is queued to be sent.	
Malware Scheduled Scan Cancellation In Progress	The instruction to cancel a scheduled Malware Scan has been sent.	
Malware Scheduled Scan Cancellation Pending (Offline)	The Agent/Appliance is offline. The instruction to cancel a scheduled Malware Scan will be sent when communication is reestablished.	
Malware Manual Scan Pending (Offline)	The Agent/Appliance is offline. The instruction to start a manually-initiated Malware Scan will be sent when communication is reestablished.	
Malware Scheduled Scan Pending (Offline)	The Agent/Appliance is offline. The instruction to start a scheduled Malware Scan will be sent when communication is reestablished.	
Update of Anti-Malware Components Pending (Offline)	The Agent/Appliance is offline. The Agent/Appliance will be updated with the latest Anti-Malware Components when communication is reestablished.	
Update of Anti-Malware Components Pending (Heartbeat)	The Agent/Appliance will be updated with the latest Anti-Malware Components at the next heartbeat.	
Update of Anti-Malware Components Pending (Schedule)	Anti-Malware Components will be updated as soon as the computer's access schedule permits.	
Update of Anti-Malware Components Pending	The instruction to update Anti-Malware Components is queued to be sent.	
Update of Anti-Malware Components In Progress	The Agent/Appliance is being updated with the latest Anti-Malware Components.	

Agent States

Agent State	Description	Notes
Activated	The Agent/Appliance has been successfully activated and is ready to be managed by the Deep Security Manager.	
Activation Required	An unactivated Agent/Appliance has been detected on the target machine. It must be activated before it can be managed by the Deep Security Manager.	
VM Stopped	The virtual machine is in a "stopped" state.	
VM Paused	The virtual machine is in a "paused" state.	
No Agent/Appliance	No Agent/Appliance was detected on the computer.	
Unknown	No attempt has been made to determine whether an Agent/Appliance is present.	
Deactivation Required	The Manager has attempted to activate an Agent/Appliance that has already been activated by another Deep Security Manager. The original Deep Security Manager must deactivate the Agent/Appliance before it can be activated by the new Manager.	
Reactivation Required	The Agent/Appliance is installed and listening and is waiting to be reactivated a Deep Security Manager.	
Online	The Agent/Appliance is online and operating as expected.	

Agent State	Description	Notes
Offline	No contact has been made with the Agent for the number of heartbeats specified in **Policy/Computer Editor > Settings > Computers** tab.	

Computer Errors

Error State	Description	Notes
Communication error	General network error.	
No route to computer.	Typically the remote host cannot be reached because of an intervening firewall or if an intermediate router is down.	
Unable to resolve hostname	Unresolved socket address.	
Activation required	An instruction was sent to the Agent/Appliance when it was not yet activated.	
Unable to communicate with Agent/Appliance	Unable to communicate with Agent/Appliance .	
Protocol error	Communication failure at the HTTP layer.	
Deactivation Required	The Agent/Appliance is currently activated by another Deep Security Manager.	
No Agent/Appliance	No Agent/Appliance was detected on the target.	
No valid software version	Indicates that no installer can be found for the platform/version requested.	
Send software failed	There was an error in sending a binary package to the computer.	
Internal error	Internal error. Please contact your support provider.	
Duplicate Computer	Two computers in the Manager's Computers list share the same IP address.	
VMware Tools Not Installed	VMware Tools (with the VMware Endpoint Driver) is not installed on a guest Virtual Machine. The VMware Endpoint Driver is required to provide Deep Security Anti-Malware and Integrity Monitoring protection. This error status will only be displayed when Deep Security is deployed in a VMware NSX environment.	

Protection Module Status

When you hover over a computer name on the **Computers** page, the state of its protection modules is displayed.

On/Off State:

State	Description
On	Module is configured in Deep Security Manager and is installed and operating on the Deep Security Agent.
Off	Module is either not configured in VDeep Security Manager, not installed and operating on the Deep Security Agent, or both.
Unknown	Indicates an error with the Firewall or Intrusion Prevention modules.

Install State:

State	Description
Not Installed	The software package containing the module has been downloaded in Deep Security Manager, but the module has not been turned on in Deep Security Manager or installed on the Agent.
Installation Pending	Module is configured in Deep Security Manager but is not installed on the Agent.
Installation in Progress	Module is being installed on the Agent.
Installed	Module is installed on the Agent. This state is only displayed when the On/Off state of the module is "Off". (If the On/Off state is "On", it means that the module has been installed on the Agent.)

State	Description
Matching Module Plug-In Not Found	The version of the software package containing the module imported into Deep Security Manager does not match the version reported by the Agent.
Not Supported/ Update Not Supported	A matching software package was found on the Agent, but it does not contain the module. "Not Supported"or "Update Not Supported" is displayed depending on whether there is already a version of this module installed on the Agent.

Configuring a Software Update Server

Deep Security Software Updates are normally hosted and distributed by Relay-enabled Agents. To deploy a Deep Security Agent on a computer, you must first import the software package for the platform into Deep Security Manager. The actual Agent install package initially only installs the core Agent functionality on to the computer. The plug-ins required for the Security Modules (Anti-Malware, Intrusion Prevention, Log Inspection, etc.) are kept off the Agent until they required. When you turn a Protection Module "on", Deep Security deploys the required plug-in to the computer via the Deep Security Relay. This is done to minimize the footprint of the Agent on the protected computer.

If you already have web servers deployed throughout your network, you may prefer to let those servers perform the task of Software Update distribution instead of deploying Relays for that purpose. To do so, you will have to mirror the software repository of the Deep Security Relay on your web servers.

Note: *Although Deep Security Agents can be instructed to get their Software Updates from a new update web server, you will still need at least one Deep Security Relay to distribute Security Updates.*

The following information describes how to set up your own software repository on a local web server.

Web Server Requirements

- **Disk Space:** 8GB
- **Ports**
    - **4122:** Agent/Appliance-to-Relay communication (TCP)
    - **4123:** Internal Relay communication to localhost (TCP)

Folder Structure

You must create a folder on the software web server which will mirror the structure of the software repository folder of a Deep Security Relay.

Note: *The procedures for mirroring folders depend on your IT environemnt and are beyond the scope of this documentation.*

The default location for the software repository folder on a Windows Relay is:

```
C:\ProgramData\Trend Micro\Deep Security Agent\relay\www\dsa\
```

The default location for the software repository folder on a Linux Relay is:

```
 /var/opt/ds_agent/relay/www/dsa/
```

The strucure of the folder is as follows:

```
|-- dsa
|     |-- <Platform>.<Architecture>
|          |--  <Filename>
|          |--  <Filename>
|          |--  ...
|
|     |-- <Platform>.<Architecture>
|          |--  <Filename>
|          |--  <Filename>
|          |--  ...
```

For example:

```
|-- dsa
|    |--  CentOS_6.x86_64
|         |--   Feature-AM-CentOS_6-9.5.1-1097.x86_64.dsp
|         |--   Feature-DPI-CentOS_6-9.5.1-1097.x86_64.dsp
|         |--   Feature-FW-CentOS_6-9.5.1-1097.x86_64.dsp
|         |--   Feature-IM-CentOS_6-9.5.1-1097.x86_64.dsp
|         |--  ...
|
|    |--  RedHat_EL6.x86_64
|         |--   Agent-Core-RedHat_EL6-9.5.1-1306.x86_64.rpm
|         |--   Feature-AM-RedHat_EL6-9.5.1-1306.x86_64.dsp
|         |--   Feature-DPI-RedHat_EL6-9.5.1-1306.x86_64.dsp
|         |--   Feature-FW-RedHat_EL6-9.5.1-1306.x86_64.dsp
|         |--  ...
|         |--   Plugin-Filter_2_6_32_131_0_15_el6_x86_64-RedHat_EL6-9.5.1-1306.x86_64.dsp
|         |--   Plugin-Filter_2_6_32_131_12_1_el6_x86_64-RedHat_EL6-9.5.1-1306.x86_64.dsp
|         |--  ...
|
|    |-- Windows.x86_64
|         |--  Agent-Core-Windows-9.5.1-1532.x86_64.msi
|         |--  Agent-Core-Windows-9.5.1-1534.x86_64.msi
|         |--  Feature-AM-Windows-9.5.1-1532.x86_64.dsp
|         |--  Feature-AM-Windows-9.5.1-1534.x86_64.dsp
|         |--  Feature-DPI-Windows-9.5.1-1532.x86_64.dsp
|         |--  Feature-DPI-Windows-9.5.1-1534.x86_64.dsp
|         |--  ...
|         |--  Plugin-Filter-Windows-9.5.1-1532.x86_64.dsp
|         |--  Plugin-Filter-Windows-9.5.1-1534.x86_64.dsp
|         |--  ...
```

Other Files and Folders on the Relay

The **dsa** folder on the Deep Security Relay contains more files and folder than those illustrated in the example above, but the only folders you need to mirror for the purposes of hosting a functioning software repository are the ones containing the files associated with the platforms and architectures of the Agents you have in use. (But there is no harm in mirroring the whole **dsa** folder, which may in fact be easier.)

Configuring Deep Security to use the new Software Repository

Now that the web server is hosting the software repository you must configure Deep Security to use it.

To configure Deep Security to use a customized web server as a Software Update repository:

1. In Deep Security Manager, go to the **Administration > System Settings > Updates** tab.
2. In the Update Web Servsers area, Enter the URL(s) of the folder(s) on your web server(s) containing the mirrored software repository contents.
3. Click **Save**.

Deep Security Agents will now get their software updates from the new software repository location.

Note: *If Deep Security Agents cannot communicate with the servers they will default to Deep Security Relays.*

Disabling Diffie-Hellman in Apache

An Apache Web server may use the Diffie-Hellman (DH) public key cryptography protocol as the "Key Exchange Algorithm" and "Authentication Method". This protocol is not supported by the Deep Security Agent/Appliance and must be disabled on an Apache Web server for SSL filtering to work.

The "Key Exchange Algorithm" and "Authentication Method" parameters are the first two fields of the " `SSLCipherSuite` " variable present in the `httpd-ssl.conf` file. To instruct Apache to not use Diffie-Hellman, " `!ADH` " must be added to these fields.

The following example shows the syntax required to disable DH key exchange and authentication methods in Apache:

```
SSLCipherSuite !ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
```

Note: *Only the first two fields are of concern with regards to disabling ADH. The " ! " tells Apache to "Not" use ADH.*

The config files may be located in different places depending on your Apache build. For example:

- **Default installation on RHEL4:** `/etc/httpd/conf.d/ssl.conf`
- **Apache 2.2.2:** `/usr/local/apache2/conf/extra/httpd-ssl.conf`

References

For more information, visit the Apache Documentation of `SSLCipherSuite` at http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite.

Encrypting Manager to DB Communication

Communication between the Deep Security Manager and the database is not encrypted by default. This is for performance reasons and because the channel between the Manager and the database may already be secure (either they are running on the same computer or they are connected by crossover cable, a private network segment, or tunneling via IPSec).

However, if the communication channel between the Deep Security Manager and the database is not secure, you should encrypt the communications between them. Do this by editing the `dsm.properties` file located in `\Deep Security Manager\webclient\webapps\ROOT\WEB-INF\`

Note: *If you are running the Deep Security Manager in multi-node mode, these changes must be made on each node.*

MS SQL Server

To encrypt communication between the Deep Security Manager and an MS SQL Server database:

1. Add the following line to `dsm.properties`:

   ```
   database.SqlServer.ssl=require
   ```
2. Stop and restart the Deep Security Manager service.

Oracle Database

To encrypt communication between the Deep Security Manager and an Oracle database:

1. Add the following lines to `dsm.properties` (example):

   ```
   database.Oracle.oracle.net.encryption_types_client=(AES256)
   database.Oracle.oracle.net.encryption_client=REQUIRED
   database.Oracle.oracle.net.crypto_checksum_types_client=(SHA1)
   database.Oracle.oracle.net.crypto_checksum_client=REQUIRED
   ```
2. Save and close the file. Stop and restart the Deep Security Manager service.

(All parameters prefixed with database.Oracle. will be passed to the Oracle driver.)

Possible values for the `encryption_types_client` are:

- AES256
- AES192
- AES128
- 3DES168
- 3DES112
- DES56C
- DES40C
- RC4_256
- RC4_128
- RC4_40

- RC4_56

Possible values for `crypto_checksum_types_client` are:

- MD5
- SHA1

For additional options consult: http://docs.oracle.com/cd/B28359_01/java.111/b31224/clntsec.htm

Running an Agent on the Database Server

Encryption should be enabled if you are using an Agent to protect the database. When you perform a Security Update, the Deep Security Manager stores new Intrusion Prevention Rules in the database. The rule names themselves will almost certainly generate false positives as they get parsed by the Agent if the data is not encrypted.

Alerts

Alert	Default Severity	Dismissible	Description
Abnormal Restart Detected	Warning	Yes	An abnormal restart has been detected on the computer. This condition may be caused by a variety of conditions. If the Agent/Appliance is suspected as the root cause then the diagnostics package (located in the Support section of the Computer Details dialog) should be invoked.
Activation Failed	Critical	No	Inability to activate may indicate a problem with the Agent/Appliance. Please check the affected Computers.
Agent configuration package too large	Warning	Yes	This is usually caused by too many Firewall and DPI Rules being assigned. Run a Recommendation Scan on the computer to determine if any Rules can be safely unassigned.
Agent Installation Failed	Critical	Yes	The Agent failed to install successfully on one or more Computers. Those Computers are currently unprotected. You must reboot the Computers which will automatically restart the Agent install program.
Agent Upgrade Recommended (Incompatible with Appliance)	Warning	No	Deep Security Manager has detected a computer with a version of the Agent that is not compatible with the Appliance. The Appliance will always filter network traffic in this configuration resulting in redundant protection. (Deprecated in 9.5)
Agent/Appliance Upgrade Recommended	Warning	No	The Deep Security Manager has detected an older Agent/Appliance version on the computer that does not support all available features. An upgrade of the Agent/Appliance software is recommended. (Deprecated in 9.5)
Agent/Appliance Upgrade Recommended (Incompatible Security Update(s))	Warning	No	Deep Security Manager has detected a computer with a version of the Agent/Appliance that is not compatible with one or more Security Updates assigned to it. An upgrade of the Agent/Appliance software is recommended.
Agent/Appliance Upgrade Recommended (New Version Available)	Warning	No	Deep Security Manager has detected one or more computers with a version of the Agent/Appliance that is older than the latest version imported into the Manager. An upgrade of the Agent/Appliance software is recommended.
Agent/Appliance Upgrade Required	Warning	No	Deep Security Manager has detected a computer with a version of the Agent/Appliance that is not compatible with this version of the Manager. An upgrade of the Agent/Appliance software is required.
An upgrade to the Rule Update system is available	Warning	No	An upgrade to the Rule Update system is available. To take advantage of the new features included in this upgrade you must reapply the most recently applied Rule Update. Go to Administration > Updates, click on "View All Rule Updates..." and reapply the most recently applied Rule Update. If you do not reapply the Rule Update now, the new features will be implemented with the application of the next Rule Update.
Anti-Malware Alert	Warning	Yes	A Malware Scan Configuration that is configured for alerting has raised an event on one or more computers.
Anti-Malware Component Failure	Critical	Yes	An Anti-Malware component failed on one or more computers. See the Event descriptions on the individual computers for specific details.
Anti-Malware Component Update Failed	Warning	No	One or more Agent/Relay failed to update Anti-Malware components. See the affected computers for more information.
Anti-Malware Engine Offline	Critical	No	The Agent/Appliance has reported that the Anti-Malware Engine is not responding. Please check the system events for the computer to determine the cause of the failure.
Anti-Malware protection is absent or out of date	Warning	No	The Agent on this computer has not received its initial Anti-Malware protection package, or its Anti-Malware protection is out of date. Make sure a Deep Security Relay is available and that the Agent has been properly configured to communicate with it. To configure Relays and other Update options, go to Administration > System Settings > Updates.
Anti-Malware Quarantine Alert for Storage Limit	Warning	Yes	Anti-Malware failed to quarantine a file because the storage limit is reached.
Application Type Misconfiguration	Warning	No	Misconfiguration of Application Types may prevent proper security coverage. Please review the system events below for details.
Application Type Recommendation	Warning	Yes	Deep Security Manager has determined that a computer on your network should be assigned an Application Type. This could be because an Agent was installed on a new computer and vulnerable applications were detected, or because a new vulnerability has been discovered in an installed application that was previously thought to be safe. To assign the

Alert	Default Severity	Dismissible	Description
			Application Type to the Computer, open the 'Computer Details' dialog box, click on 'Intrusion Prevention Rules', and assign the Application Type.
Certified Safe Software Service Offline	Warning	No	A Deep Security Manager node cannot connect to the Trend Micro Certified Safe Software Service to perform file signature comparisons for the Integrity Monitoring module. A locally cached database will be used until connectivity is restored. Make sure the Manager node has Internet connectivity and that proxy settings (if any) are correct.
Clock Change Detected	Warning	Yes	A clock change has been detected on the computer. Unexpected clock changes may indicate a problem on the computer and should be investigated before the alert is dismissed.
Communications Problem Detected	Warning	Yes	A communications problem has been detected on the computer. Communications problems indicate that the computer cannot initiate communication with the Deep Security Manager(s) because of network configuration or load reasons. Please check the System Events in addition to verifying communications can be established to the Deep Security Manager(s) from the computer. The cause of the issue should be investigated before the alert is dismissed.
Computer Not Receiving Updates	Warning	No	These Computer(s) have stopped receiving updates. Manual intervention may be required.
Computer Reboot Required	Warning	Yes	The Agent software upgrade was successful, but the computer must be rebooted for the install to be completed. The computer(s) should be manually updated before the alert is dismissed.
Computer Reboot Required for Anti-Malware Protection	Warning	No	The Anti-Malware protection on Agent has reported that the computer needs to be rebooted. Please check the system events for the computer to determine the reason for the reboot.
Configuration Required	Warning	No	One or more computers are using a Policy that defines multiple interface types where not all interfaces have been mapped.
Connection to Filter Driver Failure	Critical	No	An Appliance has reported a failure connecting to the filter driver. This may indicate a configuration issue with the filter driver running on the ESXi or with the Appliance. The Appliance must be able to connect to the filter driver in order to protect guests. The cause of the issue should be investigated and resolved.
CPU Critical Threshold Exceeded	Critical	No	The CPU critical threshold has been exceeded.
CPU Warning Threshold Exceeded	Warning	No	The CPU warning threshold has been exceeded.
Duplicate Computer Detected	Warning	Yes	A duplicate computer has been activated or imported. Please remove the duplicate computer and reactivate the original computer if necessary.
Duplicate Unique Identifiers Detected	Warning	No	Consult the Deep Security online help or guidance documents for information on managing Cloud Provider resources and troubleshooting duplicate UUIDs.
Empty Relay Group Assigned	Critical	No	These computers have been assigned an empty Relay Group. Assign a different Relay Group to the computers or add Relays to the empty Relay Group(s).
Events Suppressed	Warning	Yes	The Agent/Appliance encountered an unexpectedly high volume of events. As a result one or more events were not recorded (suppressed) to prevent a potential Denial of Service. Check the firewall events to determine the cause of the suppression.
Events Truncated	Warning	Yes	Some events were lost because the data file grew too large for the Agent/Appliance to store. This may have been caused by an unexpected increase in the number of events being generated, or the inability of the Agent/Appliance to send the data to the Deep Security Manager. For more information, see the properties of the "Events Truncated" system event on the Computer.
Firewall Engine Offline	Critical	No	The Agent/Appliance has reported that the Firewall Engine is offline. Please check the status of the engine on the Agent/Appliance.
Firewall Rule Alert	Warning	Yes	A firewall rule that is selected for alerting has been encountered on one or more computers.
Firewall Rule Recommendation	Warning	Yes	Deep Security Manager has determined that a computer on your network should be assigned an Firewall Rule. This could be because an Agent was installed on a new computer and vulnerable applications were detected, or because a new vulnerability has been discovered in an installed application that was previously thought to be safe. To assign the Firewall Rule to the Computer, open the 'Computer Details' dialog box, click on the 'Firewall Rules' node, and assign the Firewall Rule.
Heartbeat Server Failed	Warning	No	The heartbeat server failed to start properly. This may be due to a port conflict. Agents/Appliances will not be able to contact the Manager until this problem is resolved. To resolve this problem ensure that another service is not using the port reserved for use by the heartbeat server and restart the Deep Security Manager service. If you do not wish to use the heartbeat you can turn this alert off in the Alert Configuration section.
Incompatible Agent/Appliance Version	Warning	No	Deep Security Manager has detected a more recent Agent/Appliance version on the computer that is not compatible with this version of the Manager. An upgrade of the Manager software is recommended.
Insufficient Disk Space	Warning	Yes	The Agent/Appliance has reported that it was forced to delete an old log file to free up disk space for a new log file. Please immediately free up disk space to prevent loss of Intrusion Prevention, Firewall and Agent/Appliance Events.

Alert	Default Severity	Dismissible	Description
Integrity Monitoring Engine Offline	Critical	No	The Agent/Appliance has reported that the Integrity Monitoring Engine is not responding. Please check the system events for the computer to determine the cause of the failure.
Integrity Monitoring information collection has been delayed	Warning	No	The rate at which Integrity Monitoring information is collected has been temporarily delayed due to an increased amount of Integrity Monitoring data. During this time the baseline and Integrity Event views may not be current for some computers. This alert will be dismissed automatically once Integrity Monitoring data is no longer being delayed.
Integrity Monitoring Rule Alert	Warning	Yes	An integrity monitoring rule that is selected for alerting has been encountered on one or more computers.
Integrity Monitoring Rule Compilation Error	Critical	No	An error was encountered compiling an Integrity Monitoring Rule on a Computer. This may result in the Integrity Monitoring Rule not operating as expected.
Integrity Monitoring Rule Recommendation	Warning	Yes	Deep Security Manager has determined that a computer on your network should be assigned an Integrity Monitoring Rule. To assign the Integrity Monitoring Rule to the Computer, open the 'Computer Details' dialog box, click on the 'Integrity Monitoring > Integrity Monitoring Rules' node, and assign the Integrity Monitoring Rule.
Integrity Monitoring Rule Requires Configuration	Warning	No	An Integrity Monitoring Rule that requires configuration before use has been assigned to one or more computers. This rule will not be sent to the computer(s). Open the Integrity Monitoring Rule properties and select the Configuration tab for more information.
Integrity Monitoring Trusted Platform Module Not Enabled	Warning	Yes	Trusted Platform Module Not Enabled. Please ensure the hardware is installed and the BIOS setting is correct.
Integrity Monitoring Trusted Platform Module Register Value Changed	Warning	Yes	Trusted Platform Module Register Value Changed. If you have not modified the ESXi hypervisor configuration this may represent an attack.
Intrusion Prevention Engine Offline	Critical	No	The Agent/Appliance has reported that the Intrusion Prevention Engine is offline. Please check the status of the engine on the Agent/Appliance.
Intrusion Prevention Rule Alert	Warning	Yes	A Intrusion Prevention Rule that is selected for alerting has been encountered on one or more computers.
Intrusion Prevention Rule Recommendation	Warning	Yes	Deep Security Manager has determined that a computer on your network should be assigned a Intrusion Prevention Rule. This could be because an Agent was installed on a new computer and vulnerable applications were detected, or because a new vulnerability has been discovered in an installed application that was previously thought to be safe. To assign the Intrusion Prevention Rule to the Computer, open the 'Computer Details' dialog box, click on 'Intrusion Prevention Rules', and assign the Intrusion Prevention Rule.
Intrusion Prevention Rule Removal Recommendation	Warning	Yes	Deep Security Manager has determined that a computer on your network has a Intrusion Prevention Rule assigned to it that is not required. This could be because a vulnerable application was uninstalled, an existing vulnerability was patched, or the rule was unnecessarily assigned to begin with. To unassign the Intrusion Prevention Rule from the Computer, open the 'Computer Details' dialog box, click on Intrusion Prevention > Intrusion Prevention Rules, and clear the checkbox next to the Intrusion Prevention Rule.
Intrusion Prevention Rule Requires Configuration	Warning	No	A Intrusion Prevention Rule that requires configuration before use has been assigned to one or more computers. This rule will not be sent to the computer(s). Open the Intrusion Prevention Rule properties and select the Configuration tab for more information.
Log Inspection Engine Offline	Critical	No	The Agent/Appliance has reported that the Log Inspection engine has failed to initialize. Please check the system events for the computer to determine the cause of the failure.
Log Inspection Rule Alert	Warning	Yes	A log inspection rule that is selected for alerting has been encountered on one or more computers.
Log Inspection Rule Recommendation	Warning	Yes	Deep Security Manager has determined that a computer on your network should be assigned a Log Inspection Rule. To assign the Log Inspection Rule to the Computer, open the 'Computer Details' dialog box, click on the 'Log Inspection > Log Inspection Rules' node, and assign the Log Inspection Rule.

Alert	Default Severity	Dismissible	Description
Log Inspection Rule Requires Configuration	Warning	No	A Log Inspection Rule that requires configuration before use has been assigned to one or more computers. This rule will not be sent to the computer(s). Open the Log Inspection Rule properties and select the Configuration tab for more information.
Low Disk Space	Warning	No	A Deep Security Manager Node has less than 10% remaining disk space. Please free space by deleting old or unnecessary files, or add more storage capacity.
Manager Offline	Warning	No	A Deep Security Manager Node is offline. It is possible the machine has experienced a hardware or software problem, or has simply lost network connectivity. Please check the status of the Manager's computer.
Manager Time Out of Sync	Critical	No	The clock on each Manager Node must be synchronized with the clock on the database. If the clocks are too far out of sync (more than 30 seconds) the Manager Node will not perform its tasks correctly. Synchronize the clock on your Manager Node with the clock on the database.
Memory Critical Threshold Exceeded	Critical	No	The memory critical threshold has been exceeded.
Memory Warning Threshold Exceeded	Warning	No	The memory warning threshold has been exceeded.
Multiple Activated Appliances Detected	Warning	Yes	The Appliance has reported that multiple connections have been made to the filter driver on the same ESXi. This indicates that there may be multiple activated Appliances running on the same ESXi, which is not supported. The cause of the issue should be investigated before the alert is dismissed.
Network Engine Mode Incompatibility	Warning	No	Setting Network Engine Mode to Tap is only available on Agent versions 5.2 or higher. Review and update the Agent's configuration or upgrade the Agent to resolve the incompatibility.
New Pattern Update is Downloaded and Available	Warning	No	New Patterns are available as part of a Security Update. The Patterns have been downloaded to Deep Security but have not yet been applied to your computers. To apply the Update to your computers, go to the Administration > Updates > Security page.
New Rule Update is Downloaded and Available	Warning	No	New Rules are available as part of a Security Update. The Rules have been downloaded to Deep Security but have not yet been applied to Policies and sent to your computers. To apply the Update and send the updated Policies to your computers, go to the Administration > Updates > Security page.
Newer Version of Deep Security Manager is Available	Warning	No	A new version of the Deep Security Manager is available. Download the latest version from the Trend Micro Download Center at http://downloadcenter.trendmicro.com/
Newer Versions of Software Available	Warning	No	New software is available. Software can be downloaded from the Download Center.
Number of Computers exceeds database limit	Warning	No	The number of activated computers has exceeded the recommended limit for an embedded database. Performance will degrade rapidly if more computers are added and it is strongly suggested that another database option (Oracle or SQL Server) be considered at this point. Please contact Trend Micro for more information on upgrading your database.
Protection Module Licensing Expired	Warning	Yes	The Protection Module license has expired.
Protection Module Licensing Expires Soon	Warning	No	The Protection Module licensing will expire soon. You can remove this alert by changing your license on the Administration > Licenses page.
Recommendation	Warning	Yes	Deep Security Manager has determined that the security configuration of one of your computers should be updated. To see what changes are recommended, open the computer's Editor window and look through the module pages for warnings of unresolved recommendations. In the Assigned Rules area, click Assign/Unassign... to display the list of available Rules and then filter them using the "Show Recommended for Assignment" viewing filter option. (Select "Show Recommended for Unassignment" to display Rules that can safely be unassigned.)
Reconnaissance Detected: Computer OS Fingerprint Probe	Warning	Yes	The Agent/Appliance detected an attempt to identify the computer operating system via a "fingerprint" probe. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the computer's events to see the details of the probe.
Reconnaissance Detected: Network or Port Scan	Warning	Yes	The Agent/Appliance detected network activity typical of a network or port scan. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the computer's events to see the details of the scan.
Reconnaissance Detected: TCP Null Scan	Warning	Yes	The Agent/Appliance detected a TCP "Null" scan. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the computer's events to see the details of the scan.

Alert	Default Severity	Dismissible	Description
Reconnaissance Detected: TCP SYNFIN Scan	Warning	Yes	The Agent/Appliance detected a TCP "SYNFIN" scan. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the computer's events to see the details of the scan.
Reconnaissance Detected: TCP Xmas Scan	Warning	Yes	The Agent/Appliance detected a TCP "Xmas" scan. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the computer's events to see the details of the scan.
Relay Update Service Unavailable	Critical	No	A Deep Security Relay's update service is unavailable when the Relay itself is downloading Security Updates from the Update Server (or from another Relay Group). If the situation persists, try to manually initiate an update on the Relay using the "Download Security Update" option. A Relay will fail to successfully retrieve a Security Update if the Update Server is unavailable or if the update package is corrupt.
Scheduled Malware Scan Missed	Warning	No	Scheduled Malware scan tasks were initiated on computers that already had pending scan tasks. This may indicate a scanning frequency that is too high. Consider lowering the scanning frequency, or selecting fewer computers to scan during each scheduled scan job.
Send Policy Failed	Critical	No	Inability to send policy may indicate a problem with the Agent/Appliance. Please check the affected Computers.
Smart Protection Server Connection Failed	Warning	Yes	Failed to connect to a Smart Protection Server. This could be due to a configuration issue, or due to network connectivity.
Software Package Not Found	Critical	No	An Agent Software Package is required for the proper operation of one or more Virtual Appliance(s). Please import a Red Hat Enterprise 6 (64 bit) Agent Software Package with the correct version for each Appliance. If the required version is not available then please import the latest package and upgrade the Appliance to match.
Software Updates Available for Import	Warning	No	New software is available. To import new software to Deep Security, go to Administration > Updates > Software > Download Center.
Unable to communicate	Critical	No	Deep Security Manager has been unable to query the Agent/Appliance for its status within the configured period. Please check your network configuration and the affected Computer's connectivity.
Unable to Upgrade the Agent Software	Warning	Yes	Deep Security Manager was unable to upgrade the Agent software on the computer.
Upgrade of the Deep Security Manager Software Recommended (Incompatible Security Update(s))	Warning	No	Deep Security Manager has detected a computer that is using Security Updates that are not compatible with the current version of Deep Security Manager. An upgrade of Deep Security Manager software is recommended.
Upgrade of the Filter Driver Recommended (New Version Available)	Warning	No	Deep Security Manager has detected one or more ESXi Servers with a version of the Filter Driver that does not match the latest version available. An upgrade of the Filter Driver is recommended.
User Locked Out	Warning	No	Users can be locked out manually, by repeated incorrect sign-in attempts, if their password expires, or if they have been imported but not yet unlocked.
User Password Expires Soon	Warning	No	The password expiry setting is enabled and one or more Users have passwords that will expire within the next 7 days.
Virtual Appliance is Incompatible With Filter Driver	Warning	No	The Appliance is incompatible with the Filter Driver. Please ensure both are upgraded to their latest versions.
Virtual Machine Interfaces Out of Sync	Warning	No	One or more of the virtual machines monitored by a Deep Security Virtual Appliance has reported that its interfaces are out of sync with the filter driver. This means that the Appliance may not be properly monitoring the virtual machine's interfaces. The virtual machine may require manual intervention such as a configuration change, or a restart, to correct the issue.
Virtual Machine Moved to Unprotected ESXi Server	Warning	Yes	A Virtual Machine was moved to an ESXi Server that does not have an activated Deep Security Virtual Appliance.
Virtual Machine Unprotected after move to another ESXi	Warning	Yes	A Virtual Machine that was Appliance protected has been unprotected during or after it was moved to another ESXi. This may be due to an Appliance reboot or power off during the move, or it may indicate a configuration issue. The cause of the issue should be investigated before the alert is dismissed.

Alert	Default Severity	Dismissible	Description
VMware Tools Not Installed	Critical	Yes	A protected Virtual Machine in an NSX environment does not have VMware Tools installed. VMware Tools is required to protect Virtual Machines in an NSX environment.
Web Reputation Event Alert	Warning	Yes	A Web Reputation event has been encountered on one or more computers that are selected for alerting.

Event Lists

System Events

ID	Severity	Event	Notes
0	Error	Unknown Error	
100	Info	Deep Security Manager Started	
101	Info	License Changed	
102	Info	Trend Micro Deep Security Customer Account Changed	
103	Warning	Check For Updates Failed	
104	Warning	Automatic Software Download Failed	
105	Warning	Scheduled Rule Update Download and Apply Failed	
106	Info	Scheduled Rule Update Downloaded and Applied	
107	Info	Rule Update Downloaded and Applied	
108	Info	Script Executed	
109	Error	Script Execution Failed	
110	Info	System Events Exported	
111	Info	Firewall Events Exported	
112	Info	Intrusion Prevention Events Exported	
113	Warning	Scheduled Rule Update Download Failed	
114	Info	Scheduled Rule Update Downloaded	
115	Info	Rule Update Downloaded	
116	Info	Rule Update Applied	
117	Info	Deep Security Manager Shutdown	
118	Warning	Deep Security Manager Offline	
119	Info	Deep Security Manager Back Online	
120	Error	Heartbeat Server Failed	The server within Manager that listens for incoming Agent Heartbeats has failed to start. Check that the Manager's incoming heartbeat port (by default 4120) is not in use by another application on the Manager server. Once it is free, the Manager should bind to it and this error should be fixed.
121	Error	Scheduler Failed	
122	Error	Manager Message Thread Failed	An internal thread has failed. There is no resolution for this error. If it persists, contact customer support.
123	Info	Deep Security Manager Forced Shutdown	
124	Info	Rule Update Deleted	
130	Info	Credentials Generated	
131	Warning	Credential Generation Failed	
140	Info	Discover Computers	
141	Warning	Discover Computers Failed	
142	Info	Discover Computers Requested	
143	Info	Discover Computers Canceled	
150	Info	System Settings Saved	
151	Info	Software Added	
152	Info	Software Deleted	
153	Info	Software Updated	
154	Info	Software Exported	
155	Info	Software Platforms Changed	

ID	Severity	Event	Notes
160	Info	Authentication Failed	
161	Info	Rule Update Exported	
162	Info	Log Inspection Events Exported	
163	Info	Anti-Malware Event Exported	
164	Info	Security Update Successful	
165	Error	Security Update Failed	
166	Info	Check for New Software Success	
167	Error	Check for New Software Failed	
168	Info	Manual Security Update Successful	
169	Error	Manual Security Update Failed	
170	Error	Manager Available Disk Space Too Low	The Manager has determined that there is not enough disk space available to continue to function and will shutdown. When this error occurs the Manager will shutdown. The resolution is to free up disk space and restart the Manager.
171	Info	Anti-Malware Spyware Item Exported	
172	Info	Web Reputation Events Exported	
173	Info	Anti-Malware Quarantined File List Exported	
180	Info	Alert Type Updated	
190	Info	Alert Started	
191	Info	Alert Changed	
192	Info	Alert Ended	
197	Info	Alert Emails Sent	
198	Warning	Alert Emails Failed	An Alert was raised which had been configured to generate an email notification to one or more users but the email could not be sent. Make sure SMTP setting are properly configured. See Administration > System Settings > SMTP.
199	Error	Alert Processing Failed	Processing of the Alerts has failed. This may mean that the current Alert status is inaccurate. There is no resolution for this error. If it persists, contact customer support.
248	Info	Software Update: Disable Relay Requested	
249	Info	Software Update: Enable Relay Requested	
250	Info	Computer Created	
251	Info	Computer Deleted	
252	Info	Computer Updated	
253	Info	Policy Assigned to Computer	
254	Info	Computer Moved	
255	Info	Activation Requested	
256	Info	Send Policy Requested	
257	Info	Locked	
258	Info	Unlocked	
259	Info	Deactivation Requested	
260	Info	Scan for Open Ports	
261	Warning	Scan for Open Ports Failed	
262	Info	Scan for Open Ports Requested	
263	Info	Scan for Open Ports Canceled	
264	Info	Agent Software Upgrade Requested	
265	Info	Agent Software Upgrade Cancelled	
266	Info	Warnings/Errors Cleared	
267	Info	Check Status Requested	
268	Info	Get Events Requested	
270	Error	Computer Creation Failed	

ID	Severity	Event	Notes
271	Info	Agent Software Upgrade Timed Out	
272	Info	Appliance Software Upgrade Timed Out	
273	Info	Security Update: Security Update Check and Download Requested	
274	Info	Security Update: Security Update Rollback Requested	
275	Warning	Duplicate Computer	
276	Info	Update: Summary Information	
280	Info	Computers Exported	
281	Info	Computers Imported	
286	Info	Computer Log Exported	
287	Info	Relay Group Assigned to Computer	
290	Info	Group Added	
291	Info	Group Removed	
292	Info	Group Updated	
293	Info	Interface Renamed	
294	Info	Computer Bridge Renamed	
295	Info	Interface Deleted	
296	Info	Interface IP Deleted	
297	Info	Recommendation Scan Requested	
298	Info	Recommendations Cleared	
299	Info	Asset Value Assigned to Computer	
300	Info	Recommendation Scan Completed	
301	Info	Agent Software Deployment Requested	
302	Info	Agent Software Removal Requested	
303	Info	Computer Renamed	
305	Info	Scan for Integrity Requested	
306	Info	Rebuild Baseline Requested	
307	Info	Cancel Update Requested	
308	Info	Integrity Monitoring Rule Compile Issue	
309	Info	Integrity Monitoring Rule Compile Issue Resolved	
310	Info	Directory Added	
311	Info	Directory Removed	
312	Info	Directory Updated	
320	Info	Directory Synchronization	
321	Info	Directory Synchronization Finished	
322	Error	Directory Synchronization Failed	
323	Info	Directory Synchronization Requested	
324	Info	Directory Synchronization Cancelled	
325	Info	User Synchronization	Synchronization of the Users list with an Active Directory has been started.
326	Info	User Synchronization Finished	Synchronization of the Users list with an Active Directory has completed.
327	Error	User Synchronization Failed	

ID	Severity	Event	Notes
328	Info	User Synchronization Requested	
329	Info	User Synchronization Cancelled	
330	Info	SSL Configuration Created	
331	Info	SSL Configuration Deleted	
332	Info	SSL Configuration Updated	
350	Info	Policy Created	
351	Info	Policy Deleted	
352	Info	Policy Updated	
353	Info	Policies Exported	
354	Info	Policies Imported	
360	Info	VMware vCenter Added	
361	Info	VMware vCenter Removed	
362	Info	VMware vCenter Updated	
363	Info	VMware vCenter Synchronization	
364	Info	VMware vCenter Synchronization Finished	
365	Error	VMware vCenter Synchronization Failed	
366	Info	VMware vCenter Synchronization Requested	
367	Info	VMware vCenter Synchronization Cancelled	
368	Warning	Interfaces Out of Sync	This indicates that the interfaces reported by the Appliance are different than the interfaces reported by the vCenter. This can typically be resolved by rebooting the VM.
369	Info	Interfaces in Sync	
370	Info	ESXi Server Prepared	
371	Info	ESXi Server Restored	The ESXi has been restored to the state it was in before the Filter Driver software was installed.
372	Info	Filter Driver Upgraded	
373	Info	Virtual Appliance Deployed	
374	Info	Virtual Appliance Upgraded	
375	Warning	Virtual Appliance Upgrade Failed	
376	Warning	Virtual Machine Moved to Unprotected ESXi	
377	Info	Virtual Machine Moved to Protected ESXi	
378	Warning	Virtual Machine unprotected after move to another ESXi	A VM was moved to an unprotected ESXi.
379	Info	Virtual Machine unprotected after move to another ESXi Resolved	
380	Error	Filter Driver Offline	The Filter Driver on a given ESXi is offline. Use the VMware vCenter console to troubleshoot problems with the hypervisor and/or the ESXi.
381	Info	Filter Driver Back Online	
382	Info	Filter Driver Upgrade Requested	
383	Info	Appliance Upgrade Requested	
384	Warning	Prepare ESXi Failed	
385	Warning	Filter Driver Upgrade Failed	
386	Warning	Restore ESXi Failed	
387	Error	Connection to Filter Driver Failure	
388	Info	Connection to Filter Driver Success	

ID	Severity	Event	Notes
389	Error	Multiple Activated Appliances Detected	
390	Info	Multiple Activated Appliances Detected Resolved	
391	Error	Network Settings Out of Sync With vCenter Global Settings	
392	Info	Network Settings in Sync With vCenter Global Settings	
393	Error	Anti-Malware Engine Offline	The Anti-Malware Engine is offline and the Anti-Malware protection module is not functioning correctly. This is likely due to the VMware environment not meeting the requirements specified in the Installation Guide.
394	Info	Anti-Malware Engine Back Online	
395	Error	Virtual Appliance is Incompatible With Filter Driver	
396	Info	Virtual Appliance is Incompatible With Filter Driver Resolved	
397	Warning	VMware NSX Callback Authentication Failed	
398	Error	VMware Tools Not Installed	
399	Info	VMware Tools Not Installed Resolved	
410	Info	Firewall Rule Created	
411	Info	Firewall Rule Deleted	
412	Info	Firewall Rule Updated	
413	Info	Firewall Rule Exported	
414	Info	Firewall Rule Imported	
420	Info	Firewall Stateful Configuration Created	
421	Info	Firewall Stateful Configuration Deleted	
422	Info	Firewall Stateful Configuration Updated	
423	Info	Firewall Stateful Configuration Exported	
424	Info	Firewall Stateful Configuration Imported	
460	Info	Application Type Created	
461	Info	Application Type Deleted	
462	Info	Application Type Updated	
463	Info	Application Type Exported	
464	Info	Application Type Imported	
470	Info	Intrusion Prevention Rule Created	
471	Info	Intrusion Prevention Rule Deleted	
472	Info	Intrusion Prevention Rule Updated	
473	Info	Intrusion Prevention Rule Exported	
474	Info	Intrusion Prevention Rule Imported	
480	Info	Integrity Monitoring Rule Created	
481	Info	Integrity Monitoring Rule Deleted	

ID	Severity	Event	Notes
482	Info	Integrity Monitoring Rule Updated	
483	Info	Integrity Monitoring Rule Exported	
484	Info	Integrity Monitoring Rule Imported	
490	Info	Log Inspection Rule Created	
491	Info	Log Inspection Rule Deleted	
492	Info	Log Inspection Rule Updated	
493	Info	Log Inspection Rule Exported	
494	Info	Log Inspection Rule Imported	
495	Info	Log Inspection Decoder Created	
496	Info	Log Inspection Decoder Deleted	
497	Info	Log Inspection Decoder Updated	
498	Info	Log Inspection Decoder Exported	
499	Info	Log Inspection Decoder Imported	
505	Info	Context Created	
506	Info	Context Deleted	
507	Info	Context Updated	
508	Info	Context Exported	
509	Info	Context Imported	
510	Info	IP List Created	
511	Info	IP List Deleted	
512	Info	IP List Updated	
513	Info	IP List Exported	
514	Info	IP List Imported	
520	Info	Port List Created	
521	Info	Port List Deleted	
522	Info	Port List Updated	
523	Info	Port List Exported	
524	Info	Port List Imported	
525	Info	Scan Cache Configuration Created	
526	Info	Scan Cache Configuration Exported	
530	Info	MAC List Created	
531	Info	MAC List Deleted	
532	Info	MAC List Updated	
533	Info	MAC List Exported	
534	Info	MAC List Imported	
540	Info	Proxy Created	
541	Info	Proxy Deleted	
542	Info	Proxy Updated	
543	Info	Proxy Exported	
544	Info	Proxy Imported	
550	Info	Schedule Created	
551	Info	Schedule Deleted	
552	Info	Schedule Updated	
553	Info	Schedule Exported	
554	Info	Schedule Imported	
560	Info	Scheduled Task Created	

ID	Severity	Event	Notes
561	Info	Scheduled Task Deleted	
562	Info	Scheduled Task Updated	
563	Info	Scheduled Task Manually Executed	
564	Info	Scheduled Task Started	
565	Info	Backup Finished	
566	Error	Backup Failed	
567	Info	Sending Outstanding Alert Summary	
568	Warning	Failed To Send Outstanding Alert Summary	
569	Warning	Email Failed	An email notification could not be sent. Make sure SMTP setting are properly configured (Administration > System Settings > SMTP).
570	Info	Sending Report	
571	Warning	Failed To Send Report	
572	Error	Invalid Report Jar	
573	Info	Asset Value Created	
574	Info	Asset Value Deleted	
575	Info	Asset Value Updated	
576	Error	Report Uninstall Failed	
577	Error	Report Uninstalled	
580	Warning	Application Type Port List Misconfiguration	
581	Warning	Application Type Port List Misconfiguration Resolved	
582	Warning	Intrusion Prevention Rules Require Configuration	
583	Info	Intrusion Prevention Rules Require Configuration Resolved	
584	Warning	Integrity Monitoring Rules Require Configuration	
585	Info	Integrity Monitoring Rules Require Configuration Resolved	
586	Warning	Log Inspection Rules Require Configuration	
587	Info	Log Inspection Rules Require Configuration Resolved	
588	Warning	Log Inspection Rules Require Log Files	
589	Info	Log Inspection Rules Require Log Files Resolved	
590	Warning	Scheduled Task Unknown Type	
591	Info	Relay Group Created	
592	Info	Relay Group Updated	
593	Info	Relay Group Deleted	
600	Info	User Signed In	
601	Info	User Signed Out	
602	Info	User Timed Out	
603	Info	User Locked Out	
604	Info	User Unlocked	
608	Error	User Session Validation Failed	Manager is unable to confirm that the User session is the one that was initiated by a successful User sign-in/authentication. Manager will return the User to the sign-in page. User will be forced to re-authenticate.
609	Error	User Made Invalid Request	Manager received invalid request to access the audit data (Events). Access to the audit data is denied.
610	Info	User Session Validated	
611	Info	User Viewed Firewall Event	
613	Info	User Viewed Intrusion Prevention Event	

ID	Severity	Event	Notes
615	Info	User Viewed System Event	
616	Info	User Viewed Integrity Monitoring Event	
617	Info	User Viewed Log Inspection Event	
618	Info	User Viewed Quarantined File Detail	
619	Info	User Viewed Anti-Malware Event	
620	Info	User Viewed Web Reputation Event	
621	Info	User Signed In As Tenant	
622	Info	Access from Primary Tenant Enabled	
623	Info	Access from Primary Tenant Disabled	
624	Info	Access from Primary Tenant Allowed	
625	Info	Access from Primary Tenant Revoked	
626	Info	Access from Primary Tenant Expired	
650	Info	User Created	
651	Info	User Deleted	
652	Info	User Updated	
653	Info	User Password Set	
660	Info	Role Created	
661	Info	Role Deleted	
662	Info	Role Updated	
663	Info	Roles Imported	
664	Info	Roles Exported	
670	Info	Contact Created	
671	Info	Contact Deleted	
672	Info	Contact Updated	
700	Info	Agent Software Installed	
701	Error	Agent Software Installation Failed	
702	Info	Credentials Generated	
703	Error	Credential Generation Failed	
704	Info	Activated	
705	Error	Activation Failed	
706	Info	Agent Software Upgraded	
707	Warning	Agent Software Upgrade Failed	
708	Info	Deactivated	
709	Error	Deactivation Failed	
710	Info	Events Retrieved	
711	Info	Agent Software Deployed	
712	Error	Agent Software Deployment Failed	
713	Info	Agent Software Removed	
714	Error	Agent Software Removal Failed	
715	Info	Agent/Appliance Version Changed	
720	Info	Policy Sent	Agent/Appliance updated.
721	Error	Send Policy Failed	
722	Warning	Get Interfaces Failed	
723	Info	Get Interfaces Failure Resolved	

ID	Severity	Event	Notes
724	Warning	Insufficient Disk Space	An Agent has reported low disk space. Free space on the Agent's host.
725	Warning	Events Suppressed	
726	Warning	Get Agent/Appliance Events Failed	Manager was unable to retrieve Events from Agent/Appliance. This error does not mean that the data was lost on the Agent/Appliance. This error is normally caused by a network interruption while events are being transferred. Clear the error and run a "Check Status" to retry the operation.
727	Info	Get Agent/Appliance Events Failure Resolved	
728	Error	Get Events Failed	Manager was unable to retrieve audit data from Agent/Appliance. This error does not mean that the data was lost on the Agent/Appliance. This error is normally caused by a network interruption while events are being transferred. Clear the error and run a "Get Events Now" to retry the operation.
729	Info	Get Events Failure Resolved	
730	Error	Offline	Manager cannot communicate with Computer. This error does not mean that protection being provided by an Agent/Appliance is inactive. See Computer and Agent/Appliance Status for more information.
731	Info	Back Online	
732	Error	Firewall Engine Offline	The Firewall Engine is offline and traffic is flowing unfiltered. This is normally due to an error during installation or verification of the driver on the computer's OS platform. Check the status of the network driver at the computer to ensure it is properly loaded.
733	Info	Firewall Engine Back Online	
734	Warning	Computer Clock Change	A clock change has occurred on the Computer which exceeds the maximum allowed specified in Policy/Computer Editor > Settings > Computer > Heartbeat area. Investigate what has caused the clock change on the computer.
735	Warning	Misconfiguration Detected	The Agent's configuration does not match the configuration indicated in the Manager's records. This is typically because of a recent backup restoration of the Manager or the Agent. Unanticipated misconfiguration warnings should be investigated.
736	Info	Check Status Failure Resolved	
737	Error	Check Status Failed	
738	Error	Intrusion Prevention Engine Offline	The Intrusion Prevention Engine is offline and traffic is flowing unfiltered. This is normally due to an error during installation or verification of the driver on the computer's OS platform. Check the status of the network driver at the computer to ensure it is properly loaded.
739	Info	Intrusion Prevention Engine Back Online	
740	Error	Agent/Appliance Error	
741	Warning	Abnormal Restart Detected	
742	Warning	Communications Problem	The Agent is having problems communicating its status to Manager. It usually indicates network or load congestion in the Agent > Manager direction. Further investigation is warranted if the situation persists
743	Info	Communications Problem Resolved	
745	Warning	Events Truncated	
748	Error	Log Inspection Engine Offline	
749	Info	Log Inspection Engine Back Online	
750	Warning	Last Automatic Retry	
755	Info	Deep Security Manager Version Compatibility Resolved	
756	Warning	Deep Security Manager Upgrade Recommended (Incompatible Security Update(s))	
760	Info	Agent/Appliance Version Compatibility Resolved	
761	Warning	Agent/Appliance Upgrade Recommended	
762	Warning	Agent/Appliance Upgrade Required	
763	Warning	Incompatible Agent/Appliance Version	

ID	Severity	Event	Notes
764	Warning	Agent/Appliance Upgrade Recommended (Incompatible Security Update(s))	
765	Warning	Computer Reboot Required	
766	Warning	Network Engine Mode Configuration Incompatibility	
767	Warning	Network Engine Mode Version Incompatibility	
768	Warning	Network Engine Mode Incompatibility Resolved	
770	Warning	Agent/Appliance Heartbeat Rejected	
771	Warning	Contact by Unrecognized Client	
780	Info	Recommendation Scan Failure Resolved	
781	Warning	Recommendation Scan Failure	
782	Info	Rebuild Baseline Failure Resolved	
783	Warning	Rebuild Baseline Failure	
784	Info	Security Update: Security Update Check and Download Successful	
785	Warning	Security Update: Security Update Check and Download Failed	
786	Info	Scan For Change Failure Resolved	
787	Warning	Scan For Change Failure	
790	Info	Agent-Initiated Activation Requested	
791	Warning	Agent-Initiated Activation Failure	
792	Info	Manual Malware Scan Failure Resolved	
793	Warning	Manual Malware Scan Failure	A Malware Scan has failed. Use the Vmware vCenter console to check the status of the VM on which the scan failed.
794	Info	Scheduled Malware Scan Failure Resolved	
795	Warning	Scheduled Malware Scan Failure	A scheduled Malware Scan has failed. Use the Vmware vCenter console to check the status of the VM on which the scan failed.
796	Warning	Scheduled Malware Scan Task has been Missed	This occurs when a scheduled Malware Scan is initiated on a computer when a previous scan is still pending. This typically indicates that Malware Scans are being scheduled too frequently.
797	Info	Malware Scan Cancellation Failure Resolved	
798	Warning	Malware Scan Cancellation Failure	A Malware Scan cancellation has failed. Use the Vmware vCenter console to check the status of the VM on which the scan failed.
799	Warning	Malware Scan Stalled	A Malware Scan has stalled. Use the Vmware vCenter console to check the status of the VM on which the scan stalled.
800	Info	Alert Dismissed	
801	Info	Error Dismissed	
850	Warning	Reconnaissance Detected: Computer OS Fingerprint Probe	
851	Warning	Reconnaissance Detected: Network or Port Scan	
852	Warning	Reconnaissance Detected: TCP Null Scan	
853	Warning	Reconnaissance Detected: TCP SYNFIN Scan	

ID	Severity	Event	Notes
854	Warning	Reconnaissance Detected: TCP Xmas Scan	
900	Info	Deep Security Manager Audit Started	
901	Info	Deep Security Manager Audit Shutdown	
902	Info	Deep Security Manager Installed	
903	Warning	License Related Configuration Change	
910	Info	Diagnostic Package Generated	
911	Info	Diagnostic Package Exported	
912	Info	Diagnostic Package Uploaded	
913	Error	Automatic Diagnostic Package Error	
914	Info	Quarantined File Deletion Succeeded	
915	Info	Quarantined File Deletion Failed	
916	Info	Quarantined File Download Succeeded	
917	Info	Quarantined File Download Failed	
918	Info	Quarantined File Administration Utility Download Succeeded	
919	Info	Quarantined File Not Found	
920	Info	Usage Information Generated	
921	Info	Usage Information Package Exported	
922	Info	Usage Information Package Uploaded	
923	Error	Usage Information Package Error	
924	Warning	Anti-Malware Quarantine Failed (VM limit exceeded)	An infected file could not be quarantined. The maximum space allocated on the Virtual Appliance for storing the quarantined files from this VM was exceeded.
925	Warning	Anti-Malware Quarantine Failed (Quarantine limit exceeded)	An infected file could not be quarantined. The maximum space allocated on the Virtual Appliance for storing all quarantined files was exceeded.
926	Warning	Smart Protection Server Disconnected for Smart Scan	
927	Info	Smart Protection Server Connected for Smart Scan	
928	Info	Quarantined File Restoration Succeeded	
929	Warning	Quarantined File Restoration Failed	
930	Info	Certificate Accepted	
931	Info	Certificate Deleted	
932	Warning	Smart Protection Server Disconnected for Web Reputation	
933	Info	Smart Protection Server Connected for Web Reputation	
934	Info	Software Update: Anti-Malware Windows Platform Update Successful	

ID	Severity	Event	Notes
935	Error	Software Update: Anti-Malware Windows Platform Update Failed	
940	Info	Auto-Tag Rule Created	
941	Info	Auto-Tag Rule Deleted	
942	Info	Auto-Tag Rule Updated	
943	Info	Tag Deleted	
944	Info	Tag Created	
970	Info	Command Line Utility Started	
978	Info	Command Line Utility Failed	
979	Info	Command Line Utility Shutdown	
980	Info	System Information Exported	
990	Info	Manager Node Added	
991	Info	Manager Node Decommissioned	
992	Info	Manager Node Updated	
995	Info	Connection to the Certified Safe Software Service has been restored	
996	Warning	Unable to connect to the Certified Safe Software Service	
997	Error	Tagging Error	
998	Error	System Event Notification Error	
999	Error	Internal Software Error	
1101	Error	Plug-in Installation Failed	
1102	Info	Plug-in Installed	
1103	Error	Plug-in Upgrade Failed	
1104	Info	Plug-in Upgraded	
1105	Error	Plug-in Start Failed	
1106	Error	Plug-in Uninstall Failed	
1107	Info	Plug-in Uninstalled	
1108	Info	Plug-in Started	
1109	Info	Plug-in Stopped	
1110	Error	Software Package Not Found	
1111	Info	Software Package Found	
1500	Info	Malware Scan Configuration Created	
1501	Info	Malware Scan Configuration Deleted	
1502	Info	Malware Scan Configuration Updated	
1503	Info	Malware Scan Configuration Exported	
1504	Info	Malware Scan Configuration Imported	
1505	Info	Directory List Created	
1506	Info	Directory List Deleted	
1507	Info	Directory List Updated	
1508	Info	Directory List Exported	
1509	Info	Directory List Imported	
1510	Info	File Extension List Created	
1511	Info	File Extension List Deleted	
1512	Info	File Extension List Updated	
1513	Info	File Extension List Exported	
1514	Info	File Extension List Imported	

ID	Severity	Event	Notes
1515	Info	File List Created	
1516	Info	File List Deleted	
1517	Info	File List Updated	
1518	Info	File List Exported	
1519	Info	File List Imported	
1520	Info	Manual Malware Scan Pending	
1521	Info	Manual Malware Scan Started	
1522	Info	Manual Malware Scan Completed	
1523	Info	Scheduled Malware Scan Started	
1524	Info	Scheduled Malware Scan Completed	
1525	Info	Manual Malware Scan Cancellation In Progress	
1526	Info	Manual Malware Scan Cancellation Completed	
1527	Info	Scheduled Malware Scan Cancellation In Progress	
1528	Info	Scheduled Malware Scan Cancellation Completed	
1529	Info	Manual Malware Scan Paused	
1530	Info	Manual Malware Scan Resumed	
1531	Info	Scheduled Malware Scan Paused	
1532	Info	Scheduled Malware Scan Resumed	
1533	Info	Computer reboot required for Anti-Malware cleanup task	
1534	Info	Computer reboot required for Anti-Malware protection	
1536	Info	Quick Malware Scan Pending	
1537	Info	Quick Malware Scan Started	
1538	Info	Quick Malware Scan Completed	
1539	Info	Quick Malware Scan Cancellation In Progress	
1540	Info	Quick Malware Scan Cancellation Completed	
1541	Info	Quick Malware Scan Paused	
1542	Info	Quick Malware Scan Failure Resolved	
1543	Warning	Quick Malware Scan Failure	
1544	Info	Quick Malware Scan Resumed	
1550	Info	Web Reputation Settings Updated	
1551	Info	Malware Scan Configuration Updated	
1552	Info	Integrity Configuration Updated	
1553	Info	Log Inspection Configuration Updated	
1554	Info	Firewall Stateful Configuration Updated	
1555	Info	Intrusion Prevention Configuration Updated	
1600	Info	Relay Group Update Requested	
1601	Info	Relay Group Update Success	

ID	Severity	Event	Notes
1602	Error	Relay Group Update Failed	
1603	Info	Security Update: Security Update Rollback Success	
1604	Warning	Security Update: Security Update Rollback Failure	
1650	Warning	Anti-Malware protection is absent or out of date	
1651	Info	Anti-Malware module is ready	
1660	Info	Rebuild Baseline Started	
1661	Info	Rebuild Baseline Paused	
1662	Info	Rebuild Baseline Resumed	
1663	Warning	Rebuild Baseline Failure	
1664	Warning	Rebuild Baseline Stalled	
1665	Info	Rebuild Baseline Completed	
1666	Info	Scan for Integrity Started	
1667	Info	Scan for Integrity Paused	
1668	Info	Scan for Integrity Requested	
1669	Warning	Scan for Integrity Failure	
1670	Warning	Scan for Integrity Stalled	
1671	Info	Scan for Integrity Completed	
1675	Error	Integrity Monitoring Engine Offline	
1676	Info	Integrity Monitoring Engine Back Online	
1677	Error	Trusted Platform Module Error	
1678	Info	Trusted Platform Module Register Values Loaded	
1679	Warning	Trusted Platform Module Register Values Changed	
1680	Info	TPM Checking Disabled	
1700	Info	No Agent Detected	
1800	Error	Deep Security Protection Module Failure	
1900	Info	Cloud Provider Added	
1901	Info	Cloud Provider Removed	
1902	Info	Cloud Provider Updated	
1903	Info	Cloud Provider Synchronization In Progress	
1904	Info	Cloud Provider Synchronization Finished	
1905	Error	Cloud Provider Synchronization Failed	
1906	Info	Cloud Provider Synchronization Requested	
1907	Info	Cloud provider Synchronization Cancelled	
1950	Info	Tenant Created	
1951	Info	Tenant Deleted	
1952	Info	Tenant Updated	
1953	Info	Tenant Database Server Created	
1954	Info	Tenant Database Server Deleted	
1955	Info	Tenant Database Server Updated	
1957	Error	Tenant Initialization Failure	

ID	Severity	Event	Notes
2000	Info	Scan Cache Configuration Object Added	
2001	Info	Scan Cache Configuration Object Removed	
2002	Info	Scan Cache Configuration Object Updated	
2200	Info	Software Update: Anti-Malware Module Installation Started	
2201	Info	Software Update: Anti-Malware Module Installation Successful	
2202	Warning	Software Update: Anti-Malware Module Installation Failed	
2203	Info	Software Update: Anti-Malware Module Download Successful	
2204	Info	Security Update: Pattern Update on Agents/Appliances Successful	
2205	Warning	Security Update: Pattern Update on Agents/Appliances Failed	
2300	Info	Software Update: Web Reputation Module Installation Started	
2301	Info	Software Update: Web Reputation Module Installation Successful	
2302	Warning	Software Update: Web Reputation Module Installation Failed	
2303	Info	Software Update: Web Reputation Download Successful	
2400	Info	Software Update: Firewall Module Installation Started	
2401	Info	Software Update: Firewall Module Installation Successful	
2402	Warning	Software Update: Firewall Module Installation Failed	
2403	Info	Software Update: Firewall Module Download Successful	
2500	Info	Software Update: Intrusion Prevention Module Installation Started	
2501	Info	Software Update: Intrusion Prevention Module Installation Successful	
2502	Warning	Software Update: Intrusion Prevention Module Installation Failed	
2503	Info	Software Update: Intrusion Prevention Module Download Successful	
2600	Info	Software Update: Integrity Monitoring Module Installation Started	
2601	Info	Software Update: Integrity Monitoring Module Installation Successful	

ID	Severity	Event	Notes
2602	Warning	Software Update: Integrity Monitoring Module Installation Failed	
2603	Info	Software Update: Integrity Monitoring Module Download Successful	
2700	Info	Software Update: Log Inspection Module Installation Started	
2701	Info	Software Update: Log Inspection Module Installation Successful	
2702	Warning	Software Update: Log Inspection Module Installation Failed	
2703	Info	Software Update: Log Inspection Module Download Successful	
2800	Info	Software Update: Software Automatically Downloaded	
2801	Error	Software Update: Unable to retrieve Download Center inventory	
2802	Error	Software Update: Unable to download software from Download Center	
2900	Info	Software Update: Relay Module Installation Started	
2901	Info	Software Update: Relay Module Installation Successful	
2902	Warning	Software Update: Relay Module Installation Failed	
2903	Info	Software Update: Relay Module Download Successful	

Agent Events

ID	Severity	Event	Notes
Special Events			
0	Error	Unknown Agent/Appliance Event	
Driver-Related Events			
1000	Error	Unable To Open Engine	
1001	Error	Engine Command Failed	
1002	Warning	Engine List Objects Error	
1003	Warning	Remove Object Failed	
1004	Warning	Engine Returned Bad Rule Data	
1005	Warning	Upgrading Driver	
1006	Warning	Driver Upgrade Requires Reboot	
1007	Warning	Driver Upgrade Succeeded	
1008	Error	Kernel Unsupported	
Configuration-Related Events			
2000	Info	Policy Sent	
2001	Warning	Invalid Firewall Rule Assignment	
2002	Warning	Invalid Firewall Stateful Configuration	
2003	Error	Save Security Configuration Failed	
2004	Warning	Invalid Interface Assignment	
2005	Warning	Invalid Interface Assignment	
2006	Warning	Invalid Action	
2007	Warning	Invalid Packet Direction	
2008	Warning	Invalid Rule Priority	
2009	Warning	Unrecognized IP Format	
2010	Warning	Invalid Source IP List	
2011	Warning	Invalid Source Port List	
2012	Warning	Invalid Destination IP List	
2013	Warning	Invalid Destination Port List	
2014	Warning	Invalid Schedule	
2015	Warning	Invalid Source MAC List	
2016	Warning	Invalid Destination MAC List	
2017	Warning	Invalid Schedule Length	
2018	Warning	Invalid Schedule String	
2019	Warning	Invalid Intrusion Prevention Rule XML Rule	
2020	Warning	Object Not Found	
2021	Warning	Object Not Found	
2022	Warning	Invalid Rule Assignment	
2050	Warning	Firewall Rule Not Found	
2075	Warning	Traffic Stream Not Found	
2076	Warning	Intrusion Prevention Rule Not Found	
2077	Warning	Pattern List Not Found	
2078	Warning	Intrusion Prevention Rule Conversion Error	
2080	Warning	Conditional Firewall Rule Not Found	
2081	Warning	Conditional Intrusion Prevention Rule Not Found	
2082	Warning	Empty Intrusion Prevention Rule	
2083	Warning	Intrusion Prevention Rule XML Rule Conversion Error	
2085	Error	Security Configuration Error	
2086	Warning	Unsupported IP Match Type	
2087	Warning	Unsupported MAC Match Type	
2088	Warning	Invalid SSL Credential	
2089	Warning	Missing SSL Credential	
Hardware-Related Events			

ID	Severity	Event	Notes
3000	Warning	Invalid MAC Address	
3001	Warning	Get Event Data Failed	
3002	Warning	Too Many Interfaces	
3003	Error	Unable To Run External Command	
3004	Error	Unable To Read External Command Output	
3005	Error	Operating System Call Error	
3006	Error	Operating System Call Error	
3007	Error	File Error	
3008	Error	Machine-Specific Key Error	
3009	Error	Unexpected Agent/Appliance Shutdown	
3010	Error	Agent/Appliance Database Error	
3300	Warning	Get Event Data Failed	Linux error.
3302	Warning	Get Security Configuration Failed	Linux error.
3303	Error	File Mapping Error	Linux error. File type error.
3600	Error	Get Windows System Directory Failed	
3601	Warning	Read Local Data Error	Windows error.
3602	Warning	Windows Service Error	Windows error.
3603	Error	File Mapping Error	Windows error. File size error.
3700	Warning	Abnormal Restart Detected	Windows error.
3701	Info	System Last Boot Time Change	Windows error.
Communications-Related Events			
4000	Warning	Invalid Protocol Header	Content length out of range.
4001	Warning	Invalid Protocol Header	Content length missing.
4002	Info	Command Session Initiated	
4003	Info	Configuration Session Initiated	
4004	Info	Command Received	
4011	Warning	Failure to Contact Manager	
4012	Warning	Heartbeat Failed	
Agent-Related Events			
5000	Info	Agent/Appliance Started	
5001	Error	Thread Exception	
5002	Error	Operation Timed Out	
5003	Info	Agent/Appliance Stopped	
5004	Warning	Clock Changed	
5005	Info	Agent/Appliance Auditing Started	
5006	Info	Agent/Appliance Auditing Stopped	
5007	Info	Appliance Protection Change	
5008	Warning	Filter Driver Connection Failed	
5009	Info	Filter Driver Connection Success	
5010	Warning	Filter Driver Informational Event	
5100	Info	Protection Module Deployment Started	
5101	Info	Protection Module Deployment Succeeded	
5102	Error	Protection Module Deployment Failed	
5103	Info	Protection Module Download Succeeded	
5104	Info	Protection Module Disablement Started	
5105	Info	Protection Module Disablement Succeeded	
5106	Error	Protection Module Disablement Failed	
Logging-Related Events			
6000	Info	Log Device Open Error	
6001	Info	Log File Open Error	
6002	Info	Log File Write Error	
6003	Info	Log Directory Creation Error	
6004	Info	Log File Query Error	
6005	Info	Log Directory Open Error	
6006	Info	Log File Delete Error	
6007	Info	Log File Rename Error	

ID	Severity	Event	Notes
6008	Info	Log Read Error	
6009	Warning	Log File Deleted Due To Insufficient Space	
6010	Warning	Events Were Suppressed	
6011	Warning	Events Truncated	
6012	Error	Insufficient Disk Space	
6013	Warning	Agent configuration package too large	
Attack/Scan/Probe-Related Events			
7000	Warning	Computer OS Fingerprint Probe	
7001	Warning	Network or Port Scan	
7002	Warning	TCP Null Scan	
7003	Warning	TCP SYNFIN Scan	
7004	Warning	TCP Xmas Scan	
Download Security Update Events			
9050	Info	Update of Anti-Malware Component on Agent Succeeded	
9051	Error	Update of Anti-Malware Component on Agent Failed	
9100	Info	Security Update Successful	
9101	Error	Security Update Failure	
9102	Error	Security Update Failure	Specific information recorded in error message.
Relay Events			
9103	Info	Relay Web Server Disabled	
9104	Info	Relay Web Server Enabled	
9105	Error	Enable Relay Web Server Failed	
9106	Error	Disable Relay Web Server Failed	
9107	Error	Relay Web Server failed	
9108	Info	Unable to Connect to Update Source	
9109	Error	Component Update Failure	
9110	Error	Anti-Malware license is expired	
9111	Info	Security Update Rollback Success	
9112	Error	Security Update Rollback Failure	
9113	Info	Relay Replicated All Packages	
9114	Error	Relay Failed to Replicate All Packages	
Integrity Scan Status Events			
9201	Info	Integrity Scan Started	
9203	Info	Integrity Scan Terminated Abnormally	
9204	Info	Integrity Scan Paused	
9205	Info	Integrity Scan Resumed	
9208	Warning	Integrity Scan failed to start	
9209	Warning	Integrity Scan Stalled	
Smart Protection Server Status Events			
9300	Warning	Smart Protection Server Disconnected for Web Reputation	
9301	Info	Smart Protection Server Connected for Web Reputation	

Anti-Malware Events

ID	Severity	Event	Notes
9001	Info	Anti-Malware Scan Started	
9002	Info	Anti-Malware Scan Completed	
9003	Info	Anti-Malware Scan Terminated Abnormally	
9004	Info	Anti-Malware Scan Paused	
9005	Info	Anti-Malware Scan Resumed	
9006	Info	Anti-Malware Scan Cancelled	
9007	Warning	Anti-Malware Scan Cancel Failed	
9008	Warning	Anti-Malware Scan Start Failed	
9009	Warning	Anti-Malware Scan Stalled	
9010	Error	Anti-Malware Quarantine Failed (VM limit exceeded)	
9011	Error	Anti-Malware Quarantine Failed (Appliance limit exceeded)	
9012	Warning	Smart Protection Server Disconnected for Smart Scan	
9013	Info	Smart Protection Server Connected for Smart Scan	
9014	Warning	Computer reboot is required for Anti-Malware protection	
9016	Info	Anti-Malware Component Update Successful	
9017	Error	Anti-Malware Component Update Failed	

Intrusion Prevention Events

ID	Event	Notes
200	Region Too Big	A region (edit region, uri etc) exceeded the maximum allowed buffering size (7570 bytes) without being closed. This is usually because the data does not conform to the protocol.
201	Insufficient Memory	The packet could not be processed properly because resources were exhausted. This can be because too many concurrent connections require buffering (max 2048) or matching resources (max 128) at the same time or because of excessive matches in a single IP packet (max 2048) or simply because the system is out of memory.
202	Maximum Edits Exceeded	The maximum number of edits (32) in a single region of a packet was exceeded.
203	Edit Too Large	Editing attempted to increase the size of the region above the maximum allowed size (8188 bytes).
204	Max Matches in Packet Exceeded	There are more than 2048 positions in the packet with pattern match occurrences. An error is returned at this limit and the connection is dropped because this usually indicates a garbage or evasive packet.
205	Engine Call Stack Too Deep	
206	Runtime Error	Runtime error.
207	Packet Read Error	Low level problem reading packet data.
300	Unsupported Cipher	An unknown or unsupported Cipher Suite has been requested.
301	Error Generating Master Key(s)	Unable to derive the cryptographic keys, Mac secrets, and initialization vectors from the master secret.
302	Record Layer Message (not ready)	The SSL state engine has encountered an SSL record before initialization of the session.
303	Handshake Message (not ready)	The SSL state engine has encountered a handshake message after the handshake has been negotiated.
304	Out Of Order Handshake Message	A well formatted handshake message has been encountered out of sequence.
305	Memory Allocation Error	The packet could not be processed properly because resources were exhausted. This can be because too many concurrent connections require buffering (max 2048) or matching resources (max 128) at the same time or because of excessive matches in a single IP packet (max 2048) or simply because the system is out of memory.
306	Unsupported SSL Version	A client attempted to negotiate an SSL V2 session.
307	Error Decrypting Pre-master Key	Unable to un-wrap the pre-master secret from the ClientKeyExchange message.
308	Client Attempted to Rollback	A client attempted to rollback to an earlier version of the SSL protocol than that which was specified in the ClientHello message.
309	Renewal Error	An SSL session was being requested with a cached session key that could not be located.
310	Key Exchange Error	The server is attempting to establish an SSL session with temporarily generated key.
311	Error Generating Pre-Master Request	An error occurred when trying to queue the pre-master secret for decryption.
312	Key Too Large	The master secret keys are larger than specified by the protocol identifier.
313	Invalid Parameters In Handshake	An invalid or unreasonable value was encountered while trying to decode the handshake protocol.
314	No Sessions Available	
315	Compression Method Unsupported	

ID	Event	Notes
500	URI Path Depth Exceeded	too many "/" separators, max 100 path depth.
501	Invalid Traversal	Tried to use "../" above root.
502	Illegal Character in URI	Illegal character used in uri.
503	Incomplete UTF8 Sequence	URI ended in middle of utf8 sequence.
504	Invalid UTF8 encoding	Invalid/non-canonical encoding attempt.
505	Invalid Hex Encoding	%nn where nn are not hex digits.
506	URI Path Length Too Long	path length is greater than 512 characters.
507	Invalid Use of Character	use of disabled char
508	Double Decoding Exploit	Double decoding exploit attempt (%25xx, %25%xxd, etc).
700	Invalid Base64 Content	Packet content that was expected to be encoded in Base64 format was not encoded correctly.
710	Corrupted Deflate/GZIP Content	Packet content that was expected to be encoded in Base64 format was not encoded correctly.
711	Incomplete Deflate/GZIP Content	Incomplete Deflate/GZIP Content
712	Deflate/GZIP Checksum Error	Deflate/GZIP Checksum Error.
713	Unsupported Deflate/GZIP Dictionary	Unsupported Deflate/GZIP Dictionary.
714	Unsupported GZIP Header Format/Method	Unsupported GZIP Header Format/Method.
801	Protocol Decoding Search Limit Exceeded	A protocol decoding rule defined a limit for a search or pdu object but the object was not found before the limit was reached.
802	Protocol Decoding Constraint Error	A protocol decoding rule decoded data that did not meet the protocol content constraints.
803	Protocol Decoding Engine Internal Error	
804	Protocol Decoding Structure Too Deep	A protocol decoding rule encountered a type definition and packet content that caused the maximum type nesting depth (16) to be exceeded.
805	Protocol Decoding Stack Error	A rule programming error attempted to cause recursion or use to many nested procedure calls.
806	Infinite Data Loop Error	

Firewall Events

ID	Event	Notes
100	Out Of Connection	A packet was received that was not associated with an existing connection.
101	Invalid Flags	Flag(s) set in packet were invalid. This could be due to a flag that does not make sense within the context of a current connection (if any), or due to a nonsensical combination of flags. (Firewall Stateful Configuration must be On for connection context to be assessed.)
102	Invalid Sequence	A packet with an invalid sequence number or out-of-window data size was encountered.
103	Invalid ACK	A packet with an invalid acknowledgement number was encountered.
104	Internal Error	
105	CE Flags	The CWR or ECE flags were set and the Firewall Stateful Configuration specifies that these packets should be denied.
106	Invalid IP	Packet's source IP was not valid.
107	Invalid IP Datagram Length	The length of the IP datagram is less than the length specified in the IP header.
108	Fragmented	A fragmented packet was encountered with deny fragmented packets disallowed enabled.
109	Invalid Fragment Offset	
110	First Fragment Too Small	A fragmented packet was encountered, the size of the fragment was less than the size of a TCP packet (no data).
111	Fragment Out Of Bounds	The offsets(s) specified in a fragmented packet sequence is outside the range of the maximum size of a datagram.
112	Fragment Offset Too Small	A fragmented packet was encountered, the size of the fragment was less than the size of a TCP packet (no data).
113	IPv6 Packet	An IPv6 Packet was encountered, and IPv6 blocking is enabled.
114	Max Incoming Connections	The number of incoming connections has exceeded the maximum number of connections allowed.
115	Max Outgoing Connections	The number of outgoing connections has exceeded the maximum number of connections allowed.
116	Max SYN Sent	The number of half open connections from a single computer exceeds that specified in the Firewall Stateful Configuration.
117	License Expired	
118	IP Version Unknown	An IP packet other than IPv4 or IPv6 was encountered.
119	Invalid Packet Info	
120	Internal Engine Error	Insufficient resources.
121	Unsolicited UDP	Incoming UDP packets that were not solicited by the computer are rejected.
122	Unsolicited ICMP	ICMP stateful has been enabled (in Firewall Stateful Configuration) and an unsolicited packet that does not match any Force Allow rules was received.
123	Out Of Allowed Policy	The packet does not meet any of the Allow or Force Allow rules and so is implicitly denied.
124	Invalid Port Command	An invalid FTP port command was encountered in the FTP control channel data stream.
125	SYN Cookie Error	The SYN cookies protection mechanism encountered an error.
126	Invalid Data Offset	Invalid data offset parameter.
127	No IP Header	
128	Unreadable Ethernet Header	Data contained in this Ethernet frame is smaller than the Ethernet header.
129	Undefined	
130	Same Source and Destination IP	Source and destination IPs were identical.
131	Invalid TCP Header Length	

ID	Event	Notes
132	Unreadable Protocol Header	The packet contains an unreadable TCP, UDP or ICMP header.
133	Unreadable IPv4 Header	The packet contains an unreadable IPv4 header.
134	Unknown IP Version	Unrecognized IP version.
135	Invalid Adapter Configuration	An invalid adapter configuration has been received.
136	Overlapping Fragment	This packet fragment overlaps a previously sent fragment.
137	Maximum ACK Retransmit	This retransmitted ACK packet exceeds the ACK storm protection threshold.
138	Packet on Closed Connection	A packet was received belonging to a connection already closed.
139	Dropped Retransmit	Dropped Retransmit.
140	Undefined	
141	Out of Allowed Policy (Open Port)	
142	New Connection Initiated	
143	Invalid Checksum	
144	Invalid Hook Used	
145	IP Zero Payload	
146	IPv6 Source Is Multicast	
147	Invalid IPv6 Address	
148	IPv6 Fragment Too Small	
149	Invalid Transport Header Length	
150	Out of Memory	
151	Max TCP Connections	
152	Max UDP Connections	
200	Region Too Big	A region (edit region, uri etc) exceeded the maximum allowed buffering size (7570 bytes) without being closed. This is usually because the data does not conform to the protocol.
201	Insufficient Memory	The packet could not be processed properly because resources were exhausted. This can be because too many concurrent connections require buffering (max 2048) or matching resources (max 128) at the same time or because of excessive matches in a single IP packet (max 2048) or simply because the system is out of memory.
202	Maximum Edits Exceeded	The maximum number of edits (32) in a single region of a packet was exceeded.
203	Edit Too Large	Editing attempted to increase the size of the region above the maximum allowed size (8188 bytes).
204	Max Matches in Packet Exceeded	There are more than 2048 positions in the packet with pattern match occurrences. An error is returned at this limit and the connection is dropped because this usually indicates a garbage or evasive packet.
205	Engine Call Stack Too Deep	
206	Runtime Error	Runtime error.
207	Packet Read Error	Low level problem reading packet data.
300	Unsupported Cipher	An unknown or unsupported Cipher Suite has been requested.

ID	Event	Notes
301	Error Generating Master Key(s)	Unable to derive the cryptographic keys, Mac secrets, and initialization vectors from the master secret.
302	Record Layer Message (not ready)	The SSL state engine has encountered an SSL record before initialization of the session.
303	Handshake Message (not ready)	The SSL state engine has encountered a handshake message after the handshake has been negotiated.
304	Out Of Order Handshake Message	A well formatted handshake message has been encountered out of sequence.
305	Memory Allocation Error	The packet could not be processed properly because resources were exhausted. This can be because too many concurrent connections require buffering (max 2048) or matching resources (max 128) at the same time or because of excessive matches in a single IP packet (max 2048) or simply because the system is out of memory.
306	Unsupported SSL Version	A client attempted to negotiate an SSL V2 session.
307	Error Decrypting Pre-master Key	Unable to un-wrap the pre-master secret from the ClientKeyExchange message.
308	Client Attempted to Rollback	A client attempted to rollback to an earlier version of the SSL protocol than that which was specified in the ClientHello message.
309	Renewal Error	An SSL session was being requested with a cached session key that could not be located.
310	Key Exchange Error	The server is attempting to establish an SSL session with temporarily generated key.
311	Error Generating Pre-Master Request	An error occurred when trying to queue the pre-master secret for decryption.
312	Key Too Large	The master secret keys are larger than specified by the protocol identifier.
313	Invalid Parameters In Handshake	An invalid or unreasonable value was encountered while trying to decode the handshake protocol.
314	No Sessions Available	
315	Compression Method Unsupported	
500	URI Path Depth Exceeded	too many "/" separators, max 100 path depth.
501	Invalid Traversal	Tried to use "../" above root.
502	Illegal Character in URI	Illegal character used in uri.
503	Incomplete UTF8 Sequence	URI ended in middle of utf8 sequence.
504	Invalid UTF8 encoding	Invalid/non-canonical encoding attempt.
505	Invalid Hex Encoding	%nn where nn are not hex digits.
506	URI Path Length Too Long	path length is greater than 512 characters.
507	Invalid Use of Character	use of disabled char
508	Double Decoding Exploit	Double decoding exploit attempt (%25xx, %25%xxd, etc).
700	Invalid Base64 Content	Packet content that was expected to be encoded in Base64 format was not encoded correctly.
710	Corrupted Deflate/GZIP Content	Packet content that was expected to be encoded in Base64 format was not encoded correctly.

ID	Event	Notes
711	Incomplete Deflate/GZIP Content	Incomplete Deflate/GZIP Content
712	Deflate/GZIP Checksum Error	Deflate/GZIP Checksum Error.
713	Unsupported Deflate/GZIP Dictionary	Unsupported Deflate/GZIP Dictionary.
714	Unsupported GZIP Header Format/Method	Unsupported GZIP Header Format/Method.
801	Protocol Decoding Search Limit Exceeded	A protocol decoding rule defined a limit for a search or pdu object but the object was not found before the limit was reached.
802	Protocol Decoding Constraint Error	A protocol decoding rule decoded data that did not meet the protocol content constraints.
803	Protocol Decoding Engine Internal Error	
804	Protocol Decoding Structure Too Deep	A protocol decoding rule encountered a type definition and packet content that caused the maximum type nesting depth (16) to be exceeded.
805	Protocol Decoding Stack Error	A rule programming error attempted to cause recursion or use to many nested procedure calls.
806	Infinite Data Loop Error	

Integrity Monitoring Events

ID	Severity	Event	Notes
8000	Info	Full Baseline Created	Created when the Agent has been requested to build a baseline or went from 0 Integrity Monitoring Rules to n (causing the baseline to be build). This event includes information on the time taken to scan (ms), and number of entities cataloged.
8001	Info	Partial Baseline Created	Created when the Agent had a security configuration where one or more Integrity Monitoring Rules changed. This event includes information on the time taken to scan (ms), and number of entities catalogued.
8002	Info	Scan for Change Completed	Created when the Agent is requested to do a full or partial on-demand scan. This event includes information on the time taken to scan (ms), and number of CHANGES catalogued. (Ongoing scans for changes based on the FileSystem Driver or the notify do not generate an 8002 event.)
8003	Error	Unknown Environment Variable in Integrity Monitoring Rule	Created when a rule uses a ${env.EnvironmentVar} and "EnvironmentVar" is not a known environment variable. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, and the name of the unknown environment variable.
8004	Error	Bad Base in Integrity Monitoring Rule	Created when a rule contains an invalid base directory/key. For example, specifying a FileSet with a base of "c:\foo\d:\bar" would generate this event, or the invalid value could be the result of environment variable substitution the yields a bad value. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, and the bad base value.
8005	Error	Unknown Entity in Integrity Monitoring Rule	Created when an unknown EntitySet is encountered in an Integrity Monitoring Rule. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, and a comma-separated list of the unknown EntitySet names encountered.
8006	Error	Unsupported Entity in Integrity Monitoring Rule	Created when a known but unsupported EntitySet is encountered in an Integrity Monitoring Rule. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, and a comma-separated list of the unsupported EntitySet names encountered. Some EntitySet types such as RegistryKeySet are platform-specific.
8007	Error	Unknown Feature in Integrity Monitoring Rule	Created when an unknown Feature is encountered in an Integrity Monitoring Rule. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, the type of entity set (ex. FileSet), and a comma-separated list of the unknown Feature names encountered. Examples of valid Feature values are "whereBaseInOtherSet", "status", and "executable".
8008	Error	Unsupported Feature in Integrity Monitoring Rule	Created when a known but unsupported Feature is encountered in an Integrity Monitoring Rule. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, the type of entity set (ex. FileSet), and a comma-separated list of the unsupported Feature names encountered. Some Feature values such as "status" (used for Windows service states) are platform-specific.
8009	Error	Unknown Attribute in Integrity Monitoring Rule	Created when an unknown Attribute is encountered in an Integrity Monitoring Rule. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, the type of entity set (ex. FileSet), and a comma-separated list of the unknown Attribute names encountered. Examples of valid Attribute values are "created", "lastModified" and "inodeNumber".
8010	Error	Unsupported Attribute in Integrity Monitoring Rule	Created when a known but unsupported Attribute is encountered in an Integrity Monitoring Rule. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, the type of entity set (ex. FileSet), and a comma-separated list of the unsupported Attribute names encountered. Some Attribute values such as "inodeNumber" are platform-specific.
8011	Error	Unknown Attribute in Entity Set in Integrity Monitoring Rule	Created when an unknown EntitySet XML attribute is encountered in an Integrity Monitoring Rule. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, the type of entity set (ex. FileSet), and a comma-separated list of the unknown EntitySet attribute names encountered. You would get this event if you wrote <FileSet dir="c:\foo"> instead of <FileSet base="c:\foo">.
8012	Error	Unknown Registry String in Integrity Monitoring Rule	Created when a rule references a registry key that doesn't exist. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, and the name of the unknown registry string.
8013	Error	Invalid WQLSet was used. Namespace or WQL query was missing.	Indicates that the namespace is missing from a WQL query because an integrity rule XML is incorrectly formatted. This can occur only in an advanced case, with custom integrity rules that use and monitor WQL queries.
8014	Error	Invalid WQLSet was used. An	

ID	Severity	Event	Notes
		unknown provider value was used.	
8015	Warning	Inapplicable Integrity Monitoring Rule	Can be caused by a number of reasons, such as platform mismatch, nonexistent target directories or files, or unsupported functionality.
8016	Warning	Suboptimal Integrity Rule Detected	
8050	Error	Regular expression could not be compiled. Invalid wildcard was used.	

Log Inspection Events

ID	Severity	Event	Notes
8100	Error	Log Inspection Engine Error	
8101	Warning	Log Inspection Engine Warning	
8102	Info	Log Inspection Engine Initialized	

Integrity Monitoring Rules Language

The Integrity Monitoring Rules language is a declarative XML-based language that describes the system components and associated attributes that should be monitored by Deep Security. It also provides a means to specify what components within a larger set of components should be excluded from monitoring.

There are two ways to create a new Integrity Monitoring Rule: if you simply want to monitor files for unauthorized changes you can use the "Basic Rule" template. Instructions for using the Basic Rule template can be found in the documentation for the **Integrity Monitoring Rules Properties window** in the Deep Security Manager Interface Guide or the online help.

If you want to create a rule that will monitor other Entities on the computer (directories, registry values, services, etc.) you will have to write a rule using the Integrity Monitoring Rules language. (To create a new Integrity Monitoring Rule using the Integrity Monitoring Rules language, go to **Policies > Common Objects > Rules > Integrity Monitoring Rules > New Integrity Monitoring Rule > Content** and select "Custom (XML)".)

Entity Sets

System components included in an Integrity Monitoring Rule are referred to as "Entities". Each type of component is a class of Entity. For example, files, registry keys, and processes are each a class of Entity. The Integrity Monitoring Rules language provides a tag for describing a set of Entities (an Entity Set) for each class of Entity. The following **Entity Set** types are available to be used in a rule:

- **DirectorySet**: rules will scan the integrity of directories
- **FileSet**: rules will scan the integrity of files
- **GroupSet:** rules will scan the integrity of groups
- **InstalledSoftwareSet**: rules will scan the integrity of installed software
- **PortSet:** rules will scan the integrity of listening ports
- **ProcessSet**: rules will scan the integrity of processes
- **RegistryKeySet**: rules will scan registry keys
- **RegistryValueSet**: rules will scan registry values
- **ServiceSet**: rules will scan the integrity of services
- **UserSet:** rules will scan the integrity of users
- **WQLSet:** rules will monitor the integrity of the results of a Windows Management Instrumentation WQL query statement

A single Integrity Rule can contain contain multiple Entity Sets. This allows you to, for example, secure an application with a single rule that monitors multiple files and registry entries.

(This section describes Entity Sets in general. For detailed information about the individual Entity Sets, see their individual pages:***DirectorySet (page 226)***, ***FileSet (page 228)***, ***GroupSet (page 231)***, ***InstalledSoftwareSet (page 232)***, ***PortSet (page 234)***, ***ProcessSet (page 237)***, ***RegistryKeySet (page 239)***, ***RegistryValueSet (page 241)***, ***ServiceSet (page 243)***, ***UserSet (page 245)***, and ***WQLSet (page 248)***.)

Hierarchies and Wildcards

For Entity Sets that represent a hierarchical data type such as FileSet and RegistryKeySet, section-based pattern matching is supported:

- **/ (forward slash)** : demarcates sections of the pattern to be applied to levels of the hierarchy
- **** (two stars)** : matches zero or more sections

The following wildcards are supported:

- **? (question mark)** : matches one character

- `*` **(one star)** : matches zero or more characters

"Escaping" characters is also supported:

- `\` **(back slash)** : escapes the next character

The pattern is divided into sections using the " `/` " character, with each section of the pattern being applied to successive levels of the hierarchy as long as it continues to match. For example, if the pattern:

/a?c/123/*.java

is applied to the path:

/abc/123/test.java

Then:

- "`a?c` " matches "abc"
- "`123` " matches "123"
- "`*.java` " matches "test.java"

When the pattern is applied to the path:

/abc/123456/test.java

Then:

- "`a?c` " matches "abc"
- " `123` " does *not* match "123456", and so no more matching is performed

The " `**` " notation pattern matches zero or more sections, and so:

/abc/**/*.java

matches both "abc/123/test.java" and "abc/123456/test.java". It would also match "abc/test.java" and "abc/123/456/test.java".

Syntax and Concepts

This section will present some example Integrity Monitoring Rules. The examples will use the **FileSet** Entity Set but the topics and components described are common to all Entity Sets. A minimal Integrity Monitoring Rule could look like this:

```
<FileSet base="C:\Program Files\MySQL">
</FileSet>
```

The "base" attribute specifies the base directory for the FileSet. Everything else about the rule will be relative to this directory. If nothing further is added to the rule, everything (including subdirectories) below the "base" will be monitored for changes.

Note: *The " `*` " and " `?` " wildcards can be used in a "base" attribute string, but only in the last path component of the base. So this is valid:*

`base="C:\program files\CompanyName * Web Server"`

but this is not:

`base="C:\* files\Microsoft Office"`

Within an Entity Set, "include" and "exclude" tags can be used to control pattern matching. These tags have a "key" attribute that specifies the pattern to match against. The source of the key varies by Entity Set. For example, for Files and Directories it is their path, while for Ports it is the unique protocol/IP/portNumber tuple.

Note: *If a path supplied in an include/exclude rule is syntactically invalid, the Agent will generate an "Integrity Monitoring Rule Compile Issue" Agent Event and supply the rule ID and the path (after expansion) as parameters. An example of an invalid path would be* `C:\test1\D:\test2` *since a file name may not contain two volume identifiers.*

Include

The include tag is essentially a white list. Using it means that only those Entities matched by it (or other include tags) will be included. By adding an include tag, the following rule now only monitors changes to files with the name "*.exe" in the "C:\Program Files\MySQL" folder and sub folders:

```
<FileSet base="C:\Program Files\MySQL">
<include key="**/*.exe"/>
</FileSet>
```

"Includes" can be combined. The following rule will monitor changes to files with the names "*.exe" and "*.dll" in the "C:\Program Files\MySQL" folder and sub folders:

```
<FileSet base="C:\Program Files\MySQL">
<include key="**/*.exe"/>
<include key="**/*.dll"/>
</FileSet>
```

It is also possible to combine multiple criteria in a single include block, in which case **all** criteria must be true for a given Entity to be included. The following "include" tag requires that an Entity both end in ".exe" and start with "sample" to be included. Although this requirement could be represented more succinctly, the usefulness of this becomes more apparent as key patterns are combined with other features of the Entity, as described in the "Features" section below.

```
<include>
<key pattern="**/*.exe"/>
<key pattern="**/sample*"/>
</include>
```

The following is another way to express the same requirements:

```
<include key="**/*.exe">
<key pattern="**/sample*"/>
</include>
```

Exclude

The exclude tag functions as a black list of files, removing files from the set that would otherwise be returned. The following (unlikely) example would place everything but temp files under watch.

```
<FileSet base="C:\Program Files\MySQL">
<include key="**"/>
<exclude key="**/*.tmp"/>
</FileSet>
```

The following rule excludes the "MySQLInstanceConfig.exe" from the set of EXEs and DLLs:

```
<FileSet base="C:\Program Files\MySQL">
<include key="**/*.exe"/>
<include key="**/*.dll" />
<exclude key="**/MySQLInstanceConfig.exe"/>
</FileSet>
```

Like the "include" tag, the "exclude" tag can be written to require multiple criteria. The following example shows a multi-criteria "exclude" tag.

```
<exclude>
<key pattern="**/MySQLInstanceConfig*" />
<key pattern="**/*.exe" />
</exclude>
```

Case Sensitivity

The case sensitivity of pattern matching for an include/exclude tag may be controlled by the "casesensitive" attribute. The attribute has three allowed values:

- **true**
- **false**
- **platform**

The default value for this attribute is "platform", which means that the case sensitivity of the pattern will match the platform on which it is running. In the following example, both "Sample.txt" and "sample.txt" would be returned on a Windows system, but only "Sample.txt" would be returned on a Unix system:

```
<FileSet base="C:\Program Files\MySQL">
<include key="**/*Sample*"/>
</FileSet>
```

In this example, only "Sample.txt" would be returned on Windows and Unix:

```
<FileSet base="C:\Program Files\MySQL">
<include key="**/*Sample*" casesensitive="true"/>
</FileSet>
```

> *Note:* *A case sensitive setting of "true" is of limited use on a platform such as Windows which is case insensitive when it comes to most object names.*

Features

The inclusion and exclusion of Entities based on features other than their "key" is also supported for some Entity types. The set of features differs by Entity type. The following example will include all executable files. It does not depend on the file extension as previous examples using file extensions did, but instead will check the first few hundred bytes of the file to determine if it is executable on the given OS.

```
<FileSet base="C:\Program Files\MySQL">
<include key="**" executable="true"/>
</FileSet>
```

Feature attributes must appear in an "include" or "exclude" tag. To use them as part of a multi-criteria include/exclude, they must be specified as attributes of the enclosing include/exclude tag. The following example includes all files that contain the string "MySQL" in their name and are also executable:

```
<include executable="true">
<key pattern="**/*MySQL*"/>
</include>
```

The previous example can be more succinctly expressed as:

```
<include key="**/*MySQL*" executable="true"/>
```

Some feature attributes are simply matches against the value of one of the Entity's attributes. In such cases, wildcard matches using " * " and " ? " are sometimes supported. The help pages for the individual Entity Sets indicate which attributes can be used in include/exclude rules in this way, and whether they support wildcard matching or simple string matching.

Note: *Where wildcard matches are supported, it is important to note that the match is against the string value of the attribute and that no normalization takes place. Constructs available for Entity key matches such as "** " and the use of " / " to separate hierarchical components don't apply. Matching a path name on Windows requires the use of " \ " since that is the character which appears in the value of the attribute being tested, whereas Unix systems will use " / " in path values so matches against Unix paths need to use " / ".*

The following is an example of a feature match using the "state" attribute:

```
<ServiceSet>
<include state="running"/>
</ServiceSet>
```

Note: *Wildcards are not supported in state matches.*

The following example matches any processes where the path of the binary ends in "\notepad.exe":

```
<ProcessSet>
<include path="*\notepad.exe"/>
</ProcessSet>
```

The following example matches any processes where the command-line begins with "/sbin/":

```
<ProcessSet>
<include commandLine="/sbin/*"/>
</ProcessSet>
```

Note: *Be careful when using wildcards. A wildcard expression like " ** " will look at every file in every sub directory beneath "base". Creating a baseline for such an expression can take a lot of time and resources.*

ANDs and ORs

It is possible to express logical ANDs and ORs through the use of multi-criteria includes/excludes and multiple includes/excludes.

There are several ways that a multi criteria include or exclude can be used to express an AND. The most straightforward is to include multiple criteria within a single enclosing tag. The following example shows a simple multi-criteria AND-ing:

```
<include>
<key pattern="**/*MySQL*" />
<key pattern="**/*.exe"/>
</include>
```

As well, any criteria expressed as an attribute of the including tag will be grouped with the enclosed criteria as part of the multi-criteria requirement. The following example shows the previous multi-criteria "include" re-written in this way:

```
<include key="**/*.exe">
<key pattern="**/*MySQL*" />
</include>
```

Finally, if multiple criteria are expressed as attributes of an include/exclude they are treated as an AND:

```
<include executable="true" key="**/*MySQL*" />
```

ORs are expressed simply by the inclusion of multiple include/exclude tags. The following code includes files if their extensions are ".exe" OR ".dll":

```
<include key="**/*.dll" />
<include key="**/*.exe" />
```

Order of Evaluation

All "includes" are processed first, regardless of order of appearance in the rule. If an object name matches at least one "include" tag, it is then tested against the "exclude" tags. It is removed from the set of monitored objects if it matches at least one "exclude" tag.

Entity Attributes

A given Entity has a set of attributes that can be monitored. If no attributes are specified for an Entity Set (i.e. the attributes wrapper tag is not present) then the STANDARD set of attributes for that Entity is assumed. (See the *Shorthand Attributes* sections for the individual Entity Sets.)

However, for a given Entity Set only certain attributes of the Entity may be of interest for Integrity Monitoring. For example, changes to the contents of a log file are most likely expected and allowed. However changes to the permissions or ownership should be reported.

The "attributes" tag of the Entity Sets allows this to be expressed. The "attributes" tag contains a set of tags enumerating the attributes of interest. The set of allowed "attribute" tags varies depending on the Entity Set for which they are being supplied.

> Note: *If the "attributes" tag is present, but contains no entries, then the Entities defined by the rule are monitored for existence only.*

The following example monitors executable files in "C:\Program Files\MySQL" whose name includes "SQL" for changes to their "last modified", "permissions", and "owner" attributes:

```
<FileSet base="C:\Program Files\MySQL" >
<include key="**/*SQL*" executable="true"/>
<attributes>
<lastModified/>
<permissions/>
<owner/>
</attributes>
</FileSet>
```

The following example monitors the "permissions", and "owner" attributes of log files in "C:\Program Files\MySQL":

```
<FileSet base="C:\Program Files\MySQL" >
<attributes>
<permissions/>
<owner/>
</attributes>
<include key="**/*.log" />
</FileSet>
```

In the following example, the STANDARD set of attributes will be monitored. (See Shorthand Attributes, below)

```
<FileSet base="C:\Program Files\MySQL" >
<include key="**/*.log" />
</FileSet>
```

In the following example, no attributes will be monitored. Only the existence of the Entities will be tracked for change.

```
<FileSet base="C:\Program Files\MySQL" >
<attributes/>
<include key="**/*.log" />
</FileSet>
```

Shorthand Attributes

Shorthand attributes provide a way to specify a group of attributes using a single higher level attribute. Like regular attributes the set of allowed values differs based on the Entity Set for which they are being supplied.

Shorthand Attributes are useful in cases where a set of attributes naturally group together, in cases where exhaustively listing the set of attributes would be tedious, and in cases where the set of attributes represented by the high level attribute may change with time or system configuration. An example of each case follows:

Attribute	Description
STANDARD	The set of attributes to monitor for the Entity Set. This is different than "every possible attribute" for the Entity Set. For example, it would not include every possible hash algorithm, just the ones deemed sufficient. For the list of "standard" attributes for each Entity Set, see sections for the individual Entity Sets.
CONTENTS	This is Shorthand for the hash, or set of hashes, of the contents of the file. Defaults to SHA-1.

onChange

An EntitySet may be set to monitor changes in real time. If the onChange attribute of an EntitySet is set to true (the default value) then the entities returned by the EntitySet will be monitored for changes in real time. When a change is detected the Entity is immediately compared against its baseline for variation. If the onChange attribute of an EntitySet is set to false, it will be run only when a baseline is built or when it is triggered via a Scheduled Task or on demand by the Deep Security Manager.

The following sample monitors the MySQL binaries in real time:

```
<FileSet base="C:\Program Files\MySQL" onChange="true">
<include key="**/*.exe"/>
<include key="**/*.dll" />
</FileSet>
```

Environment Variables

Environment variables can be included in the base value used in Entity Sets. They are enclosed in "${}". The variable name itself is prefaced with "env.".

The following example sets the base directory of the FileSet to the path stored in the PROGRAMFILES environment variable:

```
<FileSet base="${env.PROGRAMFILES}"/>
```

Note: The values of referenced environment variables are read and stored by the Deep Security Agent on Agent startup. If the value of an environment variable changes, the Agent must be restarted to register the change.

If a referenced environment variable is not found, the Entity Sets referencing it are not scanned or monitored, but the rest of the configuration is used. An Alert is triggered indicating that the variable is not present. The Agent reports an invalid environment variable using Agent Event "Integrity Monitoring Rule Compile Issue". The ID of the Integrity Monitoring Rule and the environment variable name are supplied as parameters to the Event.

Registry values

Registry values can be included in the base value used in Entity Sets. They are enclosed in ${}. The path to the registry value itself is prefaced with "reg.". The following example sets the base directory of the FileSet to the path stored in the *"HKLM\Software\Trend Micro\Deep Security Agent\InstallationFolder*" registry value:

```
<FileSet base="${reg.HKLM\Software\Trend Micro\Deep Security Agent\InstallationFolder}"/>
```

The example above sets the base directory of the FileSet to the path stored in the *HKLM\Software\Trend Micro\Deep Security Agent\InstallationFolder* registry value.

The values of referenced registry values are read when a new or changed rule is received by the Agent. The Agent also checks all rules at startup time and will rebuild the baseline for affected Rules if any referenced registry values change.

If a referenced registry value is not found, the EntitySets referencing it are not scanned/monitored, but the rest of the configuration is used. An Alert notifying that the variable is not present is raised. The Agent reports an invalid environment variable expansion using Agent Event 8012. The ID of the Integrity Monitoring Rule and the registry value path are supplied as parameters to the Event.

Note: *A wildcard is allowed only in the last hierarchical component of a base name. For example, base="HKLM\Software\ATI*" is valid and will find both "HKLM\Software\ATI" and "HKLM\Software\ATI Technologies"; however, "base="HKLM*\Software\ATI*" is invalid.*

Use of ".."

The ".." convention for referencing a parent directory is supported in all current versions of the Agent. The Agent will attempt to normalize base directory names for FileSet and DirectorySet elements by resolving ".." references and converting Windows short names to long names. For example, on Vista the following FileSet would have a base directory of "C:\Users". On pre-Vista versions of Windows it would be "C:\Documents and Settings"

```
<FileSet base="${env.USERPROFILE}\..">
<include key="*/Start Menu/Programs/Startup/*"/>
</FileSet>
```

Best Practices

Rules should be written to only include objects and attributes that are of significance. This will ensure that no events are reported if other attributes of the object change. For example, your change monitoring policy may place restrictions on permission and ownership of files in " `/bin` ". Your Integrity Monitoring Rule should monitor owner, group, and permissions, but not other attributes like lastModified or hash values.

When using Integrity Monitoring Rules to detect malware and suspicious activity, monitor services, watch for use of NTFS data streams, and watch for executable files in unusual places such as " `/tmp` " or " `${env.windir}\temp` ".

Always be as specific as possible when specifying what objects to include in a rule. The fewer objects you include, the less time it will take to create your baseline and the less time it will take to scan for changes. Exclude objects which are expected to change and only monitor the attributes you are concerned about.

Do not:

- Use " `**/...` " from a top-level of the hierarchy such as " `/` ", "C:\", or " `HKLM\Software` "
- Use more than one content hash type unless absolutely necessary
- Reference user-specific locations such as `HKEY_CURRENT_USER` , `${env.USERPROFILE}` , or `${env.HOME}`

Any of these statements in your Integrity Monitoring Rules will cause performance issues as the Deep Security Agent searches through many items in order to match the specified patterns.

DirectorySet

The DirectorySet tag describes a set of Directories.

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
base	Sets the base directory of the DirectorySet. Everything else in the tag is relative to this directory	Yes	N/A	String values resolving to syntactically valid path (Path is not required to exist) **Note**: UNC paths are allowed by Windows Agents, but require that the remote system allow access by the "LocalSystem" account of the Agent computer. The Agent is a Windows service and runs as LocalSystem, aka NT AUTHORITY\SYSTEM. When accessing a network resource, the LocalSystem uses the computer's credentials, which is an account named *DOMAIN*\MACHINE$. The access token presented to the remote computer also contains the "Administrators" group for the computer, so remote shares must grant read privileges to either the Agent computer's account, the Agent computer's Administrators group, or "Everyone". For testing access to UNC paths, use this technique to launch a Windows command prompt running as a service under the LocalSystem account. With that you can try accessing network & local resources, or launch other applications that will run under the LocalSystem account. If the base value is not syntactically valid, the FileSet will not be processed. The rest of the config will be evaluated.
onChange	Whether the directories returned should be monitored in real time.	No	false	true, false
followLinks	Will this DirectorySet follow symbolic links.	No	false	true, false

Entity Set Attributes

These are the attributes of the Entity that may be monitored by Integrity Monitoring Rules.

- **Created:** Timestamp when the file was created
- **LastModified:** Timestamp when the file was last modified
- **LastAccessed:** Timestamp when the directory was last accessed. On Windows this value does not get updated immediately, and recording of the last accessed timestamp can be disabled as a performance enhancement. See File Times for details. The other problem with this attribute is that the act of scanning a directory requires that the Agent open the directory, which will change its last accessed timestamp.
- **Permissions:** The directory's security descriptor (in SDDL format) on Windows or Posix-style ACLs on Unix systems that support ACLs, otherwise the Unix style rwxrwxrwx file permissions in numeric (octal) format.
- **Owner:** User ID of the directory owner (commonly referred to as the "UID" on Unix)
- **Group:** Group ID of the directory owner (commonly referred to as the "GID" on Unix)
- **Flags:** Windows-only. Flags returned by the GetFileAttributes() Win32 API. Windows Explorer calls these the "Attributes" of the file: Read-only, Archived, Compressed, etc.
- **SymLinkPath:** If the directory is a symbolic link, the path of the link is stored here. On Windows, use the SysInternals "junction" utility to create the Windows equivalent of symlinks.

- **InodeNumber (Unix-only):**
- **DeviceNumber (Unix-only):** Device number of the disk on which the inode associated with the directory is stored

Short Hand Attributes

The following are the Short Hand Attributes, and the attributes to which they map.

- **STANDARD:** Created LastModified Permissions Owner Group Flags (Windows only) SymLinkPath

Meaning of "Key"

Key is a pattern to match against the path of the directory relative to the directory specified by "dir". This is a hierarchical pattern, with sections of the pattern separated by "/" matched against sections of the path separated by the file separator of the given OS.

Sub Elements

- **Include**
- **Exclude**

See the ***general description (page 218)*** of include/exclude for their allowed attributes and sub elements. Only information specific to include/excludes relating to this EntitySet class are included here.

FileSet

The FileSet tag describes a set of Files.

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
base	Sets the base directory of the FileSet. Everything else in the tag is relative to this directory.	Yes	N/A	String values resolving to syntactically valid path (Path is not required to exist). **Note**: UNC paths are allowed by Windows Agents, but require that the remote system allow access by the "LocalSystem" account of the Agent computer. The Agent is a Windows service and runs as LocalSystem, aka NT AUTHORITY\SYSTEM. When accessing a network resource, the LocalSystem uses the computer's credentials, which is an account named *DOMAIN**MACHINE*$. The access token presented to the remote computer also contains the "Administrators" group for the computer, so remote shares must grant read privileges to either the Agent computer's account, the Agent computer's Administrators group, or "Everyone". For testing access to UNC paths, use this technique to launch a Windows command prompt running as a service under the LocalSystem account. With that you can try accessing network & local resources, or launch other applications that will run under the LocalSystem account. If the base value is not syntactically valid, the FileSet will not be processed. The rest of the config will be evaluated.
onChange	Whether the files returned should be monitored in real time.	No	false	true, false
followLinks	Will this FileSet follow symbolic links.	No	false	true, false

Entity Set Attributes

These are the attributes of the FileSet that can be monitored by Integrity Monitoring Rules.

- **Created:** Timestamp when the file was created
- **LastModified:** Timestamp when the file was last modified
- **LastAccessed:** Timestamp when the file was last accessed. On Windows this value does not get updated immediately, and recording of the last accessed timestamp can be disabled as a performance enhancement. See File Times for details. The other problem with this attribute is that the act of scanning a file requires that the Agent open the file, which will change its last accessed timestamp. On Unix, the Agent will use the O_NOATIME flag if it is available when opening the file, which prevents the OS from updating the last accessed timestamp and speeds up scanning.
- **Permissions:** The file's security descriptor (in SDDL format) on Windows or Posix-style ACLs on Unix systems that support ACLs, otherwise the Unix style rwxrwxrwx file permissions in numeric (octal) format.
- **Owner:** User ID of the file owner (commonly referred to as the "UID" on Unix)
- **Group:** Group ID of the file owner (commonly referred to as the "GID" on Unix)
- **Size:** size of the file
- **Sha1:** SHA-1 hash
- **Sha256:**SHA-256 hash
- **Md5:** MD5 hash

- **Flags:** Windows-only. Flags returned by the GetFileAttributes() Win32 API. Windows Explorer calls these the "Attributes" of the file: Read-only, Archived, Compressed, etc.
- **SymLinkPath** (Unix only): If the file is a symbolic link, the path of the link is stored here. Windows NTFS supports Unix-like symlinks, but only for directories, not files. Windows shortcut objects are not true symlinks since they are not handled by the OS; the Windows Explorer handles shortcut files (*.lnk) but other applications that open a *.lnk file will see the contents of the lnk file.
- **InodeNumber** (Unix only)
- **DeviceNumber** (Unix only): Device number of the disk on which the inode associated with the file is stored
- **BlocksAllocated** (Unix only)
- **Growing:** (DSA 7.5+) contains the value "true" if the size of the file stays the same or increases between scans, otherwise "false". This is mainly useful for log files that have data appended to them. Note that rolling over a log file will trigger a change in this attribute.
- **Shrinking:** (DSA 7.5+) contains the value "true" if the size of the file stays the same or decreases between scans, otherwise "false".

Short Hand Attributes

The following are the Short Hand Attributes, and the attributes to which they map.

- **CONTENTS:** Resolves to the content hash algorithm set in **Policy/Computer Editor > Integrity Monitoring > Advanced**.
- **STANDARD:** Created, LastModified, Permissions, Owner, Group, Size, Contents, Flags (Windows only), SymLinkPath (Unix only)

Drives Mounted as Directories

Drives mounted as directories are treated as any other directory, unless they are a network drive in which case they are ignored.

Alternate Data Streams

NTFS based filesystems support the concept of alternate data streams. When this feature is used it behaves conceptually like files within the file.

Note: *To demonstrate this, type the following at the command prompt:*

```
echo plain > sample.txt
echo alternate > sample.txt:s
more < sample.txt
more < sample.txt:s
```

The first "more" will show only the text "plain", the same text that will be displayed if the file is opened with a standard text editor, such as notepad. The second "more", which accesses the "s" stream of sample.txt will display the string "alternate".

For FileSets, if no stream is specified, then all streams are included. Each stream is a separate Entity entry in the baseline. The available attributes for streams are:

- **size**
- **Sha1**
- **Sha256**
- **Md5**
- **Contents**

The following example would include both streams from the demonstration above:

```
<include key="**/sample.txt" />
```

To include or exclude specific streams, the ":" notation is used. The following example matches only the "s" stream on sample.txt and not the main sample.txt stream:

```
<include key="**/sample.txt:s" />
```

Pattern matching is supported for the stream notation. The following example would include sample.txt, but exclude all of its alternate streams:

```
<include key="**/sample.txt" />
<exclude key="**/sample.txt:*" />
```

Meaning of "Key"

Key is a pattern to match against the path of the file relative to the directory specified by "base". This is a hierarchical pattern, with sections of the pattern separated by "/" matched against sections of the path separated by the file separator of the given OS

Sub Elements

- **Include**
- **Exclude**

See the ***general description (page 218)*** of include/exclude for their allowed attributes and sub elements. Only information specific to include/excludes relating to the FileSet Entity Set class are included here.

Special attributes of Include/Exclude for FileSets:

executable

Determines if the file is executable. This does not mean that its permissions allow it to be executed. Instead the contents of the file are checked, as appropriate for platform, to determine if the file is an executable file.

Note: *This is a relatively expensive operation since it requires the Agent to open the file and examine the first kilobyte or two of its content looking for a valid executable image header. Opening and reading every file is much more expensive than simply scanning directories and matching filenames based on wildcard patterns, so any include/exclude rules using "executable" will result in slower scan times than those that do not use it.*

GroupSet

GroupSet represents a set of groups. Note these are local groups only.

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
onChange	Will be monitored in real time	No	false	true, false

Entity Set Attributes

These are the attributes of the entity that can be monitored:

- **Description:** (Windows only) The textual description of the group.
- **Group:** The group ID and name. The group name is part of the entity key, but it's still important to be able to monitor the group ID/ name pairing in case groups are renamed and given new IDs. Operating systems generally enforce security based on its ID.
- **Members:** A comma separated list of the members of the group.
- **SubGroups:** (Windows only) A comma separated list of sub-groups of the group.

Short Hand Attributes

- **Standard:** Group Members SubGroups

Meaning of "Key"

The key is the group's name. This is not a hierarchical EntitySet. Patterns are applied only to the group name. As a result the "**" pattern is not applicable. The following example monitors the "Administrators" group for additions/deletions. (The "Member" attribute is included implicitly because it is a part of the STANDARD set, and no attributes are explicitly listed.)

```
<GroupSet>
<include key="Administrators" />
</GroupSet>
```

Sub Elements

Include Exclude

See the general description of include/exclude for their allowed attributes and sub elements.

InstalledSoftwareSet

Represents a set of installed software. The make-up of the "key" used to uniquely identify an installed application is platform-specific, but it is often a shorthand version of the application name or a unique numeric value.

On Windows the key can be something readable like "FogBugz Screenshot_is1" or it can be a GUID like "{90110409-6000-11D3-8CFE-0150048383C9}". You can examine these by looking at the subkeys of HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

On Linux the key is the RPM package name, as shown by the command:

```
rpm -qa --qf "%{NAME}\n"
```

On Solaris the key is the package name as shown by the **pkginfo** command.

On HPUX the key is the application name as shown by the command:

```
/usr/sbin/swlist -a name
```

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
onChange	Will be monitored in real time	No	false	true, false

Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules. Presence of the attributes is dependent on both the platform and the application itself - installation programs do not necessarily populate all of the attributes.

- **Manufacturer:** The publisher or manufacturer of the application
- **Name:** The friendly name or display name of the application. (Not available on Linux.)
- **InstalledDate:** Date of installation. (Not available on AIX) This is normally returned as YYYY-MM-DD [HH:MM:SS], but many installers on Windows format the date string in a different manner so this format is not guaranteed.
- **InstallLocation:** The directory where the application is installed. (Only available on Windows, Solaris, and HPUX)
- **Parent:** For patches and updates, this gives the key name of this item's parent. Only available on Windows.
- **Size:** The estimated size of the application, if available. On Windows this attribute is read from the "EstimatedSize" registry value under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\*. The value in that location is expressed in KB, so the Agent multiplies it by 1024 before returning the value. Note that not all Windows applications populate the EstimatedSize field in the registry. (This attribute is not available on AIX.)
- **Version:** The version of the installed application. On Windows this comes from the "DisplayVersion" registry value.

Short Hand Attributes

These are the short hand attributes of the Entity and the attributes to which they resolve

- **STANDARD:** InstalledDate, Name, Version

Meaning of "Key"

The key is the name of the installed software. This is not a hierarchical key, so the ** pattern does not apply. On Windows the key is often a GUID, especially for anything installed via the Windows Installer (aka MSI). Use the name="XXX" feature if you need to include/exclude based on the display name rather than the GUID.

The following example would monitor for the addition and deletion of new software.

```
<InstalledSoftwareSet>
<include key="*"/>
<attributes/>
</InstalledSoftwareSet>
```

Sub Elements

- **Include**
- **Exclude**

See the ***general description (page 218)*** of include/exclude for their allowed attributes and sub elements. Only information specific to include/ excludes relating to this EntitySet class are included here.

Special attributes of Include/Exclude for InstalledSoftwareSets:

name (Windows only)

Allows wildcard matching using ? and * on the display name of the application (the "name" attribute of the Entity). For example:

```
<InstalledSoftwareSet>
<include name="Microsoft*"/>
<InstalledSoftwareSet>
```

will match all installed applications whose display name (as shown by the Control Panel) starts with "Microsoft".

manufacturer

Allows wildcard matching using ? and * on the publisher or manufacturer of the application. For example:

```
<InstalledSoftwareSet>
<include manufacturer="* Company "/>
<InstalledSoftwareSet>
```

will match all installed applications whose manufacturer ends with " Company ".

PortSet

Represents a set of listening ports.

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
onChange	Will be monitored in real time	No	false	true, false

Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules.

- **Created:** Windows only - XP SP2+ and Server 2003 SP1+ required. Returned by the GetExtendedTcpTable() or GetExtendedUdpTable() API. Indicates when the bind operation that created this TCP/UDP link occurred.
- **Listeners:** (as of 8.0.0.1063) The number of active listeners on this protocol/address/port combination. This reflects the number of sockets bound-to and listening-on the given port, and may be greater than the number of processes listening on the port if processes bind multiple sockets to the port. This attribute has no value if only one socket is bound to the given port.
- **Path:** Windows only - XP SP2+ and Server 2003 SP1+ required. Gives the short name, if available, of the module that owns the port. On Windows this comes from the GetOwnerModuleFromXxxEntry() APIs. According to Microsoft documentation, the resolution of connection table entries to owner modules is a best practice. In a few cases, the owner module name returned can be a process name, such as "svchost.exe", a service name (such as "RPC"), or a component name, such as "timer.dll".
- **Process:** (Windows only - XP SP2+ and Server 2003 SP1+ required.) Gives the full path, if available, of the module that owns the port. On Windows this comes from the GetOwnerModuleFromXxxEntry() APIs. According to Microsoft documentation, the resolution of connection table entries to owner modules is a best practice.
- **ProcessId:** (Windows only - XP SP2+ and Server 2003 SP1+ required.) Gives the PID of the process that issued the bind for this port.
- **User:** (Linux only). Gives the user that owns the port.

Meaning of "Key"

The key is in the following format:

<PROTOCOL>/<IP ADDRESS>/<PORT>

For example:

tcp/172.14.207.94/80
udp/172.14.207.94/68

IPV6

If the IP address is IPv6 the key is in the same format, but the protocol is TCP6 or UDP6 and the IP address is an IPv6 address as returned by the getnameinfo API:

tcp6/3ffe:1900:4545:3:200:f8ff:fe21:67cf/80
udp6/3ffe:1900:4545:3:200:f8ff:fe21:67cf/68

Matching of the Key

This is not a hierarchical key, so ** is not applicable. Unix-style glob matching is possible using * and ?. The following pattern matches port 80 on the IP addresses 72.14.207.90 through 72.14.207.99:

```
*/72.14.207.9?/80
```

The following pattern matches port 80 on the IP addresses 72.14.207.2, 72.14.207.20 through 72.14.207.29 as well as 72.14.207.200 through 72.14.207.255:

```
*/72.14.207.2*/80
```

The following pattern matches port 80 on any IP.

```
*/80
```

The following example would monitor for any change in the listening ports but ignore port 80 for TCP in IPV4 and IPV6:

```
<PortSet>
<include key="*"/>
<exclude key="tcp*/*/80"/>
</PortSet>
```

Sub Elements

- **Include**
- **Exclude**

See the ***general description (page 218)*** of include/exclude for their allowed attributes and sub elements. Only information specific to include/excludes relating to this EntitySet class are included here.

Special attributes of Include/Exclude for PortSets:

Various other attributes of the port may be used in include/exclude feature tests. These tests compare a value against the value of an attribute of the port; take note of the platform support for various attributes - not all attributes are available across platforms or even platform revisions, hence the use of these tests in include/exclude tags is of limited use. The feature tests support Unix glob-style wildcarding with * and ?, and there is no normalization of path separators or other characters - it is a simple match against the value of the attribute.

Path

Checks for a wildcard match against the path attribute of the port. The following example would monitor ports owned by processes running the main IIS binary:

```
<PortSet>
<include path="*\system32\inetsrv\inetinfo.exe"/>
</PortSet>
```

Process

Checks for a wildcard match against the process attribute of the port. The following example would monitor ports owned by anything running in a svchost.exe or outlook.* binary:

```
<PortSet>
<include process="svchost.exe"/>
<include process="outlook.*"/>
</PortSet>
```

User

Checks for a wildcard match against the user attribute of the port. The following example would monitor ports on a Unix system that were owned by the super-user (root):

```
<PortSet>
<include user="root"/>
</PortSet>
```

ProcessSet

Represents a set of processes.

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
onChange	Will be monitored in real time	No	false	true, false

Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules.

- **CommandLine:** The full command-line as shown by "ps -f" (Unix), "ps w" (Linux), or Process Explorer (Windows).
- **Group:** The group under which the process is running. Under Unix this is the "effective" group ID of the process, which can change over time if the process drops privileges or otherwise switches its effective group credentials. On Windows this is the current Primary Group of the process as returned by the Win32 API GetTokenInformation with a TokenInformationClass of TokenPrimaryGroup. This is the default Primary Group SID for newly created objects. In addition to a Primary Group, processes typically have one or more group credentials associated with them. Those additional group credentials are not monitored by the Agent - they can be viewed on the "Security" tab of the process properties in Process Explorer.
- **Parent:** The PID of the process that created this process.
- **Path:** The full path to the binary of the process. Not available on Solaris 8 & 9 nor HP-UX. On Windows this comes from the GetModuleFileNameEx() API. On Linux and Solaris 10 it comes from reading the symlink /proc/{pid}/exe or /proc/{pid}/path/a.out respectively.
- **Process:** The short name of the process binary (no path). For example, for "c:\windows\notepad.exe" it would be "notepad.exe" and for "/usr/local/bin/httpd" it would be "httpd".
- **Threads:** The number of threads currently executing in the process. Not available on HP-UX.
- **User:** The user under which the process is running. Under Unix this is the "effective" user ID of the process, which can change over time if the process drops privileges or otherwise switches its effective user credentials.

Short Hand Attributes

- **STANDARD:** CommandLine, Group, Parent, Path (where available), Process User

Meaning of "Key"

The key is a combination of the "Process" attribute (the short name of the executable) and the PID. The PID is appended to the name with a path separator in between, ex. notepad.exe\1234 on Windows and httpd/1234 on Unix. The use of the path separator is to allow include/exclude matching of key="abc/*" to work as expected.

Sub Elements

- **Include**
- **Exclude**

See the ***general description (page 218)*** of include for their allowed attributes and sub elements. Only information specific to include/excludes relating to this EntitySet class are included here.

Special attributes of Include/Exclude for ProcessSets:

The following example would monitor the set of running processes for notepad.exe regardless of the PID.:

```
<ProcessSet>
<include key="notepad.exe\*" />
</ProcessSet>
```

Various other attributes of a process can be used in include/exclude feature tests. The feature tests support Unix glob-style wildcarding with * and ?, and there is no normalization of path separators or other characters - it is a simple glob-style match against the value of the attribute.

CommandLine

Checks for a wildcard match against the commandLine attribute of the process. The following example would monitor any process whose command-line matches "*httpd *":

```
<ProcessSet>
<include commandLine="*httpd *" />
</ProcessSet>
```

Group

Checks for a wildcard match against the group attribute of the process. The text version of the group name is used rather than the numeric form: use "daemon" rather than "2" to test for the daemon group on Linux. The following example would monitor any process running as one of the groups root, daemon, or lp:

```
<ProcessSet>
<include group="root" />
<include group="daemon" />
<include group="lp" />
</ProcessSet>
```

Path

Checks for a wildcard match against the path attribute of the process. The path attribute is not available on some platforms. The following example would monitor any process whose binary resides under System32:

```
<ProcessSet>
<include path="*\System32\*" />
</ProcessSet>
```

User

Checks for a wildcard match against the user attribute of the process. The text version of the user name is used rather than the numeric form: use "root" rather than "0" (zero) to test for the superuser on Unix. The following example would monitor any process running as one of the built in system users (ex. NT AUTHORITY\SYSTEM, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE):

```
<ProcessSet>
<include user="NT AUTHORITY\*" />
</ProcessSet>
```

RegistryKeySet

The RegistryKeySet tag describes a set keys in the registry (Windows only).

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
base	Sets the base key of the RegistryKeySet. Everything else in the tag is relative to this key. The base must begin with one of the following registry branch names: HKEY_CLASSES_ROOT (or HKCR), HKEY_LOCAL_MACHINE (or HKLM), HKEY_USERS (or HKU), HKEY_CURRENT_CONFIG (or HKCC)	Yes	N/A	String values resolving to syntactically valid registry key path

Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules.

- **Owner**
- **Group**
- **Permissions**
- **LastModified** ("LastWriteTime" in Windows registry terminology)
- **Class**
- **SecurityDescriptorSize**

Short Hand Attributes

- **STANDARD:** Group, Owner, Permissions, LastModified

Meaning of "Key"

Registry Keys are stored hierarchically in the registry, much like directories in a file system. For the purpose of this language the "key path" to a key is considered to look like the path to a directory. For example the "key path" to the "Deep Security Agent" key of the Agent would be:

HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\Deep Security Agent

The "key" value for includes/excludes for the RegistryValueSet is matched against the key path. This is a hierarchical pattern, with sections of the pattern separated by "/" matched against sections of the key path separated by "\".

Sub Elements

- **Include**
- **Exclude**

See the ***general description (page 218)*** of include for their allowed attributes and sub elements.

RegistryValueSet

A set of Registry values (Windows only).

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
base	Sets the base key of the RegistryValueSet. Everything else in the tag is relative to this key. The base must begin with one of the registry branch names: HKEY_CLASSES_ROOT (or HKCR), HKEY_LOCAL_MACHINE (or HKLM), HKEY_USERS (or HKU), HKEY_CURRENT_CONFIG (or HKCC)	Yes	N/A	String values resolving to syntactically valid registry key

Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules:

- Size
- Type
- Sha1
- Sha256
- Md5

Short Hand Attributes

- **CONTENTS:** Resolves to the content hash algorithm set in **Policy/Computer Editor > Integrity Monitoring > Advanced**.
- **STANDARD:** Size, Type, Contents

Meaning of "Key"

Registry Values are name/value pairs stored under a key in the registry. The key under which they are stored may in turn be stored under another key, very much like files and directories on a file system. For the purpose of this language the "key path" to a value is considered to look like the path to a file. For example, the "key path" to the InstallationFolder value of the Agent would be:

HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\Deep Security Agent\InstallationFolder

The "key" value for includes/excludes for the RegistryValueSet is matched against the key path. This is a hierarchical pattern, with sections of the pattern separated by "/" matched against sections of the key path separated by "\"

Default Value

Each registry key has an unnamed or default value.

This is present for legacy support: http://blogs.msdn.com/oldnewthing/archive/2008/01/18/7145021.aspx

This value can be explicitly specified for inclusion/exclusion by using a trailing "/" in patterns. For example, "**/" will match all subordinate unnamed values, and "*Agent/**/" will match all unnamed values below a key matching "*Agent".

Note: *Registry value names may contain any printable character, including quotes, backslash, the "@" symbol, etc.*

The Agent deals with this in Entity key names by using backslash as an escape character, but only backslashes themselves are escaped. It does this so that it can tell the difference between a value name containing a backslash and a backslash that occurs as part of the registry path. This means that value names which end with a backslash character will match rules designed to match the default/unnamed value.

See the table below for example registry value names and the resulting Entity key.

Value	Escaped Form	Example
Hello	Hello	HKLM\Software\Sample\Hello
"Quotes"	"Quotes"	HKLM\Software\Sample\"Quotes"
back\slash	back\\slash	HKLM\Software\Sample\back\\slash
trailing\	trailing\\	HKLM\Software\Sample\trailing\\
		HKLM\Software\Sample\
@	@	HKLM\Software\Sample\@

Sub Elements

- **Include**
- **Exclude**

See the ***general description (page 218)*** of include/exclude for their allowed attributes and sub elements.

ServiceSet

The ServiceSet element represents a set of services (Windows only). Services are identified by the "service name", which is not the same as the "name" column shown in the Services administrative tool. The service name can be seen in the service properties and is often shorter than the value shown in the "name" column, which is actually the "Display Name" of the service. For example, the Agent has a service name of "ds_agent" and a display name of "Trend Micro Deep Security Agent".

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
onChange	Will be monitored in real time	No	false	true, false

Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules.

- **Permissions:** The service's security descriptor in SDDL format.
- **Owner:** User ID of the service owner
- **Group:** Group ID of the service owner
- **BinaryPathName:** The path plus optional command-line arguments that Windows uses to start the service.
- **DisplayName:** The "display name" of the service as shown in the properties panel of the service.
- **Description:** Description as it appears in the Services panel
- **State:** The current state of the service. One of: stopped, starting, stopping, running, continuePending, pausePending, paused
- **StartType:** How is the service started? One of: automatic, disabled, manual.
- **LogOnAs:** The name of the account that the service process will be logged on as when it runs.
- **FirstFailure:** Action to take the first time the service fails. Format is "delayInMsec,action", where action is one of None, Restart, Reboot, RunCommand.
- **SecondFailure:** Action to take the second time the service fails. Format is "delayInMsec,action", where action is one of None, Restart, Reboot, RunCommand.
- **SubsequentFailures:** Action to take if the service fails for a third or subsequent time. Format is "delayInMsec,action", where action is one of None, Restart, Reboot, RunCommand.
- **ResetFailCountAfter:** Time after which to reset the failure count to zero if there are no failures, in seconds.
- **RebootMessage:** Message to broadcast to server users before rebooting in response to the "Reboot" service controller action.
- **RunProgram:** Full command line of the process to execute in response to the RunCommand service controller action.
- **DependsOn:** Comma separated list of components that the service depends on
- **LoadOrderGroup:** The load ordering group to which this service belongs. The system startup program uses load ordering groups to load groups of services in a specified order with respect to the other groups. The list of load ordering groups is contained in the following registry value: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ServiceGroupOrder
- **ProcessId:** This is the numeric ID of the process that hosts the service. Many services may exist in a single Windows process, but for those that run in their own process, the monitoring of this attribute will allow the system to log service restarts.

Short Hand Attributes

These are the short hand attributes of the Entity and the attributes to which they resolve

- **STANDARD**: Permissions, Owner, Group, BinaryPathName, Description, State, StartType, LogOnAs, FirstFailure, SecondFailure, SubsequentFailures, ResetFailCountAfter, RunProgram, DependsOn, LoadOrderGroup, ProcessId

Meaning of "Key"

The key is the Service's name, which is not necessarily the same as the "name" column shown in the Services administrative tool (that tool shows the "display name" of the service). The service name can be seen in the service properties and is often shorter than the value shown in the "name" column.

Note: *This is not a hierarchical Entity Set. Patterns are applied only to the service name. As a result the ** pattern is not applicable.*

Sub Elements

- **Include**
- **Exclude**

See the ***general description (page 218)*** of include for their allowed attributes and sub elements. Only information specific to include/excludes relating to this Entity Set class are included here.

Special attributes of Include/Exclude for ServiceSets:

state

Include/exclude based on whether the state of the service (stopped, starting, stopping, running, continuePending, pausePending, paused). The following example would monitor the set of running services for change:

```
<ServiceSet>
<include state="running"/>
</ServiceSet>
```

UserSet

The UserSet element represents a set of users. On a Windows system it operates on users local to the system - the same users displayed by the "Local Users and Groups" MMC snap-in. Note that these are *local* users only if the DSA is running on something other than a domain controller. On a domain controller a UserSet element will enumerate all of the domain users, which may not be advisable for extremely large domains.

On Unix systems, the users monitored are whatever the "getpwent_r()" and "getspnam_r()" APIs have been configured to return.

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
onChange	Will be monitored in real time	No	false	true, false

Entity Set Attributes

These are the attributes of the entity that can be monitored:

Common Attributes

- **cannotChangePassword:** True/false indicating if the user is permitted to change their password.
- **disabled:** True/false indicating if the account has been disabled. On Windows systems this reflects the "disabled" checkbox for the user. On Unix systems this will be true if the user's account has expired or if their password has expired and they've exceeded the inactivity grace period for changing it.
- **fullName:** The display name of the user.
- **groups:** A comma-separated list of the groups to which the user belongs.
- **homeFolder:** The path to the home folder or directory.
- **lockedOut:** True/false indicating if the user has been locked out, either explicitly or due to excessive failed password attempts.
- **passwordHasExpired:** True/false indicating if the user's password has expired. Note that on Windows this attribute is only available on Windows XP and newer operating systems. (Not available in AIX)
- **passwordLastChanged:** The timestamp of the last time the user's password was changed. This is recorded by the DSA as the number of milliseconds since Jan 1 1970 UTC - Deep Security Manager renders the timestamp in local time based on this value. Note that on Unix platforms the resolution of this attribute is one day, so the time component of the rendered timestamp is meaningless. (N/A in AIX)
- **passwordNeverExpires:** True/false indicating if the password does not expire.
- **user:** The name of the user as known to the operating system. For example, "Administrator" or "root".

Windows-only Attributes

- **description:** The primary group the user belongs to.
- **homeDriveLetter:** The drive letter to which a network share is mapped as the user's home folder.
- **logonScript:** The path to a script that executes every time the user logs in.
- **profilePath:** A network path if roaming or mandatory Windows user profiles are being used.

Linux-only Attributes

- **group:** The primary group the user belongs to.
- **logonShell:** The path to the shell process for the user.
- **passwordExpiredDaysBeforeDisabled:** The number of days after the user's password expires that the account is disabled. (N/A in AIX)
- **passwordExpiry:** The date on which the user's account expires and is disabled.
- **passwordExpiryInDays:** The number of days after which the user's password must be changed.
- **passwordMinDaysBetweenChanges:** The minimum number of days permitted between password changes.
- **passwordWarningDays:** The number of days before the user's password is to expire that user is warned.

Short Hand Attributes

- **Standard:** cannotChangePassword, disabled, groups, homeFolder, passwordHasExpired, passwordLastChanged, passwordNeverExpires, user, logonScript (Windows-only), profilePath (Windows-only), group (Unix-only), logonShell (Unix-only), passwordExpiryInDays (Unix-only), passwordMinDaysBetweenChanges (Unix-only)

Meaning of "Key"

The key is the username. This is not a hierarchical EntitySet. Patterns are applied only to the user name. As a result the "**" pattern is not applicable.

The following example monitors for any user creations or deletions. (Note that attributes are explicitly excluded so group membership would not be tracked):

```
<UserSet>
<Attributes/>
<include key="*" />
</UserSet>
```

The following example would track the creation and deletion of the "jsmith" account, along with any changes to the STANDARD attributes of the account (since the STANDARD set for this EntitySet is automatically included if no specific attribute list is included):

```
<UserSet>
<include key="jsmith" />
</UserSet>
```

Sub Elements

Include Exclude

See the general description of include for their allowed attributes and sub elements.

Special attributes of Include/Exclude for UserSets

Various other attributes of the user may be used in include/exclude feature tests. These tests compare a value against the value of an attribute of the user; take note of the platform support for various attributes - not all attributes are available across platforms or even platform revisions, hence the use of these tests in include/exclude elements is of limited use. The feature tests support Unix glob-style wildcarding with * and ?, and there is no normalization of path separators or other characters - it is a simple match against the value of the attribute.

- **Disabled:** Does a true/false match against the disabled attribute of the user. The following example would monitor users with a primary group of either "users" or "daemon":

  ```
  <UserSet>
  <include disabled="true"/>
  </UserSet>
  ```

- **Group:** Does a wildcard match against the primary group of the user. This test is only applicable on Unix systems. The following example would monitor users with a primary group of either "users" or "daemon".

  ```
  <UserSet>
  <include group="users"/>
  <include group="daemon"/>
  </UserSet>
  ```

- **LockedOut:** Does a true/false match against the lockedOut attribute of the user.
- **PasswordHasExpired:** Does a true/false match against the passwordHasExpired attribute of the user.
- **PasswordNeverExpires:** Does a true/false match against the passwordNeverExpires attribute of the user.

WQLSet

The WQLSet element describes a result set from a Windows Management Instrumentation WQL query statement. WQL allows SQL-like queries to be made against many different object classes, with the results forming a table of rows where each row represents an object and each column represents the value of a specific attribute of the object.

> Note: *Many WMI queries consume a large amount of time and computer resources. It is easy to inadvertently issue a query that takes several minutes to complete and returns thousands of rows. It is highly recommended that all queries be tested before use in a WQLSet using a program like PowerShell or WMI Explorer.*

Attribute	Description	Required	Default Value	Allowed Values
namespace	Sets the namespace of the WMI query.	Yes	N/A	String values representing a valid WMI namespace. The "root\cimv2" namespace is the one most commonly used when querying Windows operating system objects, but others such as "root\directory\LDAP" and "root\Microsoft\SqlServer\ComputerManagement" can be used. See here for a small script called GetNamespaces.vbs that enumerates the available WMI namespaces on a given host.
wql	A WQL query string.	Yes	N/A	A valid WQL string. The query must include the __Path attribute for each returned object; the Agent uses the __Path attribute as the entity key when storing and reporting results, so each returned WMI object must include a __Path. If using a query string such as "SELECT * FROM ..." the __Path attribute will be available, but if using a more selective query such as "SELECT Name FROM ..." you must explicitly include __Path by writing the query as "SELECT __Path,Name FROM ...".
onChange	Whether the files returned should be monitored in real time.	No	false	true, false
provider	Optionally specifies an alternative WMI namespace provider to use.	No	none	RsopLoggingModeProvider At present this is only required/supported for group policy queries, and "RsopLoggingModeProvider" is the only supported value. Group policy queries are special since it's recommended that the RsopLoggingModeProvider be used to create a snapshot of the policy data that is present on a computer. If you create a snapshot of the policy data, the query can be performed against a consistent set of data before the system overwrites or deletes it during a refresh of policy. Creating a snapshot actually creates a new WMI namespace, so when using provider="RsopLoggingModeProvider" in a WQLSet, the namespace attribute should specify the suffix to be added to the created namespace. For example, a typical temporary namespace created by the RsopLoggingModeProvider would be "\\.\Root\Rsop\NS71EF4AA3_FB96_465F_AC1C_DFCF9A3E9010". Specify namespace="Computer" to query "\\.\Root\Rsop\NS71EF4AA3_FB96_465F_AC1C_DFCF9A3E9010\Computer". Since the temporary namespace is a one-time value, it hampers the ability of the Agent to detect changes since the value appears in the entity key. To avoid this, the Agent will remove the portion of the returned __Path value after \Rsop\ and up to the next backslash when the RsopLoggingModeProvider is used. Entity keys will therefore have prefixes like "\\.\Root\Rsop\Computer" rather than "\\.\Root\Rsop\NS71EF4AA3_FB96_465F_AC1C_DFCF9A3E9010\Computer"
timeout	Specifies a per-row timeout in milliseconds.	No	5000	1-60000 The WMI query is performed in semisynchronous mode, where result rows are fetched one at a time and there is a timeout on the fetching of a single row. If this parameter is not specified, 5000 (5 seconds) is used as the timeout value.

Entity Set Attributes

Each "row" returned by the WQL query is treated as a single Entity for integrity monitoring purposes, with the returned columns representing the attributes of the entity. Since WMI/WQL is an open-ended specification, there is no set list of available/supported attributes. The query and the schema of the WMI object being queried will determine the attributes being monitored.

For example, the WQLSet:

```
<WQLSet namespace="Computer" wql="select * from RSOP_SecuritySettings where precedence=1" provider="RsopLoggingModeProvider" />
```

will return attributes of:

ErrorCode, GPOID, KeyName, SOMID, Setting, Status, id, precedence

whereas a WQLSet that queries network adapters such as:

```
<WQLSet namespace="root\cimv2" wql="select * from Win32_NetworkAdapter where AdapterTypeId = 0" />
```

will return attributes such as:

AdapterType, AdapterTypeId, Availability, Caption, ConfigManagerErrorCode, ConfigManagerUserConfig, CreationClassName Description, DeviceID, Index, Installed, MACAddress, Manufacturer, MaxNumberControlled, Name, PNPDeviceID, PowerManagementSupported, ProductName, ServiceName, SystemCreationClassName, SystemName, TimeOfLastReset

In order to reduce the load on the Agent, it is advisable to explicitly include only the attributes that require monitoring rather than use "select * ..." in queries. This also has the benefit that changes to the WMI schema to add or remove attributes will not be reported as changes to the object unless the attributes are part of the set being monitored. With "select * from Win32_Foobar", a patch to Windows that adds a new attribute to the Win32_Foobar object class would result in the next integrity scan reporting a change for every object of that class since a new attribute has appeared.

The following are some example WMI queries which return desirable Windows system entities.

Query for Windows mounted storage devices: (selecting for * will typically result in 80% returned attributes being null or duplicate values)

```
<WQLSet namespace="root\cimv2" wql="SELECT __Path,DeviceID,VolumeName,VolumeSerialNumber,DriveType,FileSystem,Access,MediaType,Size,FreeSpace FROM Win32_LogicalDisk" />
```

To further the preceding query, the DriveType can be specified to isolate only certain types of mounted logical storage devices, such as type 2 which is a "Removable Disk": (like a removable USB storage drive)

```
<WQLSet namespace="root\cimv2" wql="SELECT __Path,DeviceID,VolumeName,VolumeSerialNumber,DriveType,FileSystem,Access,MediaType,Size,FreeSpace FROM Win32_LogicalDisk WHERE DriveType=2" />
```

(See here for details on the Win32_LogicalDisk class)

USB Storage Device notes: U3 USB devices will mount both a type 2 "Removable Disk" device and a type 3 "Compact Disc" device. Also, the above query is for storage devices only. USB non-storage devices will not be included. USB memory card adapters may appear as a type 1 "No Root Directory" device. A badly or Windows incompatible USB storage device may appear as a type 1 "Unknown" device.

Query for all known System Directories where the Drive is "F:" for relevant attributes:

```
<WQLSet namespace="root\cimv2" wql="SELECT __Path,CreationDate,LastAccessed,LastModified,Drive,Path,FileName,Caption,FileType,Readable,Writeable FROM Win32_Directory WHERE Drive='F:'" />
```

Query for all known System Files where the Drive is "F:" for relevant attributes:

```
<WQLSet namespace="root\cimv2" wql="SELECT __Path,CreationDate,LastAccessed,LastModified,Drive,Path,FileName,Name,FileType,Readable,Writeable FROM CIM_DataFile WHERE Drive='F:'" />
```

Meaning of Key

The key is the "__Path" attribute of the returned WMI object, which is generally of the form:

SystemName\Namespace:WmiObjectClass.KeyAttribute=Value[,KeyAttribute=Value...]

Some examples:

```
\\TEST-DESK\root\cimv2:Win32_QuickFixEngineering.HotFixID="KB958215-IE7",ServicePackInEffect="SP0"
\\TEST-DESK\ROOT\Rsop\NSF49B36AD_10A3_4F20_9541_B4C471907CE7\Computer:RSOP_RegistryValue.
Path="MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\LegalNoticeText",precedence=1
\\TEST-DESK\root\cimv2:BRCM_NetworkAdapter.DeviceID="8"
```

Sub Elements

Include Exclude

See the general description of "include" and "exclude" for their allowed attributes and sub elements.

For WQLSet, "include" and "exclude" sub elements should typically not be required. It is preferable to use WQL to specify the exact set of objects to be monitored since that limits the amount of work done by both the Agent and the host's WMI implementation.

The use of any include/exclude sub elements can only reduce the set of objects returned by the query; the WQL must be changed in order to return additional objects. If it is necessary to use include/exclude elements to further restrict the WQL results, "*"and "?" characters can be used as simple wildcards to match against values of the entity key.

Manually Deactivate/Stop/Start the Agent/Appliance

Deactivating the Agent/Appliance

Deactivation of the Agent/Appliance can normally be done from the Deep Security Manager that is currently managing the Agent/Appliance. If the Deep Security Manager cannot communicate with the Agent/Appliance, you may have to perform the deactivation manually.

To deactivate the Agent on Windows:

1. From a command line, change to the Agent directory (Default is **C:\Program Files\Trend Micro\Deep Security Agent**)
2. Run the following: **dsa_control.exe -r**

To deactivate the Agent on Linux:

1. Run the following: **/opt/ds_agent/dsa_control -r**

To deactivate the Appliance:

- Log into vCenter using the vSphere Client.
- From the **Virtual Agents** tab, select the Appliance and view the console
- Login by pressing F2 and entering the Appliance password (default password is "dsva")
- Select **Reset Appliance**, then confirm

Stopping or Starting the Agent

Stopping or starting the Agent can only be done locally on the host computer.

To start or stop the Agent on Windows:

- Stop: from the command line, run the following: **sc stop ds_agent**
- Start: from the command line, run the following: **sc start ds_agent**

To start or stop the Agent on Linux:

- Stop: run the following: **/etc/init.d/ds_agent stop**
- Start: run the following: **/etc/init.d/ds_agent start**

Stopping or Starting the Appliance

Stopping or starting the Appliance can only be done locally on the host computer.

To start or stop the Appliance on Linux:

- Stop: run the following: **/etc/init.d/ds_agent stop**
- Start: run the following: **/etc/init.d/ds_agent start**

Multi-Node Manager

Deep Security Manager can be run as multiple nodes operating in parallel using a single database. Running the Manager as multiple nodes provides increased reliability, redundant 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 sign in to any node to carry out their tasks. The failure of any node cannot lead to any tasks not being carried out. The failure of any node cannot lead to the loss of any data.

Each node must be running the same version of the Manager software. When performing an upgrade of the Manager software, the first Manager to be upgraded will take over all Deep Security Manager duties and shut down all the other Deep Security Manager nodes. They will appear as "offline" in the **Network Map with Activity Graph** in the **System Activity** panel of the **System Information** page with an indication that an upgrade is required. As the upgrades are carried out on the other nodes, they will automatically be brought back online and begin sharing in the DSM tasks.

Viewing Nodes

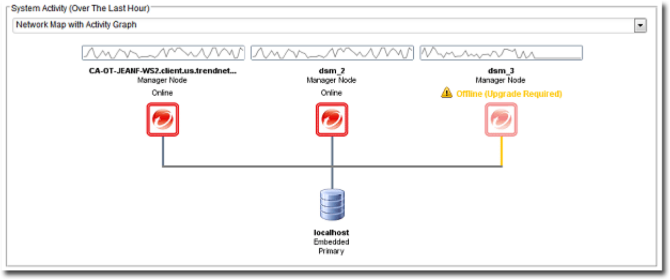
The **Network Map with Activity Graph** in the **System Activity** panel on the **System Information** page displays all Deep Security Manager nodes along with their status, combined activity and jobs being processed.

Note: *The Deep Security Manager processes many concurrent activities in a distributed pool that is executed by all online Manager nodes. All activity not derived from User input is packaged as a job and thus "runnable" on any Manager (with some exceptions for "local" jobs that are executed on each node, like cache clearing).*

The Network Map with Activity Graph

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

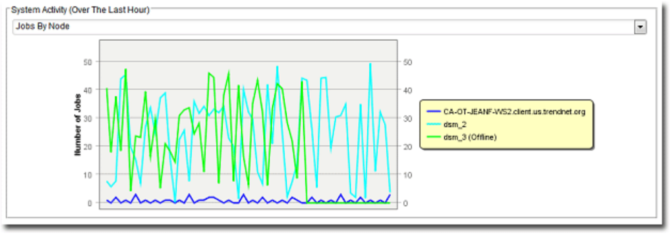
- **Online**
- **Offline**
- **Offline (Upgrade Required)**


System Activity (Over The Last Hour)
Network Map with Activity Graph
CA-OT-JEANF-WS2.client.us.trendnet...
Manager Node
Online
dsm_2
Manager Node
Online
dsm_3
Manager Node
Offline (Upgrade Required)
localhost
Embedded
Primary

Note: *All Deep Security Manager nodes periodically check the health of all other Deep Security Manager nodes. If there is a loss of connectivity with any Deep Security Manager node that lasts longer than three minutes, the node is considered offline and its tasks are redistributed among the remaining nodes.*

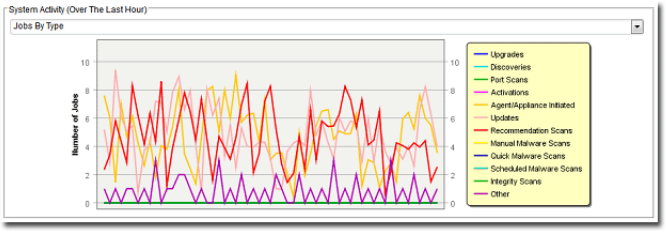
Jobs by Node

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


System Activity (Over The Last Hour)
Jobs By Node
Number of Jobs
0
10
20
30
40
50
CA-OT-JEANF-WS2.client.us.trendnet.org
dsm_2
dsm_3 (Offline)

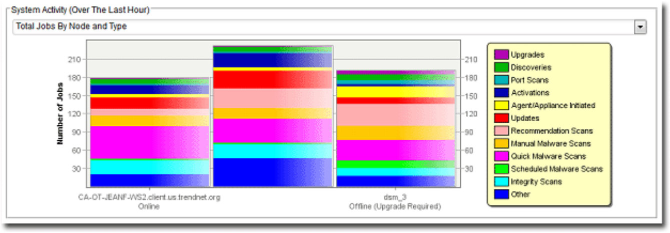
The Jobs by Type

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



Total Jobs by Node and Type

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



Adding Nodes

To add a Deep Security Manager node to the system, run the Manager install package on a new computer. When prompted, type the location of and login credentials for the database being used. Once the installer connects to the database, you can proceed with adding the node to the system. See the Installation Guide for instructions on adding Deep Security Manager nodes.

Note: *You must be using either MS SQL Server or Oracle Database to run multiple nodes.*

Note: *At no point should more than one instance of the installer be running at the same time. Doing so can lead to unpredictable results including corruption of the database.*

Decommissioning Nodes

To decommission a node:

Note: *A node must be offline (uninstalled or service halted) to be decommissioned.*

1. Click on **Managers...** in the System Information page toolbar to display the list of Manager nodes.
2. Double click on the Manager node you want to decommission to display its Properties window.
3. Click the **Decommission** button in the **Options** area.

Performance Requirements

The following guidelines provide a general idea of the infrastructure requirements for Deep Security deployments of different scales.

Disk Space

The amount of space required per computer is a function of the number of logs (events) recorded and how long they are retained. The **Network Engine** tab of the **Policy/Computer Editor > Settings** page allows you to control such settings as the maximum size of the event log files, the number of these log files to retain at any given time. Similarly, the **TCP**, **UDP**, and **ICMP** tabs on a Firewall Stateful Configuration's **Properties** window lets you configure how Firewall Stateful Configuration Event logging is performed.

These Event collection settings can be fine-tuned at the Policy and individual computer level. (See ***Policies, Inheritance and Overrides (page 257)***.)

When logging is left at default levels, an average computer will require approximately 50 MB of database disk space. One thousand computers will require 50 GB, 2000 computers will require 100 GB, etc.

Note: *At their default settings, the following modules generally consume the most disk space, in descending order: Firewall, Integrity Monitoring, Log Inspection.*

Dedicated Servers

The Deep Security Manager and the database can be installed on the same computer if your final deployment is not expected to exceed 1000 computers (real or virtual). If you think you may exceed 1000 computers, the Deep Security Manager and the database should be installed on dedicated servers. It is also important that the database and the Deep Security Manager be co-located to ensure unhindered communication between the two. The same applies to additional Deep Security Manager Nodes: dedicated, co-located servers.

Note: *It is a good idea to run multiple Manager Nodes for redundancy reasons, whether you have 1000 managed computers or not.*

Deep Security Virtual Appliance

You can protect an unlimited number of virtual machines with a Virtual Appliance on a single ESXi server. You will need to set the maximum size of heap memory in the Filter Driver to the size appropriate for the number of virtual machines.

To permanently increase the maximum size of heap memory in the Filter Driver, log in to the console and issue the "esxcfg-module" command and provide a maximum heap size in bytes.

For example, to configure up to 32 virtual machines, do the following:

The formula is:

<number of VMs> * <512 Bytes> * <number of TCP connections (default 10000) + number of UDP connections (default 1000)> + <1MB for vMotion save state>

So for 32 VMs with 10000 connections:

32 * 512Bytes * 2000 + 1000000 = 164832000 Bytes

And the command to set the value is:

```
% esxcfg-module -s DSAFILTER_HEAP_MAX_SIZE=164832000 dvfilter-dsa
```

To verify the setting, execute:

```
% esxcfg-module -g dvfilter-dsa
```

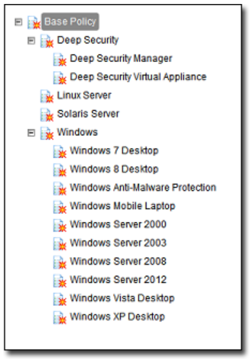
The setting will not take effect until the driver is reloaded. Reloading will either require a reboot (best option) of the ESXi server or unload/ load the driver by executing the commands:

```
% esxcfg-module -u dvfilter-dsa
% esxcfg-module dvfilter-dsa
```

Note: *The above unload/load will require all the protected VMs on the ESXi server and the DVSA to shutdown.*

Policies, Inheritance, and Overrides

Most Deep Security elements and settings operate on multiple hierarchical levels starting a parent Base Policy level, going down through multiple levels of child Policies, and finishing at the level of the Computer to which the final Policy is assigned. Deep Security provides a collection of Policies that you can use as initial templates for the design of your own Policies tailored to your environment:

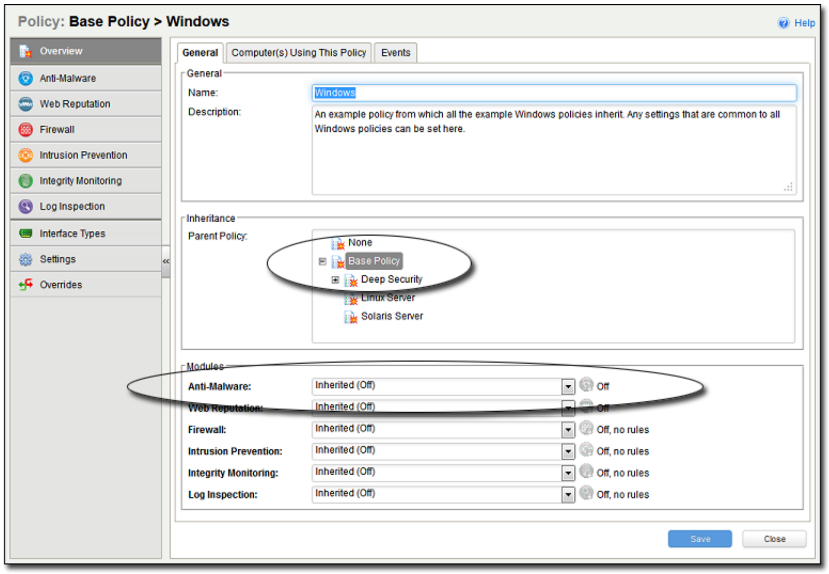


- Base Policy
  - Deep Security
    - Deep Security Manager
    - Deep Security Virtual Appliance
  - Linux Server
  - Solaris Server
  - Windows
    - Windows 7 Desktop
    - Windows 8 Desktop
    - Windows Anti-Malware Protection
    - Windows Mobile Laptop
    - Windows Server 2000
    - Windows Server 2003
    - Windows Server 2008
    - Windows Server 2012
    - Windows Vista Desktop
    - Windows XP Desktop

Inheritance

Child Policies inherit their settings from their parent Policies. This allows you to create a Policy tree that begins with a base parent policy configured with settings and rules that will apply to all computers. This parent policy can then have a set of child and further descendant policies which have progressively more specific targeted settings. Your Policy trees can be built based on any kind of classification system that suits your environment. For example, the **Deep Security** branch in the Policy tree that comes with Deep Security has two child Policies, one designed for a server hosting the Deep Security Manager and one designed for the Deep Security Virtual Appliance. This is a role-based tree structure. Deep Security also has three branches designed for specific operating systems, Linux, Solaris, and Windows. The windows branch has further child Policies for various sub-types of Windows operating systems.

In the **Windows** Policy editor on the **Overview** page, you can see that the **Windows** Policy was created as a child of the **Base** Policy.The Policy's Anti-Malware setting is **Inherited (Off)**:



Policy: Base Policy > Windows

General

Name: Windows

Description: An example policy from which all the example Windows policies inherit. Any settings that are common to all Windows policies can be set here.

Inheritance

Parent Policy:

- None
- Base Policy
  - Deep Security
  - Linux Server
  - Solaris Server

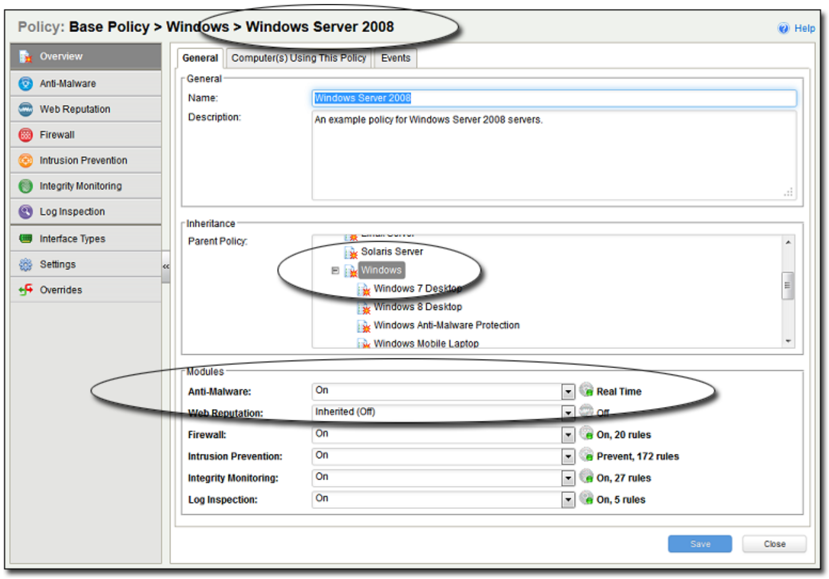
Modules

Anti-Malware:	Inherited (Off)	Off
Web Reputation:	Inherited (Off)	Off
Firewall:	Inherited (Off)	Off, no rules
Intrusion Prevention:	Inherited (Off)	Off, no rules
Integrity Monitoring:	Inherited (Off)	Off, no rules
Log Inspection:	Inherited (Off)	Off, no rules

This means that the setting is inherited from the parent **Base** Policy, and that if you were to change the Anti-Malware setting in the **Base** Policy from **Off** to **On**, the setting would change in the **Windows** Policy as well. (The **Windows** Policy setting setting would then read **Inherited (On)**. The value in parentheses always shows you what the current inherited setting is.)

Overrides

The **Windows Server 2008** Policy is a child Policy of the **Windows** Policy. Here the Anti-Malware setting is no longer inherited -- it is overridden and hard-set to **On**:



Policy: Base Policy > Windows > Windows Server 2008

General

Name: Windows Server 2008

Description: An example policy for Windows Server 2008 servers.

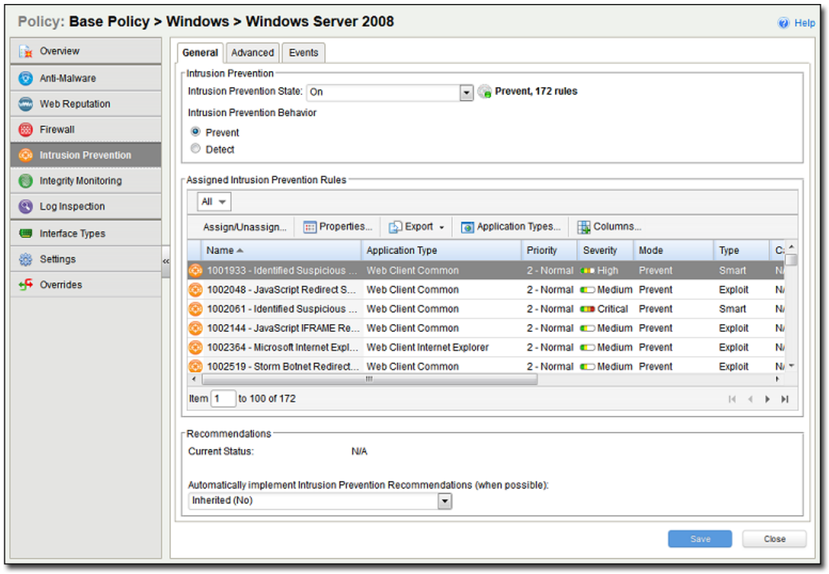
Inheritance

Parent Policy:
- Solaris Server
- Windows
  - Windows 7 Desktop
  - Windows 8 Desktop
  - Windows Anti-Malware Protection
  - Windows Mobile Laptop

Modules

Anti-Malware:	On	Real Time
Web Reputation:	Inherited (Off)	Off
Firewall:	On	On, 20 rules
Intrusion Prevention:	On	Prevent, 172 rules
Integrity Monitoring:	On	On, 27 rules
Log Inspection:	On	On, 5 rules

Looking further into the **Windows 2008 Server** Policy, we can see that Intrusion Prevention is also **On**, and looking at the **Intrusion Prevention** page we see that a set of Intrusion Prevention Rules are assigned:



Policy: Base Policy > Windows > Windows Server 2008

Intrusion Prevention

Intrusion Prevention State: On — Prevent, 172 rules

Intrusion Prevention Behavior

● Prevent
○ Detect

Assigned Intrusion Prevention Rules

Name ▲	Application Type	Priority	Severity	Mode	Type	C:
1001933 - Identified Suspicious ...	Web Client Common	2 - Normal	High	Prevent	Smart	N/
1002048 - JavaScript Redirect S...	Web Client Common	2 - Normal	Medium	Prevent	Exploit	N/
1002061 - Identified Suspicious ...	Web Client Common	2 - Normal	Critical	Prevent	Smart	N/
1002144 - JavaScript IFRAME Re...	Web Client Common	2 - Normal	Medium	Prevent	Exploit	N/
1002364 - Microsoft Internet Expl...	Web Client Internet Explorer	2 - Normal	Medium	Prevent	Exploit	N/
1002519 - Storm Botnet Redirect...	Web Client Common	2 - Normal	Medium	Prevent	Exploit	N/

Item 1 to 100 of 172

Recommendations

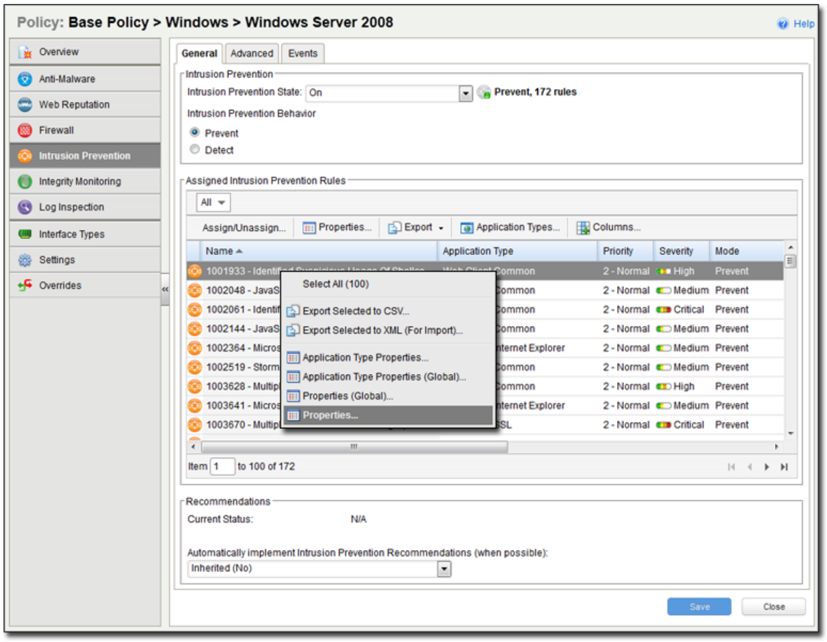
Current Status: N/A

Automatically implement Intrusion Prevention Recommendations (when possible): Inherited (No)

Overriding Object Properties

The Intrusion Prevention Rules that are included in this Policy are copies of the Intrusion Prevention Rules stored by the Deep Security Manager which are available for use by any other Policies. If you want to change the properties of a particular Rule, you have two choices: modify the properties of the Rule globally so that the changes you make apply to all instances where the Rule is in use, or modify the properties locally so that the changes you make only apply locally. The default editing mode in a Computer or Policy editor is **local**. If you click **Properties** on the **Assigned Intrusion Prevention Rules** area toolbar, any changes you make in the Properties window that appears will only apply locally. (Some properties like the Rule name can't be edited locally, only globally.)

Right-clicking a rule displays a context menu which gives you the two Properties editing mode options: selecting **Properties...** will open the local editor window and **Properties (Global)...** will open the global editor window.



Policy: Base Policy > Windows > Windows Server 2008

Intrusion Prevention

Intrusion Prevention State: On — Prevent, 172 rules

Intrusion Prevention Behavior

● Prevent
○ Detect

Assigned Intrusion Prevention Rules

Name	Application Type	Priority	Severity	Mode
1001933 - Identif	Web Client Common	2 - Normal	High	Prevent
1002048 - JavaS	ommon	2 - Normal	Medium	Prevent
1002061 - Identif	ommon	2 - Normal	Critical	Prevent
1002144 - JavaS	ommon	2 - Normal	Medium	Prevent
1002364 - Micros	nternet Explorer	2 - Normal	Medium	Prevent
1002519 - Storm	ommon	2 - Normal	Medium	Prevent
1003628 - Multip	ommon	2 - Normal	High	Prevent
1003641 - Micros	nternet Explorer	2 - Normal	Medium	Prevent
1003670 - Multip	SL	2 - Normal	Critical	Prevent

Item 1 to 100 of 172

Recommendations

Current Status: N/A

Automatically implement Intrusion Prevention Recommendations (when possible): Inherited (No)

Most of the shared Common Objects in Deep Security can have their properties overridden at any level in the Policy hierarchy right down to the individual computer level.

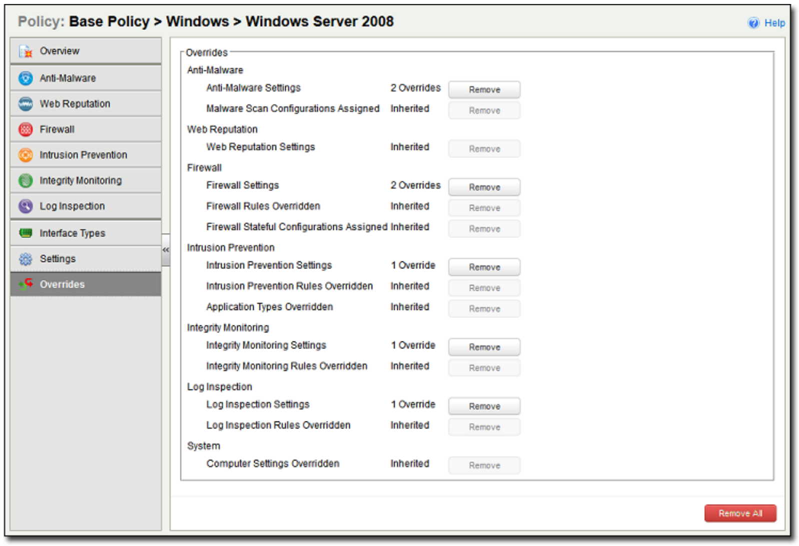
Overriding Rule Assignment

You can always assign additional Rules at any Policy or computer level. However, Rules that are in effect at a particular Policy or computer level because their assignment is inherited from a parent Policy cannot be unassigned locally. They must be unassigned at the Policy level where they were initially assigned.

If you find yourself overriding a large number of settings, you should probably consider branching your parent Policy.

Seeing the Overrides on a Computer or Policy at a glance

You can see the number of settings that have been overridden on a Policy or a computer by going to the **Overrides** page in the computer or Policy Editor:



Policy: **Base Policy > Windows > Windows Server 2008**

Overrides

Anti-Malware		
Anti-Malware Settings	2 Overrides	Remove
Malware Scan Configurations Assigned	Inherited	Remove
Web Reputation		
Web Reputation Settings	Inherited	Remove
Firewall		
Firewall Settings	2 Overrides	Remove
Firewall Rules Overridden	Inherited	Remove
Firewall Stateful Configurations Assigned	Inherited	Remove
Intrusion Prevention		
Intrusion Prevention Settings	1 Override	Remove
Intrusion Prevention Rules Overridden	Inherited	Remove
Application Types Overridden	Inherited	Remove
Integrity Monitoring		
Integrity Monitoring Settings	1 Override	Remove
Integrity Monitoring Rules Overridden	Inherited	Remove
Log Inspection		
Log Inspection Settings	1 Override	Remove
Log Inspection Rules Overridden	Inherited	Remove
System		
Computer Settings Overridden	Inherited	Remove

Overrides are displayed by protection module. You can revert system or module overrides by clicking the **Remove** button.

Ports Used

Deep Security Manager

Port: 4119 (default)

- Use:
  - Access to Deep Security Manager Web console browser interface.
  - Access to Deep Security Manager by an ESXi server to request the Deep Security Filter Driver during the preparation of an ESXi server for Anti-Malware protection.
  - Requests for Security Updates by the Deep Security Virtual Appliance.
- Protocol: TCP
- Initiated By:
  - Web Browser
  - ESXi server
  - Deep Security Virtual Appliance
- Connected To: Deep Security Manager
- Proxy: No
- Configuration: This port is configured during the Deep Security Manager installation process.

Port: 4120 (default)

- Use: Agent/Appliance-initiated communication with the Manager. The Agent/Appliance sends Events to the Manager, and the Manager sends Configuration Updates.
- Protocol: TCP
- Initiated By: Agent/Appliance
- Connected To: Deep Security Manager
- Proxy: No
- Configuration: This port is configured during the Deep Security Manager installation process.

Agent/Appliance

Port: 4118

- Use: Manager-to-Agent/Appliance communication.
- Protocol: TCP
- Initiated By: Deep Security Manager
- Connected To: Agent/Appliance
- Proxy: No
- Configuration: This port is not configurable. (Contact your support provider if this port assignment is problematic.)

Deep Security Relay

Port: 4122

- Use: Agent-to-Relay communication
- Protocol: TCP
- Initiated By: Relays and Agents
- Connected To: Deep Security Relay
- Proxy: No
- Configuration: This port is configured during the Deep Security Manager installation process.

Port: 4123

- Use: Internal Relay communication
- Protocol: TCP
- Initiated By: Relay (internally to localhost)
- Connected To: Deep Security Relay
- Proxy: No
- Configuration: This port is not configurable and is invisible to outside machines.

SQL Server Database Server

Port: 1433, 1434

- Use: Manager-to-database communication (required to connect the database to the Deep Security Manager)
- Protocol: TCP for 1433, UDP for 1434
- Initiated By: Deep Security Manager
- Connected To: SQL database server
- Proxy: No
- Configuration: This port is configured during the Deep Security Manager installation process.

Oracle Database Server

Port: 1521

- Use: Manager-to-database communication (required for SQL if you are using Oracle)
- Protocol: TCP
- Initiated By: Deep Security Manager
- Connected To: Oracle database server
- Proxy: No
- Configuration: This port is configured during the Deep Security Manager installation process.

Syslog Facility

Port: 514 (default)

- Use: Syslog
- Protocol: UDP
- Initiated By: Agent/Appliance
- Connected To: Syslog facility
- Proxy: No
- Configuration: This port can be configured in **Administration > System Settings > SIEM**.

SMTP Server

Port: 25 (default)

- Use: E-mail Alerts
- Protocol: TCP
- Initiated By: Deep Security Manager
- Connected To: Specified SMTP server
- Proxy: No
- Configuration: This port can be configured in **Administration > System Settings > SMTP**.

Trend Micro Update Server

Port: 80

- Use: Connection to Trend Micro Update Server
- Protocol: HTTP and SOCKS
- Initiated By: Deep Security Manager
- Connected To: Trend Micro Update Server
- Proxy: Yes (optional)
- Configuration: The proxy address and port can be configured in **Administration > System Settings > Updates**.

Port: 443

- Use: Connection to Trend Micro Update Server
- Protocol: HTTP and SOCKS
- Initiated By: Deep Security Relay
- Connected To: Trend Micro Update Server
- Proxy: Yes (optional)
- Configuration: The proxy address and port can be configured in **Administration > System Settings > Updates**.

LDAP Server

Port: 389

- Use: LDAP directory addition or Deep Security Manager
- Protocol: TCP
- Initiated By: Deep Security Manager
- Connected To: LDAP server
- Proxy: No
- Configuration: This port can be configured in the **Add Directory** wizard on the **Computers** page.

Smart Protection Network (Global Server)

Port: 80

- Use: Web Reputation Service
- Protocol: TCP
- Initiated By: Deep Security Agent/Appliance
- Connected To: Smart Protection Network
- Proxy: Yes (optional)
- Configuration: The proxy address and port can be configured in **Policy/Computer Editor > Web Reputation> Smart Protection**.

Port: 443

- Use: Smart Feedback and File Reputation Service
- Protocol: TCP
- Initiated By: Deep Security Manager and Deep Security Agent/Appliance
- Connected To: Smart Protection Network
- Proxy: Yes (optional)
- Configuration: The Smart Protection Network proxy address and port can be configured in **Policy/Computer Editor > Anti-Malware > Smart Protection**.

Smart Protection Server (Locally Installed)

Port: 5274

- Use: Web Reputation Service
- Protocol: TCP
- Initiated By: Deep Security Agent/Appliance
- Connected To: Smart Protection Server
- Proxy: Yes (optional)

- Configuration: The proxy address and port can be configured in **Policy/Computer Editor > Web Reputation> Smart Protection**.

Port: 443

- Use: File Reputation Service
- Protocol: TCP
- Initiated By: Deep Security Agent/Appliance
- Connected To: Smart Protection Server
- Proxy: Yes (optional)
- Configuration: The proxy address and port can be configured in **Policy/Computer Editor > Anti-Malware > Smart Protection**.

Certified Safe Software Service

Port: 443

- Use: Certified Safe Software Service
- Protocol: TCP
- Initiated By: Deep Security Manager
- Connected To: Certified Safe Software Service
- Proxy: Yes (optional)
- Configuration: The Certified Safe Software Service HTTP proxy can be configured on the **Administration > System Settings > Updates** tab.

DNS Server

Port: Randomly selected

- Use: DNS lookup for hostnames
- Protocol: TCP
- Initiated by: Deep Security Manager
- Connected to: DNS server
- Proxy: No
- Configuration: The port is randomly selected when the Deep Security Manager needs to lookup a hostname.

ESXi server

Port: 443

- Use: the Deep Security Manager communicates with the ESXi server on port 443 when you deploy an Virtual Appliance to the ESXi
- Protocol: HTTPS
- Initiated by: Deep Security Manager

- Connected to: ESXi server
- Proxy: No
- Configuration: No configuration required.
- Notes: The vCenter provides three URLs on the ESXi to the Deep Security Manager to upload the three vmdk's that make up the Virtual Appliance. Deep Security Manager establishes an HTTPS connection and POSTS the vmdk's to the ESXi.

Local Software Distribution Web Server

Port: 80 or 443

- Use: Agents can be configured to request their Software Updates from these web servers instead of Deep Security Relays
- Protocol: HTTP or HTTPS
- Initiated by: Deep Security Agent
- Connected to: Local software distribution server
- Proxy: No
- Configuration: No configuration required. Port is defined in web server url.
- Notes: For information on configuring software distribution web servers, see ***Configuring a Software Web Server (page 177)***.

Teamed NICs

Installing the Windows and Solaris Agents in a Teamed NICs Environment

"Teamed NICs" describes using multiple Ethernet adapters in parallel to increase data transfer speed or to provide redundancy. The following information provides guidance for configuring teamed NICs installations in Windows and Solaris so that they are compatible with the Deep Security Agent. If you encounter difficulties, please contact your support provider.

Windows

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 to 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. To function properly, the Agent must be bound only to the virtual interface created by the teaming software.

Note: *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*

Note: *Using the Agent in a teamed NICs environment on Windows 2000 is not supported.*

Note: *The Agent's network driver is bound to the network interfaces only at install or upgrade time. After installation, it is not possible 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 host 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.*

Solaris

IPMP failover (active-standby) mode in Solaris allows two NICs to have the same hardware (MAC) address. Since the Deep Security Agent identifies adapters by their MAC address, such duplication prevents the Agent from functioning properly.

The solution is to manually assign unique MAC addresses to each adapter.

Sample ifconfig output:

```
# ifconfig -a
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
inet 10.20.30.40 netmask 0
ether 8:0:20:f7:c3:f

hme1: flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 8
inet 0.0.0.0 netmask 0
ether 8:0:20:f7:c3:f
```

The "ether" line displays the adapter's MAC address. If any interfaces are showing identical MAC addresses and are connected to the same subnet, new unique MAC addresses must be set manually using the following ifconfig command:

```
# ifconfig <interface> ether <new MAC address>
```

Although the chance of a MAC address conflict is extremely small, you should verify that there isn't one by using the snoop command to search for the chosen MAC address. Then use the ping command to test connection to the broadcast address of the subnet.

Note: *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.*

The Deep Security Virtual Appliance Interface

The Deep Security Virtual Appliance interface can be accessed by opening the VMware vSphere Client, selecting the Appliance in the navigation panel, and clicking on the **Console** tab.

System Information

Displays the Appliance version and build number, the URL of the Deep Security Manager managing this Appliance, and the time zone of the Appliance.

Configure Password

The current password for Accessing this Appliance console. The default password ("dsva") should be changed after installation.

Configure Management Network

Displays the Appliance hostname and IP address. Initially the Appliance is given the default hostname "dsva". The IP address is assigned by the local DHCP server. If you do not have a DHCP server, you must enter the IP Address, Netmask, Default gateway, Primary DNS, and Secondary DNS information manually. (Hit Enter to enter editing mode.)

Note: *If you are deploying multiple Virtual Appliances, make sure to change the hostnames to avoid DNS problems.*

Support

Please visit the Trend Micro customer support Web site for assistance with any of your Trend Micro Products:

Trend Micro Customer Support

Privacy Policy

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

TREND MICRO

TREND MICRO INCORPORATED
10101 North De Anza Blvd. Cupertino, CA., 95014, USA
Tel:+1(408)257-1500/1-800 228-5651   Fax:+1(408)257-2003   info@trendmicro.com

www.trendmicro.com

Item Code: APEM96331/140306