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

http://www.trendmicro.com/download

Trend Micro, the Trend Micro t-ball logo, Deep Security, Control Server Plug-in, Damage Cleanup Services, eServer Plug-in, InterScan, Network VirusWall, ScanMail, ServerProtect, and TrendLabs are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Document version: 1.0
Document number: APEM95863/130213
Release date: April 2013
Document generated: May 15, 2013 (9:33:43)
# Table of Contents

**Introduction** ........................................................................................................................................... 8

- About Deep Security ................................................................................................................................. 9
- System Requirements ................................................................................................................................. 13
- What's New in Deep Security 9 SP1 ........................................................................................................... 15

**The Deep Security Manager Console** ................................................................................................... 19

- Dashboard .................................................................................................................................................. 20
- Alerts ............................................................................................................................................................ 22
- Events and Reports ..................................................................................................................................... 23
  - System Events ......................................................................................................................................... 24
  - Anti-Malware Events ............................................................................................................................... 26
  - Quarantined Files ..................................................................................................................................... 29
- Web Reputation Events .............................................................................................................................. 32
- Firewall Events .......................................................................................................................................... 35
- Intrusion Prevention Events ...................................................................................................................... 38
- Integrity Monitoring Events ...................................................................................................................... 41
- Log Inspection Events .............................................................................................................................. 43
- Generate Reports ....................................................................................................................................... 46
- Computers .................................................................................................................................................. 48
- Computer and Agent ................................................................................................................................. 60
- Policies ....................................................................................................................................................... 65
- Policies ....................................................................................................................................................... 67
  - Firewall Rules ......................................................................................................................................... 69
  - Intrusion Prevention Rules ................................................................................................................... 74
    - Application Types ............................................................................................................................... 78
  - Integrity Monitoring Rules ................................................................................................................... 80
  - Log Inspection Rules .......................................................................................................................... 84
- Common Objects ......................................................................................................................................... 87
- Contexts ..................................................................................................................................................... 88
- Firewall Stateful Configurations ............................................................................................................... 90
- Malware Scan Configurations ................................................................................................................ 94
- Schedules .................................................................................................................................................. 103
- Tags ............................................................................................................................................................ 104
- Directory Lists ......................................................................................................................................... 105
- File Extension Lists ............................................................................................................................... 109
General..................................................................................................................................................................................... 164
Advanced.......................................................................................................................................................................................... 165
Events............................................................................................................................................................................................... 166
Interfaces/Interface Types .................................................................................................................................................................. 167
Settings........................................................................................................................................................................................... 168
  Computer......................................................................................................................................................................................... 169
  Network Engine.............................................................................................................................................................................. 173
  Scanning......................................................................................................................................................................................... 179
  SIEM ............................................................................................................................................................................................. 180
Updates (Computer Editor only)..................................................................................................................................................... 181
Overrides.......................................................................................................................................................................................... 182
Administration.................................................................................................................................................................................. 183
  System Settings................................................................................................................................................................................ 184
    Tenants......................................................................................................................................................................................... 185
    Agents.......................................................................................................................................................................................... 188
    Alerts.......................................................................................................................................................................................... 191
    Contexts ..................................................................................................................................................................................... 192
    SIEM .......................................................................................................................................................................................... 193
    SNMP......................................................................................................................................................................................... 194
    Ranking........................................................................................................................................................................................ 195
    System Events.............................................................................................................................................................................. 197
    Security....................................................................................................................................................................................... 198
    Updates ...................................................................................................................................................................................... 200
    Smart Feedback......................................................................................................................................................................... 202
    SMTP ......................................................................................................................................................................................... 203
    Storage ....................................................................................................................................................................................... 204
    Advanced.................................................................................................................................................................................... 205
  Scheduled Tasks..............................................................
  Event-Based Tasks.......................................................... 208
Manager Nodes.................................................................................................................................................................................. 210
  Tenants.......................................................................................................................................................................................... 213
  Licenses........................................................................................................................................................................................ 215
  Users............................................................................................................................................................................................ 216
  Roles............................................................................................................................................................................................ 217
  Contacts........................................................................................................................................................................................ 221
  System Information....................................................................................................................................................................... 225
  Updates........................................................................................................................................................................................ 227
The Deep Security Virtual Appliance Interface........................................................................................................................ 229

Configuration and Management......................................................................................................................................................... 232
Multi-Tenancy (Advanced) ......................................................................................................................... 414
Protecting a Mobile Laptop .......................................................................................................................... 421

Reference ...................................................................................................................................................... 433

Advanced Logging Policy Modes .................................................................................................................. 434
Command-Line Instructions .......................................................................................................................... 437
Communication .............................................................................................................................................. 446
More About Event Tagging ............................................................................................................................ 447
Disabling Diffie-Hellman in Apache ............................................................................................................ 451
Encrypting DSM to DB Communication ..................................................................................................... 452
Agent ............................................................................................................................................................. 454
Intrusion Prevention Events .......................................................................................................................... 467
Firewall Events ............................................................................................................................................ 471
System Events ............................................................................................................................................. 474
Policies, Inheritance, and Overrides ........................................................................................................... 505
Integrity Monitoring Rules Language .......................................................................................................... 510
DirectorySet ................................................................................................................................................ 522
FileSet ......................................................................................................................................................... 525
GroupSet ................................................................................................................................................... 529
InstalledSoftwareSet .................................................................................................................................. 531
PortSet ......................................................................................................................................................... 534
ProcessSet .................................................................................................................................................. 537
RegistryKeySet .......................................................................................................................................... 540
RegistryValueSet ....................................................................................................................................... 542
ServiceSet .................................................................................................................................................. 545
UserSet ....................................................................................................................................................... 548
WQLSet ......................................................................................................................................................... 552
Manually Deactivate/Stop/Start the Agent .................................................................................................... 556
Manually Upgrade the Agent on a Computer ............................................................................................... 558
Multi-Node Manager .................................................................................................................................. 560
Performance Requirements .......................................................................................................................... 563
Ports Used by Deep Security .......................................................................................................................... 565
Teamed NICs ................................................................................................................................................ 571
Support ........................................................................................................................................................ 573
Introduction
About Deep Security

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 bi-directional 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 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.

• **Deep Security Relay**: The Deep Security Relay delivers updates to the Agents and Virtual Appliances. The Relay has an embedded Agent to provide local protection on the host machine.


### 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 runs as a VMware virtual machine and protects the other virtual machines on the same ESX 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.

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.
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**: Microsoft Windows 2012 (64-bit), Windows Server 2008 (64-bit), Windows Server 2008 R2 (64-bit), Windows 2003 Server SP2 (64-bit), Red Hat Linux 5/6 (64-bit)
- **Database**: Oracle 11g, Oracle 10g, Microsoft SQL Server 2012 (All Service Packs), Microsoft SQL Server 2008 (All Service Packs)
- **Web Browser**: Firefox 12+, Internet Explorer 8.x, Internet Explorer 9.x, Internet Explorer 10.x, Chrome 20+, Safari 5+. (Cookies must be enabled in all browsers.)

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

Deep Security Virtual Appliance

- **Memory**: 2GB
- **Disk Space**: 20GB
- **Operating System**: VMware vCenter 5.x and ESX/ESXi 5.x

*Note*: For specifics about the VMware vShield environment see the Installation Guide.

Deep Security Agent

- **Memory**:
  - with Anti-Malware: 512MB
  - without Anti-Malware: 128MB
- **Disk Space**: 500MB
- **Supported Platforms**: Windows, Solaris, Linux, AIX, HP-UX

*Note*: Trend Micro endeavors to provide Deep Security Agents for new versions of each platform as they are released and may discontinue support for retired versions. See the Installation Guide and release notes for the currently supported versions of each platform.

*Note*: The HP-UX Agents only support Integrity Monitoring and Log Inspection. For the latest information, consult the Install Guide and the Agent release notes.
Windows Agents running on Windows XP or Windows 2003 will not function in an IPv6 environment.

Agent-based Malware Scans on Linux are supported only on Red Hat 4 32-bit and Red Hat 5/6 64-bit platforms.

Deep Security Relay

- **Memory:** 512MB
- **Disk Space:** 500MB
- **Supported Platforms:** Windows, Linux RHEL 5/6

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.
What's New in Deep Security 9 SP1

Deep Security 9 SP1

Trusted Common Baseline

Trusted Common baseline is a new method of auto-tagging Integrity Monitoring Events within a group computers. Using this method, you can identify a group of computers that are known to be malware free and implement a set of Integrity Monitoring Rules on them. When changes to files are detected on any computers in the group, Deep Security will look for the presence of files in that same changed state on the other computers in the group. If a match is found, the Event associated with the changed file can be tagged as safe. For more information on Trusted Common Baseline event Tagging, see Event Tagging (page 393) and More About Event Tagging (page 447).

Ability to Update Anti-Malware Patterns Without Updating Anti-Malware Engines

There is now an option to configure a Deep Security Relay Group to distribute only Anti-Malware Pattern updates and not the Anti-Malware engine software. The option can be found on a Relay Group's Properties window by going to the Administration > System Settings > Updates tab and clicking on View Relay Group... to display the Relay Groups window, then double-clicking on a Relay Group. For more information, see Relay Groups (page 283).

Supported Platforms

Deep Security 9 SP1 supports some additional platforms including Solaris 11, HPUX, and AIX. For a list of currently supported platforms, see the Deep Security 9 SP1 Installation Guide.

Additional Language Support

The Deep Security Manager interface is now available in Japanese, Simplified Chinese, and English. As well as being able to set the default language at install time, each Deep Security User can set their user interface language individually. (To change a User's language setting, go to Administration > Users and edit the Properties of the User account.)

The Deep Security Notifier is available in several additional languages, including German, French, Spanish, Italian, Russian, Japanese, Korean, Simplified Chinese, Traditional Chinese. The display language is determined by the locale settings of the computer on which the Notifier is installed.
Performance Improvements and Bug Fixes

Deep Security 9 SP1 includes a number of performance improvements and the resolution of some known issues. For a description of these, please see the accompanying release notes.

Deep Security 9

Multi-Tenancy

Multi-Tenancy lets you create independent installations of Deep Security within your enterprise. You can create Deep Security Tenancies for individual departments or lines of business within your organization. Each Tenant has access to all the functionality of Deep Security except core system settings. Tenants can be made responsible for the creation and management their own assets, Users, Policies and Rules independently of other Tenants. No Tenant's assets or security components are visible to any other Tenants. Each Tenancy is independent and isolated from every other Tenancy.

Multi-Level Policy Inheritance

Deep Security now supports multiple levels of policy inheritance. A newly created policy can be configured to inherit all or some of its settings from a parent policy. This lets you create a tree structure of security policies which get progressively more granular and detailed. For example, you can create a parent policy called "Windows Server" and two child policies, "Windows Server 2008" and "Windows Server 2003", which inherit from their parent policy. Each of those child policies can in turn have child policies of their own for different editions of Windows Server:

Child Policies can inherit all their settings from their parent Policy, or specific settings can be overridden.
Protection of Virtual Machines deployed on VMware vCloud and Amazon EC2 Infrastructure

Deep Security now provides support for virtual machines deployed in VMware vCloud and Amazon EC2 environments. This support include:

- discovery and synchronization of virtual datacenter organizational views or provider based virtual datacenter views
- identification and management of VM instances in the cloud environment
- activation and Policy assignment for VMs in the cloud environment and their clones to enable auto-scaling.
- service catalog support in the vCloud Director
- dashboard/Alerts/reporting based on a Tenant's particular vDataCenter configuration

See Cloud Account (page 319).

Improved performance and efficiency of Malware scans in both Agent-based and Agentless environments

On Windows Agents, the Quick Scan option carries out a fast high level scan of areas that are most commonly at risk of infection. In Agentless environments, Malware scanning has been optimized to prevent multiple scans of resources shared across virtual machines. (See VMware vCenter (page 316)).

Full IPv6 Support

IPv6 is now supported by the Deep Security Firewall and Intrusion Prevention modules. Existing Rules will be applied to both IPv4 and IPv6 traffic. New Rules can be created that apply to IPv4 or IPv6 specifically or both.

Agentless Recommendation Scans

Recommendations Scans can now be performed on virtual machines being protected by a Deep Security Virtual Appliance. Intrusion Prevention and Integrity Monitoring Rules can be automatically assigned based on the result of a recommendation scan and Firewall Rules can be automatically assigned based on the result of a scan for open ports.

Improvements to the automation of Agent installation, activation, and Policy assignment

Scripting support has been added to Deep Security to allow the automated deployment and activation of Agents. Upon activation, Agents can automatically run a recommendation scan and implement a Security Policy. See Deployment Scripts (page 323).
Improved control of Event-based Tasks for discovered assets.

Tasks such as Policy, Rule, and Group assignment can be automatically carried out on newly discovered assets based on their hostnames, IPs, Tenancy ID, Tenancy Template, Instance Type, or other cloud asset properties. See *Event-Based Tasks (page 210)*.

Support for VMware Trusted Platform Module (TPM) on ESX/ESXi.

VMware TPM is a hardware-based encryption module attached to an ESX/ESXi which creates a signature of data logged during the ESX boot sequence. A change to the TPM signature indicates that the ESX boot sequence has changed which could represent an attack (a change that replaces or alters a critical component in the hypervisor). The Deep Security Integrity Monitoring module can monitor TPM signatures and raise Alerts if changes are detected.
The Deep Security Manager
Console
Dashboard

The Dashboard provides a quick at-a-glance view of the state of the Deep Security system. When you sign in to the Deep Security Manager the layout of the Dashboard is preserved from your last session.

Date/Time Range

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

Displaying Events according to Tags

"Widgets"

Information panels ("widgets") can be rearranged on the page by dragging them to a new location. Widgets can also be added to or removed from the Dashboard display.

Click Add/Remove Widgets... at the top right of the dashboard to view the list of widgets available for display.
Many widgets will display data in a tool tip if you hover the mouse over certain areas. Many will also let you "drill down" to the data. For example, clicking a column in a History chart widget takes you to the corresponding **Events** page listing all the Events that occurred on that day or hour.

To remove a widget from the Dashboard, click the "X" in its top-right corner.

**Note:**  
Note the trend indicators next to the numeric values in the 1x1 widgets. An upward or downward pointing triangle indicates an increase or decrease compared to the previous time period, and a flat line indicates no significant change.

### Saving Multiple 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:

You can edit the name of a Dashboard layout by clicking on the layout tab title.
Alerts

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

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

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

Alerts that can't be dismissed (like "Relay Update Service Not Available") will be dismissed automatically when the condition no longer exists.

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.
Events and Reports

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

- **System Events** (page 24)
- **Anti-Malware Events** (page 26)
  - **Quarantined Files** (page 29)
- **Web Reputation Events** (page 32)
- **Firewall Events** (page 35)
- **Intrusion Prevention Events** (page 38)
- **Log Inspection Events** (page 43)
- **Generate Reports** (page 46)
System Events

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

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

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

- **Add Tag(s):** Add an Event Tag to this event (See *Event Tagging (page 447).* )
- **Remove Tag(s):** Remove exiting Event Tags

**View**

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

**General**

**General Information**

- **Time:** The time according to the system clock on the computer hosting the Deep Security Manager.
- **Level:** The severity level of event that occurred. Event levels include **Info, Warning,** and **Error.**
- **Event ID:** The event type's unique identifier.
- **Event:** The name of the event (associated with the event ID.)
- **Target:** The system object associated with the event will be identified here. Clicking the object's identification will display the object's properties sheet.
- **Action Performed By:** If the event was initiated by a User, that User's username will be displayed here. Clicking the username will display the **User Properties** window.
- **Manager:** The hostname of the Deep Security Manager computer.

**Description**

If appropriate, the specific details of what action was performed to trigger this entry in the system event log will be displayed here.
Tags

The Tags tab displays tags that have been attached to this Event. For more information on Event tagging, see Policies > Common Objects > Other > Tags, and More About Event Tagging (page 447) in the Reference section.

Filter the List and/or Search for an Event

The Period toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The Computers toolbar lets you organize the display of event log entries by computer groups or computer Policies.

Clicking Advanced Search toggles the display of the search bar.

Pressing the "Add Search Bar" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the "Submit Request" button (at the right of the toolbars with the right-arrow on it).

Export

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

Auto-Tagging

Clicking Auto-Tagging... displays a list of existing System Event Auto-Tagging Rules.
Anti-Malware Events

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

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

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 447).**)
- **Remove Tag(s)** from this event.
- View the **Computer Details window** of the computer that generated the log entry.
- View **Quarantined File Details** of the file associated with this event. (Only available if the action associated with this event was quarantined.)

Columns for the Anti-Malware Events display:

- **Time:** Time the event took place on the computer.
- **Computer:** The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)
- **Infected File:** The location and name of the infected file.
- **Tag(s):** Event tags associated with this event.
- **Malware:** The name of the malware that was found.
- **Scan Type:** The type of scan that found the malware (Real-Time, Scheduled, or Manual).
- **Result:** Displays the results of the actions specified in the Malware Scan Configuration associated with event.
  - **Cleaned:** Deep Security successfully terminated processes or deleted registries, files, cookies, or shortcuts, depending on the type of malware.
  - **Clean Failed:** Malware could not be cleaned for a variety of possible reasons.
  - **Deleted:** An infected file was deleted.
- **Delete Failed:** An infected file could not be deleted for a variety of possible reasons. For example, the file may be locked by another application, is on a CD, or is in use. If possible, Deep Security will delete the infected file once it is released.

- **Quarantined:** An infected file was moved to the quarantine folder.

- **Quarantine Failed:** An infected file could not be quarantined for a variety of possible reasons. For example, the file may be locked by another application, is on a CD, or is in use. If possible, Deep Security will quarantine the infected file once it is released. It is also possible that file exceeded the maximum quarantined file size settings on the Policy/Computer Editor > Anti-Malware > Advanced tab.

- **Access Denied:** Deep Security has prevented the infected file from being accessed without removing the file from the system.

- **Passed:** Deep Security did not take any action but logged the detection of the malware.
  
  - **Event Origin:** Indicates from which part of the Deep Security System the event originated.
  - **Reason:** The Malware Scan Configuration that was in effect when the malware was detected.

### 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 447) in the Reference section.

### Filter the List and/or Search for an Event

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

The **Period** toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The **Computers** toolbar lets you organize the display of event log entries by computer groups or computer Policies.

![Advanced Search](image)

Advanced Search functions (searches are not case sensitive):

- **Contains:** The entry in the selected column contains the search string
• **Does Not Contain:** The entry in the selected column does not contain the search string
• **Equals:** The entry in the selected column exactly matches the search string
• **Does Not Equal:** The entry in the selected column does not exactly match the search string
• **In:** The entry in the selected column exactly matches one of the comma-separated search string entries
• **Not In:** The entry in the selected column does not exactly match any of the comma-separated search string entries

Pressing the "plus" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the submit button (at the right of the toolbars with the right-arrow on it).

**Export**

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

**Auto-Tagging...**

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

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

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

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

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

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

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

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

**Details**

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

• **Detection Time:** Date/Time (on the infected computer) that the infection was detected.
• **Infected File(s):** The name of the infected file.
• **Malware:** The name of the malware that was found.
• **Scan Type:** Indicates whether the malware was detected by a Real-time or Scheduled Scan.
• **Scan Result:** The result of the action taken by Deep Security when the malware was detected.
• **Computer:** The computer on which this file was found. (If the computer has been removed, this entry will read "Unknown Computer").

**Filter the List and/or Search for a Quarantined File**

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

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

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

![Advanced Search Options](image)

Advanced Search functions (searches are not case sensitive):

• **Contains:** The entry in the selected column contains the search string.
• **Does Not Contain:** The entry in the selected column does not contain the search string.
• **Equals:** The entry in the selected column exactly matches the search string.
• **Does Not Equal:** The entry in the selected column does not exactly match the search string.
• **In:** The entry in the selected column exactly matches one of the comma-separated search string entries.
• **Not In:** The entry in the selected column does not exactly match any of the comma-separated search string entries.

Pressing the "plus" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the submit button (at the right of the tool bars with the right-arrow on it).

• **Infected File:** Shows the name of the infected file and the specific security risk.
• **Malware:** Names the malware infection.
• **Computer:** Indicates the name of the computer with the suspected infection.

### Manually Restoring Quarantined Files

To manually restore a quarantined file, you must use the quarantined file decryption utility to decrypt the file and then move it back to its original location. The decryption utility is in a zip file, QFAdminUtil_32.zip, located in the "util" folder under the Deep Security Manager root directory. The zipped file contains two utilities which perform the same function: QDecrypt.exe and QDecrypt.com. Running QDecrypt.exe invokes an open file dialog that lets you select the file for decryption. QDecrypt.com is a command-line utility with the following options:

• `/h, --help`: show this help message
• `--verbose`: generate verbos log messages
• `/i, --in=<str>`: quarantined file to be decrypted, where `<str>` is the name of the quarantined file
• `/o, --out=<str>`: decrypted file output, where `<str>` is the name given to the resulting decrypted file
Web Reputation Events

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

Once collected by the Deep Security Manager, Event logs are kept for a period of time which can be set Administration > System Settings > Storage.

From the main page you can:

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

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

- Add Tag(s): Add an Event Tag to this event (See Event Tagging (page 447).)
- Remove Tag(s): Remove exiting event Tags
- Add to Allow List: Add the URL that triggered this Event to the list of Allowed URLs. (To view or Edit the Allowed and Blocked lists, go to the Exceptions tab on the main Web Reputation page.)
- Computer Details: View the Details window of the computer that generated the log entry

Columns for the Web Reputation Events display:

- Time: Time the event took place on the computer.
- Computer: The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer").
- URL: The URL that triggered this event.
- Tag(s): Event tags associated with this event.
- Risk: What was the risk level of the URL that triggered the event ("Suspicious", "Highly Suspicious", "Dangerous", "Untested", or "Blocked by Administrator").
- Rank:
- Event Origin: Indicates from which part of the Deep Security System the event originated.
View Event Properties

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

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

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

The Tags tab displays tags that have been attached to this Event. For More information on Event tagging, see Policies > Common Objects > Other > Tags, and More About Event Tagging (page 447) in the Reference section.

Filter the List and/or Search for an Event

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

The Period toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The Computers toolbar lets you organize the display of event log entries by computer groups or computer Policies.

Advanced Search functions (searches are not case sensitive):

- Contains: The entry in the selected column contains the search string
- Does Not Contain: The entry in the selected column does not contain the search string
- Equals: The entry in the selected column exactly matches the search string
- Does Not Equal: The entry in the selected column does not exactly match the search string
- In: The entry in the selected column exactly matches one of the comma-separated search string entries
- Not In: The entry in the selected column does not exactly match any of the comma-separated search string entries
Pressing the "plus" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the submit button (at the right of the toolbars with the right-arrow on it).

Export

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

Auto-Tagging

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

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

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

Firewall Event icons:

- Single Event
- Single Event with data
- Folded Event
- Folded Event with data

**Note:** Event folding occurs when multiple events of the same type occur in succession. This saves disk space and protects against DoS attacks that may attempt to overload the logging mechanism.

From the main page you can:

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

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

- Add Tag(s): Add an Event Tag to this event (See Event Tagging (page 447).)
- Remove Tag(s): Remove exiting event Tags
- Computer Details: View the Details window of the computer that generated the log entry

Columns for the Firewall Events display:

- Time: Time the event took place on the computer.
- Computer: The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)
- Reason: Log entries on this page are generated either by Firewall Rules or by Firewall Stateful Configuration settings. If an entry is generated by a Firewall Rule, the column entry will be prefaced
by "Firewall Rule:" followed by the name of the Firewall Rule. Otherwise the column entry will display the Firewall Stateful Configuration setting that generated the log entry. (For a listing of possible packet rejection reasons, see "Packet Rejection Reasons" in the Reference section.)

- **Action:** The action taken by the Firewall Rule or Firewall Stateful Configuration. Possible actions are: Allow, Deny, Force Allow, and Log Only.
- **Rank:** The Ranking system provides a way to quantify the importance of Intrusion Prevention and Firewall Events. By assigning "asset values" to computers, and assigning "severity values" to Intrusion Prevention Rules and Firewall Rules, the importance ("Rank") of an Event is calculated by multiplying the two values together. This allows you to sort Events by Rank when viewing Intrusion Prevention or Firewall Events.
- **Direction:** The direction of the affected packet (incoming or outgoing).
- **Interface:** The MAC address of the interface through which the packet was traveling.
- **Frame Type:** The frame type of the packet in question. Possible values are "IPV4", "IPV6", "ARP", "REVARP", and "Other: XXXX" where XXXX represents the four digit hex code of the frame type.
- **Protocol:** Possible values are "ICMP", "ICMPV6", "IGMP", "GGP", "TCP", "PUP", "UDP", "IDP", "ND", "RAW", "TCP+UDP", AND "Other: nnn" where nnn represents a three digit decimal value.
- **Flags:** Flags set in the packet.
- **Source IP:** The packet's source IP.
- **Source MAC:** The packet's source MAC address.
- **Source Port:** The packet's source port.
- **Destination IP:** The packet's destination IP address.
- **Destination MAC:** The packet's destination MAC address.
- **Destination Port:** The packet's destination port.
- **Packet Size:** The size of the packet in bytes.

---

**Note:** *Log-only rules will only generate a log entry if the packet in question is not subsequently stopped either by a deny rule, or an allow rule that excludes it. If the packet is stopped by one of those two rules, those rules will generate a log entry and not the log-only rule. If no subsequent rules stop the packet, the log-only rule will generate an entry.*

---

**View Event Properties**

Double-clicking an event displays the Properties window for that entry which displays all the information about the event on one page. The Tags tab displays tags that have been attached to this Event. For More information on Event tagging, see Policies > Common Objects > Other > Tags, and Event Tagging (page 447) in the Reference section.

**Filter the List and/or Search for an Event**

Selecting "Open Advanced Search" from the "Search" drop-down menu toggles the display of the advanced search options.
The **Period** toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The **Computers** toolbar lets you organize the display of event log entries by computer groups or computer Policies.

![Firewall Events toolbar](image)

Advanced Search functions (searches are not case sensitive):

- **Contains**: The entry in the selected column contains the search string
- **Does Not Contain**: The entry in the selected column does not contain the search string
- **Equals**: The entry in the selected column exactly matches the search string
- **Does Not Equal**: The entry in the selected column does not exactly match the search string
- **In**: The entry in the selected column exactly matches one of the comma-separated search string entries
- **Not In**: The entry in the selected column does not exactly match any of the comma-separated search string entries

Pressing the "plus" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the submit button (at the right of the toolbars with the right-arrow on it).

**Export**

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

**Auto-Tagging**

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

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

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

From the main page you can:

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

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

- Add Tag(s): Add an Event Tag to this event (See Event Tagging (page 447).)
- Remove Tag(s): Remove existing event Tags
- Computer Details: View the Details window of the computer that generated the log entry

Columns for the Intrusion Prevention Events display:

- Time: Time the event took place on the computer.
- Computer: The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer").
- Reason: The Intrusion Prevention Rule associated with this event.
- Application Type: The Application Type associated with the Intrusion Prevention Rule which caused this event.
- Action: What action the Intrusion Prevention Rule took (Allow, Deny, Force Allow, Log Only, or Detect Only (if the rule is in Detect Only mode)).
- Rank: The Ranking system provides a way to quantify the importance of Intrusion Prevention and Firewall Events. By assigning "asset values" to computers, and assigning "severity values" to Intrusion Prevention Rules and Firewall Rules, the importance ("Rank") of an Event is calculated by multiplying the two values together. This allows you to sort Events by Rank when viewing Intrusion Prevention or Firewall Events.
- Severity: The Intrusion Prevention Rule's severity value.
- Tag: Any tags attached with the Event.
- **Flow**: whether the packets(s) that triggered this event was travelling with or against the direction of traffic being monitored by the Intrusion Prevention Rule.
- **Direction**: The direction of the packet (incoming or outgoing)
- **Interface**: The MAC address of the interface through which the packet was passing.
- **Frame Type**: The frame type of the packet in question. Possible values are "IPV4", "IPV6", "ARP", "REVARP", and "Other: XXXX" where XXXX represents the four digit hex code of the frame type.
- **Protocol**: Possible values are "ICMP", "ICMPV6", "IGMP", "GGP", "TCP", "PUP", "UDP", "IDP", "ND", "RAW", "TCP+UDP", AND "Other: nnn" where nnn represents a three digit decimal value.
- **Flags**: Flags set in the packet.
- **Source IP**: The packet's source IP.
- **Source MAC**: The packet's source MAC address.
- **Source Port**: The packet's source port.
- **Destination IP**: The packet's destination IP address.
- **Destination MAC**: The packet's destination MAC address.
- **Destination Port**: The packet's destination port.
- **Packet Size**: The size of the packet in bytes.

**View Event Properties**

Double-clicking an event displays the Properties window for that entry. The Tags tab displays tags that have been attached to this Event. For More information on Event tagging, see Policies > Common Objects > Other > Tags, and Event Tagging (page 447) in the Reference section.

**Filter the List and/or Search for an Event**

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

The Period toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The Computers toolbar lets you organize the display of event log entries by computer groups or computer Policies.
Advanced Search functions (searches are not case sensitive):

- **Contains**: The entry in the selected column contains the search string
- **Does Not Contain**: The entry in the selected column does not contain the search string
- **Equals**: The entry in the selected column exactly matches the search string
- **Does Not Equal**: The entry in the selected column does not exactly match the search string
- **In**: The entry in the selected column exactly matches one of the comma-separated search string entries
- **Not In**: The entry in the selected column does not exactly match any of the comma-separated search string entries

Pressing the "plus" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the submit button (at the right of the toolbars with the right-arrow on it).

**Export**

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

**Auto-Tagging**

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

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

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

From the main page you can:

- View the properties of an individual event
- Filter the list: Use the Period and Computer toolbars to filter the list of events
- Export the event list data to a CSV file
- Add an Auto-Tagging Rule
- Search for a particular event

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

- Add Tag(s): Add an Event Tag to this event (See Event Tagging (page 447).)
- Remove Tag(s): Remove exiting event Tags
- Computer Details: View the Details window of the computer that generated the log entry
- Integrity Monitoring Rule Properties: View the properties of the Integrity Monitoring Rule associated with this event

View Event Properties

Double-clicking an event displays the Properties window for that entry which displays all the information about the event on one page. The Tags tab displays tags that have been attached to this Event. For More information on Event tagging, see Policies > Common Objects > Other > Tags, and Event Tagging (page 447) in the Reference section.

Filter the List and/or Search for an Event

The Period toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The Computers toolbar lets you organize the display of event log entries by computer groups or computer Policies.

Use the "Search" or "Advanced Search" options to search, sort, or filter displayed events.
Advanced Search functions (searches are not case sensitive):

- **Contains**: The entry in the selected column contains the search string
- **Does Not Contain**: The entry in the selected column does not contain the search string
- **Equals**: The entry in the selected column exactly matches the search string
- **Does Not Equal**: The entry in the selected column does not exactly match the search string
- **In**: The entry in the selected column exactly matches one of the comma-separated search string entries
- **Not In**: The entry in the selected column does not exactly match any of the comma-separated search string entries

**Export**

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

**Auto-Tagging**

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

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

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

From the main page you can:

1. View ( ) the properties of an individual event
2. Search ( ) for a particular event
3. Filter the list: Use the Period and Computer toolbars to filter the list of events
4. Export ( ) the event list data to a CSV file

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

- Add Tag(s): Add an Event Tag to this event (See Event Tagging (page 447).)
- Remove Tag(s): Remove exiting event Tags
- Computer Details: View the Details window of the computer that generated the log entry
- Log Inspection Rule Properties: View the properties of the Log Inspection Rule associated with this event

View Event Properties

Double-clicking an event displays the Properties window for that entry which displays all the information about the event on one page. The Tags tab displays tags that have been attached to this Event. For More information on Event tagging, see Policies > Common Objects > Other > Tags, and Event Tagging (page 447) in the Reference section.

Filter the List and/or Search for an Event

The Period toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The Computers toolbar lets you organize the display of event log entries by computer groups or computer Policies.

Use the "Search" or "Advanced Search" options to search, sort, or filter displayed events.
Advanced Search functions (searches are not case sensitive):

- **Contains**: The entry in the selected column contains the search string
- **Does Not Contain**: The entry in the selected column does not contain the search string
- **Equals**: The entry in the selected column exactly matches the search string
- **Does Not Equal**: The entry in the selected column does not exactly match the search string
- **In**: The entry in the selected column exactly matches one of the comma-separated search string entries
- **Not In**: The entry in the selected column does not exactly match any of the comma-separated search string entries

**Export**

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

**Auto-Tagging**

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

You can use Auto-tagging to automatically apply tags for the Log Inspection groups. LI rules have groups associated with them in the rules. For example:

```xml
<rule id="18126" level="3">
  <if_sid>18101</if_sid>
  <id>20158</id>
  <description>Remote access login success</description>
  <group>authentication_success</group>
</rule>

<rule id="18127" level="8">
  <if_sid>18104</if_sid>
  <id>646|^647</id>
  <description>Computer account changed/deleted</description>
</rule>
```
Each group name has a "friendly" name string associated with it. In the above example, "authentication_success" would be "Authentication Success", "account_changed" would be "Account Changed". When this checkbox is set, the friendly names are automatically added as a tag for that event. If multiple rules trigger, multiple tags will be attached to the event.
Generate Reports

Deep Security Manager produces reports in PDF, or RTF formats. Most of the reports generated by the 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 which contains event data, you have the option to filter the report data using Event Tags. Select All for only tagged 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.

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 hourly level of granularity, but beyond three days, the time period can only be specified on a daily level of granularity.

Computer Filter

Set the computers whose data will be included in the report.

Encryption

Reports can be protected with the password of the currently signed in User or with a new password for this report only.
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 which periodically generate and distribute Reports to any number of Users and Contacts. For more information on Scheduled Tasks, go to Administration > Scheduled Tasks.
Computers

The Computers section of the Deep Security Manager is where you manage and monitor the computers on your network. This page regularly refreshes itself to display the most current information. (You can modify the refresh rate on a per-User basis. Go to Administration > User Management > Users and double-click on a User to open the User Properties window. The Computer List refresh rate can be set in the Refresh Rate area on the Settings tab.)

Computer icons:

- Ordinary computer (a physical computer or a virtual machine being managed as a physical computer)
- Deep Security Relay
- ESX Server
- Virtual computer (a virtual machine being managed as part of an imported VMware vCenter)
- Virtual computer (started)
- Virtual computer (stopped)
- Virtual computer (suspended)
- Virtual Appliance
- Virtual Appliance (started)
- Virtual Appliance (stopped)
- Virtual Appliance (suspended)

Preview Panes

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

Ordinary Computer

The preview pane for an ordinary computer displays the presence of an Agent, its status, and details about the Anti-Malware, Web Reputation, Firewall, Intrusion Prevention, Integrity Monitoring, and Log Inspection modules.
Deep Security Relay

The preview pane for a Deep Security Relay displays its status, the number of Security Update components it has available for distribution, and the status of the Protection modules provided by its embedded Deep Security Agent.

ESX Server

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

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

![Virtual Appliance Preview Pane]

Virtual Machine

The preview pane for a virtual machine displays whether it is being protected by a Virtual Appliance, an in-guest Agent, or both. It displays details about the components running on the virtual machine. Since the Appliance is not capable of providing Log Inspection protection at this time, it will appear as "Not Capable". Firewall and Intrusion Prevention configuration will always be the same for both the Appliance and the in-guest Agent.

![Virtual Machine Preview Pane]

**Note:** Remember that a virtual machine can run an Agent as though it were an ordinary computer managed by the Deep Security Manager. It does not need to be "imported" into the Manager by way of a vCenter integration. For more information on VMware integration, see (page 316) the Installation Guide.

Adding Computers to the Deep Security Manager

For more detailed instructions on adding computers to the Deep Security Manager see *Adding Computers* (page 307).
After being installed on a computer, an Agent must be "activated" by the Deep Security Manager. During this process, the Deep Security Manager sends a "fingerprint" to the Agent. From that point on, the Agent will only accept instructions from a Manager with that unique fingerprint.

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

Define a New Computer

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

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

Discover Computers

Clicking **Discover...** in the toolbar displays the **Discover Computers** dialog. During discovery, the Manager searches the network for any visible computers that are not already listed. When a new computer is found, the Manager attempts to detect whether an Agent is present. When discovery is complete, the Manager displays all the computers it has detected and displays their status in the **Status** column. After discovery operations, a computer can be in one of the following states:

- **Discovered (No Agent/Appliance)**: The computer has been detected but no Agent/Appliance is present. The computer may also be in this state if an Agent/Appliance is installed but has been previously activated and is configured for Agent/Appliance initiated communications. In this case, you will have to deactivate the Agent/Appliance on the computer and reactivate it from the Manager.
- **Discovered (Activation Required)**: The Agent is installed and listening for communication from the Manager, but has not been activated. This status may also indicate that the Agent/Appliance is installed and listening, and has been activated, but is not yet being managed by the Manager. This could occur if this Manager was at one point managing the Agent/Appliance, but the Agent/Appliance's public certificate is no longer in the Manager's database. This may be the case if the if the computer was removed from the Manager and then discovered again. To begin managing
the Agent/Appliance on this computer, right-click the computer and select "Activate/Reactivate". Once reactivated, the status will change to "Online".

- **Discovered (Deactivation Required):** The Agent/Appliance is installed and listening, but it has already been activated by another Manager. In this case the Agent/Appliance must be deactivated prior to activation by this Manager.

- **Discovered (Unknown):** The computer has been detected but the presence or absence of an Agent/Appliance cannot be ascertained.

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

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

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

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

### Add Directory

Deep Security Manager can connect to and synchronize with a Microsoft Active Directory. For detailed instructions on importing a list of computers from an Active Directory, see [Active Directory (page 311)](#).

### Add VMware vCenter

Deep Security Manager supports a tight integration with VMware vCenter and ESX Server. You can import the organizational and operational information from vCenter and ESX nodes and allow detailed application of security to an enterprise's VMware infrastructure. For detailed instructions on importing virtual computers from a VMware system, see [VMware vCenter (page 316)](#).
Add Cloud Account

Deep Security can connect to and manage computers (virtual or physical) supplied by Amazon's EC2 and VMware's vCloud services. For detailed instructions on adding computers from a Cloud Provider, see Cloud Account (page 319).

Search for a Computer

Use the Search textbox to search for a particular computer among already discovered (i.e. listed) computers. (To find a computer on the network that is not yet listed, use New ()). For more sophisticated search options, use the "Advanced Search" option below it.

Advanced Search functions (searches are not case sensitive):

- **Contains**: The entry in the selected column contains the search string
- **Does Not Contain**: The entry in the selected column does not contain the search string
- **Equals**: The entry in the selected column exactly matches the search string
- **Does Not Equal**: The entry in the selected column does not exactly match the search string
- **In**: The entry in the selected column exactly matches one of the comma-separated search string entries
- **Not In**: The entry in the selected column does not exactly match any of the comma-separated search string entries

Export Selected Computers

Export your computers list to an XML or CSV file. You may wish to do this to backup your computer information, integrate it with other reporting systems, or if you are migrating computers to another Deep Security Manager. (This will save you the trouble of re-discovering and scanning computers from the new Manager.)

**Note:** The exported computers file does not include any assigned Policies, Firewall Rules, Firewall Stateful Configurations or Intrusion Prevention Rules. In order to export this configuration information use the Policy export option in the Policies page.

Activate/Reactivate the Agent/Appliance on a Computer

When a computer is unmanaged the Agent/Appliance must be activated to move the computer into a managed state. Prior to activation the Agent/Appliance will be one of the following states: On the Computers page, right-click the computer whose Agent/Appliance you wish to Activate/Reactivate and select "Activate/Reactivate" from the Actions menu. (Alternatively, you can click the Activate or Reactivate button in the computer's Details window.)
• **No Agent/Appliance:** Indicates there is no Agent/Appliance running or listening on the default port. The "No Agent/Appliance" status can also mean that an Agent/Appliance is installed and running but is working with another Manager and communications are configured as "Agent/Appliance Initiated", and so the Agent/Appliance is not listening for this Manager. (If you wish to correct the latter situation, you will have to deactivate the Agent from the computer).

• **Activation Required:** The Agent/Appliance is installed and listening, and is ready to be activated by the Manager.

• **Reactivation Required:** The Agent/Appliance is installed and listening and is waiting to be reactivated by the Manager.

• **Deactivation Required:** The Agent/Appliance is installed and listening, but has already been activated by another Manager.

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

After a successful activation the Agent/Appliance state will change to "Online". If the activation failed the computer status will display "Activation Failed" with the reason for the failure in brackets. Click this link to display the system event for more details on the reason for the activation failure.

---

**Note:** Although IPv6 traffic is supported by Deep Security 8 and earlier Agents and Appliances, it is blocked by default. To allow IPv6 traffic on Deep Security 8 Agents and Appliances, go to the Advanced Network Engine Settings area of the Settings > Network Engine tab in a Policy or Computer editor and set the Block IPv6 for 8.0 and Above Agents and Appliances option to No.

---

**Check the Status of a Computer**

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

**Deactivate the Agent/Appliance on a Computer**

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

**Update the Agent Configuration on a Computer**

Updating the Agent Configuration on a computer deploys any configuration changes you have made for that computer from the Manager to the Agent. Updates occur automatically at every heartbeat, but if you wish to apply your changes immediately, you can use this option. The **Update Configuration** button can be used to override the computer access schedule or to force the Manager to retry an update if the previous attempt failed.
The automatic updates actually occur immediately if the communications are not Agent/Appliance initiated, and they occur on the next heartbeat if Agent/Appliance initiated.

Get Events from Computer(s)

Override the normal event retrieval schedule (usually every heartbeat) and retrieve the Event logs from the computer(s) now.

Clear Warnings/Errors

This command will clear any warnings or errors generated for a computer whose Agent has been reset locally or has been removed from the network before a User has had a chance to deactivate or delete the computer from the list of computers.

Lock an Agent

You can lock the Agent on a computer if you are going to perform some maintenance on it and don't want to trigger a series of Alerts on the Manager.

Unlock an Agent

Unlock a locked Computer. (See above.)

Upgrade the Agent Software on a Computer

To upgrade an Agent you first need to add an authenticated Agent Install program to the Deep Security Manager.

Note: Agent Self-Protection must be disabled on computers that you want to upgrade. To configure Agent Self-Protection, go to the Computers tab on the Policy/Computer Editor > Settings page.
1. Go to the Software tab in the Administration > System Settings > Updates page and click the Import Software... button.
2. If you don't already have an Install program locally, click the download link to see if any upgrades are available.
3. Select the install program (.msi, .rpm, or .zip) and click Next.
4. If you are uploading the software from a remote computer this may take a couple of seconds (Firefox displays a message in its status bar ("sending request to computer") but IE displays nothing.)
5. If the install program does not appear to be in the correct format an error message will appear at the top of the page.

Once an install program has been imported you can use it to upgrade one or more Agents.

1. On the Computers page, right-click the computers whose Agents you wish to upgrade and select "Upgrade Agent software". (Alternatively, you can click the Upgrade Agent button in the computer's Details window.)
2. If there are no installers of an appropriate platform and version (the version must be higher than the Agent's) the following message will be displayed: "There are no authenticated Agent Software Install Programs available for the selected computer(s) platform or version. Please add an appropriate Agent Software Install Program using the Software panel in the Administration > Updates page before upgrading the Deep Security Agents." Otherwise a dialog appears allowing you to select a specific version (or simply the latest version for the platform) and an upgrade schedule (or the default "use computer access schedule.")

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

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

Full Scan for Malware

Performs a Full Malware Scan on the selected computers. The actions taken by a Full Scan depend on the Malware Manual Scan Configuration in effect on this computer. See Malware Scan Configurations (page 94) for more information.

Quick Scan for Malware

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

Scan Computers for Open Ports

Scan for Open Ports performs a port scan on all selected computers and checks the Agent installed on the computer to determine whether its state is either "Deactivation Required", "Activation Required", "Agent Reactivate Required", or "Online". (The scan operation, by default, scans ports 1-1024. This range can be changed in Policy/Computer Editor > Settings > Scanning.)

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

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

Cancel any Currently Executing Port Scans

If you have initiated a set of port scans to a large number of computers and/or over a large range of ports and the scan is taking too long, use this option to cancel the scans.

Scan for Recommendations

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

Clear Recommendations

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

Note: This action will not un-assign any rules that were assigned because of past recommendations.
Scan for Integrity Changes

Integrity Monitoring tracks changes to a computer's system and files. It does by creating a baseline and then performing periodic scans to compare the current state of the computer to the baseline. For more information see the documentation for the Integrity Monitoring page.

Rebuild Baseline for Computer

Rebuild a baseline for Integrity Monitoring on this computer.

Move a Computer to a Computer Group

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

Assign a Policy to a Computer

This opens a window with a drop-down list allowing you to assign a Policy to the computer. The name of the Policy assigned to the computer will appear in the Policy column on the Computers page.

**Note:** If you apply other settings to a computer (for example, adding additional Firewall Rules, or modifying Firewall Stateful Configuration settings), the name of the Policy will be in bold indicating that the default settings have been changed.

Assign an Asset Value

Asset values allow you to sort computers and events by importance. The various Security Rules have a severity value. When rules are triggered on a computer, the severity values of the rules are multiplied by the asset value of the computer. This value is used to rank events in order of importance. For more information see Administration > System Settings > Ranking.

Assign a Relay Group

To select a Relay Group for this computer to Download Updates from, right-click the computer and choose Actions > Assign a Relay Group....

Delete a Computer

If you delete a computer, all information pertaining to that computer is deleted along with it. If you re-discover the computer, you will have to re-assign a Policy and whatever rules were assigned previously.
Examine Events Associated with a Computer

Examine system and administrative events (that is, non security-related events) associated with a particular computer.

Examine a Computer's Event Logs

Examine the latest event logs uploaded from the Agent on this computer.

Add a New Computer Group

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

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

Discover computers by importing from an LDAP-based directory (such as Microsoft Active Directory). Computers are imported, and synchronized according to the structure in the directory. For more information, see Adding Computers (page 307).

Remove a Group

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

Move Computers from the Current Group to Another

You can move a computer from one computer group to another but keep in mind that Policies are applied at the computer level, not the computer group level. Moving a computer from one computer group to another has no effect on the Policy assigned to that computer.

View or Edit the Properties of a Computer Group

The properties of groups include their name and description.
Computer and Agent/Appliance 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 either 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 454)](#) and [System Events (page 474)](#) in the Reference section.

### Computer States

<table>
<thead>
<tr>
<th>Computer State</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovered</td>
<td>Computer has been added to the Computers List via the Discovery process.</td>
<td></td>
</tr>
<tr>
<td>Unmanaged</td>
<td>Unmanaged by this Deep Security Manager, unactivated, and can't be communicated with until activated.</td>
<td></td>
</tr>
<tr>
<td>Managed</td>
<td>An Agent is present and activated with no pending operations or errors.</td>
<td></td>
</tr>
<tr>
<td>Updating</td>
<td>The Agent/Appliance is being updated with a combination of new configuration settings and security updates.</td>
<td></td>
</tr>
<tr>
<td>Update Pending (Schedule)</td>
<td>The Agent/Appliance will be updated with a combination of new configuration settings and security updates once the computer's access schedule permits.</td>
<td></td>
</tr>
<tr>
<td>Update Pending (Heartbeat)</td>
<td>An update will be performed at the next heartbeat.</td>
<td></td>
</tr>
<tr>
<td>Update Pending (Offline)</td>
<td>The Manager cannot currently communicate with the Agent/Appliance. An update is ready to be applied once the Agent/Appliance comes back online.</td>
<td></td>
</tr>
<tr>
<td>Scanning for Open Ports</td>
<td>The Manager is scanning the Computer for open ports.</td>
<td></td>
</tr>
<tr>
<td>Activating</td>
<td>The Manager is activating the Agent/Appliance.</td>
<td></td>
</tr>
<tr>
<td>Activating (Delayed)</td>
<td>The activation of the Agent/Appliance is delayed by the amount of time specified in the relevant event-based task.</td>
<td></td>
</tr>
<tr>
<td>Activated</td>
<td>The Agent/Appliance is activated.</td>
<td></td>
</tr>
<tr>
<td>Deactivating</td>
<td>The Manager is deactivating the Agent/Appliance. This means that the Agent/Appliance is available for activation and management by another Deep Security Manager.</td>
<td></td>
</tr>
<tr>
<td>Computer State</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Deactivate Pending (Heartbeat)</td>
<td>A deactivate instruction will be sent from the Manager during the next heartbeat.</td>
<td></td>
</tr>
<tr>
<td>Locked</td>
<td>The computer is in a locked state. While 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.</td>
<td></td>
</tr>
<tr>
<td>Multiple Errors</td>
<td>Multiple errors have occurred on this computer. See the computer's system events for details.</td>
<td></td>
</tr>
<tr>
<td>Multiple Warnings</td>
<td>Multiple warnings are in effect on this computer. See the computer's system events for details.</td>
<td></td>
</tr>
<tr>
<td>Upgrading Agent</td>
<td>The Agent software on this computer is in the process of being upgraded to a newer version.</td>
<td></td>
</tr>
<tr>
<td>Scanning for Recommendations</td>
<td>A Recommendation Scan is underway.</td>
<td></td>
</tr>
<tr>
<td>Scan for Recommendations</td>
<td>A Recommendation Scan will be initiated once the computer's Access Schedule permits.</td>
<td></td>
</tr>
<tr>
<td>Scan for Recommendations</td>
<td>The Manager will initiate a Recommendation Scan at the next heartbeat.</td>
<td></td>
</tr>
<tr>
<td>Scan for Recommendations</td>
<td>The Agent/Appliance is currently offline. The Manager will initiate a Recommendation Scan when communication is reestablished.</td>
<td></td>
</tr>
<tr>
<td>Scan for Recommendations</td>
<td>An instruction to start an Integrity Scan is queued to be sent.</td>
<td></td>
</tr>
<tr>
<td>Scan for Recommendations</td>
<td>An Integrity Scan is currently in progress.</td>
<td></td>
</tr>
<tr>
<td>Scan for Recommendations</td>
<td>The Agent/Appliance is currently offline. The Manager will initiate an Integrity Scan when communication is reestablished.</td>
<td></td>
</tr>
<tr>
<td>Scan for Recommendations</td>
<td>An instruction to rebuild a system baseline for Integrity Monitoring is queued to be sent.</td>
<td></td>
</tr>
<tr>
<td>Scan for Recommendations</td>
<td>The Integrity Monitoring engine is currently rebuilding a system baseline.</td>
<td></td>
</tr>
<tr>
<td>Scan for Recommendations</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Checking Status</td>
<td>The agent state is being checked.</td>
<td></td>
</tr>
<tr>
<td>Getting Events</td>
<td>The Manager is retrieving Events from the Agent/Appliance.</td>
<td></td>
</tr>
<tr>
<td>Prepared</td>
<td>The ESX has been prepared for the installation of the Virtual Appliance. (The Filter Driver has been installed.)</td>
<td>ESX</td>
</tr>
<tr>
<td>Unprepared</td>
<td>The ESX has not been prepared for the installation of the Virtual Appliance. (The Filter Driver has been installed.)</td>
<td>ESX</td>
</tr>
<tr>
<td>Filter Driver Offline</td>
<td>The Filter Driver on the ESX is offline.</td>
<td>ESX</td>
</tr>
<tr>
<td>Upgrade Recommended</td>
<td>A newer version of the Agent or Appliance is available. An software upgrade is recommended.</td>
<td>ESX</td>
</tr>
<tr>
<td>Malware Manual Scan Pending</td>
<td>The instruction to perform a manually-initiated Malware Scan has not yet been sent.</td>
<td></td>
</tr>
<tr>
<td>Malware Manual ScanQueued</td>
<td>The instruction to perform a manually-initiated Malware Scan is queued.</td>
<td></td>
</tr>
<tr>
<td>Computer State</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>Malware Manual Scan In Progress</td>
<td>A manually-initiated Malware Scan is in progress.</td>
<td></td>
</tr>
<tr>
<td>Malware Manual Scan Paused</td>
<td>A manually-initiated Malware Scan has been paused.</td>
<td></td>
</tr>
<tr>
<td>Malware Manual Scan Cancellation Pending</td>
<td>The instruction to cancel a manually-initiated Malware Scan is queued to be sent.</td>
<td></td>
</tr>
<tr>
<td>Malware Manual Scan Cancellation In Progress</td>
<td>The instruction to cancel a manually-initiated Malware Scan has been sent.</td>
<td></td>
</tr>
<tr>
<td>Malware Manual Scan Cancellation Pending (Offline)</td>
<td>The Appliance is offline. The instruction to cancel a manually-initiated Malware Scan will be sent when communication is reestablished.</td>
<td></td>
</tr>
<tr>
<td>Malware Scheduled Scan Pending</td>
<td>The instruction to cancel a scheduled Malware Scan has not yet been sent.</td>
<td></td>
</tr>
<tr>
<td>Malware Scheduled Scan Queued</td>
<td>The instruction to cancel a scheduled Malware Scan is queued.</td>
<td></td>
</tr>
<tr>
<td>Malware Scheduled Scan In Progress</td>
<td>A scheduled Malware Scan is in progress.</td>
<td></td>
</tr>
<tr>
<td>Malware Scheduled Scan Paused</td>
<td>A scheduled Malware Scan has been paused.</td>
<td></td>
</tr>
<tr>
<td>Malware Scheduled Scan Cancellation Pending</td>
<td>The instruction to cancel a scheduled Malware Scan is queued to be sent.</td>
<td></td>
</tr>
<tr>
<td>Malware Scheduled Scan Cancellation In Progress</td>
<td>The instruction to cancel a scheduled Malware Scan has been sent.</td>
<td></td>
</tr>
<tr>
<td>Malware Scheduled Scan Cancellation Pending (Offline)</td>
<td>The Agent/Appliance is offline. The instruction to cancel a scheduled Malware Scan will be sent when communication is reestablished.</td>
<td></td>
</tr>
<tr>
<td>Malware Manual Scan Pending (Offline)</td>
<td>The Agent/Appliance is offline. The instruction to start a manually-initiated Malware Scan will be sent when communication is reestablished.</td>
<td></td>
</tr>
<tr>
<td>Malware Scheduled Scan Pending (Offline)</td>
<td>The Agent/Appliance is offline. The instruction to start a scheduled Malware Scan will be sent when communication is reestablished.</td>
<td></td>
</tr>
<tr>
<td>Update of Anti-Malware Components Pending (Offline)</td>
<td>The Agent/Appliance is offline. The Agent/Appliance will be updated with the latest Anti-Malware Components when communication is reestablished.</td>
<td></td>
</tr>
<tr>
<td>Update of Anti-Malware Components Pending (Heartbeat)</td>
<td>The Agent/Appliance will be updated with the latest Anti-Malware Components at the next heartbeat.</td>
<td></td>
</tr>
</tbody>
</table>
## Computer State

<table>
<thead>
<tr>
<th>Computer State</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update of Anti-Malware Components Pending (Schedule)</td>
<td>Anti-Malware Components will be updated as soon as the computer's access schedule permits.</td>
<td></td>
</tr>
<tr>
<td>Update of Anti-Malware Components Pending</td>
<td>The instruction to update Anti-Malware Components is queued to be sent.</td>
<td></td>
</tr>
<tr>
<td>Update of Anti-Malware Components In Progress</td>
<td>The Agent/Appliance is being updated with the latest Anti-Malware Components.</td>
<td></td>
</tr>
</tbody>
</table>

## Agent States

<table>
<thead>
<tr>
<th>Agent State</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activated</td>
<td>The Agent/Appliance has been successfully activated and is ready to be managed by the Deep Security Manager.</td>
<td></td>
</tr>
<tr>
<td>Activation Required</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>VM Stopped</td>
<td>The virtual machine is in a &quot;stopped&quot; state.</td>
<td></td>
</tr>
<tr>
<td>VM Paused</td>
<td>The virtual machine is in a &quot;paused&quot; state.</td>
<td></td>
</tr>
<tr>
<td>No Agent/Appliance</td>
<td>No Agent/Appliance was detected on the ESX server.</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>No attempt has been made to determine whether an Agent/Appliance is present.</td>
<td></td>
</tr>
<tr>
<td>Deactivation Required</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Reactivation Required</td>
<td>The Agent/Appliance is installed and listening and is waiting to be reactivated a Deep Security Manager.</td>
<td></td>
</tr>
<tr>
<td>Online</td>
<td>The Agent/Appliance is online and operating as expected.</td>
<td></td>
</tr>
<tr>
<td>Offline</td>
<td>No contact has been made with the Agent for the number of heartbeats specified in Policy/Computer Editor &gt; Settings &gt; Computers tab.</td>
<td></td>
</tr>
</tbody>
</table>

## Computer Errors

<table>
<thead>
<tr>
<th>Error State</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication error</td>
<td>General network error.</td>
<td></td>
</tr>
<tr>
<td>No route to computer.</td>
<td>Typically the remote host cannot be reached because of an intervening firewall or if an intermediate router is down.</td>
<td></td>
</tr>
<tr>
<td>Unable to resolve hostname</td>
<td>Unresolved socket address.</td>
<td></td>
</tr>
<tr>
<td>Error State</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Activation required</td>
<td>An instruction was sent to the Agent/Appliance when it was not yet activated.</td>
<td></td>
</tr>
<tr>
<td>Unable to communicate with Agent/Appliance</td>
<td>Unable to communicate with Agent/Appliance.</td>
<td></td>
</tr>
<tr>
<td>Protocol error</td>
<td>Communication failure at the HTTP layer.</td>
<td></td>
</tr>
<tr>
<td>Deactivation Required</td>
<td>The Agent/Appliance is currently activated by another Deep Security Manager.</td>
<td></td>
</tr>
<tr>
<td>No Agent/Appliance</td>
<td>No Agent/Appliance was detected on the target.</td>
<td></td>
</tr>
<tr>
<td>No valid software version</td>
<td>Indicates that no installer can be found for the platform/version requested.</td>
<td></td>
</tr>
<tr>
<td>Send software failed</td>
<td>There was an error in sending a binary package to the computer.</td>
<td></td>
</tr>
<tr>
<td>Internal error</td>
<td>Internal error. Please contact your support provider.</td>
<td></td>
</tr>
<tr>
<td>Duplicate Computer</td>
<td>Two computers in the Manager's Computers list share the same IP address.</td>
<td></td>
</tr>
</tbody>
</table>
Policies

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

- Policies (page 67)

Common Objects

The Common Objects pages list objects that can be shared by many constructs like Policies and Rules throughout Deep Security. This can be considered the root repository for shared objects. The Policy and Computer editor windows display the same list of objects but the properties of these common objects can be overridden for the Policy or the specific computer. For more information on how Common Object properties can be inherited and overridden at the Policy or computer level, see Policies, Inheritance and Overrides (page 505).

Rules

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

- Firewall Rules (page 69)
- Intrusion Prevention Rules (page 74)
- Integrity Monitoring Rules (page 80)
- Log Inspection Rules (page 84)

Lists

- Directory Lists (page 105)
- File Extension Lists (page 109)
- File Lists (page 110)
- IP Lists (page 114)
- MAC Lists (page 115)
- Port Lists (page 116)

Other

- Contexts (page 88)
- Firewall Stateful Configurations (page 90)
• Malware Scan Configurations (page 94)
• Schedules (page 103)
• Tags (page 104)
Policies

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

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

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

**Note:** Do not import Policies from a newer Security Update into a system running an older Security Update. The new Policy may reference rules that do not exist in the older version. Always make sure your Security Updates are current.

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

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

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

**Note:** You can create a new Policy based on a Recommendation Scan of a computer. To do so, select a computer and run a Recommendation Scan. (Right-click the computer on the Computers page and select Actions > Scan for Recommendations). When the scan is complete, return to the Policies page and click New to display the New Policy wizard. When prompted, choose to base the new Policy on "an existing computer's current configuration". Then select "Recommended Application Types and Intrusion Prevention Rules", "Recommended Integrity Monitoring Rules", and "Recommended Log Inspection Rules" from among the computer's properties.

**Note:** The Policy will consist only of recommended elements on the computer, regardless of what Rules are currently assigned to that computer.
To assign a Policy to a computer:

1. In the Deep Security Manager, go to Computers.
2. Select your computer from the computers list, right click and choose Actions > Assign Policy.
3. Select the Policy from the hierarchy tree and click OK.

For more information on how to use Policies to protect your computers, see Quick Start: Protecting a Server (page 237).

For more information on how child Policies in a hierarchy tree can inherit or override the settings and rules of parent Policies, see Policies, Inheritance and Overrides (page 505).

After assigning a Policy to a computer, you should still run periodic Recommendation Scans on your to make sure that all vulnerabilities on the computer are protected. See Recommendation Scans (page 385) for more information.
Firewall Rules

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

**Note:** Solaris Agents will only examine packets with an IP frame type, and Linux Agents will only examine packets with IP or ARP frame types. Packets with other frame types will be allowed through. Note that the Virtual Appliance does not have these restrictions and can examine all frame types, regardless of the operating system of the virtual machine it is protecting.

Firewall Rule icons:

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

From the main page you can:

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

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

Clicking New (>New<) or Properties (>Properties<) displays the Firewall Rules Properties window.
Firewall Rule Properties

General Information

- **Name**: The name of the Firewall Rule.
- **Description**: A detailed description of the Firewall Rule.
- **Action**: Your Firewall Rule can behave in four different ways. These are described here in order of precedence:
  1. The traffic can **bypass** the firewall completely. This is a special rule that can cause the packets to bypass the Firewall and Intrusion Prevention engine entirely. Use this setting for media intensive protocols where filtering may not be desired. To find out more about the bypass rule, see "Bypass Rule" in the Reference section.
  2. It can **log only**. This means it will only make an entry in the logs and not interfere with the traffic.
  3. It can **force allow** defined traffic (it will allow traffic defined by this rule without excluding any other traffic.)
  4. It can **deny** traffic (it will deny traffic defined by this rule.)
  5. It can **allow** traffic (it will exclusively allow traffic defined by this rule.)

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

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

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

  **Note**: The priority determines the order in which rules are applied. High priority rules get applied before low priority rules. For example, a port 80 incoming deny rule with a priority of 3 will drop a packet before a port 80 incoming force allow rule with a priority of 2 ever gets applied to it.

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

  **Note**: You can exclusively select **IPv4** or **IPv6**. To specify either (both), select **IP**.
**Note:** For a list of frame types, see the Internet Assigned Numbers Authority (IANA) Web site.

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

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

**Packet Source**

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

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

**Packet Destination**

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

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

**Specific Flags**

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

**Events**

Select whether to enable or disable logging Events because of this Rule. If event logging is enabled, you can record the packet data with the Event.
**Note:** Note that any form of allow Rule (Allow, Force Allow, Bypass) will not log any events because they would overwhelm the database.

### Options

#### Alert

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

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

#### Schedule

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

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

### Context

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

Contexts are designed to be associated with Firewall and Intrusion Prevention Rules. If the conditions defined in the Context associated with a Rule are met, the Rule is applied.

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

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

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

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

Intrusion Prevention Rule icons:

- Normal Intrusion Prevention Rules
- Intrusion Prevention Rules that operate according to a schedule
- Intrusion Prevention Rules that have configuration options

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

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

Clicking New ( ) or Properties ( ) displays the **Intrusion Prevention Rule Properties** window.

---

**Note:** Note the **Configuration** tab. Intrusion Prevention Rules from Trend Micro are not directly editable through Deep Security Manager. Instead, if the Intrusion Prevention Rule requires (or allows) configuration, those configuration options will be available on the **Configuration** tab. Custom Intrusion Prevention Rules that you write yourself will be editable, in which case the **Rules** tab will be visible.
Intrusion Prevention Rule Properties

General Information

- **Name:** The name of the Intrusion Prevention Rule.
- **Description:** The description of the Intrusion Prevention Rule.
- **Minimum Agent/Appliance Version:** The minimum version of the Deep Security Agent/Appliance required to implement this Intrusion Prevention Rule.

Details

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

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

- **Priority:** The priority level of the Intrusion Prevention Rule. Higher priority rules are applied before lower priority rules.
- **Severity:** Setting the severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as sorting criteria when viewing a list of Intrusion Prevention Rules. More importantly, each severity level is associated with a severity value; this value is multiplied by a computer's Asset Value to determine the Ranking of an Event. (See Administration > System Settings > Ranking.)
- **CVSS Score:** A measure of the severity of the vulnerability according the National Vulnerability Database.
- **Detect Only:** Use this checkbox when testing new rules. By checking this box, the rule will create a log entry prefaced with the words "detect only:" but will not interfere with traffic. If you set the "disable logging" checkbox in the next panel (below), the rule's activity will not be logged regardless of whether "Detect Only" is checked or not.

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

Events

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

**Identification (Displayed for Trend Micro rules only)**

- **Type:** Can be either Smart (one or more known and unknown (zero day) vulnerabilities), Exploit (a specific exploit, usually signature based), or Vulnerability (a specific vulnerability for which one or more exploits may exist).
- **Issued:** The date the Rule was released (not downloaded).
- **Last Updated:** The last time the Rule was modified either locally or during Security Update download.
- **Identifier:** The rule's unique identifier tag.

**Vulnerability (Displayed for Trend Micro rules only)**

Displays information about this particular vulnerability. When applicable, the Common Vulnerability Scoring System (CVSS) is displayed. (For information on this scoring system, see the CVSS page at the National Vulnerability Database.)

**Configuration (Displayed for Trend Micro rules only)**

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

---

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

**View Rules (Available for custom Intrusion Prevention Rules only)**

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

Alert

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

Schedule

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

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

Context

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

Contexts are designed to be associated with Firewall and Intrusion Prevention Rules. If the conditions defined in the Context associated with a Rule are met, the Rule is applied.

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

Recommendation Options

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

Assigned To

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

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

Application Type icons:

• Normal Application Types
• Application Types that have configuration options

From the main page you can:

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

Clicking New or Properties displays the Application Type Properties window.

General

General Information

The name and description of the Application Type. "Minimum Agent/Appliance Version" tells you what version of the Deep Security Agent/Appliance is required to support this Application Type.
Connection

- **Direction**: The direction of the initiating communication. That is, the direction of the first packet that establishes a connection between two computers. For example, if you wanted to define an Application Type for Web browsers, you would select "Outgoing" because it is the Web browser that sends the first packet to a server to establish a connection (even though you may only want to examine traffic traveling from the server to the browser). The Intrusion Prevention Rules associated with a particular Application Type can be written to examine individual packets traveling in either direction.

- **Protocol**: The protocol this Application Type applies to.

- **Port**: The port(s) this Application Type monitors. *(Not the port(s) over which traffic is exclusively allowed.)*

Configuration

The **Configuration** tab displays options that control how Intrusion Prevention Rules associated with this Application Type behave. For example, the "Web Server Common" Application Type has an option to "Monitor responses from Web Server". If this option is deselected, Intrusion Prevention Rules associated with this Application Type will not inspect response traffic over source port 80.

Options

Items in the **Options** tab control how the Deep Security Manager uses and applies the Application Type. For example, most Application Types have an option to exclude them from Recommendation Scans. This means that if the "Exclude from Recommendations" options is selected, a Recommendation Scan will not recommend this Application Type and its associated Intrusion Prevention Rules for a computer even if the application in question is detected.

Assigned To

The **Assigned To** tab lists the Intrusion Prevention Rules associated with this Application Type.
Integrity Monitoring Rules

Integrity Monitoring Rules allow the Deep Security Agents to scan for and detect changes to a computer's files, directories, and registry keys and values, as well as changes in installed software, processes, listening ports, and running services. These changes are logged as Events in the Manager and can be configured to generate Alerts like any other Events. Integrity Monitoring Rules can be assigned directly to computers or can be made part of a Policy.

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

Integrity Monitoring Rule icons:

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

From the main page you can:

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

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

Clicking New or Properties displays the Integrity Monitoring Rules Properties window.

Integrity Monitoring Rule Properties

General Information

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

Setting the severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as sorting criteria when viewing a list of Integrity Monitoring Rules. More importantly, each severity level is associated with a severity value; this value is multiplied by a computer's Asset Value to determine the Ranking of an Event. (See Administration > System Settings > Ranking.)

Content

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

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

This section of the help describes the use of the Registry Value and File templates. For information on writing Integrity Monitoring Rules in XML using the Custom (XML) template, see Integrity Monitoring Rule Language (page 510) in the Reference section.

Registry Value Template

Base Key

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

Value Names

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

Attributes

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

Base Directory

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

File Names

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

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

Attributes

The following file attributes can be monitored for change:

- **Created:** Timestamp when the file was created.
- **LastModified:** Timestamp when the file was last modified.
- **LastAccessed:** Timestamp when the file was last accessed. On Windows this value does not get updated immediately, and recording of the last accessed timestamp can be disabled as a performance enhancement. See File Times for details. The act of scanning a file requires that the Agent open the file, which will change its last accessed timestamp. On Unix, the Agent will use the O_NOATIME flag if it is available when opening the file, which will prevent the OS from updating the last accessed timestamp and will speed up scanning.
- **Permissions:** The file's security descriptor (in SDDL format) on Windows or Posix-style ACLs on Unix systems that support ACLs, otherwise the Unix style rwxrwxrwx file permissions in numeric (octal) format.
- **Owner:** User ID of the file owner (commonly referred to as the "UID" on Unix).
- **Group:** Group ID of the file owner (commonly referred to as the "GID" on Unix).
- **Size:** size of the file.
- **Sha1:** SHA-1 hash.
- **Sha256:** SHA-256 hash.
- **Md5:** MD5 hash.
- **Flags:** Windows-only. Flags returned by the GetFileAttributes() Win32 API. Windows Explorer calls these the "Attributes" of the file: Read-only, Archived, Compressed, etc.
- **SymLinkPath** (Unix only): If the file is a symbolic link, the path of the link is stored here. Windows NTFS supports Unix-like symlinks, but only for directories, not files. Windows shortcut objects are
not true symlinks since they are not handled by the OS; the Windows Explorer handles shortcut files (*.lnk) but other applications that open a *.lnk file will see the contents of the lnk file.

- **InodeNumber** (Unix only): The inode number of the file.
- **DeviceNumber** (Unix only): Device number of the disk on which the inode associated with the file is stored.
- **BlocksAllocated** (Unix only): The number of blocks allocated to store the file.

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

- Created
- LastModified
- Permissions
- Owner
- Group
- Size
- Contents
- Flags (Windows only)
- SymLinkPath (Unix only)

**Options**

Triggers an Alert if the rule is triggered.

**Assigned To**

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

The OSSEC Log Inspection Engine is integrated into Deep Security Deep Security Agents (6.0+) and gives Deep Security the ability to inspect the logs and events generated by the operating system and applications running on the computer. Log Inspection Rules can be assigned directly to computers or can be made part of a Policy. Like Integrity Monitoring Events, Log Inspection events can be configured to generate Alerts in the Deep Security Manager.

Log Inspection icons:

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

From the main page you can:

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

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

**Note:** Deep Security Manager ships with a standard set of OSSEC Log Inspection Rules. For more information on Log Inspection, see Examining a Log Inspection Rule (page 382) and Log Inspection (page 361). For further assistance in writing your own Log Inspection Rules using the XML-based language, consult the OSSEC documentation or contact your support provider.

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

**General**

The name and a description for your new rule.
**Content**

**Template**

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

**General Information**

Enter a Rule ID. A Rule ID is a unique identifier for the rule. OSSEC defines 100000 - 109999 as the space for User-defined rules. (Deep Security Manager will pre-populate the field with a new unique Rule ID.)

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

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

**Pattern Matching**

This is the pattern the rule will look for in the logs. The rule will be triggered on a match. Pattern matching supports Regular Expressions or simpler String Patterns. The "String Pattern" pattern type is faster than RegEx but it only supports three special operations:

- \(^\) (caret): specifies the beginning of text
- \(\$\) (dollar sign): specifies the end of text
- \(|\) (pipe): to create a "OR" between multiple patterns

**Composite**

**Frequency** is the number of times the rule has to match within a specific time frame before the rule is triggered.

**Time Frame** is the period of time in seconds within which the rule has to trigger a certain number of times (the frequency, above) to log an event.

**Dependency**

Setting a dependency on another rule will cause your rule to only log an event if the rule specified in this area has also triggered.
Files

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

Options

Alert

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

The "Alert Minimum Severity" setting is only used if you have written "multiple rules" within your rule -- something that cannot be done using the "Basic" template. However, if after creating your rule using the "Basic" template, you edit the XML of the rule and add additional rules to the XML which have different severity levels, you can use the "Alert Minimum Severity Level" drop-down menu to set the minimum severity from the multiple rules which will trigger an Alert.

Assigned To

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

Recommendations

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

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

Common Objects include:

- Directory Lists (page 105)
- File Lists (page 110)
- File Extension Lists (page 109)
- IP Lists (page 114)
- MAC Lists (page 115)
- Port Lists (page 116)
- Contexts (page 88)
- Schedules (page 103)
Contexts

Contexts are a powerful way of implementing different security policies depending on the computer's network environment.

Contexts are designed to be associated with Firewall and Intrusion Prevention Rules. If the conditions defined in the Context associated with a Rule are met, the Rule is applied. (To link a Security Rule to a Context, go to the Options tab in the Security Rule's Properties window and select the Context from the "Context" drop-down menu.)

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

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

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

---

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

---

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

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

Clicking New (●) or Properties(▲▼) displays the Context Properties window.

Context Properties

General Information

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

Options

Context applies when Domain Controller connection is

Specifying an option here will determine whether or not the Firewall Rule is in effect depending on the ability of the computer to connect to its Domain Controller or its Internet Connectivity. (Conditions for testing Internet Connectivity can be configured in Administration > System Settings > Contexts.)

If the Domain Controller can be contacted directly (via ICMP), the connection is "Local". If it can be contacted via VPN only, then the connection is "Remote (VPN) ".

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

---

**Note:** The Internet Connectivity Test is only performed if the computer is unable to connect to its Domain Controller.

Context Applies to Interface Isolation Restricted Interfaces

This context will apply to network interfaces on which traffic has been restricted through the use of Interface Isolation. (Primarily used for Allow or Force Allow Firewall Rules.)

Assigned To

The Assigned To tab displays a list of the rules making use of this Context.
Firewall Stateful Configurations

Deep Security's Firewall Stateful Configuration mechanism analyzes each packet in the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions. In the case of stateless protocols like UDP and ICMP, a pseudo-stateful mechanism is implemented based on historical traffic analysis. Packets are handled by the stateful mechanism as follows:

1. A packet is passed to the stateful routine if it has been allowed through by the static Firewall Rule conditions,
2. The packet is examined to determine whether it belongs to an existing connection by checking a connection table created by the stateful mechanism for matching end points, and
3. The TCP header is examined for correctness (e.g. sequence numbers, flag combinations, etc.).

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

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

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

**Firewall Stateful Configuration Properties**

**General Information**

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

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

  Attackers sometimes create and send fragmented packets in an attempt to bypass Firewall Rules.

  **Note:** The Firewall Rule engine, by default, performs a series of checks on fragmented packets. This is default behavior and cannot be reconfigured. Packets with the following characteristics are dropped:

  - **Invalid fragmentation flags/offset**: A packet is dropped when either the **DF** and **MF** flags in the IP header are set to 1, or the header contains the **DF** flag set to 1 and an **Offset** value different than 0.
  - **First fragment too small**: A packet is dropped if its **MF** flag is set to 1, its **Offset** value is at 0, and it has total length of less than 120 bytes (the maximum combined header length).
  - **IP fragment out of boundary**: A packet is dropped if its **Offset** flag value combined with the total packet length exceeds the maximum datagram length of 65535 bytes.
  - **IP fragment offset too small**: A packet is dropped if it has a non-zero **Offset** flag with a value that is smaller than 60 bytes.

TCP

TCP Packet Inspection

- **Deny TCP packets containing CWR, ECE flags**: These flags are set when there is network congestion.

  **Note:** RFC 3168 defines two of the six bits from the Reserved field to be used for ECN (Explicit Congestion Notification), as follows:

  - Bits 8 to 15: CWR-ECE-URG-ACK-PHS-RST-SYN-FIN
  - TCP Header Flags Bit Name Reference:
    - Bit 8: CWR (Congestion Window Reduced) [RFC3168]
    - Bit 9: ECE (ECN-Echo) [RFC3168]

  Automated packet transmission (such as that generated by a denial of service attack, among other things) will often produce packets in which these flags are set.
• **Enable TCP stateful inspection**: Enable stateful inspection at the TCP level. If you enable stateful TCP inspection, the following options become available:
  - **Enable TCP stateful logging**: TCP stateful inspection events will be logged.
  - **Limit the number of incoming connections from a single computer to**: Limiting the number of connections from a single computer can lessen the effect of a denial of service attack.
  - **Limit the number of outgoing connections to a single computer to**: Limiting the number of outgoing connections to a single computer can significantly reduce the effects of Nimda-like worms.
  - **Limit the number of half-open connections from a single computer to**: Setting a limit here can protect you from DoS attacks like SYN Flood. Although most servers have timeout settings for closing half-open connections, setting a value here can prevent half-open connections from becoming a significant problem. If the specified limit for SYN-SENT(remote) entries is reached, subsequent TCP packets from that specific computer will be dropped.

  **Note:** When deciding on how many open connections from a single computer to allow, choose your number from somewhere between what you would consider a reasonable number of half-open connections from a single computer for the type of protocol being used, and how many half-open connections from a single computer your system can maintain without getting congested.

  - **Enable ACK Storm protection when the number of already acknowledged packets exceeds**: Set this option to log an event that an ACK Storm attack has occurred.
    - **Drop Connection when ACK Storm detected**: Set this option to drop the connection if such an attack is detected.

**FTP Options**

The following FTP options only apply to versions 8 of the Deep Security Agents and earlier. They will have no effect on versions 9 of the Agents or later.

- **Active FTP**
  - **Allow Incoming**: Allow Active FTP when this computer is acting as a server.
  - **Allow Outgoing**: Allow Active FTP when this computer is acting as client.

- **Passive FTP**
  - **Allow Incoming**: Allow Passive FTP when this computer is acting as a server.
  - **Allow Outgoing**: Allow Passive FTP when this computer is acting as a client.

**UDP**

- **Enable UDP stateful inspection**: Check to enable stateful inspection of UDP traffic.
Note: The UDP stateful mechanism drops unsolicited incoming UDP packets. For every outgoing UDP packet, the rule will update its UDP "stateful" table and will then only allow a UDP response if it occurs within 60 seconds of the request. If you wish to allow specific incoming UDP traffic, you will have to create a Force Allow rule. For example, if you are running a DNS server, you will have to create a Force Allow rule to allow incoming UDP packets to destination port 53.

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

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

ICMP

- Enable ICMP stateful inspection: Check to enable stateful inspection of ICMP traffic.

Note: The ICMP (pseudo-)stateful mechanism drops incoming unsolicited ICMP packets. For every outgoing ICMP packet, the rule will create or update its ICMP "stateful" table and will then only allow a ICMP response if it occurs within 60 seconds of the request. (ICMP pair types supported: Type 0 & 8, 13 & 14, 15 & 16, 17 & 18.)

With stateful ICMP inspection enabled, you can, for example, only allow an ICMP echo-reply in if an echo-request has been sent out. Unrequested echo-replies could be a sign of several kinds of attack including a Smurf amplification attack, a Tribe Flood Network communication between master and daemon, or a Loki 2 back-door.

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

Assigned To

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

Deep Security allows you to create a variety of Malware Scan Configurations to automatically handle the way the detection of malware is processed. Configuration options include what files to scan, whether the scanning is done in real time or on a scheduled basis, and what actions to carry out if malware is detected. This page lets you define global Malware Scan Configurations. How, in what combination, and when these configurations are in effect on a computer is set at the Policy and at the computer levels. Also, as with most elements in Deep Security, many global settings can be overridden at the Policy and computer levels. (See Policies, Inheritance and Overrides (page 505) for more information.)

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

From the global Malware Scan Configuration page you can:

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

Properties

General

General Information

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

Scan Settings

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

**Note:** **IntelliScan** is a method of identifying which files to scan that is more efficient than the standard "All files" option, though inherently less secure since it does not scan "all files". For executable files (that is, .zip, .exe), the true file type is determined from the file content. In the event that a file is not executable (i.e. .txt), IntelliScan will use the file header to verify the true file type.

### Exclusions

Allows you to exclude specific directories, files, and file extensions from being scanned. For example, if you are creating a Malware Scan Configuration for a Microsoft Exchange server, you should exclude the SMEX quarantine folder to avoid re-scanning files that have already been confirmed to be malware.

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

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

<table>
<thead>
<tr>
<th>Exclusion</th>
<th>Format</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory</td>
<td>DIRECTORY</td>
<td>Excludes all files in the specified directory and all files in all subdirectories.</td>
<td>C:\Program Files&lt;br&gt;Excludes all files in the &quot;Program Files&quot; directory and all subdirectories.</td>
</tr>
<tr>
<td>Directory with wildcard (*)</td>
<td>DIRECTORY*</td>
<td>Excludes any subdirectories with any subdirectory name, but does not exclude the files in the specified directory.</td>
<td>C:\abc&lt;br&gt;Excludes all files in all subdirectories of &quot;abc&quot; but does not exclude the files in the &quot;abc&quot; directory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note:

The scan exclusion directory settings accept either forward slash "/" or backslash \\ to support both Windows and Linux conventions.
<table>
<thead>
<tr>
<th>Exclusion</th>
<th>Format</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| Directory with wildcard (*) | DIRECTORY\* | Excludes any subdirectories with the a matching name, but does not exclude the files in that directory and any subdirectories. | Matches: 
C:\abc\wx
C:\abc\123wx
Does not match: 
C:\abc\wx
C:\abc\123wx |
| | | | C:\\* |
| | | | Matches: 
C:\abc\ |
C:\abc\1
C:\abc\123 |
Does not match: 
C:\abc |
C:\abx\ |
C:\xyz\ |
C:\abc\\wx |
| | | | Matches: 
C:\abc\wx |
C:\abc\123wx |
Does not match: 
C:\abc\wx\ |
C:\abc\123wx\ |
C:\abc\\wx\* |
| | | | Matches: 
C:\abc\wxz |
C:\abc\wx123z |
Does not match: 
C:\abc\wxz\ |
C:\abc\wx123z\ |
C:\abc\\wxz* |
| | | | Matches: 
C:\abc\wx |
C:\abc\wx\ |
C:\abc\wx12 |
C:\abc\wx12\345\ |
C:\abc\wxz\ |
<table>
<thead>
<tr>
<th>Exclusion</th>
<th>Format</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| Environment variable | ${ENV VAR}  | Excludes all files and subdirectories defined by an environment variable with the format ${ENV VAR}. For a Virtual Appliance, the value pairs for the environment variable must be defined in System Setting > Computers Tab > Environment Variable Overrides. | ${windir}  
If the variable resolves to "c:\windows", excludes all the files in "c:\windows" and all its subdirectories. |
| Comments  | DIRECTORY    | Allows you to add comments to your exclusion definitions.                                                                                                                                                  | c:\abc  
#Exclude the abc directory                                              |

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

<table>
<thead>
<tr>
<th>Exclusion</th>
<th>Format</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| File        | FILE      | Excludes all files with the specified file name regardless of its location or directory.                                                                                                                     | abc.doc  
Excludes all files named "abc.doc" in all directories.  
Does not exclude "abc.exe". |
| File path   | FILEPATH  | Excludes the specific file specified by the file path.                                                                                                                                                     | C:\Documents\abc.doc  
Excludes only the file named "abc.doc" in the "Documents" directory. |
| File with wildcard (*) | FILE*     | Excludes all files with a matching pattern in the file name.                                                                                                                                             | abc*.exe  
Excludes any file that has prefix of "abc" and extension of ".exe".  
*.db  
Matches:  
123.db  
abc.db  
Does not match:  
123db  
123.abd  
ebe.db  
*db  
Matches:  
123.db  
123db |
<table>
<thead>
<tr>
<th>Exclusion</th>
<th>Format</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
|           | File with wildcard (*) | FILE.EXT* | Excludes all files with a matching pattern in the file extension. | abc.v*  
Excludes any file that has file name of "abc" and extension beginning with ".v".  
abc.*pp  
Matches:  
abc.pp  
abc.app  
Does not match:  
wxy.app  
abc.a*p  
Matches:  
ac.ap  
a123p  
Does not match:  
abc.pp  
abc.*  
Matches:  
abc.123  
abc.xyz  
Does not match:  
wxy.123  
a.*.ap  
Matches:  
a.ap  
ac.ap  
File with wildcard (*) | FILE*.EXT* | Excludes all files with a matching pattern in the file name and in the extension. | ac.db  
dacb  
db  
Does not match:  
db123  
wxy*.db  
Matches:  
wxy.db  
wxy123.db  
Does not match:  
wxydb  
abc.v*  
Excludes any file that has file name of "abc" and extension beginning with ".v".  
abc.*pp  
Matches:  
abc.pp  
abc.app  
Does not match:  
wxy.app  
abc.a*p  
Matches:  
ac.ap  
a123p  
Does not match:  
abc.pp  
abc.*  
Matches:  
abc.123  
abc.xyz  
Does not match:  
wxy.123  
a.*.ap  
Matches:  
a.ap  
ac.ap |
Exclusion | Format | Description | Example
--- | --- | --- | ---
|  |  |  | a123c.ap
|  |  |  | ac.a456p
|  |  |  | a123c.a456p
|  |  | Does not match: | ad.aa
| Environment variable | ${ENV VAR} | Excludes files specified by an environment variable with the format ${ENV VAR}. These can be defined or overridden using System Setting > Computers Tab > Environment Variable Overrides. | ${myDBFile} Excludes the file "myDBFile".
| Comments | FILEPATH #Comment | Allows you to add comments to your exclusion definitions. | C:\Documents\abc.doc #This a comment

**Actions**

**Recognized Malware**

Upon detection

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

**Note:** *ActiveAction is a predefined set of cleanup actions that are optimized for each malware category. Trend Micro continually adjusts the actions in ActiveAction to ensure that individual detections are handled properly. ActiveAction scan actions are updated along with virus pattern updates.*

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

<table>
<thead>
<tr>
<th>Malware Type</th>
<th>Real-Time Scan</th>
<th>Manual/Scheduled Scan</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus</td>
<td>Clean</td>
<td>Clean</td>
<td>Viruses are able to infect normal files by inserting malicious code. Typically, whenever an infected file is opened, the malicious code automatically runs and delivers a payload in addition to infecting other files. Some of the more common types of viruses include COM and EXE infectors, macro viruses, and boot sector viruses.</td>
</tr>
<tr>
<td>Trojan</td>
<td>Quarantine</td>
<td>Quarantine</td>
<td>Trojans are non-infecting executable malware files that do not have file infection capabilities.</td>
</tr>
<tr>
<td>Packer</td>
<td>Quarantine</td>
<td>Quarantine</td>
<td>Packers are compressed and/or encrypted executable programs. To evade detection, malware authors often pack existing malware under several layers of compression and encryption. Anti-malware checks executable files for compression patterns associated with malware.</td>
</tr>
</tbody>
</table>
### Malware Scan Configurations

<table>
<thead>
<tr>
<th>Malware Type</th>
<th>Real-Time Scan</th>
<th>Manual/Scheduled Scan</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spyware (Grayware)</td>
<td>Quarantine</td>
<td>Quarantine</td>
<td>Although possibly legitimate, grayware exhibit spyware-like behavior and may be unwanted.</td>
</tr>
<tr>
<td>Possible malware</td>
<td>Pass</td>
<td>Pass</td>
<td>Files detected as possible malware are typically unknown malware components. By default, these detections are logged and files are anonymously sent back to Trend Micro for analysis.</td>
</tr>
<tr>
<td>Cookies</td>
<td>N/A</td>
<td>Delete</td>
<td>Cookies are text files stored by a Web browser. Cookies contain site-related data such as authentication information and site preferences. Cookies are not executable and cannot be infected; however, they can be used as spyware. Even cookies sent from legitimate websites can be used for malicious purposes.</td>
</tr>
<tr>
<td>Other Threats</td>
<td>Clean</td>
<td>Clean</td>
<td>The Other Threats category includes joke programs, which display false notifications or manipulate screen behavior, but are generally harmless.</td>
</tr>
</tbody>
</table>

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

1. **Pass:** Allows full access to the infected file without doing anything to the file. (An Anti-Malware Event will still be recorded.)
2. **Clean:** Cleans a cleanable file before allowing full access to the file. (Not available for Possible Malware.)
3. **Delete:** Deletes the infected file.
4. **Deny Access:** This scan action can only be performed during Real-time scans. When Deep Security detects an attempt to open or execute an infected file, it immediately blocks the operation. If a Malware Scan Configuration with the "Deny Access" option selected is applied during a Manual or Scheduled scan, a "Pass" action will be applied and an Anti-Malware Event will be recorded.
5. **Quarantine:** Moves the file to the quarantine directory on the Virtual Appliance. (Once quarantined, you can download the file to a location of your choice. See [Anti-Malware > Quarantined Files](#) for more information.)

### Possible malware

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

General Options

- **Enable Spyware/Grayware Scan**: The Spyware Scan Engine scans for Spyware/Grayware and performs the actions specified on the Actions tab.

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

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

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

- **Scan Embedded Microsoft Office Objects**: Certain versions of Microsoft Office, including Office 2000 and 2003, use Object Linking and Embedding (OLE) to insert files and other objects into Office files. These embedded objects can contain malicious code. Because embedded objects can contain other objects, there can be multiple layers of embedding within a single Office file. To reduce the impact on performance, you can select to scan only a few layers of embedded objects within each file.
  - **Scan for exploit code in Microsoft Office Objects**: Exploit Detection heuristically identifies malware by checking Microsoft Office files for exploit code.

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

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

  **Note**: Because IntelliTrap identifies such files as security risks and may incorrectly block safe files, consider quarantining (not deleting or cleaning) files when you enable IntelliTrap. If users regularly exchange real-time compressed executable files, disable IntelliTrap. IntelliTrap uses the following Anti-Malware components: Virus Scan Engine, IntelliTrap Pattern, IntelliTrap Exception Pattern.

- **Enable Network Directory Scan (Real-Time only)**: To scan files and folders in network shares and mapped network drives, enable this option.
- **Scan files when (Real-Time only):** Choose between scanning files only when they are opened for reading, or when they are opened for both reading and writing.

- **CPU Usage (Manual/Scheduled Scan only):** Specifies the CPU resources allocated to scanning.
  - **High:** Scans files one after another without pausing
  - **Medium:** Recommended; pauses when overall CPU usage exceeds 50%
  - **Low:** Pauses when overall CPU usage exceeds 20%

**Alert**

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

**Assigned To**

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

Schedules are reusable timetables.

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

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

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

Schedule Properties

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

Assigned To

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

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

In addition to the manual tagging of events, automated event tagging can be accomplished via the use of a "Trusted Computer" which is particularly useful for managing Integrity Monitoring events. For example, a planned rollout of a patch can be applied to the trusted computer, the events associated with the application of the patch can be tagged as "Patch X", similar events raised on other systems can automatically be tagged as "acceptable changes" thereby reducing the number of events that need to analyzed by an administrator.

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

Tags

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

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

Auto-Tag Rules

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

For information on Event Tagging procedures, see Event Tagging (page 447).
Directory Lists

**Directory Lists** are reusable lists of directories.

From the main page you can:

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

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

**Directory List Properties**

**General Information**

The name and description of the directory list.

**Directory(s)**

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

**Supported Formats**

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

The following table describes the syntax available for defining Directory Lists:
<table>
<thead>
<tr>
<th>Directory</th>
<th>Format</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory</td>
<td>DIRECTORY</td>
<td>Includes all files in the specified directory and all files in all subdirectories.</td>
<td>C:\Program Files\Includes all files in the &quot;Program Files&quot; directory and all subdirectories.</td>
</tr>
<tr>
<td>Network Resource</td>
<td>NETWORKRESOURCE</td>
<td>Includes files on a computer included as a network resource on a targeted computer.</td>
<td>\12.34.56.78\some-comp-name\Includes all files on a network resource identified using an IP or a hostname.</td>
</tr>
<tr>
<td>Directory with wildcard (*)</td>
<td>DIRECTORY*</td>
<td>Includes any subdirectories with any subdirectory name, but does not include the files in the specified directory.</td>
<td>C:\abc*\Includes all files in all subdirectories of &quot;abc&quot; but does not include the files in the &quot;abc&quot; directory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\abc\wx*z\Matches: C:\abc\wxz\C:\abc\wx123z\Does not match: C:\abc\wx\C:\abc\wx123z</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\abc\wx*x\Matches: C:\abc\wx\C:\abc\123wx\x\Does not match: C:\abc\wx\C:\abc\123wx</td>
</tr>
<tr>
<td>Directory with wildcard (*)</td>
<td>DIRECTORY*</td>
<td>Includes any subdirectories with the a matching name, but does not include the files in that directory and any subdirectories.</td>
<td></td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
| C:\abc\*                    |             | Matches:  
C:\abc\  
C:\abc\1  
C:\abc\123  
Does not match:  
C:\abc  
C:\abx\  
C:\xyz\ |
| C:\abc\*wx                   |             | Matches:  
C:\abc\wx  
C:\abc\123wx  
Does not match:  
C:\abc\wx\  
C:\abc\123wx\ |
| C:\abc\*wz                   |             | Matches:  
C:\abc\wz  
C:\abc\wx123z  
Does not match:  
C:\abc\wz\  
C:\abc\wx123z\ |
| C:\abc\*x                    |             | Matches:  
C:\abc\wx  
C:\abc\wx\  
C:\abc\wx12  
C:\abc\wx12\345\  
C:\abc\wxz\  
Does not match:  
C:\abc\wx123z\ |
<p>| Environment variable         | ${ENV VAR} | Includes all files and subdirectories defined by an environment variable with the format ${ENV VAR}. For a Virtual Appliance, the value pairs for the environment variable must be defined in System Setting &gt; Computers Tab &gt; Environment Variable Overrides. |
| ${windir}                   |             | If the variable resolves to &quot;c:\windows&quot;, Includes all the files in &quot;c:\windows&quot; and all its subdirectories. |</p>
<table>
<thead>
<tr>
<th>Directory</th>
<th>Format</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments</td>
<td>DIRECTORY #Comment</td>
<td>Allows you to add comments to your inclusion definitions.</td>
<td>c:\abc #Include the abc directory</td>
</tr>
</tbody>
</table>

### Assigned To

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

The File Extension Lists page contains a list of file extensions that are used by Malware Scan Configurations. For example, one list of file extensions can be used by multiple Malware Scan Configurations as files to include in a scan. Another list of file extensions can be used by multiple Malware Scan Configurations as files to exclude from a scan.

From the main page you can:

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

Clicking New or Properties displays the File Extension Lists Properties window.

File Extension List Properties

General Information

The name and description of the file extension list.

File Extensions(s)

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

Assigned To

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

**File Lists** are reusable lists of files.

**General**

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

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

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

**File List Properties**

**General Information**

The name and description of the file list.

**File(s)**

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

**Supported Formats**

---

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

---

The following table describes the syntax available for defining File List inclusions:
<table>
<thead>
<tr>
<th>Inclusion</th>
<th>Format</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>FILE</td>
<td>Includes all files with the specified file name regardless of its location or directory.</td>
<td>abc.doc</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Includes all files named &quot;abc.doc&quot; in all directories. Does not include &quot;abc.exe&quot;.</td>
</tr>
<tr>
<td>File path</td>
<td>FILEPATH</td>
<td>Includes the specific file specified by the file path.</td>
<td>C:\Documents\abc.doc</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Includes only the file named &quot;abc.doc&quot; in the &quot;Documents&quot; directory.</td>
</tr>
<tr>
<td>File with wildcard (*)</td>
<td>FILE*</td>
<td>Includes all files with a matching pattern in the file name.</td>
<td>abc*.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Includes any file that has prefix of &quot;abc&quot; and extension of &quot;.exe&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>*db</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Matches:</td>
<td>123.db</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>abc.db</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not match:</td>
<td>123db</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>123.abd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>cbc.db</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>*db</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Matches:</td>
<td>123.db</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>123db</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ac.db</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>acdb</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>db</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not match:</td>
<td>db123</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>wxy*.db</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Matches:</td>
<td>wxy.db</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>wxy123.db</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not match:</td>
<td>wxydb</td>
</tr>
<tr>
<td>Inclusion</td>
<td>Format</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>File with</td>
<td>FILE.EXT*</td>
<td>Includes all files with a matching pattern in the file extension.</td>
<td>* Example</td>
</tr>
<tr>
<td>wildcard (*)</td>
<td></td>
<td></td>
<td><code>abc.v*</code> Includes any file that has file name of &quot;abc&quot; and extension beginning with &quot;.v&quot;.</td>
</tr>
<tr>
<td>File with</td>
<td>FILE.<em>.EXT</em></td>
<td>Includes all files with a matching pattern in the file name and in the extension.</td>
<td>* Example</td>
</tr>
<tr>
<td>wildcard (*)</td>
<td></td>
<td></td>
<td><code>a*c.a*p</code> Matches: <code>ac.ap</code>, <code>a123c.ap</code>, <code>ac.a456p</code> Does not match: <code>abc.pp</code></td>
</tr>
<tr>
<td>Environment</td>
<td>${ENV VAR}</td>
<td>Includes files specified by an environment variable with the format <code>${ENV VAR}</code>. These can be defined or overridden using System Setting &gt; Computers Tab &gt; Environment Variable Overrides.</td>
<td>* Example</td>
</tr>
<tr>
<td>variable</td>
<td></td>
<td></td>
<td><code>$[myDBFile]</code> Includes the file &quot;myDBFile&quot;.</td>
</tr>
<tr>
<td>Comments</td>
<td>FILEPATH</td>
<td>Allows you to add comments to your inclusion definitions.</td>
<td>* Example</td>
</tr>
<tr>
<td></td>
<td>#Comment</td>
<td></td>
<td><code>C:\Documents\abc.doc #This a comment</code></td>
</tr>
</tbody>
</table>
Assigned To

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

Use the **IP Lists** page to create reusable lists of IP addresses for use by multiple Firewall Rules.

From the main page you can:

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

Clicking **New** ( ![new] ) or **Properties** ( ![properties] ) displays the IP List **Properties** window.

**IP List Properties**

**General Information**

The name and description of the IP list.

**IPs**

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

**Supported Formats**

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

**Assigned To**

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

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

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

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

MAC List Properties

General Information

The name and description of the list.

MAC(s)

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

Supported Formats

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

Assigned To

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

Use the Port Lists page to create reusable lists of ports.

From the main page you can:

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

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

Port List Properties

General Information

The name and description of the list.

Port(s)

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

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

Supported Formats

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

Assigned To

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

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

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

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

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

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

The Policy Overview page has the following tabbed sections:

- General (page 119)
- Computer(s) Using This Policy (page 120)
- Events (page 121)
General

- **Name**: Appears in the Display Name column and in brackets next to the Hostname value.
- **Description**: a description of the computer.

Inheritance

Identifies the parent Policy (if any) from which the current Policy inherits its settings.

Modules

- **Anti-Malware**:
  - When Anti-Malware protection is on and either Real-Time or Scheduled scanning is in effect, Anti-Malware status will be "On" and the Anti-Malware status light will be green.
  - When Anti-Malware protection is on but neither Real-Time nor Scheduled scanning is in effect, Anti-Malware status will be "On" and the Anti-Malware status light will be blue.
  - When Anti-Malware protection is off and either Real-Time or Scheduled scanning is in effect, Anti-Malware status will be "Off" and the Anti-Malware status light will be blue.
  - When Anti-Malware protection is off and neither Real-Time nor Scheduled scanning is in effect, Anti-Malware status will be "Off" and the Anti-Malware status light will be blue.

- **Web Reputation**: Whether Web Reputation is on or off.
- **Firewall**: Whether the Firewall is on or off and how many rules are in effect.
- **Intrusion Prevention**: Whether Intrusion Prevention is on or off and how many rules are in effect.
- **Integrity Monitoring**: Whether Integrity Monitoring is on or off and how many rules are in effect (Agent only).
- **Log Inspection**: Whether Log Inspection is on or off and how many rules are in effect (Agent only).
Computer(s) Using This Policy

Lists computers to which this Policy has been assigned.
Events

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

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

1. View (View) the details (properties) of a system event
2. Search (Search) for a particular system event
3. Export (Export) currently displayed system events to a CSV file

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

- Add Tag(s): Add an Event Tag to this event (See Event Tagging (page 447).)
- Remove Tag(s): Remove exiting Event Tags

View

Selecting an event and clicking View (View) displays the Event ViewerProperties window.

General

General Information

- **Time:** The time according to the system clock on the computer hosting the Deep Security Manager.
- **Level:** The severity level of event that occurred. Event levels include Info, Warning, and Error.
- **Event ID:** The event type's unique identifier.
- **Event:** The name of the event (associated with the event ID.)
- **Target:** The system object associated with the event will be identified here. Clicking the object's identification will display the object's properties sheet.
- **Event Origin:** The Deep Security component from which the Event originated.
- **Action Performed By:** If the event was initiated by a User, that User's username will be displayed here. Clicking the username will display the User Properties window.
- **Manager:** The hostname of the Deep Security Manager computer.
Description

If appropriate, the specific details of what action was performed to trigger this entry in the system event log will be displayed here.

Tags

The Tags tab displays tags that have been attached to this Event. For More information on Event tagging, see Policies > Common Objects > Other > Tags, and Event Tagging (page 447) in the Reference section.

Filter the List and/or Search for an Event

The Period toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The Computers toolbar lets you organize the display of event log entries by computer groups or computer Policies.

Clicking Search > Open Advanced Search toggles the display of the advanced search bar.

Pressing the "Add Search Bar" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the "Submit Request" button (at the right of the toolbars with the right-arrow on it).

Export

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

Auto-Tagging

Clicking Auto-Tagging... displays a list of existing System Event Auto-Tagging Rules.
Overview (Computer Editor)

The computer Overview page has the following tabbed sections:

- General (page 124)
- Actions (page 127)
- Events (page 130)
General

- **Hostname**: Appears in the Name column on the Computers page. The name must be either the IP address of the computer or the hostname of the computer. (Either a fully qualified hostname or a relative hostname may be used if a hostname is used instead of an IP address.)
- **Display Name**: Appears in the Display Name column and in brackets next to the Hostname value.
- **Description**: a description of the computer.
- **Platform**: Details of the computer's OS will appear here.
- **Group**: The computer group to which the computer belongs appears in the drop-down list. You can reassign the computer to any other existing computer group.
- **Policy**: The Policy (if any) that has been assigned to this computer.

**Note:** Keep in mind that if you unassign a Policy from a computer, Rules may still be in effect on the computer if they were assigned independently of the Policy.

- **Asset Importance**: Deep Security Manager uses a ranking system to quantify the importance of Security Events. Rules are assigned a Severity Level (high, medium, low, etc.), and Assets (computers) are assigned an "Asset Importance" level. These levels have numerical values. When a Rule is triggered on a computer the Asset Importance value and the Severity Level value are multiplied together. This produces a score which is used to sort Events by importance. (Event ranking can be seen in the Events pages.) Use this Asset Importance drop-down list to assign an Asset Importance level to this computer. (To edit the numerical values associated with severity and importance levels, go to Administration > System Settings > Ranking.)
- **Download Updates From**: Use the dropdown list to select which Relay Group the Agent/Appliance on this computer will download Security Updates from.
- **Lock Computer (Prevents all communication)**: Setting this option blocks all communications between the Agent/Appliance and the Manager. The computer's Policy is still active (all rules are still applied to all traffic), but should any Alerts be generated, they will not be sent to the Manager.

**Note:** You may wish to lock out a computer if you are going to perform some maintenance on it and don't want a series of Alerts to appear in the Manager.

Status

- **Status**: 
  - When the computer is unmanaged the status represents the state of the Agent/Appliance with respect to activation. The status will display either "Discovered" or "New" followed by
the Agent/Appliance state in brackets ("No Agent/Appliance", "Unknown", "Reactivation Required", "Activation Required", or "Deactivation Required").

- When the computer is managed and no computer errors are present, the status will display "Managed" followed by the state of the Agent/Appliance in brackets ("Online" or "Offline").
- When the computer is managed and the Agent/Appliance is in the process of performing an action (e.g., "Integrity Scan in Progress", "Upgrading Agent(Install Program Sent)", etc.) the task status will be displayed.
- When there are errors on the computer (e.g., "Offline", "Update Failed", etc.) the status will display the error. When more than one error is present, the status will display "Multiple Errors" and each error will be listed beneath.

- **Anti-Malware:**
  - When Anti-Malware protection is on and either Real-Time or Scheduled scanning is in effect, Anti-Malware status will be "On" and the Anti-Malware status light will be green.
  - When Anti-Malware protection is on but neither Real-Time nor Scheduled scanning is in effect, Anti-Malware status will be "On" and the Anti-Malware status light will be blue.
  - When Anti-Malware protection is off and neither Real-Time nor Scheduled scanning is in effect, Anti-Malware status will be "Off" and the Anti-Malware status light will be blue.
  - When Anti-Malware protection is off and neither Real-Time nor Scheduled scanning is in effect, Anti-Malware status will be "Off" and the Anti-Malware status light will be blue.

- **Web Reputation:** Whether Web Reputation is on or off.
- **Firewall:** Whether the Firewall is on or off and how many rules are in effect.
- **Intrusion Prevention:** Whether Intrusion Prevention is on or off and how many rules are in effect.
- **Integrity Monitoring:** Whether Integrity Monitoring is on or off and how many rules are in effect (Agent only).
- **Log Inspection:** Whether Log Inspection is on or off and how many rules are in effect (Agent only).
- **Online:** Indicates whether the Manager can currently communicate with the Agent/Appliance.
- **Last Communication:** The last time the Manager successfully communicated with the Agent/Appliance on this computer.
- **Check Status:** This button allows you to force the Manager to perform an immediate heartbeat operation to check the status of the Agent/Appliance. Check Status will not perform an update of the Agent/Appliance. (If an update is required click the Update Now button on the Actions tab.) When Manager to Agent/Appliance Communications is set to "Agent/Appliance Initiated" the Check Status button is disabled. (Checking status will not update the logs for this computer. To update the logs for this computer, go to the Actions tab.)
- **Clear Warnings/Errors:** Dismisses any Alerts or errors on this computer.
- **ESX Server:** If the computer is a virtual machine protected by a Virtual Appliance, the hosting ESX Server is displayed.
- **Appliance:** If the computer is a virtual machine protected by a Virtual Appliance, the protecting Appliance is displayed.
- **ESX Version:** If the computer is an ESX Server, the ESX version number is displayed.
• **Filter Driver version:** If the computer is an ESX Server, the Filter Driver version number is displayed.

• **Guests:** If the computer is an ESX Server, the Virtual Appliance and Guests are displayed.

• **Appliance Version:** If the computer is a Virtual Appliance, the Appliance version number is displayed.

• **Anti-Malware Ready:** If the computer is a virtual machine, Anti-Malware Ready indicates whether or not the VMware vShield Endpoint Thin Client has been installed. If the computer is a Virtual Appliance, Anti-Malware Ready indicates whether or not the VMware vShield Endpoint driver has been installed on the hosting ESXi server.

• **Protected Guests On:** If the computer is a Virtual Appliance, the IP of the ESX Server and the protected Guest are displayed.

**VMware Virtual Machine Summary**

This section displays a summary of hardware and software configuration information about the virtual machine on which the Agent/Appliance is running (VMware virtual machines only).
Actions

Activation

A newly installed Deep Security Agent/Appliance needs to be "activated" by the Deep Security Manager before Policies, Rules, requests for Event logs, etc. can be sent to it. The activation procedure includes the exchange of SSL keys which uniquely identify a Manager (or one of its nodes) and an Agent/Appliance to each other. Once activated by a Deep Security Manager, an Agent/Appliance will only accept instructions or communicate with the Deep Security Manager which activated it (or one of its nodes).

An unactivated Agent/Appliance can be activated by any Deep Security Manager.

Agents/Appliances can only be deactivated locally on the computer or from the Deep Security Manager which activated it. If an Agent/Appliance is already activated, the button in this area will read Reactivate rather than Activate. Reactivation has the same effect as Activation. A reactivation will reset the Agent/Appliance to the state it was in after first being installed and initiate the exchange of a new set of SSL keys.

When using coordinated protection, the protection provided by Agents and Appliances can be deactivated/reactivated separately.

Policy

When you change the configuration of an Agent/Appliance on a computer using the Deep Security Manager (Apply a new Intrusion Prevention Rule, change logging settings, etc.) the Deep Security Manager has to send the new information to the Agent/Appliance. This is a "Send Policy" instruction. Policy updates usually happen immediately but you can force an update by clicking the Send Policy button.

Software

This displays the version of the Agent/Appliance currently running on the computer. If a newer version of the Agent/Appliance is available for the computer's platform you can click the Upgrade Agent... or Upgrade Appliance... button to remotely upgrade the Agent or Appliance from the Deep Security Manager. You can configure the Deep Security Manager to trigger an Alert if new Agent/Appliance versions for any of your computers by going to Administration > Updates in the main Deep Security Manager window.

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

The Create Diagnostic Package... button creates a snapshot of the state of the Agent/Appliance on the computer. Your support provider may request this for troubleshooting purposes.

If you have lost communication with the Computer, a diagnostics package can be created locally.

To create a diagnostics package locally on a Windows computer:

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

To create a diagnostics package locally on a Linux computer:

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

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

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

TPM (ESX hypervisors only)

The Trusted platform Module (TPM) is a security feature implemented by VMware on its ESX hypervisors. During the boot sequence, an ESX writes a SHA-1 hash of each hypervisor component to a set of registers as it loads. An unexpected change in these values from one boot sequence to the next can indicate a possible security issue worth investigating. Deep Security can monitor the TPM on an ESX after every boot and raise an Alert if it detects any changes. If you select the option to enable TPM monitoring on an ESX which doesn't support it, the option will be automatically disabled.

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

The minimum requirements for TPM monitoring are:
- Deep Security Manager 9
- vCenter 5.1
- ESX 5.1
- TPM/TXT installed and enabled on the ESX (consult your VMware documentation for details)
- the Deep Security Integrity Monitoring Module must be On for this ESX.
Events

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

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

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

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

- **Add Tag(s):** Add an Event Tag to this event (See *Event Tagging (page 447)*.)
- **Remove Tag(s):** Remove exisiting Event Tags

**View**

Selecting an event and clicking **View** displays the **Event ViewerProperties** window.

**General**

**General Information**

- **Time:** The time according to the system clock on the computer hosting the Deep Security Manager.
- **Level:** The severity level of event that occurred. Event levels include **Info**, **Warning**, and **Error**.
- **Event ID:** The event type's unique identifier.
- **Event:** The name of the event (associated with the event ID.)
- **Target:** The system object associated with the event will be identified here. Clicking the object's identification will display the object's properties sheet.
- **Action Performed By:** If the event was initiated by a User, that User's username will be displayed here. Clicking the username will display the **User Properties** window.
- **Manager:** The hostname of the Deep Security Manager computer.
Description

If appropriate, the specific details of what action was performed to trigger this entry in the system event log will be displayed here.

Tags

The Tags tab displays tags that have been attached to this Event. For more information on Event tagging, see Policies > Common Objects > Other > Tags, and Event Tagging (page 447) in the Reference section.

Filter the List and/or Search for an Event

The Period toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The Computers toolbar lets you organize the display of event log entries by computer groups or computer Policies.

Clicking Advanced Search toggles the display of the search bar.

Pressing the "Add Search Bar" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the "Submit Request" button (at the right of the toolbars with the right-arrow on it).

Export

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

Auto-Tagging

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

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

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

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

The Anti-Malware page has the following tabbed sections:

- General (page 133)
- Smart Protection (page 134)
- Advanced (page 135)
- Quarantined Files (page 137)
- Events (page 138)
General

Anti-Malware

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

Real-Time Scan

By assigning a Malware Scan Configuration here, you are enabling Real-Time Scan mode for computer to which this Policy is assigned. Up to five Malware Scan Configurations can be applied to computers via a Policy. They are applied in order of priority and according to the schedule during which they are active.

---

**Note:** "No Schedule" means the configuration will never be active.

---

**Note:** Remember that Manual, Scheduled, and Real-Time scans can have different properties.

---

Manual Scan

Select the Malware Scan Configuration to use when manually initiating a scan.

Scheduled Scan

Select the Malware Scan Configuration to use when a running a scan that is initiated by a Scheduled Task

Malware Scan (Computer Editor only)

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

Smart Scan

Smart Scan shifts much of the malware and spyware scanning functionality to a Smart Protection Server. It keeps local pattern files small and reduces the size and number of updates required by Agents/Appliances. Smart Scan uses the Smart Protection Network's File Reputation Service which can be accessed on the global Smart Protection Network or on a locally installed Smart Protection Server.

**Note:** A computer that is configured to use Smart Scan will not download full Anti-Malware patterns locally. Therefore if your Anti-Malware license expires while a computer is configured to use Smart Scan, switching Smart Scan off will not result in local patterns being used to scan for malware since no Anti-Malware patterns will be present locally.

Smart Protection Server for File Reputation

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

Select the **When off domain, connect to global Smart Protection Service. (Windows only.)** option to use the global Smart Protection Service if the computer is off domain. The computer is considered to be off domain if it cannot connect to its domain controller. (This option is for Windows Agents only.)

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

Quarantined Files

**Maximum disk space used to store quarantined files:** This setting determines how much disk space can be used to store quarantined files. It applies globally to all computers: physical machines, virtual machines, and Virtual Appliances. The setting can be overridden at the Policy level and at the Computer level. This setting should be increased at the Policy or Computer level for Virtual Appliances if they are likely to be storing quarantined files for multiple virtual machines.

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

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

Scan Limitation

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

Resource Allocation for Malware Scans

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

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

Allowed Spyware/Grayware

- **Enable allowed Spyware/Grayware:** Use this setting to maintain a list of allowed applications that have been identified as spyware/grayware by Deep Security.
Spyware/grayware can be added to the approved list in one of two ways. You can add it using an Anti-Malware Event where the application was detected or you can manually enter the name of the spyware/grayware.

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

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

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

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

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

---

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

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

---

**Local Event Notification**

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

**VM Scan Cache**

**Scan Caching** is used by the Virtual Appliance to maximize the efficiency of Malware and Integrity Monitoring Scans of virtual machines. For information on Scan Cache configurations, see *Virtual Appliance Scan Caching (page 293)*.
Quarantined Files

Quarantined Files are displayed the same way as they are in the main Deep Security Manager window except that only files that were quarantined on this computer are listed. (See Quarantined Files (page 29).)
Events

Anti-Malware Events are displayed the same way they are in the main Deep Security Manager window except that only events associated with this Policy or specific computer are displayed. (See *Anti-Malware Events (page 26).*
Web Reputation

The Web Reputation module blocks web pages based on their reputation ratings. It queries the Trend Micro Smart Protection Network servers for these ratings, which are aggregated from multiple sources, including web page links, domain and IP address relationships, spam sources, and links in spam messages. By obtaining ratings from the Smart Protection Network, Web Reputation uses the latest available information to block harmful pages.

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

The Web Reputation Service page has the following tabbed sections:

- General (page 140)
- Exceptions (page 141)
- Smart Protection (page 142)
- Advanced (page 143)
- Events (page 144)
General

Web Reputation

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

Security Level

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

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

Select a security level to implement:

**High**: blocks pages that are:

- Dangerous
- Highly suspicious
- Suspicious

**Medium**: blocks pages that are:

- Dangerous
- Highly suspicious

**Low**: blocks pages that are:

- Dangerous

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

- Unrated by Trend Micro
Exceptions

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

**Note:** The *Allowed* list takes precedence over the *Blocked* list. URLs that match entries in the *Allowed* list are not checked against the *Blocked* list.

Allowed

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

- **Allow URLs from the domain:** Allow all pages from the domain. Sub-domains are supported. Only include the domain (and optionally sub-domain) in the entry. For example, "example.com" and "another.example.com" are valid entries.
- **Allow the URL:** The URL as entered will be allowed. Wildcards are supported. For example, "example.com/shopping/coats.html", and "example.com/shopping/*" are valid entries.

Blocked

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

- **Block URLs from the domain:** Block all pages from the domain. Sub-domains are supported. Only include the domain (and optionally sub-domain) in the entry. For example, "example.com" and "another.example.com" are valid entries.
- **Block the URL:** The URL as entered will be blocked. Wildcards are supported. For example, "example.com/shopping/coats.html", and "example.com/shopping/*" are valid entries.
- **Block URLs containing this keyword:** Any URL containing the keyword will be blocked.
Smart Protection

Smart Protection Server for Web Reputation Service

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

Select the "When off domain, connect to global Smart Protection Service. (Windows only.)" option to use the global Smart Protection Service if the computer is off domain. The computer is considered to be off domain if it cannot connect to its domain controller. (This option is for Windows Agents only.)

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

Blocking page

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

Alert

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

Ports

Select specific ports to monitor for potentially harmful web pages.

Local Event Notification

Display local notifications via the Deep Security Notifier (page 399) when access to a malicious Web site is blocked.
Events

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

The **Firewall** module provides bi-directional stateful firewall protection. It prevents Denial of Service attacks and provides coverage for all IP-based protocols and frame types as well as filtering for ports and IP and MAC addresses.

The Firewall page contains the following tabbed sections:

- General (page 146)
- Interface Isolation (page 148)
- Reconnaissance (page 149)
- Advanced (page 151)
- Events (page 152)
General

Firewall

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

Firewall Stateful Configurations

Select which Firewall Stateful Configuration to apply to this Policy. If you have defined multiple Interfaces for this Policy (above), you can specify independent configurations for each interface.

Port Scan (Computer Editor only)

Last Port Scan: The last time that the Deep Security manager ran a port scan on this computer.

Scanned Ports: The port which were scanned during the most recent port scan.

Open Ports: Listed beneath the IP address of the local computer will be a list of ports that were found to be open.

The Scan For Open Ports and the Cancel Port Scan buttons let you initiate or cancel a port scan on this computer. Deep Security Manager will scan the range of ports defined in Policy/Computer Editor > Settings > Scanning > Open Ports > Ports to Scan.

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

Assigned Firewall Rules

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

From an Editor window, you can edit a Firewall Rule so that your changes apply only locally in the context of your editor (either the Computer or Policy Editor), or you can edit the Rule so that the changes apply globally to all other Policies and Computers that are using the Rule.

To edit the Rule locally, select the Rule and click Properties...( ) or right-click the Rule and click Properties...
To edit the Rule globally, right-click the Rule and click Properties (Global)...
Interface Isolation

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

Interface Patterns

When Interface Isolation is enabled, The firewall will try to match the Java Regular Expression Patterns to interface names on the local computer. Only interfaces matching the highest priority pattern will be permitted to transmit traffic. Other interfaces (which match any of the remaining patterns on the list) will be "restricted". Restricted Interfaces will block all traffic unless an Allow Firewall Rule is used to allow specific traffic to pass through.

Note: For information on Java regular expression syntax use, see http://docs.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html

Selecting Limit to one active interface will restrict traffic to only a single interface (even if more than one interface matches the highest priority pattern).
Reconnaissance

Reconnaissance Scans

The **Reconnaissance** page allows Users to enable and configure traffic analysis settings on all or selected computers.

- **Reconnaissance Scan Detection Enabled**: Turn the ability to detect reconnaissance scans on or off.
- **Computers/Networks on which to perform detection**: Choose from the drop-down list the IPs to protect. Choose from existing IP Lists. (You can use the Policies > Common Objects > Lists > IP Lists page to create an IP List specifically for this purpose.)
- **Do not perform detection on traffic coming from**: Select from a set of IP Lists which computers and networks to ignore. (As above, you can use the Policies > Common Objects > Lists > IP Lists page to create an IP List specifically for this purpose.)

For each type of attack, the Agent/Appliance can be instructed to send the information to the Deep Security Manager where an Alert will be triggered. You can configure the Manager to send an email notification when the Alerts are triggered. (See Administration > System Settings > Alerts . The Alerts are: "Network or Port Scan Detected", "Computer OS Fingerprint Probe Detected", "TCP Null Scan Detected", "TCP FIN Scan Detected", and "TCP Xmas Scan Detected.") Select **Notify DSM Immediately** for this option.

**Note:** Stateful Inspection must be on and TCP and UDP Logging enabled for Reconnaissance protection to function. Stateful Inspection can be enabled on the Policy/Computer Editor > Firewall > General tab and logging can be enabled on the Policy/Computer Editor > Firewall > Advanced tab.

Once an attack has been detected, you can instruct the Agents/Appliances to block traffic from the source IPs for a period of time. Use the **Block Traffic** drop-down lists to set the number of minutes.

- **Computer OS Fingerprint Probe**: The Agents/Appliances will recognize and react to active TCP stack OS fingerprinting attempts.
- **Network or Port Scan**: The Agents/Appliances will recognize and react to port scans.
- **TCP Null Scan**: The Agents/Appliances will refuse packets with no flags set.
- **TCP SYNFIN Scan**: The Agents/Appliances will refuse packets with only the SYN and FIN flags set.
- **TCP Xmas Scan**: The Agents/Appliances will refuse packets with only the FIN, URG, and PSH flags set or a value of 0xFF (every possible flag set).

**Note:** "Computer OS Fingerprint Probe" and "Network or Port Scans" differ from the other three types of reconnaissance in that they cannot be recognized by a single packet.
The Agent/Appliance reports a computer or port scan if it detects that a remote IP is visiting an abnormal ratio of IPs to ports. Normally an Agent/Appliance computer will only see traffic destined for itself, so a port scan is by far the most common type of probe that will be detected. However, if a computer is acting as a router or bridge it could see traffic destined for a number of other computers, making it possible for the Agent/Appliance to detect a computer scan (ex. scanning a whole subnet for computers with port 80 open).

Detecting these scans can take several seconds since the Agent/Appliance needs to be able to track failed connections and decide that there are an abnormal number of failed connections coming from a single computer in a relatively short period of time.

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

Note: Deep Security Agents running on Windows computers with browser applications may occasionally report false-positive reconnaissance scans due to residual traffic arriving from closed connections.

Note: For the "Notify DSM Immediately" option to work, the Agents/Appliances must be configured for Agent/Appliance initiated or bi-directional communication in Policy/Computer Editor > Settings > Computer. If enabled, the Agent/Appliance will initiate a heartbeat to the Deep Security Manager immediately upon detecting the attack or probe.
Advanced

Events

Set whether to generate Events for packets that are "Out of Allowed Policy". These are packets that have been blocked because they have not been specifically allowed by an Allow Firewall Rule. Setting this option to Yes may generate a large number of Events depending the Firewall Rules you have in effect.
Events

Firewall Events are displayed the same way as they are in the main Deep Security Manager window except that only Events relating to this Policy or specific computer are displayed.
Intrusion Prevention

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

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

- **General** (page 154)
- **Advanced** (page 156)
- **Events** (page 158)
General

Intrusion Prevention

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

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

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

---

**Note:** This setting only applies when the Network Engine is operating Inline; that is, live traffic is being streamed through the Deep Security network engine. The alternative to Inline mode is Tap mode, where the live traffic is cloned, and it is only this cloned traffic that is analyzed by the network engine. Prevent mode is impossible when in Tap mode because the network engine does not control the live traffic stream.

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

---

Assigned Intrusion Prevention Rules

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

From an Editor window, you can edit a Intrusion Prevention Rule so that your changes apply only locally in the context of your editor (either the Computer or Policy Editor), or you can edit the Rule so that the changes apply globally to all other Policies and Computers that are using the Rule.

**To edit the Rule locally**, select the Rule and click **Properties**... or right-click the Rule and click **Properties**...

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

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

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

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

Event Data

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

- **Log All Packet Data**: Record the packet data for Events that are not associated with specific Firewall or Intrusion Prevention Rules. That is, log packet data for Events such as "Dropped Retransmit" or "Invalid ACK".

  Note: Events that have been aggregated because of Event folding cannot have their packet data saved.

- **Log only one packet within period**: If the above is not set, but this is set, then most logs will only contain the header data with a full packet being attached only periodically.

- **Period for Log only one packet within period**: The period between when full packet data will be logged if the above is set.

- **Maximum data size to store when packet data is captured**: The maximum size of header or packet data to be attached to a log.

Rule Updates

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

SSL Configurations (Computer editors only)

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

To create a new SSL Configuration, click New and follow the steps in the SSL Configuration wizard.
If the computer you are configuring is being installed on the computer hosting the Deep Security Manager, the wizard will provide you with credentials that are already stored in the Deep Security Manager.

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

**Assignment**

- **General Information:** The name and description of the SSL configuration, and whether it is enabled on this computer.
- **Interface Assignments:** Which interfaces this configuration is being applied to.
- **IP Assignment:** Which IP(s) this configuration applies to.
- **Port Selection:** Which port(s) this configuration applies to.

**Credentials**

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

---

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

---

For information on setting up SSL filtering, see *SSL Data Streams (page 389).*
Events

Log Inspection Events are displayed the same way as they are in the main Deep Security Manager window except that only Events relating to this Policy or specific computer are displayed.
Integrity Monitoring

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

The Integrity Monitoring page has the following tabbed sections:

- General (page 160)
- Advanced (page 161)
- Events (page 162)
General

Integrity Monitoring

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

Integrity Scan (Computer Editor only)

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

Baseline (Computer Editor only)

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

Assigned Integrity Monitoring Rules

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

From an Editor window, you can edit an Integrity Monitoring Rule so that your changes apply only locally in the context of your editor (either the Computer or Policy Editor), or you can edit the Rule so that the changes apply globally to all other Policies and Computers that are using the Rule.

To edit the Rule locally, select the Rule and click Properties... or right-click the Rule and click Properties...

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

Recommendations

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

Content Hash Algorithms

Select the hash algorithm(s) that will be used by the Integrity Monitoring module to store baseline information. You can select more than one algorithm, but this is not recommended because of the detrimental effect on performance.

VM Scan Cache

For information on Integrity Monitoring Scan Cache Configurations, see *Virtual Appliance Scan Caching (page 293).*
Events

Integrity Monitoring Events are displayed the same way as they are in the main Deep Security Manager window except that only Events relating to this Policy or specific computer are displayed.
Log Inspection

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

The Log Inspection page has the following tabbed sections:

- *General (page 164)*
- *Advanced (page 165)*
- *Events (page 166)*
General

Log Inspection

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

Assigned Log Inspection Rules

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

From an Editor window, you can edit a Log Inspection Rule so that your changes apply only locally in the context of your editor (either the Computer or Policy Editor), or you can edit the Rule so that the changes apply globally to all other Policies and Computers that are using the Rule.

To edit the Rule locally, select the Rule and click Properties... or right-click the Rule and click Properties...

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

Recommendations

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

Severity Clipping

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

Store events at the Agent/Appliance for later retrieval by DSM when they equal or exceed the following severity level: This setting determines which Log Inspection Events are kept in the database and displayed in the Log Inspection Events page.
Events

Log Inspection Events are displayed the same way as they are in the main Deep Security Manager window except that only Events relating to this Policy or specific computer are displayed.
Interfaces/Interface Types

Interfaces (Computer Editor)

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

Interface Types (Policy Editor)

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

Network Interface Specificity

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

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

The Matches defines a wild-card based interface name match to auto map the interfaces to the appropriate interface type. Examples would be "Local Area Connection *", "eth*", and "Wireless *". When an interface cannot be mapped automatically, an Alert is triggered. You can manually map it from the Interfaces page in the computer editor for a particular computer.

Note: If interfaces are detected on the computer that don't match any of these entries, the Manager will trigger an Alert.

Interface Type X (Interface Patterns)

To enforce interface isolation, set the Enable Interface Isolation option on the Policy/Computer Editor > Firewall > Interface Isolation tab and enter string patterns that will match the names of the interfaces on a computer (in order of priority). You can use Java regular expression syntax (http://docs.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html) when creating your list of interfaces.

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

- Computer (page 169)
- Network Engine (page 173)
- Scanning (page 179)
- SIEM (page 180)
Computer

Communication Direction

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

- **Manager Initiated:** With this option selected, all Manager to Agent/Appliance communications are initiated by the Manager. This includes security configuration updates, heartbeat operations, and requests for Event logs.

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

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

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

**Note:** To enable communications between the Manager and the Agents/Appliances, the Manager automatically implements a (hidden) Firewall Rule (priority four, Bypass) which opens port 4118 on the Agents/Appliances to incoming TCP/IP traffic. The default settings open the port to any IP address and any MAC address. You can restrict incoming traffic on this port by creating a new priority 4, Force Allow or Bypass Firewall Rule, which only allows incoming TCP/IP traffic from specific IP and/or MAC addresses. This new Firewall Rule will replace the hidden Firewall Rule if the settings match the following:
**action**: force allow or bypass

**priority**: 4 - highest

**packet's direction**: incoming

**frame type**: IP

**protocol**: TCP

**packet's destination port**: 4118 (or a list or range that includes 4118)

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

---

**Heartbeat**

- **Heartbeat Interval (in minutes)**: How much time passes between heartbeats.

- **Number of Heartbeats that can be missed before an Alert is raised**: Several missed heartbeats in a row may indicate a problem with the Agent/Appliance or the computer. This setting determines how many missed heartbeats are allowed to go by before the Manager triggers an Alert. (For example, entering three will cause the Manager to trigger an Alert on the fourth missed heartbeat.)

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

---

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

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

---

**Send Policy Changes Immediately**

By default, any time you make a change to any element in the Deep Security system, all affected computers are immediately updated. For example, if you edit a port list, all computers already making use of that port list will get updated immediately. (If you make such a change and then look at the **Computers** page, you will see the updates happening.) Not setting the **Automatically update all affected computers after changing any aspect of the Deep Security System** option means that after any changes, you will have to find affected computers on the **Computers** page, right-click them and choose "Update Agent(s) Now" from the context menu.
Troubleshooting

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

Agent Self-Protection

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

- **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent:** This will prevent local users from uninstalling the Agent, stopping the Agent service, modifying Agent-related Windows Registry entries, or modifying Agent-related files.
  - **Local override requires password:** It is possible that a Deep Security Manager loses the ability to communicate with an Agent. In such cases you will have to interact with the Agent locally using the Agent's command-line interface. Enter a password here to password-protect the local command-line functionality. (Recommended.)

  Note: Store this password in a safe location. If you lose or forget the password you will have to contact your support provider for assistance in overriding this protection.

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

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

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

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

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

dsa_control --harden=1 --passwd=password

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

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

• dsa_control --reset

Environment Variable Overrides

Environment variables are used by the Integrity Monitoring module to represent some standard locations in the directory system of the Windows operating system. For example, the Microsoft Windows - 'Hosts' file modified Integrity Monitoring rule, which monitors changes to the Windows hosts file, looks for that file in the C:\WINDOWS\system32\drivers\etc folder. However not all Windows installations use the C:\WINDOWS\ directory, so the Integrity Monitoring rule uses the WINDIR environment variable and represents the directory this way as %WINDIR%\system32\drivers\etc.

Note: Environment variables are used primarily by the Virtual Appliance when performing Agentless Integrity Monitoring on a virtual machine. This is because the Virtual Appliance has no way of knowing if the operating system on a particular virtual machine is using standard directory locations.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALLUSERSPROFILE</td>
<td>C:\ProgramData</td>
</tr>
<tr>
<td>COMMONPROGRAMFILES</td>
<td>C:\Program Files\Common Files</td>
</tr>
<tr>
<td>PROGRAMFILES</td>
<td>C:\Program Files</td>
</tr>
<tr>
<td>SYSTEMDRIVE</td>
<td>C:</td>
</tr>
<tr>
<td>SYSTEMROOT</td>
<td>C:\Windows</td>
</tr>
<tr>
<td>WINDIR</td>
<td>C:\Windows</td>
</tr>
</tbody>
</table>

To override any of these environment variables:

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

The Agent/Appliance's network engine can operate Inline or in Tap Mode. When operating Inline, the live packet stream passes through the network engine. Stateful tables are maintained, Firewall Rules are applied and traffic normalization is carried out so that Intrusion Prevention Rules can be applied to payload content. When operating in Tap Mode, the live packet stream is cloned and diverted from the main stream. In Tap Mode, the live packet stream is not modified; all operations are carried out on the cloned stream.

Events

You can set the maximum size of each individual log file and how many of the most recent files are kept. Event log files will be written to until they reach the maximum allowed size, at which point a new file will be created and written to until it reaches the maximum size and so on. Once the maximum number of files is reached, the oldest will be deleted before a new file is created. Event log entries usually average around 200 bytes in size and so a 4MB log file will hold about 20,000 log entries. How quickly your log files fill up depends on the number of rules in place.

- **Maximum size of the event log files (on Agent/Appliance):** Adjust these settings if you begin to see "Insufficient Disk Space" Alerts for one or more computers.
- **Number of event log files to retain (on Agent/Appliance):** Adjust these settings if you begin to see "Insufficient Disk Space" Alerts for one or more computers.
**Note:** Events are records of individual events. Counters are a record of the number of times individual events have occurred. Events are used to populate the Events pages. Counters are used to populate the Dashboard Widgets (number of Firewall Events over the last 7 days, etc.) and the Reports. You might want to collect only counters if, for example, you are using syslog for event collection; events can potentially take up a lot of disk space and you may not want to store the data twice.

- **Do Not Record Events with Source IP of:** This option is useful if you want Deep Security to not make record Events for traffic from certain trusted computers.

**Note:** The following three settings let you fine tune Event aggregation. To save disk space, Deep Security Agents/Appliances will take multiple occurrences of identical events and aggregate them into a single entry and append a "repeat count", a "first occurrence" timestamp, and a "last occurrence" timestamp. To aggregate event entries, Deep Security Agents/Appliances need to cache the entries in memory while they are being aggregated before writing them to disk.

- **Cache Size:** Determines how many types of events to track at any given time. Setting a value of 10 means that 10 types of events will be tracked (with a repeat count, first occurrence timestamp, and last occurrence timestamp). When a new type of event occurs, the oldest of the 10 aggregated events will be flushed from the cache and written to disk.
- **Cache Lifetime:** Determines how long to keep a record in the cache before flushing it to disk. If this value is 10 minutes and nothing else causes the record to be flushed, any record that reaches an age of 10 minutes gets flushed to disk.
- **Cache Staletime:** Determines how long to keep a record whose repeat count has not been recently incremented. If Cache Lifetime is 10 minutes and Cache Staletime is two minutes, an event record which has gone two minutes without being incremented will be flushed and written to disk.

**Note:** Regardless of the above settings, the cache is flushed whenever Events are sent to the Deep Security Manager.

### Advanced

Use Custom Driver Settings

- **CLOSED timeout:** For gateway use. When a gateway passes on a "hard close" (RST), the side of the gateway that received the RST will keep the connection alive for this amount of time before closing it.
- **SYN_SENT Timeout:** How long to stay in the SYN-SENT state before closing the connection.
- **SYN_RCVD Timeout:** How long to stay in the SYN_RCVD state before closing the connection.
- **FIN_WAIT1 Timeout:** How long to stay in the FIN-WAIT1 state before closing the connection.
• **ESTABLISHED Timeout**: How long to stay in the ESTABLISHED state before closing the connection.

• **ERROR Timeout**: How long to maintain a connection in an Error state. (For UDP connections, the error can be caused by any of a variety of UDP problems. For TCP connections, the errors are probably due to packets being dropped by the firewall.)

• **DISCONNECT Timeout**: How long to maintain idle connections before disconnecting.

• **CLOSE_WAIT Timeout**: How long to stay in the CLOSE-WAIT state before closing the connection.

• **CLOSING Timeout**: How long to stay in the CLOSING state before closing the connection.

• **LAST_ACK Timeout**: How long to stay in the LAST-ACK state before closing the connection.

• **ACK Storm timeout**: The maximum period of time between retransmitted ACKs within an ACK Storm. In other words, if ACKs are being retransmitted at a lower frequency then this timeout, they will NOT be considered part of an ACK Storm.

• **Boot Start Timeout**: For gateway use. When a gateway is booted, there may already exist established connections passing through the gateway. This timeout defines the amount of time to allow non-SYN packets that could be part of a connection that was established before the gateway was booted to close.

• **Cold Start Timeout**: Amount of time to allow non-SYN packets that could belong to a connection that was established before the stateful mechanism was started.

• **UDP Timeout**: Maximum duration of a UDP connection.

• **ICMP Timeout**: Maximum duration of an ICMP connection.

• **Allow Null IP**: Allow or block packets with no source and/or destination IP address.

• **Block IPv6 on Agents and Appliances versions 8 and earlier**: Block or Allow IPv6 packets on older version 8 Agents and Appliances.

  **Note:** *Deep Security Agents and Appliances versions 8 and older are unable to apply Firewall or DPI Rules to IPv6 network traffic and so the default setting for these older versions is to block IPv6 traffic.*

• **Block IPv6 on Agents and Appliances versions 9 and later**: Block or Allow IPv6 packets on current Agents and Appliances.

• **Connection Cleanup Timeout**: Time between cleanup of closed connections (see next).

• **Maximum Connections per Cleanup**: Maximum number of closed connections to cleanup per periodic connection cleanup (see previous).

• **Block Same Src-Dest IP Address**: Block or allow packets with same source and destination IP address. (Doesn't apply to loopback interface.)

• **Maximum TCP Connections**: Maximum simultaneous TCP Connections.

• **Maximum UDP Connections**: Maximum simultaneous UDP Connections.

• **Maximum ICMP Connections**: Maximum simultaneous ICMP Connections.

• **Maximum Events per Second**: Maximum number of events that can be written per second.

• **TCP MSS Limit**: The MSS is the Maximum Segment Size (or largest amount of data) that can be sent in a TCP packet without being fragmented. This is usually established when two computers
establish communication. However, in some occasions, the traffic goes through a router or switch that has a smaller MSS. In this case the MSS can change. This causes retransmission of the packets and the Agent/Appliance logs them as "Dropped Retransmit". In cases where there are large numbers of Dropped Retransmit event entries, you may wish to lower this limit and see if the volume is reduced.

- **Number of Event Nodes**: The maximum amount of kernel memory the driver will use to store log/event information for folding at any one time.

**Note**: Event folding occurs when many Events of the same type occur in succession. In such cases, the Agent/Appliance will "fold" all the events into one.

- **Ignore Status Code**: This option lets you ignore certain types of Events. If, for example, you are getting a lot of "Invalid Flags" you can simply ignore all instances of that Event.
- **Ignore Status Code**: Same as above.
- **Ignore Status Code**: Same as above.
- **Advanced Logging Policy**:
  - **Bypass**: No filtering of Events. Overrides the "Ignore Status Code" settings (above) and other advanced settings, but does not override logging settings defined in the Deep Security Manager. For example, if Firewall Stateful Configuration logging options set from a Firewall Stateful Configuration Properties window in the Deep Security Manager will not be affected.
  - **Default**: Will switch to "Tap Mode" (below) if the engine is in Tap Mode, and will switch to "Normal" (above) if the engine is in Inline Mode. **Normal**: All Events are logged except dropped retransmits.
  - **Backwards Compatibility Mode**: For support use only.
  - **Verbose Mode**: Same as "Normal" but including dropped retransmits.
  - **Stateful and Normalization Suppression**: Ignores dropped retransmit, out of connection, invalid flags, invalid sequence, invalid ack, unsolicited udp, unsolicited ICMP, out of allowed policy.
  - **Stateful, Normalization, and Frag Suppression**: Ignores everything that "Stateful and Normalization Suppression" ignores as well as events related to fragmentation.
  - **Stateful, Frag, and Verifier Suppression**: Ignores everything "Stateful, Normalization, and Frag Suppression" ignores as well as verifier-related events.
  - **Tap Mode**: Ignores dropped retransmit, out of connection, invalid flags, invalid sequence, invalid ack, max ack retransmit, packet on closed connection.

**Note**: For a more comprehensive list of which Events are ignored in **Stateful and Normalization Suppression; Stateful, Normalization, and Frag Suppression; Stateful, Frag, and Verifier Suppression; and Tap modes**, see Advanced Logging Policy Modes in the Reference section.

- **Silent TCP Connection Drop**: When Silent TCP Connection Drop is on, a RST packet is only sent to the local stack. No RST packet is sent on the wire. This reduces the amount of information sent back to a potential attacker.
If you enable the Silent TCP Connection Drop you must also adjust the DISCONNECT Timeout. Possible values for DISCONNECT Timeout range from 0 seconds to 10 minutes. This must be set high enough that the connection is closed by the application before it is closed by the Deep Security Agent/Appliance. Factors that will affect the DISCONNECT Timeout value include the operating system, the applications that are creating the connections, and network topology.

**Enable Debug Mode:** When in debug mode, the Agent/Appliance captures a certain number of packets (specified by the setting below: Number of Packets to retain in Debug Mode). When a rule is triggered and debug mode is on, the Agent/Appliance will keep a record of the last X packets that passed before the rule was triggered. It will return those packets to the Manager as Debug Events.

**Note:** Debug mode can very easily cause excessive log generation and should only be used under Client Services supervision.

**Number of Packets to retain in Debug Mode:** The number of packets to retain and log when debug mode is on.

**Log All Packet Data:** Record the packet data for Events that are not associated with specific Firewall or Intrusion Prevention Rules. That is, log packet data for Events such as "Dropped Retransmit" or "Invalid ACK".

**Note:** Events that have been aggregated because of Event folding cannot have their packet data saved.

**Log only one packet within period:** If the above is not set, but this is set, then most logs will only contain the header data with a full packet being attached only periodically.

**Period for Log only one packet within period:** The period between when full packet data will be logged if the above is set.

**Maximum data size to store when packet data is captured:** The maximum size of header or packet data to be attached to a log.

**Generate Connection Events for TCP:** Generates a Firewall Event every time a TCP connection is established.

**Generate Connection Events for ICMP:** Generates a Firewall Event every time an ICMP connection is established.

**Generate Connection Events for UDP:** Generates a Firewall Event every time a UDP connection is established.

**Bypass CISCO WAAS Connections:** This mode bypasses stateful analysis of TCP sequence numbers for connections initiated with the proprietary CISCO WAAS TCP option selected. This protocol carries extra information in invalid TCP Sequence and ACK numbers that interfere with stateful firewall checks. Only enable this option if you are using CISCO WAAS and you are seeing connections with Invalid SEQ or Invalid ACK in the firewall logs. When this option is selected, TCP stateful sequence number checks are still performed for non WAAS enabled connections.
- **Drop Evasive Retransmit**: Incoming packets containing data that has already been processed will be dropped to avoid possible evasive retransmit attack techniques.

- **Verify TCP Checksum**: The segment's checksum field data will be used to assess the integrity of the segment.

- **Minimum Fragment Offset**: Defines the minimum acceptable IP fragment offset. Packets with offsets less than this will be dropped with reason "IP fragment offset too small". If set to 0 no limit is enforced. (default 60)

- **Minimum Fragment Size**: Defines the minimum acceptable IP fragment size. Fragmented packets that are smaller than this will be dropped with reason "First fragment too small" as potentially malicious. (default 120)

- **SSL Session Size**: Sets the maximum number of SSL session entries maintained for SSL session keys.

- **SSL Session Time**: Sets how long SSL session renewal keys are valid before they expire.

- **Fragment Timeout**: How long to keep fragmented packets.

- **Maximum number of fragmented IP packets to keep**: If configured to do so, the Intrusion Prevention Rules will edit the content of a packet (or packet fragment) if that content is considered suspicious. This setting determines how long after editing to wait for the remaining packet fragments before discarding the packet.

- **Send ICMP to indicate fragmented packet timeout exceeded**: Whether not to indicate to remote computer with an ICMP packet that a connection timeout has been exceeded
Scanning

Scanning for Open Ports

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

Scanning for Recommendations

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

Virtual Appliance Scans (Policy editor only)

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

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

Event Forwarding Frequency (From the Agent/Appliance)

Select how often events are sent from the Agent/Appliance to Alert recipients. (Enter Syslog configuration below.)

Event Forwarding

The Events from each of the protection modules can be forwarded to a remote computer via syslog. For information on configuring Syslog, see *Syslog Integration (SIEM) (page 271)*.
Updates (Computer Editor only)

The Security Updates page lists the individual components of a Security Update that are in effect on this computer.

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

**Rollback Security Updates**: rolls back the current Security Update to the one previously in effect on this computer.
Overrides

Policies in Deep Security are intended to be created in a hierarchical structure. As an administrator you begin with one or more base Policies from create multiple levels of child Policies which get progressively more granular in their detail. You can assign broadly applicable Rules and other configuration settings at the top level Policies and then get more targeted and specific as you go down through levels of child Policies, eventually arriving at Rule and configuration assignments at the individual computer level.

As well as assigning more granular settings as you move down through the Policy tree, you can also override settings from higher up the Policy tree. ThisOverrides page shows you whether and how many settings have been overridden at this Policy or specific computer level. To undo the Overrides at this level, click the Remove button.

For more information, see Policies, Inheritance and Overrides (page 505).
Administration

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

- The **system Settings (page 184)** section lets you control the administration of the Deep Security system.
- The **System Information (page 227)** page contains details about the current state of the Deep Security Manager.
- All currently defined tags are displayed in the **Tags (page 104)** page.
- The **Scheduled Tasks (page 208)** section provides the ability to configure recurring automated tasks.
- The **Event-Based Tasks (page 210)** section provides the ability to configure tasks that will be performed upon the occurrence of specific events.
- Use the **Roles (page 221)** section to define various Roles with different rights. Roles are then assigned to Users.
- Use the **Users (page 217)** section to create and modify User accounts for Users of the Deep Security Manager.
- Use the **Contacts (page 225)** section to create and modify contacts.
- The **license (page 216)** page displays details about your Trend Micro product license such as which Deep Security protection modules are available and how many computers you are licensed to install Agent/Appliance software on.
- The **Updates (page 229)** section allows you to manage security and software updates.
System Settings

The System Settings page contains the following tabbed pages:

- Tenants (page 185)
- Agents (page 188)
- Alerts (page 191)
- Contexts (page 192)
- SIEM (page 193)
- SNMP (page 194)
- Ranking (page 195)
- System Events (page 197)
- Security (page 198)
- Updates (page 200)
- Smart Feedback (page 202)
- SMTP (page 203)
- Storage (page 204)
- Advanced (page 205)
Tenants

Multi-Tenant Options

- **Multi-Tenant License Mode:** The multi-Tenant license mode can be changed after multi-Tenant is setup, however it is important to note that switching from inherited to per-Tenant will cause existing Tenants to no longer have any licensed module.

- **Allow Tenants to use the Relays in my "Default Relay Group" (for unassigned Relays):** gives Tenants automatic access to relays setup in the primary Tenant. This saves Tenants from having to setup dedicated relays for security updates.

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

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

- **Allow Tenants to use the "Backup" Scheduled Task:** Determines if the Backup Scheduled Task should be available to Tenants. In most cases backups should be managed by the database administrator and this option should be left checked.

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

- **Allow Tenants to run Host Discovery (directly and as a Scheduled Task):** Determines if discovery is exposed. This may not be desirable in service provider environments where network discovery has been prohibited.

- **Allow Tenants to run Port Scan (directly and as a Scheduled Task):** Determines if port scans can be executed. This may not be desirable in service provider environments where network scan has been prohibited.

- **Allow Tenants to synchronize with vCenter:** Determines if vCenter connectivity should be exposed. If the deployment is intended for a public service, this option should most likely be disabled since there will not be a route to the vCenter from a hosted service.

- **Allow Tenants to synchronize with Cloud Connectors:** Determines if Tenants can setup cloud sync. This is generally applicable to any deployment.

- **Allow Tenants to synchronize with Directories:** Determines if Tenants can setup both User and Computer sync with Directories (LDAP or Active Directory for Computers, Active Directory only for users). If the deployment is intended for a public service, this option should most likely be disabled since there will not be a route to the directory from a hosted service.
• New Tenants should automatically check for software updates:
• Lock down the following configuration options (all Tenants use the options configured for the Primary Tenant):
  ◦ **Agents Tab - Data Privacy Settings:** Allows the Primary Tenant to configure data privacy settings. (This setting only applies to "Allow Packet Data Capture on Encrypted Traffic (SSL)" in on the Administration > System Settings > Agents tab.)
  ◦ **SIEM Tab (All Tenants use the settings located on the SIEM tab for ALL event types and syslog is relayed via the Manager):** Allows the primary Tenant to configure syslog for all Tenants at once. In CEF format the Tenant name is included as TrendMicroDsTenant.
  ◦ **SMTP Tab:** Locks all settings on the SMTP tab.
  ◦ **Storage Tab:** Locks all settings on the Storage tab.

**Database Servers**

By default all Tenants will be created on the same database server Deep Security Manager was installed with. In order to provide additional scalability Deep Security Manager supports adding additional database servers.

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

- create databases,
- delete databases and
- define schema.

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

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

For information on setting up database user accounts for multi-tenancy see [Multi-Tenancy (page 402)].

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

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

**New Tenant Template**

The Tenant Template feature provides a convenient way of creating a customized "out-of-the-box" experience for new Tenants.
The process involves:

1. Creating a new Tenant
2. Logging in as that Tenant
3. Customizing the example Policies (adding/removing/modifying) and the Security Update version (applying newer versions)
4. Return to the primary Tenant and run the Tenant template wizard
5. Select the Tenant to snapshot

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

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

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

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

**Protection Usage Monitoring**

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

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

Use these options determine which additional additional Tenant computer details are recorded.
Agents

Hostnames

Update the "Hostname" entry if an IP is used as a hostname and a change in IP is detected on the computer after Agent/Appliance-initiated communication or discovery: Turn this option on if, for example, your network has no DNS and you are using dynamic IPs. (Deep Security Manager always identifies computers/Agents/Appliances by their unique fingerprint, not their IP addresses.)

Agent-Initiated Activation

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

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

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

<table>
<thead>
<tr>
<th>Usage: dsa_control [/a &lt;str&gt;] [/g &lt;str&gt;] [/c &lt;str&gt;] [/r]</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>/a &lt;str&gt;</td>
<td>Activate Agent with DSM at specified URL. URL format must be &quot;dsm://hostOrIp:port/&quot;</td>
</tr>
<tr>
<td>/g &lt;str&gt;</td>
<td>Agent URL. Defaults to &quot;<a href="https://127.0.0.1:4118/">https://127.0.0.1:4118/</a>&quot;</td>
</tr>
<tr>
<td>/c &lt;str&gt;</td>
<td>Certificate file</td>
</tr>
<tr>
<td>/r</td>
<td>Reset Agent configuration</td>
</tr>
</tbody>
</table>

Note: You can instruct Deep Security Manager to send a default Policy to self-activating Agents which do not already have a Policy assigned to them. Use the Policy to assign (when no Policy is currently assigned) to select a Policy.

If you allow Agent-Initiated Activated Activation, there are several further options you can configure:
Specify on which computers you will allow Agent-Initiated Activation:

- **For Any Computers**: Any computers, whether they are already listed on the Deep Manager's Computers page or not.
- **For Existing Computers**: Only computers already listed on the Computers page.
- **For Computers on the following IP List**: Only computers whose IP address has a match on the specified IP List.

Policy to assign (if Policy not assigned by activation script): The security Policy to assign to the computer if no Policy has been specified in the activation script.

**Note:** If an Event-Based Task exists which assigns Policies to computers where activation is agent-initiated, the Policy specified in the Event-Based Task will override the Policy assigned here or in the activation script.

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

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

Allow reactivation of cloned VMs: When a new VM clone which is running an already activated Deep Security Agent sends a heartbeat to the Deep Security Manager, the Deep Security Manager will recognize it as a clone and reactivate it as a new computer. No Policies or Rules that may have been in place on the original VM will be assigned to the new VM. It will be just a like a newly activated computer.

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

**Note:** For more information on Agent-Initiated Activation, see Command-Line Instructions (page 437) and Deployment Scripts (page 323).
Data Privacy

**Allow packet data capture on encrypted traffic (SSL):** The Intrusion Prevention module allows you to record the packet data that triggers Intrusion Prevention Rules. This setting lets you turn off data capture when Intrusion Prevention rules are being applied to encrypted traffic.

Agentless vCloud Protection

**Allow Appliance protection of vCloud VMs:** Allow virtual machines in a vCloud environment to be protected by a Deep Security Virtual Appliance and let the security of those virtual machines be managed by Tenants in a Multi-Tenancy Deep Security environment.
Alerts

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

**Length of time an Update can be pending before raising an Alert**: The amount of time that can pass between an instruction to perform a security update being sent and the instruction being carried out before an Alert is raised.

**Alert Event Forwarding (from the Manager)**

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

Use this page to configure the settings Deep Security will use to determine whether a protected computer has Internet connectivity or not. Some Deep Security Rules can be applied conditionally depending on the computer's network connectivity conditions. This is known as "Location Awareness". The Internet connectivity condition options for a particular rule can be configured on the Options tab of the rule's Properties window. The Internet Connectivity Test can also be used when implementing Interface Isolation. (See Interface Isolation (page 148) and Interfaces/Interface Types (page 167).)

Internet Connectivity Test

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

  Note: Use Java regular expression syntax (http://docs.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html) to match patterns in the returned content.

  (If you are certain of the returned content you can use a simple string of characters.)

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

Example

For example, to test Internet connectivity, you could use the URL "http://www.example.com", and the string "This domain is established to be used for illustrative examples in documents" which is returned by the server at that URL.
SIEM

System Event Notification (from the Manager)

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

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

For information on configuring Syslog, see *Syslog Integration (SIEM) (page 271).*
SNMP

Forward System Events to a Remote Computer (via SNMP)

Deep Security supports SNMP for forwarding System Events to a computer from the Manager. The MIB file ("DeepSecurity.mib") is located in \Trend Micro\Deep Security Manager\util

**Note:** SNMP Event forwarding is not available to Tenant accounts.
Ranking

The Ranking system provides a way to quantify the importance of Events. By assigning "asset values" to computers, and assigning severity or risk values to Rules, the importance ("Rank") of an Event is calculated by multiplying the two values together. This allows you to sort Events by Rank.

Web Reputation Event Risk Values

Risk values for Web Reputation Events are linked to the three levels of Risk used by the Web Reputation settings on the General tab of the Web Reputation page:

- **Dangerous**: corresponds to "A URL that has been confirmed as fraudulent or a known source of threats."
- **Highly Suspicious**: corresponds to "A URL that is suspected to be fraudulent or a known source of threats."
- **Suspicious**: corresponds to "A URL that is associated with spam or possibly compromised."
- **Blocked by Administrator**: A URL that is on the Web Reputation Service Blocked list.
- **Untested**: A URL that does not have a risk level.

Firewall Rule Severity Values

Severity values for Firewall Rules are linked to their actions: Deny, Log Only, and Packet Rejection. (The latter refers to packets rejected because of a Firewall Stateful Configuration setting.) Use this panel to edit the severity values which will be multiplied by a computer's asset value to determine the rank of a Firewall Event. (A Firewall Rule's actions can viewed and edited in the Rule's Properties window.)

Intrusion Prevention Rule Severity Values

Intrusion Prevention Rule Severity Values are linked to their severity levels: Critical, High, Medium, Low, or Error. Use this panel to edit their values which will be multiplied by a computer's asset value to determine the rank of a Intrusion Prevention Event. A Intrusion Prevention Rule's severity setting can be viewed in the Rule's Properties window.

Integrity Monitoring Rule Severity Values

Integrity Monitoring Rule Severity Values are linked to their severity levels: Critical, High, Medium, or Low. Use this panel to edit their values which will be multiplied by a computer's asset value to determine the rank of
an Integrity Monitoring Event. An Integrity Monitoring Rule's severity can be viewed in the Rule's Properties window.

Log Inspection Rule Severity Values

Log Inspection Rule Severity Values are linked to their severity levels: Critical, High, Medium, or Low. Use this panel to edit their values which will be multiplied by a computer's asset value to determine the rank of a Log Inspection Event. A Log Inspection Rule's severity level can be viewed and edited from the Rule's Properties window.

Asset Values

Asset Values are not associated with any of their other properties like Intrusion Prevention Rules or Firewall Rules. Instead, Asset Values are properties in themselves. A computer's Asset Value can be viewed and edited from the computer's Details window. To simplify the process of assigning asset values, you can predefined some values that will appear in the Asset Importance drop-down list in the first page of the computer's Details window. To view existing predefined computer Asset Values, click the View Asset Values... button in this panel. The Asset Values window displays the predefined settings. These values can be changed, and new ones can be created. (New settings will appear in the drop-down list for all computers.)
System Events

"System Events" include changes to the configuration of an Agent/Appliance, the Deep Security Manager, or Users. They also include errors that may occur during normal operation of the Deep Security system. This page is used to set whether particular events are recorded and whether notifications of the Events should be sent as configured in the System Events area on the Administration > Settings > SIEM or Administration > Settings > SNMP tabs.

For a list of all possible System Events, see System Events (page 474) in the Reference section.
Security

User Security

- **Session Timeout (min):** Specify the period of inactivity after which a User will be required to sign in again.
- **Incorrect Sign-In Attempts (Before Lock Out):** The number of times an individual User (i.e. with a specific username) can attempt to sign in with an incorrect password before he is locked out. Only a User with "Can Edit User Properties" rights can unlock a locked-out User.
- **User Password Minimum Length:** The minimum number of characters required in a password.
- **User Password Requires Both Letters and Numbers:** Letters (a-z, A-Z) as well as numbers (0-9) must be used as part of the password.
- **User Password Requires Both Upper and Lower Case Characters:** Upper and lower case characters must be used.
- **User Password Requires Non-Alphanumeric Characters:** Passwords must include non-alphanumeric characters.

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

**Note:** A note about being signed in as two Users at once: Remember that Firefox sets session cookies on a per-process basis, and not on a per-window basis. This means that if for some reason you want to be signed in as two Users at the same time, you will either have to use two different browsers (if one of them is Firefox), or sign in from two separate computers.

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

Sign In Page Message

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

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

To ensure maximum protection you must keep your pattern files, anti-malware engines, and software components current. The Updates tab on the Administration > System Settings page allows you to set the location where Deep Security Manager checks for updates. To see the status of current updates, go to the Administration > Updates page.

Relays

- **Trend Micro Update Server**: Connect to the default Trend Micro Update Server.
- **Other Update Source**: If you were given an alternative source for updates, enter the URL here including "http://" or "https://". (SSL connections are supported.)
- **Allow Agents/Appliances to download Security Updates from this source if Deep Security Relays are not available**: If an Agent/Appliance cannot communicate with the Relay, it will update directly from the Trend Micro Update Server (or other update source).
- **Agents can update Anti-Malware Patterns and Engines automatically when not in contact with Deep Security Manager**: Even though an Agent cannot communicate with the Deep Security Manager, it will continue to receive updates from its configured source.
- **View Relay Groups...**: Displays the Relay Groups window from which you can:
  - Create, Edit, and Delete Relay Groups
  - View Relay Group properties

Note: For more information on Relays and Relay Groups, see Deep Security Relays in the Reference section.

Proxy Server for Security Updates, CSSS, License Notifications, and Smart Feedback

Specify a proxy server for Security Updates, Certified Safe Software Service (CSSS), license notifications, and Smart Feedback.

Note: Changes to the proxy settings for CSSS will not take effect until the Deep Security Manager and all Manager nodes are restarted.

Deep Security Rule Updates

- **Automatically assign new Intrusion Prevention Rules as required by updated Application Types and Intrusion Prevention Rule dependencies**: New Intrusion Prevention Rules in Security Updates are associated with Application Types (HTTP Server, DNS Client, MS SQL Server, etc.). If this
option is checked, new Intrusion Prevention Rules can automatically be assigned to computers on which the new Intrusion Prevention Rule's associated Application Type is active. Two conditions must be met for a rule to be automatically assigned to a computer:

1. This option must be selected on this page.
2. The rule itself, created by Trend Micro, must be designed to allow auto-assignment. (Some rules, although associated with an Application Type, are not intended to be auto-assigned. The Deep Security Manager will recognize these rules and not apply them even if this option is checked.)

- **Allow Deep Security Rule Updates to set an Alert on new Intrusion Prevention Rules:** Some new Intrusion Prevention Rules are considered important enough by Trend Micro that they are set to trigger an Alert by default. Clearing this will override that default behavior.

### Legacy Updates (Deep Security 7.5 only)

| **Note:** | These legacy options will only be visible if you are a managing an ESX running Deep Security version 7.5. |

You have three location options:

- **Trend Micro Update Server:** Connect to the default Trend Micro Update Server.
- **Other Update Source:** If you were given an alternative source for updates, enter the URL here (including "http://").
- **Intranet location containing a copy of the current file:** If you retrieve the update file separately and store it on another computer, enter the file's location here.

| **Note:** | When entering the username, you must include the domain or hostname (or IP address), i.e. "domain\username" or "hostname\username". |

By default, the connection from the Deep Security Manager to the Trend Micro Update Server is unencrypted. To encrypt the connection to Trend Micro Update Server:

1. Select **Other Update Source**.
2. Copy the default Trend Micro Update Server location and paste it into the Other update source URL textbox and change "http" to "https". (For example:
   "https://tmds75-p.activeupdate.trendmicro.com/activeupdate")
3. Click **Save**
Smart Feedback

The Trend Micro Smart Protection Network uses a global network of threat intelligence sensors to continually update email, web, and file reputation databases in the cloud, identifying and blocking threats in real time. Deep Security can access the Smart Protection Service directly or you can install local Smart Protection Servers. Smart Protection Servers are designed to localize operations to the corporate network to optimize efficiency.

Smart Feedback

Trend Micro Smart Feedback provides continuous communication between Trend Micro products and the company's 24/7 threat research centers and technologies. With Smart Feedback, products become an active part of the Trend Micro Smart Protection Network, where large amounts of threat data is shared and analyzed in real time. This interconnection enables never before possible speeds at identifying, analyzing, and stopping new threats -- a level of responsiveness that addresses the thousands of new threats and threat variants released daily.

---

**Note:** Smart Feedback will use the proxy settings defined in the Proxy Server for Security Updates, CSSS, License Notifications, and Smart Feedback area on the Administration > System Settings > Updates tab.

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

---

Smart Protection Server software along with installation and configuration instructions are available from the Trend Micro Download Center at [http://downloadcenter.trendmicro.com](http://downloadcenter.trendmicro.com).
SMTP

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

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

Data Pruning

These settings define how long to store Event records and Counters, older Security Updates, and older versions of Agent/Appliance software before a purge removes them from the database.

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

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

Note: Logs are used to populate the Events pages. Counters are data aggregated from the logs. They are used to generate Reports and populate the Dashboard widgets.
Advanced

Load Balancers

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

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

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

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

Pluggable

"Pluggables" are Modules, Reports and Add-Ons for the Deep Security Manager. Trend Micro occasionally produces new or additional versions of these which are distributed as self-installing packages.

Proxy

Define the proxy servers that will be available for use by various Deep Security clients and services (for example, the proxy servers for Smart Protection in Policy/Computer Editor > Anti-Malware > Smart Protection).

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

<table>
<thead>
<tr>
<th>Service</th>
<th>Client</th>
<th>HTTP Support</th>
<th>Socks4 Support</th>
<th>Socks5 Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updates</td>
<td>DSA/DSVA/DSR</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Licensing and product registration</td>
<td>DSM</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Certified Safe Software Service</td>
<td>DSM</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Smart Feedback</td>
<td>DSA/DSR</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
SOAP Web Service API

Much of the Deep Security Manager's functionality can be controlled via SOAP-invoked Web services. The WSDL can be found at the URL displayed in the panel on the page. For assistance with Deep Security Manager's Web services API contact your support provider.

**Note:** A User's ability to access Web Services in the Deep Security Manager will depend on that User being granted the appropriate privileges. These privileges are associated with the Role the User has been assigned. The setting is found on the General tab of the Role properties window found at **Administration > User Management > Roles**.

Status Monitoring API

The REST Status Monitoring API lets you query the Deep Security Manager (including individual Manager Nodes) for status information such as CPU and memory usage, number of queued jobs, total and Tenant-specific database size. For assistance with Deep Security Manager's REST Status Monitoring API contact your support provider.

Export

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

Whois

The Whois lookup to be used when logging Intrusion Prevention and Firewall Events. Enter the search URL using "[IP]" as a placeholder for the IP address to look up. (For example, "http://reports.internic.net/cgi/whois?whois_nic=[IP]&type=nameserver").

Licenses

- **Hide Unlicensed Modules For New Users**: Determines whether unlicensed modules are hidden rather than simply grayed out for subsequently created Users. (This setting can be overridden on a per-User basis on the **Administration > User Management > Users > Properties** window).

Scan Cache Configurations

Click **View Scan Cache Configurations**... to display a list of saved Scan Cache Configurations. Scan Cache Configurations are settings used by the Virtual Appliance to maximize the efficiency of Anti-Malware and Integrity Scans in a virtualized environment. See **Virtual Appliance Scan Caching (page 293)** for more information.
Logo

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

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

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

From the main page you can:

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

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

Scheduled Tasks

The following Tasks can be scheduled:

- **Generate Report**: Automatically generate reports and optionally have them emailed to a list of Users.
- **Discover Computers**: Periodically check for new computers on the network by scheduling a Discovery operation. You will be prompted for an IP range to check and asked to specify which computer group the new computer will be added to.
- **Alert Summary**: Generate an email listing all outstanding (unresolved) Alerts.
- **Run Script**: If the Syslog options do not meet your event notification requirements, it may be possible for Trend Micro to provide a solution using custom-written scripts. Contact Trend Micro for more information.
- **Scan Computers for Integrity Changes**: Causes the Deep Security Manager to perform an Integrity Scan to compare a computer's current state against its baseline.
- **Scan computers for Malware**: Schedules a Malware Scan. The configuration of the scan is the same as that specified on the Policy/Computer Editor > Anti-Malware page for each computer.
- **Synchronize Directory**: Synchronize the Computers list with an added LDAP directory. (Only available if you have added an LDAP directory to the Deep Security Manager.)
- **Update Computers**: Periodically perform an update operation on selected computers. An update operation ensures that all configuration changes made in the Deep Security Manager have been applied.
- **Download Security Update**: Regularly check for security Updates and download and optionally install them if any are available.
• **Scan Computers for Recommendations**: Causes the Deep Security Manager to scan the computer(s) for common applications and then make recommendations based on what is detected.

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

• **Check for New Software**: Check if new versions of the Manager, Agents, Appliance or Filter Driver are available.

• **Scan Computers for Open Ports**: Schedule periodic port scans on one or more computers. You can specify individual computers or all computers belonging to a particular computer group. The ports that will be scanned are those defined on the **Scanning** tab in the **Policy/Computer Editor > Settings** page.

• **Backup**: Perform regular database backups. (This option is only available if you are using a Derby or Microsoft SQL Server database.)
Event-Based Tasks

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

From the main page you can:

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

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

**Events**

The following Events can be monitored:

- **Computer Created (by System)**: A Computer being added to the Deep Security Manager during synchronization with an Active Directory or Cloud Provider account, or the creation of a virtual machine on a managed ESX server running a Virtual Appliance.
- **Computer Moved (by System)**: A virtual machine being moved from one vApp to another within the same ESX, or a virtual machine on a ESX being move from one datacenter to another or from one ESX to another (including from an unmanaged ESX Server to a managed ESX Server running a Virtual Appliance.)
- **Agent-Initiated Activation**: An Agent is activated using Agent-Initiated Activation.
- **IP Address Changed**: A computer has begun using a different IP.

**Conditions**

You can require specific match conditions to be met in order for the Task to be carried out. Use **Java regular expression syntax** ([http://docs.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html](http://docs.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html)) to match patterns in the following fields:

- **Computer Name**
- **vCenter name**
- **Cloud Provider Name**
- **Cloud Instance Security Group**
- **Cloud Instance Image ID**
• **ESX Name**
• **Folder Name**
• **Platform**

The following table shows some Java regular expression examples:

<table>
<thead>
<tr>
<th>To match this:</th>
<th>Use this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder Alpha</td>
<td>Folder\ Alpha</td>
</tr>
<tr>
<td>FIN-1234</td>
<td>FIN-\d+</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>FIN-.*</td>
</tr>
<tr>
<td>RD-ABCD</td>
<td>RD-\w+</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>RD-.*</td>
</tr>
<tr>
<td>AB</td>
<td>ABC*</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>ABC</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>ABCCCCCCCCCCCC</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows 2003</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Windows XP</td>
<td>.<em>Windows.</em></td>
</tr>
<tr>
<td>Red Hat 6</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Some/Linux123</td>
<td>.<em>Red.</em></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>abcFreeBSD</td>
<td></td>
</tr>
</tbody>
</table>

These next two conditions match True or False conditions:

• **Appliance Protection Available**
• **Appliance Protection Activated**

The last condition option looks for matches to an IP in an IP list:

• **Last Used IP Address**

*Note:* Depending on the source of the new computer, some fields may not be available. For example, "Platform" would not be available for computers added as a result of the synchronization with an Active Directory.
Actions

The following actions can be taken depending on which of the above events is detected:

- **Activate Computer Delay (in minutes):** The new Computer is automatically activated after a specified number of minutes.
- **Assign Policy:** The new Computer is automatically assigned a Policy. (The Computer must be activated first.)
- **Assign to Relay Group:** The new Computer is automatically assigned a Relay Group from which to receive Security Updates.
- **Assign to Computer Group:** The Computer is placed in one of the Computer Groups on the Computers page.

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

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

- **Hostname:** The hostname of the Deep Security Manager host computer.
- **Description:** A description of the Manager node.
- **Performance:** A Deep Security Manager's performance can be affected by several factors including number of CPUs, available bandwidth, and database responsiveness. The Manager's default performance settings are designed to be suited for most installation environments. However, if you experience performance issues your support provider may suggest that you change the Performance Profile assigned to one or more of your Deep Security Manager nodes. (You should not change these settings without first consulting your support provider.)
  - **Aggressive:** This Performance Profile is optimized for installations where the Deep Security Manager is installed on a dedicated server. The following table gives an indication of how some common concurrent operations are distributed per Manager node using the Aggressive Performance Profile:

<table>
<thead>
<tr>
<th>Operation</th>
<th>2-core system</th>
<th>8-core system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activations</td>
<td>10</td>
<td>20</td>
</tr>
<tr>
<td>Updates</td>
<td>25</td>
<td>50</td>
</tr>
<tr>
<td>Recommendation Scans</td>
<td>5</td>
<td>12</td>
</tr>
<tr>
<td>Check Status</td>
<td>100</td>
<td>Same (100)</td>
</tr>
<tr>
<td>Agent/Appliance-Initiated Heartbeats</td>
<td>20 Active</td>
<td>50 Active</td>
</tr>
<tr>
<td></td>
<td>40 Queued</td>
<td>40 Queued</td>
</tr>
<tr>
<td>Simultaneous Endpoint Disk &amp; Network Jobs</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Simultaneous Endpoint Disk &amp; Network Jobs per ESX</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

- **Limited Disk and Network Usage:** This is a older setting you might see if you have upgraded to Deep Security 9. It is identical to "Aggressive".
- **Standard:** This Performance Profile is optimized for installations where the Deep Security Manager and the database share the same host. The following table gives an indication of how some common concurrent operations are distributed per Manager node using the Standard Performance Profile:

<table>
<thead>
<tr>
<th>Operation</th>
<th>2-core system</th>
<th>8-core system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activations</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>Updates</td>
<td>16</td>
<td>46</td>
</tr>
<tr>
<td>Recommendation Scans</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>Check Status</td>
<td>65</td>
<td>100</td>
</tr>
<tr>
<td>Operation</td>
<td>2-core system</td>
<td>8-core system</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Agent/Appliance-Initiated Heartbeats</td>
<td>20 Active</td>
<td>50 Active</td>
</tr>
<tr>
<td></td>
<td>40 Queued</td>
<td>40 Queued</td>
</tr>
<tr>
<td>Simultaneous Endpoint Disk &amp; Network Jobs</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Simultaneous Endpoint Disk &amp; Network Jobs per ESX</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Operation</th>
<th>2-core system</th>
<th>8-core system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activations</td>
<td>10</td>
<td>20</td>
</tr>
<tr>
<td>Updates</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>Recommendation Scans</td>
<td>5</td>
<td>12</td>
</tr>
<tr>
<td>Check Status</td>
<td>100</td>
<td>Same (100)</td>
</tr>
<tr>
<td>Agent/Appliance-Initiated Heartbeats</td>
<td>20 Active</td>
<td>50 Active</td>
</tr>
<tr>
<td></td>
<td>40 Queued</td>
<td>40 Queued</td>
</tr>
<tr>
<td>Simultaneous Endpoint Disk &amp; Network Jobs</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Simultaneous Endpoint Disk &amp; Network Jobs per ESX</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>

**Note:** All performance profiles limit the number of concurrent component updates to 100 per Relay Group.

- **Status:** Indicates whether the Deep Security Manager node whose properties you are viewing is online and active from the perspective of the Deep Security Manager node you are logged into.
- **Options:** You can choose to decommission the Manager node. The node has to be offline (uninstalled or service halted) to be decommissioned.

For more information on multi-node Deep Security Manager installations, see *Multi-Node Manager (page 560).*
Tenants

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

- Create a **New Tenant**
- **Delete** a Tenant
- Examine or modify the **Properties** of an existing Tenant
- Sign in as one of the Tenants
- **Export** one or more Tenants to a CSV file. (Either export them all by selecting **Export to CSV** from the drop-down list or export only those that are selected by choosing **Export Selected to CSV**)
- **Add/Remove Columns** columns can be added or removed by clicking **Add/Remove Columns**. The order in which the columns are displayed can be controlled by dragging them into their new position. Listed items can be sorted and searched by the contents of any column.

Clicking **New** or **Properties** displays the Tenant **Properties** window.
Licenses

Displays details about your Trend Micro Deep Security product licenses. Deep Security consists of five module packages: Anti-Malware and Web Reputation; Firewall and Intrusion Prevention; Integrity Monitoring; Log Inspection; and Multi-Tenancy. Each module package can be licensed fully or for a trial basis. You can see an individual package's license status by clicking View Details. Contact Trend Micro if you wish to upgrade your license. If Trend Micro has provided you with a new activation code, click Enter New Activation Code... and enter it there. Newly licensed features will be immediately available.

When a license expires, existing functionality will persist but updates will no longer be delivered.

Alerts will be raised if any module is about to expire or has expired.
Users

Users refers to all Deep Security Manager account holders. Use this section to create, modify, and delete User accounts. From the Users page, you can:

- Create New User accounts
- Examine or modify the Properties of an existing User account
- Set (or change) the Password for a User account
- Delete a User account
- Search for a particular User
- Synchronize with a Directory list of Users
- View System Events associated with this User
- Set or change the Role for this User

Clicking New or Properties displays the User Properties window.

General

General Information

- **Username:** The username associated with this User's password.
- **Name:** The name of the account holder.
- **Description:** A description of the account holder.
- **Role:** Use the drop-down list to assign a pre-defined Role to this User. (Assigning Roles can also be done using the right-click menu when in List View mode.)

**Note:** The Deep Security Manager comes pre-configured with two Roles: Full Access and Auditor. The "Full Access" Role grants the User all possible privileges in terms of managing the Deep Security system such as creating, editing and deleting computers, computer groups, Policies, Rules, etc. The "Auditor" Role gives the User the ability to view all the information in the Deep Security system but not the ability to make any modifications except to his personal settings (password, contact information, view preferences, etc.) Roles with various levels of system access rights can be created and modified in the Roles page or by selecting "New..." in the Roles drop-down list.

- **Language:** The language that will be used in the interface when this User logs in.
- **Locked Out:** Checking this will keep this User from being able to sign in to the Manager. (If a User enters the wrong password too many times when trying to sign in, he will be locked out automatically. Clear this if you have resolved this situation.) (Locking or unlocking a User can also be done from the right-click menu when in List View Mode.)
Options

Click the **Set Password** button to change or assign the password for this User. Password requirements such as minimum length, upper and lower case, etc. can be set in **Administration > System Settings > Security**.

Contact Information

This User's contact information. Checking the **Receive Notifications** checkbox will include this User in the list of Users who receive email notifications when Alerts are triggered.

Settings

Module

- **Hide Unlicensed Modules**: determines whether unlicensed modules will be hidden rather than simply grayed out for this User. (This option can be set globally on the **Administration > System Settings > Advanced** tab)

Refresh Rate

- **Status Bar**: this setting determines how often the Manager's status bar refreshes during various operations such as discovering or scanning computers.
- **Alerts List/Summary**: How often to refresh the data on the **Alerts** page in List view or Summary view.
- **Menu/Computers List**: How often to refresh the data on the **Computers** page.

| Note: The Last Successful Update column value will not be recalculated unless the page is manually reloaded. |

- **Computer Details window**: The frequency with which an individual computer's property page refreshes itself with the latest information (if required).

List Views

- **Remember last Tag filter on each page**: Events pages let you filter displayed events by Tag(s). This List Views setting determines if the "Tag" filter setting is retained when you navigate away from and return to an Events page.
- **Remember last Time filter on each page**: Events pages let you filter displayed events by Time period and computer(s). These List Views settings determine if the "Period" and "Computer" filter settings are retained when you navigate away from and return to an Events page.
• **Remember last computer filter on each page:** Events pages let you filter displayed events by Time period and computer(s). These List Views settings determine if the "Period" and "Computer" filter settings are retained when you navigate away from and return to an Events page.

• **Remember last Advanced Search on each page:** If you have performed an "Advanced Search" on an Events page, this setting will determine if the search results are kept if you navigate away from and return to the page.

• **Optimal number of items to show on a single page:** Screens that display lists of items will display a certain number of items per "Page". To view the next page, you must use the pagination controls. Use this setting to change the number of list-items displayed per page.

• **Maximum number of items to show on a single page:** Many lists on the Deep Security Manager are grouped into categories. For example, Intrusion Prevention Rules can be grouped according to Application Type. The Deep Security Manager will try to avoid splitting these groups when paginating and can override the "Optimal" setting (above) to keep items in the same group together. Use this setting to set a firm maximum on the number of items to display per page. If the number of items in a group exceeds this number, the group will be split and the group title will display information that this has been done.

• **Maximum number of items to retrieve from database:** This setting limits the number of that can retrieved from the database for display. This prevents the possibility of the Deep Security Manager getting bogged down trying to display an excessive number of results from a database query. If a query produces more than this many results, a message will appear at the top of the display informing you that only a portion of the results are being displayed.

---

**Note:** Increasing these values will affect Deep Security Manager performance.

---

**Reports**

• **Enable PDF Encryption:** Determines if Reports exported in PDF format are password protected.

**Reset to Default Settings:** Reset all settings on this page to their defaults.

**Synchronizing with a Directory**

The User list can be synchronized with an Active Directory, allowing Users to sign in with the password stored in the directory. Clicking **Synchronize with Directory** in the toolbar will display the **Synchronize with Directory** wizard. Type the name of the directory server and your access credentials. You will then be prompted to select which Active Directory Group of Users to import and whether they will be Users or Contacts. Once they've been imported, you are given the option to create a Scheduled Task to periodically synchronize with the directory to keep your list up to date. The imported list of Users are locked out of the Deep Security Manager by default. You will have to modify their Properties to allow them to sign in to the Manager.
Filtering the Active Directory

The first page of the Synchronize with Directory wizard has an area called Search Options where you can write filters to specify a subset of Users to import into the Deep Security Manager. The filter language follows the Internet Engineering Task Force "Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters RFC 4515".

The default filter, "(objectClass=group)", imports all Users.

The RFC 4515 filter syntax can be used to filter for specific Users and/or Groups in a directory. For example, the following filter would import only Users who are members of an Active Directory group called "DeepSecurityUsers": "(&(objectClass=group)(cn=DeepSecurityUsers))".


**Note:** The new Users, although being in the "locked out" state, are given the "Full Access" User Role.
Roles

Deep Security uses Role-based access control to restrict Users' access to various parts of the Deep Security system. Once you have installed the Deep Security Manager you should create individual accounts for each User and assign each User a Role that will restrict their activities to all but those necessary for the completion of their duties.

Deep Security comes pre-configured with two Roles:

- **Full Access:** The Full Access Role grants the User all possible privileges in terms of managing the Deep Security system including creating, editing, and deleting computers, computer groups, Policies, Rules, Malware Scan Configurations, and others.
- **Auditor:** The Auditor Role gives the User the ability to view all the information in the Deep Security system but without the ability to make any modifications except to their own personal settings, such as password, contact information, dashboard layout preferences, and others.

**Note:** Depending on the level of access granted, controls in the Manager interface will be either visible and changeable, visible only but disabled, or hidden. For a list of the rights granted in the pre-configured Roles, as well as the default rights settings when creating a new Role, see User Management (page 296).

You can create new Roles which can restrict Users from editing or even seeing Deep Security objects such as specific computers, the properties of security Rules, or the System Settings.

Before creating User accounts, identify the Roles that your Users will take and itemize what Deep Security objects those Roles will require access to and what the nature of that access will be (viewing, editing, creating, etc.). Once you have created your Roles, you can then begin creating User accounts and assigning them specific Roles.

**Note:** Do not create a new Role by duplicating and then modifying the Full Access Role. To ensure that a new Role only grants the rights you intend, create the new Role by clicking **New** in the toolbar. The rights for a new Role are set at the most restrictive settings by default. You can then proceed to grant only the rights that are required. If you duplicate the Full Access Role and then apply restrictions, you risk granting some rights that you did not intend.

From the main page you can:

- Create **New** Roles
- Examine or modify the **Properties** of an existing Role
- **Duplicate** (and then modify) existing Roles
- **Delete** a Role
Clicking **New** or **Properties** displays the **Role properties window** with five tabs (**Role Properties, Computer Rights, User Rights, Configuration Rights, and Assigned To**).

### Role Properties

**General Information**

The name and description of this Role.

**Access Type**

Select whether Users with this Role will have access to the Deep Security Manager's Web-based user interface or the Deep Security Manager's Web service API, or both.

---

**Note:** To enable the Web service API, go to **Administration > System Settings > Advanced > SOAP Web Service API**.

### Computer Rights

**Computer and Group Rights**

Use the **Computer and Group Rights** panel to confer viewing, editing, deleting, Alert-dismissal, and Event tagging rights to Users in a Role. These rights can apply to all computers and computer groups or they can be restricted to only certain computers. If you wish to restrict access, select the **Selected Computers** radio button and put a check next to the computer groups and computers that Users in this Role will have access to.

---

**Note:** These Rights restrictions will affect not only User's access to computers in Deep Security Manager, but also what information is visible, including Events and Alerts. As well, email notifications will only be sent if they relate to data that User's have access rights to.

Four basic options are available:

- **Allow viewing of non-selected computers and data:** If Users in this Role have restricted edit/delete/dismiss-Alerts rights, you can still allow them to view (but not change) information about other computers by checking this box.

- **Allow viewing of events and Alerts not related to computers:** Set this option to allow Users in this Role to view non-computer-related information (for example, System Events, like Users being locked out, new Firewall Rules being created, IP Lists being deleted, etc.)
The previous two settings affect data Users have access to. Although Users’ abilities to make changes to computers have been restricted, these two settings control whether they can see information relating to computers they don’t otherwise have access to. This includes receiving email notifications related to those computers.

- **Allow new computers to be created in selected computer groups**: Set this option to Users in this Role to create new computers in the computer groups they have access to.
- **Allow sub-groups to be added/removed in selected computer groups**: Set this option to allow Users in this Role to create and delete sub-groups within the computer groups they have access to.

**Advanced Rights**

- **Allow computer file imports**: Allow Users in this Role to import computers using files created using the Deep Security Manager’s **Computer Export** option.
- **Allow directories to be added/removed and synchronized**: Allow Users in this Role to add/remove and synchronize computers that are being managed using an LDAP-based directory like MS Active Directory.
- **Allow VMware vCenters to be added, removed and synchronized**: Allow Users in this Role to add, remove and synchronize VMware vCenters.

**Policy Rights**

Determines the rights a User in a particular Role has to create, delete, modify, or import Policies.

**User Rights**

The options on the **User Rights** tab allow you to set what kind of authority Users in this Role have over other Users.

- **Change own password and contact information only**: Users in this Role can their own password and contact information only.
- **Create and manage Users with equal or less access**: Users in this Role can create and manage any Users who do not have any privileges greater than theirs. If there is even a single privilege that exceeds those of the Users with this Role, the Users with this Role will not be able to create or manage them.
- **Have full control over all Roles and Users**: Gives Users in this Role the ability to create and edit and Users or Roles without restrictions.
Custom Rights

You can further restrict "delegated" Users' ability to create/edit/delete Users and Roles using the options in the Custom Rights panel. Those options have the following restrictions when the Delegate option is selected:

- **Create**: Can only create Users with equal or lesser rights.
- **Edit**: Can only edit a User (or set/reset password) with equal or lesser rights.
- **Delete**: Can only delete Users with equal or lesser rights.

Delegate Authority

Selecting the Delegate Authority option will limit the authority of Users in this Role. They will only be able to effect changes to Users that have equal or lesser rights than themselves. They will not be able to create, edit, or delete Roles. This ability can be further limited by deselecting any of the create/edit/delete Users options in the Custom Rights panel above.

Other Rights

Roles can be restricted with respect to the Deep Security objects they can manipulate. Default settings for new Roles are "View Only" or "Hide" for each element, but these rights can be expanded to "Full Control", or customized by choosing "Custom" from the drop-down list.

Assigned To

The Assigned To tab displays a list of the Users who have been assigned this Role.
Contacts

Users can create "Contacts". Contacts cannot sign in to the Deep Security Manager but they can periodically be sent reports (using Scheduled Tasks). Contacts can be assigned a "clearance" level that maps to existing Roles. When a Contact is sent a report, the report will not contain any information not accessible to a User of the same level.

From the Contacts page, you can:

- Create New Contacts (.CREATE_CONTACT)
- Examine or modify the Properties of an existing contact (CONTACT_PROPERTIES)
- Delete a contact (DELETE_CONTACT)
- Synchronize (SYNCHRONIZE) with a Directory

Clicking New (CREATE_CONTACT) or Properties (CONTACT_PROPERTIES) displays the Contact properties window.

General Information

The name, description, and preferred language of this contact.

Contact Information

The email address entered here is the email address to which reports will be sent if this contact is included in a report distribution list. (See the Reports page for more information.)

Clearance

The Role specified here determines the information this contact will be allowed to see. For instance, if a computer Report has been scheduled to be sent to this contact, only information on the computers that his Role permits him access to will be included in the report.

Reports

Select whether or not reports will be encrypted for this User.

Synchronizing with a Directory

The Contact list can be synchronized with an Active Directory. Clicking Synchronize with Directory in the toolbar will display the Synchronize with Directory wizard. Type the name of the directory server and your
access credentials. You will then be prompted to select which group of Users to import and whether they will be Users or Contacts. Once they've been imported, you are given the option to create a Scheduled Task to periodically synchronize with the directory to keep your list up to date.
System Information

Create a Diagnostic Package...

Clicking **Create Diagnostic Package...** in the Toolbar displays the **Diagnostic Package** wizard which will create a zip file containing Install/Uninstall and Debug Logs, System Information, Database Contents (last hour only for time-sensitive items), File Listing, and Properties Files (Passwords Removed). This information can be given to your support provider to help troubleshoot any problems.

---

**Note:** The default maximum size of a diagnostic package is approximately 200MB. A command line instruction is available to increase the size of the diagnostic package:

```
    dsm_c -action changesetting -name configuration.diagnosticMaximumFileSize -value ####
```

The following example increases the size of the package to 1GB (1000MB):

```
    dsm_c -action changesetting -name configuration.diagnosticMaximumFileSize -value 1000
```

Do not change the size of the diagnostic package unless instructed to do so by your support provider.

---

Extensions...

Extensions can be reports or plug-ins for the Deep Security Manager.

Demo Mode...

If you are evaluating Deep Security in a test environment and want to see what a full Deep Security installation in an enterprise environment looks like, you can enable Demo Mode by clicking **Demo Mode...** on the **System Information** page toolbar.

When in Demo Mode, the Manager populates its database with simulated computers, Events, Alerts, and other data. Initially, seven days worth of data is generated but new data is generated on an ongoing basis to keep the Manager's Dashboard, Reports and Events pages populated with data.

---

**Note:** While Demo Mode can be used with mixed real and simulated computers, it is **not** intended to be used in a production environment!
Demo mode can be turned off the same way.

About

This panel displays the version number of the Deep Security Manager node you are currently logged in to.

System Activity (Over The Last Hour)

This panel displays various graphs detailing activities carried out by the different Manager nodes. For details on the information displayed in the System Activity panel, see Multi Node Manager (page 560).

System Details

This panel displays detailed system information used for troubleshooting by your support provider.
Updates

The **Updates** page displays the status of current updates in your Deep Security environment. To configure the update source, go to Administration > System Settings > Updates.

Security Updates

The **Security Updates** tab displays the status of current updates in use on your Agents / Appliances. The list of updates is grouped according to the protection module that they are used by.

- **Component**: The type of update component.
- **Platform**: The operating system for which the update is intended.
- **Current Version**: The version of the Security Update currently downloaded from Trend Micro to Deep Security and being distributed by the Relays and the Deep Security Manager.
- **Last Updated**: When the currently downloaded Security Update was retrieved from Trend Micro.
- **Up-to-date**: The number of Agents/Appliances that have been updated with the currently downloaded Security Update and the number of computers being protected.
- **Out-of-date**: The number of Agents/Appliances that have not been updated with the currently downloaded component.
- **Percent Updated**: The percentage of Agents/Appliances and protected computers that have been updated with the latest versions of the component available from the Relays and the Deep Security Manager.

The version numbers of the Security Update components in effect on a computer can be found on the Computer Editor > Updates page.

Click the **Download Security Updates...** button to instruct the Relays to download the latest Security Updates from Trend Micro and then instruct the Agents/Appliances to download the Security Updates from the Relays. If you are running older versions of the Appliance (version 7.x), required updates will be downloaded from Trend Micro to the Deep Security Manager and distributed to the older Appliances from there.

**Note:** By default, Deep Security will distribute Anti-Malware and Web Reputation Updates and Intrusion Prevention, Log Inspection, and Integrity Monitoring Rule Updates at the same time. You can configure Deep Security to only distribute the Anti-Malware and Web Reputation Updates by going to the Administration > System Settings > Updates tab and de-selecting the Automatically apply new Rule Updates to Policies option in the Rule Updates area.

Click the **Apply Latest Rule Update...** button to apply the latest Intrusion Prevention, Log Inspection, and Integrity Monitoring Rule Updates. This button will be disabled if the latest Rule Updates available from the Relays have already been applied. (If the Automatically apply new Rule Updates to Policies option in the Rule Updates area on the Administration > System Settings > Updates tab is selected, this button will...
always be disabled except during the brief time between the Relays getting a new Rule Update and applying them to Policies.)

The View All Rule Updates... button displays a list of the most recent Intrusion Prevention, Integrity Monitoring, and Log Inspection Rules that have been downloaded to the Deep Security Manager's database. If required you can reapply the current Rule set to computers being protected by Deep Security or rollback to a previous Rule set. You can configure the number of Rule Updates that are kept in the Deep Security Manager's database by going to the Data Pruning area in the Administration > System Settings > Storage tab.

Software Updates

Available software packages will include new versions of the Manager, the Agents, the Virtual Appliance, the Relays, and the Deep Security Filter Driver.

- **Package Name:** The file name of the software package (which will include the version number).
- **Download Center Version:** The version of the software available from Trend Micro Download Center.
- **Imported Version:** The latest version of the software imported to the Manager. (The Manager can store older versions of software packages. You can configure the number of previous software versions to store in the Data Pruning area on the Administration > System Settings > Storage tab.)
- **Release Date:** The release date of the version available from the Download Center.
- **Up-to-date:** Number of software components that that have been updated to the latest version available from Trend Micro.
- **Out-of-date:** Number of software components that that have not been updated to the latest version available from Trend Micro.
- **Percentage Updated:** A representation of the percentage of software components which have been updated to the latest version available from Trend Micro.

**Note:** Security Updates and Software upgrades of Agents, Virtual Appliances, and Relays can all be deployed using the Deep Security Manager. New versions of the Deep Security Manager, however, must be installed independently of your current Deep Security Manager. That is, you must download the new version from the Trend Micro Download Center, run the installer, and follow the instructions to perform a software upgrade.

Click **Open Download Center...** to open a new browser window which will take you to the Trend Micro Download Center where Deep Security software packages are available for download.

Once you have downloaded the software packages you need, you will have to import them into the Deep Security Manager. Click **Import Software...** to import the software package into the Deep Security Manager.

Click **View Imported Software...** to open a window displayed a list of downloaded and imported software. From this window, you can also generate sample deployment scripts that can be used to install and activate Agents.
Before deploying new software, be sure to check the Trend Micro Download Center for any accompanying documentation, including Installation Guides and release notes.

Relays

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.

Embedded in each Deep Security Relay is a fully functional Deep Security Agent which can be assigned a Policy designed specifically to protect Relays.

The Relays tab displays the status of current updates that have been downloaded from Trend Micro and are available for distribution from your Relays.

• The list of updates is grouped according to the protection module that they are used by.
• **Component**: The type of update component.
• **Product Name**: The Software component and language version for which the update is intended. (Agents and Virtual Appliances will automatically download the correct updates.)
• **Platform**: The operating system for which the update is intended.
• **Current Version**: The version of the Security Update currently downloaded from Trend Micro to Deep Security.
• **Last Updated**: When the currently downloaded Security Update was retrieved from Trend Micro.
• **Up-to-date**: The sum of the number of Relays that have been updated with the currently downloaded Security Update and the number of computers being protected.
• **Out-of-date**: The sum of the number of Relays that have not been updated with the currently downloaded component and the number of computers being protected.
• **Percent Updated**: A representation of the percentage of Relays that have been updated to the latest version of the component.

The list of Components also includes some items that are downloaded and used by the Relays but are not distributed to Agents/Appliances, such as Manifests.
The Deep Security Virtual Appliance Interface

The Deep Security Virtual Appliance interface can be accessed by opening the VMware vSphere Client, selecting the DSVA in the navigation panel, and clicking on the Console tab.

System Information

Displays the DSVA 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.

Configure Time Zone

The Virtual Appliance's time zone can be changed if required.

Set Date and Time

The Virtual Appliance's date and time can be set if required.

Virtual Agents

Lists all activated Agents on the Appliance. (Deactivated Agents don't appear.)
Reset Appliance

Deactivates the Virtual Appliance. This means that all rules are erased from the Appliance, the Appliance is unlinked from its Deep Security Manager, and it can be activated by a new Manager.

Reboot System

Reboots the Virtual Appliance. Previous configuration information is maintained.

Note: When an Agent is first listed, it is listed under its Uniformly Unique Identification (UUID). Once selected, the listed name changes to its VMware virtual machine Name.
Configuration and Management

This part of the documentation describes how to configure and manage the components of Deep Security from the system in general to configuration of the individual protection modules.

- **Quick Start: System Configuration:** A guide to configuring the basic Deep Security system settings (page 246) from enabling regular automatic security updates to setting up email notifications.
- **Quick Start: Protecting a Server:** A guide to protecting a standard Windows server (page 237) with Deep Security.
- **System:** Describes the functionality and configuration of Deep Security system settings:
  - **Communication (page 256)** describes how the different Deep Security components communicate with each other.
  - **Customize the Dashboard (page 258)** describes how to create custom dashboard layout for yourself or other Users.
  - **Events, Alerts, and Reports (page 261)** describes how to stay abreast of Deep Security events by monitoring Events, configuring and generating Alerts, and producing periodic customized Reports.
  - **Set Up Email Alerts (page 266)** describes how to configure Deep Security to send email notifications of important Deep Security Events to various users.
  - **Alerts (page 268)** 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 270)** describes how to set which port are scanned during one of Deep Security's Port Scans.
  - **Syslog Integration (SIEM) (page 271)** describes how to configure Deep Security to send Events to a SIEM via Syslog.
  - **Relay Groups (page 283)** 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.
  - **Software Updates (page 286)** describes how to manage Deep Security software updates.
  - **Security Updates (page 288)** describes how to manage Deep Security security updates.
  - **Virtual Appliance Scan Caching (page 293)** 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 296)** 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 304)** describes how to perform (and automate) a backup of your Deep Security data.

• **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 308)** 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 311)** You can import a Microsoft Active Directory or any other LDAP-based directory service.
  - **Importing computers from a VMware vCenter (page 316)** You can import a VMware vCenter and provide the hosted VMs with Agent-based or Agentless protection.
  - **Importing computers from a Cloud Provider (page 319)** You can import virtual machines being hosted on VMware vCloud or Amazon EC2 infrastructures.
  - **Using a deployment script (page 323)** 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.

• **Deploying Protection:** How to enable protection on your computers using the Deep Security Agent (page 326) or Agentlessly (page 328) using the Deep Security Virtual Appliance.

• **Protection Modules:** Describes configuration of the Deep Security protection modules.
  - The **Anti-Malware (page 336)** 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 Reputation (page 341)** 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 343)** is an NDIS-based, bi-directional, 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 357)** 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 359) 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 361) 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.

- **Configure Recommendation Scans**: How to configure *Recommendation Scans* (page 385) which are performed 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.

- **SSL Data Streams**: How to configure filtering of *SSL traffic* (page 389).

- **Events, Alerts, and Reports**: The functionality and configuration of Deep Security *Events, Alerts, and Reports* (page 261).


- **Multi-Tenancy**: How to enable, configure, and manage the *Multi-Tenancy* (page 402) capabilities of Deep Security which let you create multiple distinct management environments using a single Deep Security Manager and database server installation.

- **Protecting a Mobile Laptop**: How to *protect a mobile laptop* (page 421), with information about using the location awareness of Deep Security.
Quick Start: Protecting a Server

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

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 installed (but not activated) Deep Security Agent on the computer you wish to protect. And finally, we will assume that you have a Deep Security Relay installed 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.
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**.

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**.

![Image of the New Computer wizard](image1.jpg)

**Note:** *An Agent can be configured to automatically initiate its own activation upon installation. For details, see Command-Line Instructions (page 437).*

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

![Image of the confirmation message](image2.jpg)
5. Leave the **Open Computer Details on 'Close'** option unselected 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 had the we 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:

![Deep Security Manager interface](image)

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:

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:
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:

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:

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 filter list. To unassign a Rule, deselect the checkbox next to its name.
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 505).*

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 Rule Recommendations:** 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.
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.

Schedule Regular Security Updates

If you follow the steps described in Quick Start: System Configuration (page 246), 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 471)** and **Intrusion Prevention Events (page 467)**.

---

### 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.
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 Deep Security Relay
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 Deep Security Relay

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

**Note:** Relays are always organized into Relay Groups, even if it’s a only a group of one. Deep Security has a default Relay Group (named "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 283).

To view your Deep Security Relays, go to the Administration > System Settings > Updates tab and click View Relay Groups... in the Relays area: (Make sure you are on the Updates tab on the System Settings page and not the Updates page located parallel to the System Settings page.)
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:

![Relay Group Properties window](image)

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 *Configuring the Deep Security Relay 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 find the Relay in your Computers list and check that it can retrieve updates from Trend Micro.

Go to the **Administration > Updates > Security Updates** tab and click the **Download Security Updates ...** button.
This will display the **Security Update** Wizard which contacts the Trend Micro Update Servers and downloads the latest Security Updates and distributes them to your computers. If upon completion the wizard displays the success message it means your Relay can communicate with the Update servers:

**Note:** If your Relays are unable to update their Components, see *Configuring the Deep Security Relay* 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**. There you should see at least one Scheduled Task called **Daily Download Security Updates**:
Double-click the Scheduled Task to view its **Properties** window:

Notice that (in this case) the **Download Security Updates** Scheduled Task is set to perform a Security Update everyday at 19:25.

---

**Note:** If you don't have a **Download 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:
Double-click on an Alert see its Properties window where you can set the Alert options for email notification:

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:

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:

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:
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 Server* (page 237) or *Protecting a Mobile Laptop* (page 421) for a quick guide to protecting those two kinds of computer resources.
System

- **Communication (page 256)** describes how the different Deep Security components communicate with each other.
- **Customize the Dashboard (page 258)** describes how to create custom dashboard layout for yourself or other Users.
- **Events, Alerts, and Reports (page 261)** describes how to stay abreast of Deep Security events by monitoring Events, configuring and generating Alerts, and producing periodic customized Reports.
- **Set Up Email Alerts (page 266)** describes how to configure Deep Security to send email notifications of important Deep Security Events to various users.
- **Alerts (page 268)** 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 270)** describes how to set which port are scanned during one of Deep Security's Port Scans.
- **Syslog Integration (SIEM) (page 271)** describes how to configure Deep Security to send Events to a SIEM via Syslog.
- **Relay Groups (page 283)** 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.
- **Software Updates (page 286)** describes how to manage Deep Security software updates.
- **Security Updates (page 288)** describes how to manage Deep Security security updates.
- **Virtual Appliance Scan Caching (page 293)** 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 296)** 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 304)** 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 and 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 > 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.

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 389).
Communication

Who Initiates Communication

At the default setting (Bi-directional), 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. **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/Appliance itself periodically check for updates and control heartbeat operations. If this is the case, select **Agent/Appliance Initiated**.

---

**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 on a Policy further down the Policy tree along the branch that leads to your computer, or on an individual computers.

**To configure Communication Direction on 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 "Bi-directional"), 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 "Bi-directional"), 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 bi-directional communication to work.
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.)

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:

![Dashboard with Computer Filter]

**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:

![Dashboard with Tag Filter]

For more information on tagging see *Event Tagging (page 393)*.

**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.)

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:
Events, Alerts, and Reports

Events

Deep Security will record security Events when a protection module Rule or condition is triggered (like Malware being detected and quarantined or an Intrusion Prevention Rule blocking traffic), 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 256) 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 447).)
• 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 447).

Filter the List and/or Search for an Event

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

The Period toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The Computers toolbar lets you organize the display of event log entries by computer groups or computer Policies.

Advanced Search functions (searches are not case sensitive):

• Contains: The entry in the selected column contains the search string
• Does Not Contain: The entry in the selected column does not contain the search string
• Equals: The entry in the selected column exactly matches the search string
• Does Not Equal: The entry in the selected column does not exactly match the search string
• In: The entry in the selected column exactly matches one of the comma-separated search string entries
• Not In: The entry in the selected column does not exactly match any of the comma-separated search string entries

Pressing the "plus" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the submit button (at the right of the toolbars with the right-arrow on it).
Export

Clicking **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 447)*.)

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...** ( ).
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 which contains event data, you have the option to filter the report data using Event Tags. Select All for only tagged 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.

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 hourly level of granularity, but beyond three days, the time period can only be specified on a daily level of granularity.

Computer Filter

Set the computers whose data will be included in the report.

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 which periodically generate and distribute Reports to any number of Users and Contacts. For more information on Scheduled Tasks, go to Administration > Scheduled Tasks.
Set Up Email Alerts

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 271).
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....

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.
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:** For the emails to be sent, you must configure the SMTP settings on the Administration > System Settings > SMTP tab.
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:

<table>
<thead>
<tr>
<th>Signature IDs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Custom Intrusion Prevention Rule</td>
</tr>
<tr>
<td>20</td>
<td>Log-Only Firewall Rule</td>
</tr>
<tr>
<td>21</td>
<td>Deny Firewall Rule</td>
</tr>
<tr>
<td>30</td>
<td>Custom Integrity Monitoring Rule</td>
</tr>
<tr>
<td>40</td>
<td>Custom Log Inspection Rule</td>
</tr>
<tr>
<td>100-299</td>
<td>Out of &quot;Allowed&quot; Policy Firewall Rule</td>
</tr>
<tr>
<td>300-399</td>
<td>SSL Events</td>
</tr>
<tr>
<td>500-899</td>
<td>Firewall Stateful Configuration Events</td>
</tr>
<tr>
<td>1,000,000-1,999,999</td>
<td>Trend Micro Intrusion Prevention Rule</td>
</tr>
<tr>
<td>2,000,000-2,999,999</td>
<td>Trend Micro Integrity Rule</td>
</tr>
<tr>
<td>3,000,000-3,999,999</td>
<td>Trend Micro Log Inspection Rule</td>
</tr>
<tr>
<td>4,000,000-4,999,999</td>
<td>Trend Micro Anti-Malware</td>
</tr>
<tr>
<td>5,000,000-5,999,999</td>
<td>Trend Micro Web Reputation</td>
</tr>
</tbody>
</table>

**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.

**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 sp=49617 dpt=80 cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=1
TrendMicroDsPacketData=AFB...
<table>
<thead>
<tr>
<th>Extension Field</th>
<th>Name</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| 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                                    |
### 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 dvhost=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=R0VUI9zP3...

<table>
<thead>
<tr>
<th>Extension Field</th>
<th>Name</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>smac</td>
<td>Source MAC Address</td>
<td>Source computer network interface MAC address.</td>
<td>smac= 00:0E:04:2C:02:B3</td>
</tr>
<tr>
<td>spt</td>
<td>Source Port</td>
<td>(For TCP and UDP protocol only) Source computer connection port.</td>
<td>spt=1032 spt=443</td>
</tr>
<tr>
<td>src</td>
<td>Source IP Address</td>
<td>Source computer IP Address.</td>
<td>src=192.168.1.105 src=10.10.251.231</td>
</tr>
<tr>
<td>TrendMicroDsFrameType</td>
<td>Ethernet frame type</td>
<td>Connection Ethernet frame type.</td>
<td>TrendMicroDsFrameType=IP TrendMicroDsFrameType=ARP TrendMicroDsFrameType=RevARP TrendMicroDsFrameType=NetBEUI</td>
</tr>
<tr>
<td>TrendMicroDsPacketData</td>
<td>Packet data</td>
<td>(If include packet data is set) A Base64 encoded copy of the packet data.</td>
<td>TrendMicroDsPacketData=AA...BA=</td>
</tr>
</tbody>
</table>

- **act**
  - Action
  - The action taken by the Intrusion Prevention rule. Can contain: Block, Reset, Insert, Delete, Replace or Log. If the rule or the network engine is operating in detect-only mode, the action value will be proceeded by "IDS:.".
  - Examples: 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.
  - Examples: cn1=113

- **cn1Label**
  - Host ID
  - The friendly name label for the field cn1.
  - Examples: cn1Label=Host ID

- **cn3**
  - Intrusion Prevention
  - Position within packet of data that triggered the event.
  - Examples: cn3=37
<table>
<thead>
<tr>
<th>Extension Field</th>
<th>Name</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn3Label</td>
<td>Intrusion Prevention Packet Position</td>
<td>The friendly name label for the field cn3.</td>
<td>cn3Label=Intrusion Prevention Packet Position</td>
</tr>
<tr>
<td>cnt</td>
<td>Repeat Count</td>
<td>The number of times this event was sequentially repeated.</td>
<td>cnt=8</td>
</tr>
<tr>
<td>cs1</td>
<td>Intrusion Prevention Filter Note</td>
<td>(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.</td>
<td>cs1=Drop_data</td>
</tr>
<tr>
<td>cs1Label</td>
<td>Intrusion Prevention Note</td>
<td>The friendly name label for the field cs1.</td>
<td>cs1Label=Intrusion Prevention Note</td>
</tr>
<tr>
<td>cs2</td>
<td>TCP Flags</td>
<td>(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.</td>
<td>cs2=0x10 ACK cs2=0x14 ACK RST</td>
</tr>
<tr>
<td>cs2Label</td>
<td>TCP Flags</td>
<td>The friendly name label for the field cs2.</td>
<td>cs2Label=TCP Flags</td>
</tr>
<tr>
<td>cs3</td>
<td>Packet Fragmentation Information</td>
<td>The &quot;DF&quot; field will be present if the IP &quot;Don't Fragment&quot; bit is set. The &quot;MF&quot; field will be present if the &quot;IP Mote Fragments&quot; bit is set.</td>
<td>cs3=MF cs3=DF MF</td>
</tr>
<tr>
<td>cs3Label</td>
<td>Fragmentation Bits</td>
<td>The friendly name label for the field cs3.</td>
<td>cs3Label=Fragmentation Bits</td>
</tr>
<tr>
<td>cs4</td>
<td>ICMP Type and Code</td>
<td>(For the ICMP protocol only) The ICMP type and code stored in their respective order delimited by a space.</td>
<td>cs4=11 0 cs4=8 0</td>
</tr>
<tr>
<td>cs4Label</td>
<td>ICMP</td>
<td>The friendly name label for the field cs4.</td>
<td>cs4Label=ICMP Type and Code</td>
</tr>
<tr>
<td>cs5</td>
<td>Intrusion Prevention Stream Position</td>
<td>Position within stream of data that triggered the event.</td>
<td>cs5=128 cs5=20</td>
</tr>
<tr>
<td>cs5Label</td>
<td>Intrusion Prevention Stream Position</td>
<td>The friendly name label for the field cs5.</td>
<td>cs5Label=Intrusion Prevention Stream Position</td>
</tr>
<tr>
<td>Extension Field</td>
<td>Name</td>
<td>Description</td>
<td>Examples</td>
</tr>
<tr>
<td>-----------------</td>
<td>------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>cs6</td>
<td>Intrusion Prevention Filter Flags</td>
<td>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.</td>
<td>The following example would be a summed combination of 1 (Data truncated) and 8 (Have Data): cs6=9</td>
</tr>
<tr>
<td>cs6Label</td>
<td>Intrusion Prevention Flags</td>
<td>The friendly name label for the field cs6.</td>
<td>cs6=Intrusion Prevention Filter Flags</td>
</tr>
<tr>
<td>dmac</td>
<td>Destination MAC Address</td>
<td>Destination computer network interface MAC address.</td>
<td>dmac= 00:0C:29:2F:09:B3</td>
</tr>
</tbody>
</table>
| 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. | TrendMicroDsPacketData=AA...BA= |
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

<table>
<thead>
<tr>
<th>Extension Field</th>
<th>Name</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>src</td>
<td>Source IP Address</td>
<td>Source Deep Security Manager IP Address.</td>
<td>src=10.52.116.23</td>
</tr>
<tr>
<td>suser</td>
<td>Source User</td>
<td>Source Deep Security Manager user account.</td>
<td>suser=MasterAdmin</td>
</tr>
<tr>
<td>target</td>
<td>Target entity</td>
<td>The event target entity. The target of the event maybe the administrator account logged into Deep Security Manager, or a Computer.</td>
<td>target=MasterAdmin target=server01</td>
</tr>
<tr>
<td>msg</td>
<td>Details</td>
<td>Details of the System event. May contain a verbose description of the event.</td>
<td>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...</td>
</tr>
</tbody>
</table>

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 dvhost=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: ..
<table>
<thead>
<tr>
<th>Extension Field</th>
<th>Name</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn1</td>
<td>Host ID</td>
<td>The Agent Computer internal identifier which can be used to uniquely identify the Agent Computer from a given syslog event.</td>
<td>cn1=113</td>
</tr>
<tr>
<td>cn1Label</td>
<td>Host ID Label</td>
<td>The friendly name label for the field cn1.</td>
<td>cn1Label=Host ID</td>
</tr>
<tr>
<td>cs1</td>
<td>Specific Sub-Rule</td>
<td>The Log Inspection sub-rule which triggered this event.</td>
<td>cs1=Multiple Windows audit failure events</td>
</tr>
<tr>
<td>cs1Label</td>
<td>LI Description</td>
<td>The friendly name label for the field cs1.</td>
<td>cs1Label=LI Description</td>
</tr>
<tr>
<td>duser</td>
<td>User Information</td>
<td>(If parse-able username exists) The name of the target user initiated the log entry.</td>
<td>duser=(no user)</td>
</tr>
<tr>
<td>f-path</td>
<td>Target entity</td>
<td>The Log Inspection rule target entity. May contain a file or directory path, registry key, etc.</td>
<td>f-path=Application</td>
</tr>
<tr>
<td>msg</td>
<td>Details</td>
<td>Details of the Log Inspection event. May contain a verbose description of the detected log event.</td>
<td>msg=WinEvtLog: Application: AUDIT_FAILURE(20187): pgEvent: (no user): no domain: SERVER01: Remote login failure for user 'xyz'</td>
</tr>
<tr>
<td>shost</td>
<td>Source Hostname</td>
<td>Source computer Hostname</td>
<td>shost=webserver01.corp.com</td>
</tr>
<tr>
<td>src</td>
<td>Source IP Address</td>
<td>Source computer IP Address.</td>
<td>src=192.168.1.105</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>src=10.10.251.231</td>
</tr>
</tbody>
</table>

**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".

<table>
<thead>
<tr>
<th>Extension Field</th>
<th>Name</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>act</td>
<td>Action</td>
<td>The action detected by the integrity rule. Can contain: created, updated, detected or renamed.</td>
<td>act=created act=deleted</td>
</tr>
<tr>
<td>Extension Field</td>
<td>Name</td>
<td>Description</td>
<td>Examples</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>cn1</td>
<td>Host ID</td>
<td>The Agent Computer internal identifier which can be used to uniquely identify the Agent Computer from a given syslog event.</td>
<td>cn1=113</td>
</tr>
<tr>
<td>cn1Label</td>
<td>Host ID</td>
<td>The friendly name label for the field cn1.</td>
<td>cn1Label=Host ID</td>
</tr>
<tr>
<td>filePath</td>
<td>Target Entity</td>
<td>The integrity rule target entity. May contain a file or directory path, registry key, etc.</td>
<td>filePath=C:\WINDOWS\system32\drivers\etc\hosts</td>
</tr>
<tr>
<td>msg</td>
<td>Attribute changes</td>
<td>(For &quot;updated&quot; action only) A list of changed attribute names. If &quot;Relay via Manager&quot; is selected, all event action types include a full description.</td>
<td>msg=lastModified,sha1,size</td>
</tr>
<tr>
<td>oldfilePath</td>
<td>Old target entity</td>
<td>(For &quot;renamed&quot; 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.</td>
<td>oldFilePath=C:\WINDOWS\system32\logfiles\ds_agent.log</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Extension Field</th>
<th>Name</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn1</td>
<td>Host ID</td>
<td>The Agent Computer internal identifier which can be used to uniquely identify the Agent Computer from a given syslog event.</td>
<td>cn1=1</td>
</tr>
<tr>
<td>cn1Label</td>
<td>Host ID</td>
<td>The friendly name label for the field cn1.</td>
<td>cn1Label=Host ID</td>
</tr>
<tr>
<td>cn2</td>
<td>File Size</td>
<td>The size of the quarantine file. This extension is included only when the &quot;direct forward&quot; from Agent/Appliance is selected.</td>
<td>cn2=100</td>
</tr>
<tr>
<td>cn2Label</td>
<td>File Size</td>
<td>The friendly name label for the field cn2.</td>
<td>cn2Label=Quarantine File Size</td>
</tr>
<tr>
<td>filePath</td>
<td>Filepath</td>
<td>The location of the target file.</td>
<td>filePath=C:(virus)ei1.txt</td>
</tr>
<tr>
<td>act</td>
<td>Action</td>
<td>The action carried out by the Anti-malware engine. Possible values are: Deny Access, Quarantine, Delete, Pass, and Clean.</td>
<td>act=Clean act=Pass</td>
</tr>
<tr>
<td>msg</td>
<td>Message</td>
<td>The type of scan. Possible values are: Realtime, Scheduled, and Manual.</td>
<td>msg=Realtime msg=Scheduled</td>
</tr>
<tr>
<td>fszize</td>
<td>Filesize</td>
<td>The size of the target file in bytes.</td>
<td>fszize=120</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Extension Field</th>
<th>Name</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn1</td>
<td>Host Identifier</td>
<td>The Agent Computer internal identifier which can be used to uniquely identify the Agent Computer from a given syslog event.</td>
<td>cn1=1</td>
</tr>
<tr>
<td>cn1Label</td>
<td>Host ID</td>
<td>The friendly name label for the field cn1.</td>
<td>cn1Label=Host ID</td>
</tr>
<tr>
<td>request</td>
<td>Request</td>
<td>The URL of the request.</td>
<td>request=site.com</td>
</tr>
<tr>
<td>msg</td>
<td>Message</td>
<td>The type of action. Possible values are: Safe, Suspicious, Highly Suspicious, Dangerous, Blocked By Admin, Untested.</td>
<td>msg=Safe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>msg=Suspicious</td>
</tr>
</tbody>
</table>
Relay Groups

Deep Security Relays are used to provide Deep Security Updates to Deep Security Agents and Appliances as they become available from the Trend Micro Update Server.

Deep Security 9 Relays were designed as a performance improvement and allow the load of providing updates to be removed from the Deep Security Manager machine and distributed across many Relay servers. The Deep Security Manager instructs the Deep Security Relays to get the latest updates and when new updates are available, Agents and Appliances are automatically directed to pull their updates from the Relays.

Deep Security organizes Relays into Relay Groups. For maximum efficiency, Relays in a selected group can be configured to provide the updates to specific Agents/Appliances. Trend Micro recommends that Agents on computers in a particular geographic region or office should be configured to download updates from a local Relay Group.

At its simplest, a Relay Group may contain only one member Relay. However to improve performance and redundancy, a Relay Group can be configured to contain more than one member Relay. 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 that when a Deep Security 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 Deep Security 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.

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 Deep Security Relays, from Administration > System Settings > Updates, click the View Relay Groups... button.
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:** *Deep Security Relays not yet configured into any Relay Group are automatically configured as members of the "Default Relay Group".*

Newly activated Deep Security Relays will be automatically notified by the Deep Security 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 dropdown 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 ctrl-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 dropdown 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 Deep Security Manager's **Computers** page. See **Event-Based Tasks** (page 210) 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 the Administration > System Settings > Updates tab and click on View Relay Group... to display the Relay Groups window.
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 Deep Security 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 > Software Updates, and click the Download Security Updates... button.

To perform security updates on specific Agents/Appliances, select the Agent/Appliance from the Computers list, then from the Actions menu select Download Security Update.

To schedule a regular Download Security Update task, go to Administration > Scheduled Tasks, and create a new Scheduled Task of the Download Security Update type.
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:

When you receive and Alert that new software is available, you have to manually download the software from Trend Micro and import it into the Deep Security Manager.

To download and import software from Trend Micro into the Deep Security Manager:

1. Go to Administration > Updates and click Open Download Center... on the Software Updates tab. This will open the Trend Micro Download Center in a browser window.
2. Navigate to the Deep Security section of the site and download the new versions of the software.
3. Once the software is downloaded, copy the files to a location that is accessible by the computer hosting the Deep Security Manager.
4. Back on the Administration > Updates > Software Updates tab, click Import Software... This will open the Import Software wizard.
5. Use the wizard to browse to the location of the software files that you downloaded and import it into the Deep Security Manager.
Once the software is imported into the Deep Security Manager, you can upgrade the Deep Security Agents, Appliances, and Relays by right-clicking on them in the Computers page and selecting **Actions > Upgrade Agent/Appliance/Relay** software.
Security Updates

Deep Security periodically needs to be updated with the latest security components: Anti-Malware and Rule Updates ("Security Updates"), and Software upgrades ("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:

**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 9 SP1 Installation Guide**.

To configure security updates, you will have 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:

Relays

In the Relays 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 which 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 if the Relay Group they are configured to update from is not available, select the Allow Agents/Appliances to update from this source if Deep Security Relays are not available option. To allow Agents to update (either from a Relay or the Update server) when not in contact with a Deep Security Manager, select Agents can update components automatically when not in contact with Deep Security Manager. (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.)

Deep Security Rule Updates

Automatically apply new Deep Security Rule Updates: 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 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.

Proxy Servers

If your Relays connect to the internet (and to Trend Micro Update servers) through a proxy, you can specify proxies on the Administration > System Settings > Updates 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 into Relay from one Relay Group to another.

To view your current Relay Groups or to create new Relay Groups, go to the Administration > System Settings > Updates tab and click View Relay Groups... in the Relays area.

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.

![Relay Group Properties dialog box](https://example.com/relay_group_properties.png)
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:

\texttt{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.

\textbf{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 > System Settings > Updates
2. In the Relays area, select "Other Update Source:" and enter https://localhost:4122
3. Click Save.
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 Scans and one hour for Real-Time 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 regular expressions to refer to multiple files and locations with a single expression.

| 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 > Scan > 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 four. If you increase this number beyond eight, 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 DSVA system memory accordingly.
User Management

Deep Security has Users, Roles, and Contacts.

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 which 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.
Role-Based Editing Privileges

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

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.
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.

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

<table>
<thead>
<tr>
<th>RIGHTS</th>
<th>SETTINGS BY ROLE</th>
<th>Hide/View-Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Inspection Decoders</td>
<td>Full (Can Create, Edit, Delete)</td>
<td>View-Only</td>
</tr>
<tr>
<td>Directory Lists</td>
<td>Full (Can Create, Edit, Delete)</td>
<td>View-Only</td>
</tr>
<tr>
<td>Files Lists</td>
<td>Full (Can Create, Edit, Delete)</td>
<td>View-Only</td>
</tr>
<tr>
<td>Files Extension Lists</td>
<td>Full (Can Create, Edit, Delete)</td>
<td>View-Only</td>
</tr>
<tr>
<td>IP Lists</td>
<td>Full (Can Create, Edit, Delete)</td>
<td>View-Only</td>
</tr>
<tr>
<td>MAC Lists</td>
<td>Full (Can Create, Edit, Delete)</td>
<td>View-Only</td>
</tr>
<tr>
<td>Port Lists</td>
<td>Full (Can Create, Edit, Delete)</td>
<td>View-Only</td>
</tr>
<tr>
<td>Contexts</td>
<td>Full (Can Create, Edit, Delete)</td>
<td>View-Only</td>
</tr>
<tr>
<td>Schedules</td>
<td>Full (Can Create, Edit, Delete)</td>
<td>View-Only</td>
</tr>
<tr>
<td>System Settings (Global)</td>
<td>Full (Can View, Edit System Settings (Global))</td>
<td>View-Only</td>
</tr>
<tr>
<td>System Information</td>
<td>Full (Can View System Information, Can Edit and Decommission Manager Nodes, Can Manage System Extensions)</td>
<td>View-Only</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>Full (Can Create Diagnostic Packages)</td>
<td>View-Only</td>
</tr>
<tr>
<td>Tagging (Advanced)</td>
<td>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)</td>
<td>View-Only</td>
</tr>
<tr>
<td>Tasks</td>
<td>Full (Can View, Add, Edit, Delete Tasks, Execute Tasks)</td>
<td>View-Only</td>
</tr>
<tr>
<td>Contacts</td>
<td>Full (Can View, Create, Edit, Delete Contacts)</td>
<td>View-Only</td>
</tr>
<tr>
<td>Licenses</td>
<td>Full (Can View, Change License)</td>
<td>View-Only</td>
</tr>
<tr>
<td>Updates</td>
<td>Full (Can Add, Edit, Delete Software; Can View Update For Components; Can Download, Import, Apply Update Components; Can Delete Deep Security Rule Updates)</td>
<td>View-Only</td>
</tr>
<tr>
<td>Asset Values</td>
<td>Full (Can Create, Edit, Delete Asset Values)</td>
<td>View-Only</td>
</tr>
<tr>
<td>Certificates</td>
<td>Full (Can Create, Delete SSL Certificates)</td>
<td>View-Only</td>
</tr>
<tr>
<td>Update Relay Lists</td>
<td>Full (Can Create, Edit, Delete Relay Lists)</td>
<td>View-Only</td>
</tr>
<tr>
<td>Custom settings corresponding to &quot;Change own password and contact information only&quot; option</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------</td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can View Users</td>
<td>Not allowed</td>
<td></td>
</tr>
<tr>
<td>Can Create New Users</td>
<td>Not allowed</td>
<td></td>
</tr>
<tr>
<td>Can Edit User Properties</td>
<td>Not allowed</td>
<td></td>
</tr>
<tr>
<td>(User can always edit select</td>
<td></td>
<td></td>
</tr>
<tr>
<td>properties of own account)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can Delete Users</td>
<td>Not allowed</td>
<td></td>
</tr>
<tr>
<td>Roles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can View Roles</td>
<td>Not allowed</td>
<td></td>
</tr>
<tr>
<td>Can Create New Roles</td>
<td>Not allowed</td>
<td></td>
</tr>
<tr>
<td>Can Edit Role Properties</td>
<td>Not allowed</td>
<td></td>
</tr>
<tr>
<td>(Warning: conferring this right</td>
<td></td>
<td></td>
</tr>
<tr>
<td>will let users with this Role</td>
<td></td>
<td></td>
</tr>
<tr>
<td>edit their own rights)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can Delete Roles</td>
<td>Not allowed</td>
<td></td>
</tr>
<tr>
<td>Delegate Authority</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can only manipulate users</td>
<td>Not allowed</td>
<td></td>
</tr>
<tr>
<td>with equal or lesser rights</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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        | Allowed                          |
| (User can always edit select    |                                  |
| properties of own account)      |                                  |
| Can Delete Users                | Allowed                          |
| Roles                           |                                  |
| Can View Roles                  | Not allowed                      |
| Can Create New Roles            | Not allowed                      |
| Can Edit Role Properties        | Not allowed                      |
| (Warning: conferring this right |                                  |
| will let users with this Role   |                                  |
| edit their own rights)          |                                  |
| Can Delete Roles                | Not allowed                      |
| Delegate Authority              |                                  |
| Can only manipulate users       | Allowed                          |
| with equal or lesser rights     |                                  |

The custom settings corresponding to the **Have full control over all Roles and users** option are listed in the following table:
<table>
<thead>
<tr>
<th>Custom settings corresponding to &quot;Have full control over all Roles and users&quot; option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
</tr>
<tr>
<td>Can View Users</td>
</tr>
<tr>
<td>Can Create New Users</td>
</tr>
<tr>
<td>Can Edit User Properties (User can always edit select properties of own account)</td>
</tr>
<tr>
<td>Can Delete Users</td>
</tr>
<tr>
<td>Roles</td>
</tr>
<tr>
<td>Can View Roles</td>
</tr>
<tr>
<td>Can Create New Roles</td>
</tr>
<tr>
<td>Can Edit Role Properties (Warning: conferring this right will let users with this Role edit their own rights)</td>
</tr>
<tr>
<td>Can Delete Roles</td>
</tr>
<tr>
<td>Delegate Authority</td>
</tr>
<tr>
<td>Can only manipulate users with equal or lesser rights</td>
</tr>
</tbody>
</table>
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 be 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 internal database (Derby), 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).

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.
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 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 308)** 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 311)** You can import a Microsoft Active Directory or any other LDAP-based directory service.
- **Importing computers from a VMware vCenter (page 316)** You can import a VMware vCenter and provide the hosted VMs with Agent-based or Agentless protection.
- **Importing computers from a Cloud Provider (page 319)** You can import virtual machines being hosted on VMware vCloud or Amazon EC2 infrastructures.
- **Using a deployment script (page 323)** 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 Instructions (page 437).

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.
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 283).

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 Active Directory. Computers are imported and synchronized according to the structure in the directory.

To import a MS 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

Host 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](http://msdn.microsoft.com/en-us/library/aa746475(v=vs.85).aspx)

**Importing Hosts**

Deep Security can import a list of computers from Active Directory and use it to populate its Computers list. This process replicates the Active Directory folder structure in Deep Security. Replicating the Active Directory structure in the Computer list facilitates mapping of Deep Security Manager Roles with domain access rights in Active Directory.

To add a directory to Deep Security Manager:

1. Click **Computers** on the navigation bar to go to the Computers section.
2. Click the arrow to the right of the **New** button to display the drop-down menu and select **Add Directory**...
   
   This starts the Add Directory Wizard.
3. On the **Enter the server information** page, provide the address and logon credentials. You can use one of the following access methods:

<table>
<thead>
<tr>
<th>Method</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous</td>
<td>389</td>
<td>No passwords required. Unprotected traffic</td>
</tr>
<tr>
<td>Userid/Password</td>
<td>389</td>
<td>Password required. Unprotected traffic</td>
</tr>
<tr>
<td>Anonymous SSL</td>
<td>636</td>
<td>No password required. Traffic over SSL</td>
</tr>
<tr>
<td>Userid/Password SSL</td>
<td>636</td>
<td>Password required. Traffic over SSL</td>
</tr>
<tr>
<td>Userid/Password StartTLS</td>
<td>389</td>
<td>Password required. Traffic over TLS</td>
</tr>
</tbody>
</table>

4. Click **Next**.
5. Once the Directory server authenticates the access request, the wizard presents a page that prompts you for additional information about the directory schema. Enter the schema information and click **Finish**.
6. The next page displays a report on the number of computers that were imported. Click **Next**.
7. In the final page, you are presented with the option to create a scheduled task to keep the important data synchronized with data on the Directory server. Select the option to create a schedule task and click **Close**.
Importing Users and Contacts

Deep Security can import user account information from Active Directory and create corresponding Deep Security accounts. 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.

To import users and contacts:

1. In the navigation panel, click on Administration > User management > Users or Administration > User management > Contacts.
2. Click the Synchronize with Directory button. If this is the first time user and 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 hosts.) 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. All other 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 host 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 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.

The Coordinated Approach

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 virtual machines are protected by the coordinated approach, if the Agent goes offline, then protection from the Appliance is automatically activated.

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:

<table>
<thead>
<tr>
<th></th>
<th>Supported by Appliance</th>
<th>Supported by Agent</th>
<th>Coordinated Approach Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Malware</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Web Reputation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Firewall</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Intrusion Prevention</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Integrity Monitoring</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Log Inspection</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Note:** Some features are not available on all platforms. For a complete detailed list of supported features by platform, see the Installation Guide.

Adding a VMware vCenter

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

1. Right-click on **Computers** in the navigation panel and select **Add VMware vCenter...** to start the **Add VMware vCenter** wizard.
2. Provide the server address (IP or hostname) and port, a name and description, and the username and password for the ESX Server. Click **Next**.
3. Enter the vShield Manager Server Address, Username and Password. Click **Next**.
4. In **Deep Security Virtual Appliance global network configuration**, use the recommended default configuration. Click **Next**.

**Note:** The VMKernel VNIC IP by default uses 169.254.50.1. It is possible that some other vShield products are already installed on the ESXi. If so, re-use the existing configuration. If there is already an existing product that created the vmservice-vmknic-pg and assigned an address 169.254.1.1, make sure the IP Address is configured the same in VMKernel VNIC IP.

5. Accept the vShield Manager SSL certificate and the VMware default certificate.
6. The **Add VMware vCenter** wizard will display the details of the vCenter being added.
7. Click **Finish**.
8. "The VMware vCenter has been successfully added" message will be displayed. Click Close.

**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 9 Installation Guide.
Cloud Account

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

- Amazon EC2
- VMware vCloud

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 manage 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.
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 Organization's 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 Amazon AWS resources into the Deep Security Manager, the User 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**.

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.

### Managing a Cloud Account

To implement Deep Security protection on your Cloud Provider VMs, you must install an Agent and assign a Policy to the VM 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 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.

To generate a deployment script:


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 (page 229).)

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 (optional)

6. Select the Computer Group (optional)

7. 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.)

When copying the deployment script into the **User Data** field for a **Windows** deployment, **you must add the following XML tags around the script:**

```
<powershell>
{script from deployment script generator}
</powershell>
```

**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](http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cloudformation-waitcondition-article.html)

**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 ESX 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 307).

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 (page 229).)
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.
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. The Virtual Appliance uses VMware's VMsafe-NET API to intercept network traffic at the hypervisor. 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. The VMware vShield Manager manages VMware vShield Endpoint which in turn communicates with the VMware Thin Agents. The last two components provide the API which Deep Security uses to provide Anti-Malware protection.

Preparing your VMware environment for Anti-Malware protections involves:
1. Deploying the VMware vShield Manager
2. Installing the vShield Endpoint Host Driver on the ESXi hypervisor
3. Installing vShield Endpoint Thin Agents on the virtual machines you want to protect

For detailed instructions on how to setup the VMware environment including system requirements, installation steps and configuration, refer to the Trend Micro Deep Security 9 SP1 Installation Guide.

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
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, consult your Trend Micro Deep Security 9 SP1 Installation Guide.

**Implementing VM Protection with the Deep Security Virtual Appliance**

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

1. Right-click on Computers in the navigation panel and select Add VMware vCenter... to start the Add VMware vCenter wizard.
2. Provide the server address (IP or hostname) and port, a name and description, and the username and password for the ESX Server. Click Next.
3. Enter the vShield Manager Server Address, Username and Password. Click Next.
4. In Deep Security Virtual Appliance global network configuration, use the recommended default configuration. Click Next.
The VMKernel VNIC IP by default uses 169.254.50.1. It is possible that some other vShield products are already installed on the ESXi. If so, re-use the existing configuration. If there is already an existing product that created the vmservice-vmknic-pg and assigned an address 169.254.1.1, make sure the IP Address is configured the same in VMKernel VNIC IP.

5. Accept the vShield Manager SSL certificate and the VMware default certificate.
6. The Add VMware vCenter wizard will display the details of the vCenter being added.
7. Click Finish.
8. "The VMware vCenter has been successfully added" message will be displayed. Click Close.

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.

To prepare the ESXi for the Virtual Appliance deployment:

To proceed, the Deep Security Filter Driver software package must already be downloaded from the Trend Micro download center and imported into the Deep Security Manager. You can perform both these operations from the Administration > Updates page.

1. Under Computers in the Deep Security Manager navigation panel, click on the newly added vCenter to display the vCenter components and select Hosts and Clusters.
2. Find the ESXi host on the Computers page (its Status column should read "Unprepared"), right-click on it, and select Actions > Prepare ESX Server to display the Prepare ESX Server wizard. Click Next.
3. The ESXi must be put into maintenance mode before the first of two Virtual Appliance components (the Filter Driver) can be installed. Select Yes to allow the Deep Security Manager to manage this process automatically. Click Next.
4. The ESXi host will now be placed in maintenance mode, the Filter Driver will be installed, and the ESXi host will be restarted. When the wizard indicates that the process is complete, click Close.

You can monitor this process in the VMware vSphere Client management console.

The Filter Driver is now installed on the ESXi host.

To deploy the Virtual Appliance to the ESXi:

To proceed, the Deep Security Virtual Appliance software package must already be downloaded from the Trend Micro download center and imported into the Deep Security Manager. You can perform both these operations from the Administration > Updates page.
1. Right-click on the ESXi host on the Computers page (the Status column should now read "Prepared"), and select Actions > Deploy Appliance... to display the Deep Security Virtual Appliance wizard. Click Next.

2. Give the Virtual Appliance a Name and select a Datastore for the Appliance.

3. Select the Folder for the Datacenter and select the Management Network for the Appliance. Click Next.

4. Define the Appliance Hostname. Enter the IPv6 Address and/or IPv4 Address for the Appliance. (DHCP is enabled by default). Click Next.

5. Select Thick Provisioned format (recommended). (Thick Provisioned Format uses all the allocated disk space, while Thin Provisioned Format uses the least amount of disk space).

6. Click Finish and wait for few minutes for the DSVA to be uploaded.

7. The Virtual Appliance will now be deployed on the ESXi host. (Once again, this procedure can be monitored in the VMware vSphere Client management console.) When the Virtual Appliance deployment is complete, click Close.

The Virtual Appliance is now displayed along with the other computers in the vCenter group on the Computers page.

**Note:** When a Virtual Appliance is deployed in a VMware environment that makes use of the VMware Distributed Resource Scheduler (DRS), it is important that the Appliance does not get vMotioned along with the virtual machines as part of the DRS process. Virtual Appliances must be "pinned" to their particular ESX host. You must proactively change the DRS settings for all the Virtual Appliances to "Manual" or "Disabled" (recommended) so that they will not be vMotioned by the DRS. If a Virtual Appliance (or any virtual machine) is set to "Disabled", vCenter Server will not migrate that virtual machine or provide migration recommendations for it. This is known as "pinning" the virtual machine to its registered host. This is the recommended course of action for Virtual Appliances in a DRS environment. (An alternative is to deploy the Virtual Appliance onto a local store as opposed to a shared store. When the Virtual Appliance is deployed onto a local store it cannot be vMotioned by DRS.) For further information on DRS and pinning virtual machines to a specific ESX consult your VMware documentation.

**Note:** The Deep Security Manager puts the ESX into maintenance mode during an install or upgrade of the Deep Security Filter Driver. (This done during the "Prepare ESX" phase of installation.) When an ESXi already hosting a Virtual Appliance is put into maintenance mode, the Deep Security Manager will automatically power the Virtual Appliance off and back on again when exiting maintenance mode. If the ESXi is put into maintenance mode by means other than through the Deep Security Manager, the Virtual Appliance is not powered off/on automatically.

To activate the Virtual Appliance:

1. Right-click on the Virtual Appliance in the Computers > vCenter list and select Actions > Activate Appliance to display the Activate Deep Security Appliance wizard. Click Next.
2. For Policy, select Deep Security Virtual Appliance. Click Next.
3. When the Virtual Appliance has been successfully activated, click Close.

The Status of the Virtual Appliance will now read "Managed (Online)".

**To enable Virtual Appliance protection on guest virtual machines:**

1. Right-click on a virtual machine in the computer list and select Actions > Activate.
2. The Status column for the virtual machine will change to "Managed (Online)".

The virtual machine is now protected by the Virtual Appliance even though no in-guest Agent is installed on the virtual machine. Policies can be assigned to this virtual machine like any other computer being managed by Deep Security Manager.

Once the Virtual Appliance is installed, any virtual machines that are added to the ESXi host afterwards can be automatically activated and a Policy can be automatically applied. New virtual machines can automatically be assigned Policies when detected.

---

**Note:** The Virtual Appliance requires that all VMs that are to be protected have been assigned unique UUIDs by the vCenter. A situation with duplicate UUIDs can occur if you copy a VM. After copying a VM, you are asked by vCenter whether the new VM is a copy or whether it was moved. If you select the *I copied it* option, vCenter will assign it a new UUID. However, if you select the *I moved it* option (when in fact it was copied), vCenter will not assign it a new UUID. You will then have two VMs with the same UUID which will cause problems for the Virtual Appliance. If the Virtual Appliance is instructed to protect multiple VMs with the same UUID, an Alert will be raised and the operation will fail.

---

**To implement coordinated protection by installing an Agent on a virtual machine:**

To install a Deep Security Agent on a virtual machine, follow the same procedures as for any physical computer. A virtual machine being protected by both a Virtual Appliance and an Agent is referred to as "coordinated protection". The Virtual Appliance and the Agent are in constant communication. As long as the Virtual Appliance detects the presence of an Agent on the virtual machine, it will pass all traffic to the Agent and let the Agent apply the security rules to the traffic. If the Agent fails or is stopped, the Virtual Appliance will take over the job of applying security rules to traffic.

---

**Note:** When a Policy is applied to an Agent on a VM that is also protected by a Virtual Appliance, then a copy of that Policy also goes to the Virtual Appliance. When the Agent is running on a VM, the Virtual Appliance is actually sitting idle. If the communication between the Virtual Appliance and the Agent is interrupted (by the Agent going offline for some reason), then the Appliance starts protecting the VM with the same Policy.
Both the ESXi and the Virtual Appliance may try to look up the hostname of the Manager and not find it if the Manager is in a different DNS domain. You can solve this by renaming the Manager to its fully qualified domain name (FQDN). To rename the Manager, go to Administration > System Information > System Activity. Make sure Network Map with Activity Graph is selected, then click on the Manager in the Network Map to display the Manager’s Properties window and edit the Hostname field to the FQDN.

The Virtual Appliance cannot perform Log Inspection or Integrity Monitoring because it is not running on the VM being protected. To perform Log Inspection or Integrity Monitoring on a VM, an in-guest Deep Security Agent must be installed.

Scan Caching

Scan Caching improves the efficiency of on-demand scans performed by the Virtual Appliance. It eliminates the unnecessary scanning of identical content across multiple VMs in large VMware deployments.

In addition,

- Integrity Monitoring scan caching speeds up Integrity Monitoring scans by sharing Integrity Monitoring scan results
- Anti-Malware on-demand caching speeds up scans on subsequent cloned/similar VMs
- Anti-Malware Real-time caching speeds up VM boot and application access time
- Concurrent Scan feature allows further overall scan time improvement by allowing multiple VMs to be scanned concurrently

High Availability Environments

If you intend to take advantage of VMware High Availability (HA) capabilities, make sure that the HA environment is established before you begin installing Deep Security. All ESXi hypervisors used for recovery operations must be imported into the Deep Security Manager with their vCenter, they must be "prepared", and a Deep Security Virtual Appliance must be installed on each one. Setting up the environment in this way will ensure that Deep Security protection will remain in effect after a HA recovery operation.

When a Virtual Appliance is deployed in a VMware environment that makes use of the VMware Distributed Resource Scheduler (DRS), it is important that the Appliance does not get vMotioned along with the virtual machines as part of the DRS process. Virtual Appliances must be "pinned" to their particular ESXi host. You must actively change the DRS settings for all the Virtual Appliances to "Manual" or "Disabled" (recommended) so that they will not be vMotioned by the DRS. If a Virtual Appliance (or any virtual machines) is set to "Disabled", vCenter Server does not migrate that virtual machine or provide migration recommendations for it. This is known as "pinning" the virtual machine to its registered host. This is the recommended course of action for
Virtual Appliances in a DRS environment. (An alternative is to deploy the Virtual Appliance onto a local store as opposed to a shared store. When the Virtual Appliance is deployed onto a local store it cannot be vMotioned by DRS.) For further information on DRS and pinning virtual machines to a specific ESXi host consult your VMWare documentation.

**Note:** If a virtual machine is vMotioned by HA from an ESXi protected by a DSVA to an ESXi that is not protected by a DSVA, the virtual machine will become unprotected. If the virtual machine is subsequently vMotioned back to the original ESXi, it will not automatically be protected again unless you have created an Event-based Task to activate and protect computers that have been vMotioned to an ESXi with an available DSVA. For more information, see [Event-Based Tasks](page 210).
Protection Modules


- The **Anti-Malware (page 336)** 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 Reputation (page 341)** 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 343)** is an NDIS-based, bi-directional, 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 357)** 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 359)** 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 361)** 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.

<table>
<thead>
<tr>
<th>Targets</th>
<th>Full Scan</th>
<th>Quick Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drivers</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Trojan</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Process Image</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Memory</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Boot Sector</td>
<td>5</td>
<td>-</td>
</tr>
</tbody>
</table>
## Smart Scan

Smart Scan references threat signatures that are stored on Trend Micro servers. When Smart Scan is enabled, the Deep Security first scans for security risks locally. If the 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 endpoints
- Reduces the cost and overhead associated with corporate-wide pattern deployments
- Lowers kernel memory consumption on endpoints. 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.**
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 inline 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 an NDIS-based, bi-directional, 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 inline 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 Driver 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**
• **Other** (for which you must provide a protocol number)
Direction

The Deep Security firewall is a bi-directional 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:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Closed Port</td>
<td>Returns an RST packet</td>
</tr>
<tr>
<td>Open Port</td>
<td>No response, exposing existence of the open port</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Note: Traffic permitted by a Force Allow Rule will still be subject to analysis by the Intrusion Prevention module.</th>
</tr>
</thead>
</table>

- **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.
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 DSM traffic rule in favor of the new custom rule provided it has the following characteristics:
The custom rule must use the above parameters to replace the default rule. Ideally, the IP address or MAC address of the actual DSM 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 DSM 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 DSM 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:

![Diagram of rule actions]

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 stateful analysis is enabled, 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.

- 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)

---

**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 inline 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 Driver 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 510)** 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 382).
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 (page 84) as well as Examining a Log Inspection Rule (page 382) 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 event 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:

```xml
<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:
Custom rules must have ID values between 100,000 to 119,999.

You can define additional subgroups within the parent group using the `<group>` tag. This subgroup can reference any of the groups listed in the following table:

<table>
<thead>
<tr>
<th>Group Type</th>
<th>Group Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reconnaissance</strong></td>
<td>connection_attempt</td>
<td>Connection attempt</td>
</tr>
<tr>
<td></td>
<td>web_scan</td>
<td>Web scan</td>
</tr>
<tr>
<td></td>
<td>recon</td>
<td>Generic scan</td>
</tr>
<tr>
<td><strong>Authentication Control</strong></td>
<td>authentication_success</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>authentication_failed</td>
<td>Failure</td>
</tr>
<tr>
<td></td>
<td>invalid_login</td>
<td>Invalid</td>
</tr>
<tr>
<td></td>
<td>login_denied</td>
<td>Login Denied</td>
</tr>
<tr>
<td></td>
<td>authentication_failures</td>
<td>Multiple Failures</td>
</tr>
<tr>
<td></td>
<td>adduser</td>
<td>User account added</td>
</tr>
<tr>
<td></td>
<td>account_changed</td>
<td>User Account changed or removed</td>
</tr>
<tr>
<td><strong>Attack/Misuse</strong></td>
<td>automatic_attack</td>
<td>Worm (nontargeted attack)</td>
</tr>
<tr>
<td></td>
<td>exploit_attempt</td>
<td>Exploit pattern</td>
</tr>
<tr>
<td></td>
<td>invalid_access</td>
<td>Invalid access</td>
</tr>
<tr>
<td></td>
<td>spam</td>
<td>Spam</td>
</tr>
<tr>
<td></td>
<td>multiple_spam</td>
<td>Multiple spam messages</td>
</tr>
<tr>
<td></td>
<td>sql_injection</td>
<td>SQL injection</td>
</tr>
<tr>
<td></td>
<td>attack</td>
<td>Generic attack</td>
</tr>
<tr>
<td></td>
<td>virus</td>
<td>Virus detected</td>
</tr>
<tr>
<td><strong>Access Control</strong></td>
<td>access Denied</td>
<td>Access denied</td>
</tr>
<tr>
<td></td>
<td>access_allowed</td>
<td>Access allowed</td>
</tr>
<tr>
<td></td>
<td>unknown_resource</td>
<td>Access to nonexistent resource</td>
</tr>
<tr>
<td></td>
<td>firewall_drop</td>
<td>Firewall drop</td>
</tr>
<tr>
<td></td>
<td>multiple_drops</td>
<td>Multiple firewall drops</td>
</tr>
<tr>
<td></td>
<td>client misconfig</td>
<td>Client misconfiguration</td>
</tr>
<tr>
<td></td>
<td>client_error</td>
<td>Client error</td>
</tr>
<tr>
<td><strong>Network Control</strong></td>
<td>new_host</td>
<td>New host detected</td>
</tr>
<tr>
<td></td>
<td>ip_spoof</td>
<td>Possible ARP spoofing</td>
</tr>
<tr>
<td>Group Type</td>
<td>Group Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>System Monitor</td>
<td>service_start</td>
<td>Service start</td>
</tr>
<tr>
<td></td>
<td>system_error</td>
<td>System error</td>
</tr>
<tr>
<td></td>
<td>system_shutdown</td>
<td>Shutdown</td>
</tr>
<tr>
<td></td>
<td>logs_cleared</td>
<td>Logs cleared</td>
</tr>
<tr>
<td></td>
<td>invalid_request</td>
<td>Invalid request</td>
</tr>
<tr>
<td></td>
<td>promise</td>
<td>Interface switched to promiscuous mode</td>
</tr>
<tr>
<td></td>
<td>policy_changed</td>
<td>Policy changed</td>
</tr>
<tr>
<td></td>
<td>config_changed</td>
<td>Configuration changed</td>
</tr>
<tr>
<td></td>
<td>low_diskspace</td>
<td>Low disk space</td>
</tr>
<tr>
<td></td>
<td>time_changed</td>
<td>Time changed</td>
</tr>
</tbody>
</table>

**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.

```xml
<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.

```xml
<rule id="100123" level="5">
  <decoded_as>sshd</decoded_as>
  <description>Logging every decoded sshd message</description>
</rule>
```
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....

Note: To look for a specific string in a log, use the `<match></match>`. Here is a Linux sshd failed password log:

Jan 1 12:34:56 linux_server sshd[1231]: Failed password for invalid user jsmith from 192.168.1.123 port 1799 ssh2

Use the `<match></match>` tag to search for the "password failed" string.

```xml
<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:

<table>
<thead>
<tr>
<th>Regex Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\w</td>
<td>A-Z, a-z, 0-9 single letters and numerals</td>
</tr>
<tr>
<td>\d</td>
<td>0-9 single numerals</td>
</tr>
<tr>
<td>\s</td>
<td>single space</td>
</tr>
<tr>
<td>\t</td>
<td>single tab</td>
</tr>
<tr>
<td>\p</td>
<td>()*+,.:-;&lt;&gt;?[]</td>
</tr>
<tr>
<td>\W</td>
<td>not \w</td>
</tr>
<tr>
<td>\D</td>
<td>not \d</td>
</tr>
<tr>
<td>\S</td>
<td>not \s</td>
</tr>
<tr>
<td>\</td>
<td>anything</td>
</tr>
<tr>
<td>+</td>
<td>match one or more of any of the above (for example, \w+, \d+)</td>
</tr>
<tr>
<td>*</td>
<td>match zero or more of any of the above (for example, \w*, \d*)</td>
</tr>
<tr>
<td>^</td>
<td>indicates the beginning of a string (&quot;somestring&quot;)</td>
</tr>
</tbody>
</table>
Regex Syntax | Description
---|---
$ | 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>` 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>` tag:

```xml
<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>` tag essentially creates a hierarchical set of rules. That is, by including an `<if_sid>` tag in a rule, the rule becomes a child of the rule referenced by the `<if_sid>` tag. Before applying any rules to a log, the Log Inspection engine assesses the `<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.
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:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>match</td>
<td>A pattern</td>
<td>Any string to match against the event (log).</td>
</tr>
<tr>
<td>regex</td>
<td>A regular expression</td>
<td>Any regular expression to match against the event (log).</td>
</tr>
<tr>
<td>decoded_as</td>
<td>A string</td>
<td>Any prematched string.</td>
</tr>
<tr>
<td>srcip</td>
<td>A source IP address</td>
<td>Any IP address that is decoded as the source IP address. Use &quot;!&quot; to negate the IP address.</td>
</tr>
<tr>
<td>dstip</td>
<td>A destination IP address</td>
<td>Any IP address that is decoded as the destination IP address. Use &quot;!&quot; to negate the IP address.</td>
</tr>
<tr>
<td>srcport</td>
<td>A source port</td>
<td>Any source port (match format).</td>
</tr>
<tr>
<td>dstport</td>
<td>A destination port</td>
<td>Any destination port (match format).</td>
</tr>
<tr>
<td>user</td>
<td>A username</td>
<td>Any username that is decoded as a username.</td>
</tr>
<tr>
<td>program_name</td>
<td>A program name</td>
<td>Any program name that is decoded from the syslog process name.</td>
</tr>
<tr>
<td>hostname</td>
<td>A system hostname</td>
<td>Any hostname that is decoded as a syslog hostname.</td>
</tr>
<tr>
<td>time</td>
<td>A time range in the format</td>
<td>The time range that the event must fall within for the rule to trigger.</td>
</tr>
<tr>
<td></td>
<td>hh:mm - hh:mm or hh:mm am - hh:mm pm</td>
<td></td>
</tr>
<tr>
<td>weekday</td>
<td>A weekday (sunday, monday, tuesday, etc.)</td>
<td>Day of the week that the event must fall on for the rule to trigger.</td>
</tr>
<tr>
<td>id</td>
<td>An ID</td>
<td>Any ID that is decoded from the event.</td>
</tr>
<tr>
<td>url</td>
<td>A URL</td>
<td>Any URL that is decoded from the event.</td>
</tr>
</tbody>
</table>

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.

```xml
<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:

```xml
<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:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>if_sid</td>
<td>A rule ID</td>
<td>Adds this rule as a child rule of the rules that match the specified signature ID.</td>
</tr>
<tr>
<td>if_group</td>
<td>A group ID</td>
<td>Adds this rule as a child rule of the rules that match the specified group.</td>
</tr>
<tr>
<td>if_level</td>
<td>A rule level</td>
<td>Adds this rule as a child rule of the rules that match the specified severity level.</td>
</tr>
<tr>
<td>description</td>
<td>A string</td>
<td>A description of the rule.</td>
</tr>
<tr>
<td>info</td>
<td>A string</td>
<td>Extra information about the rule.</td>
</tr>
<tr>
<td>cve</td>
<td>A CVE number</td>
<td>Any Common Vulnerabilities and Exposures (CVE) number that you would like associated with the rule.</td>
</tr>
<tr>
<td>options</td>
<td>alert_by_email, no_email_alert, no_log</td>
<td>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.</td>
</tr>
</tbody>
</table>

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:

```xml
<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.
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:

```xml
<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:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>same_source_ip</td>
<td>Specifies that the source IP address must be the same.</td>
</tr>
<tr>
<td>same_dest_ip</td>
<td>Specifies that the destination IP address must be the same.</td>
</tr>
<tr>
<td>same_dst_port</td>
<td>Specifies that the destination port must be the same.</td>
</tr>
<tr>
<td>same_location</td>
<td>Specifies that the location (hostname or agent name) must be the same.</td>
</tr>
<tr>
<td>same_user</td>
<td>Specifies that the decoded username must be the same.</td>
</tr>
<tr>
<td>same_id</td>
<td>Specifies that the decoded id must be the same.</td>
</tr>
</tbody>
</table>

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.

```xml
<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.

```xml
<rule id="100130" level="10" frequency="5" timeframe="600">
  <if_matched_regex>^Failed password</if_matched_regex>
  <same_source_ip />
```
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:

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.

8. Now select the **Custom (XML)** option. The information you have entered will be used to generate the XML for your rule.

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.
**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":

```xml
<rule name="cms">
  <group name="windows">
    <if_group>authentication</if_group>
    <id>100</id>
    <description>CMS User Login success event.</description>
  </group>
</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.

```xml
<rule name="cms">
  <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>
```

```xml
<rule name="cms">
  <if_group>authentication</if_group>
  <id>100</id>
  <group>authentication_failure</group>
  <description>CMS User Login failure event.</description>
</rule>
```

```xml
<rule name="cms">
  <if_group>authentication</if_group>
  <id>101</id>
  <group>authentication_failure</group>
  <description>CMS User 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">
```
<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>
</rule>
<rule id="100008" level="10">
<if_group>cms_error</if_group>
<id>^200|^201|^202|^203|^204|^205</id>
<description>CMS Database error event.</description>
</rule>

<rule id="100009" level="10">
<if_group>cms_error</if_group>
<id>^206|^207|^208|^209|^230|^231|^232|^233|^234|^235|^236|^237|^238|^239|^240|^241|^242|^243|^244|^245|^246|^247|^248|^249</id>
<description>CMS Runtime error event.</description>
</rule>

<rule id="100010" level="0">
<if_sid>100000</if_sid>
<status>^INFORMATION</status>
<description>CMS General informational event.</description>
</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>
Log Inspection Rule Severity Levels and their Recommended Use

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 0</td>
<td>Ignored, no action taken</td>
<td>Primarily used to avoid false positives. These rules are scanned before all the others and include events with no security relevance.</td>
</tr>
<tr>
<td>Level 1</td>
<td>no predefined use</td>
<td></td>
</tr>
<tr>
<td>Level 2</td>
<td>System low priority notification</td>
<td>System notification or status messages that have no security relevance.</td>
</tr>
<tr>
<td>Level 3</td>
<td>Successful/authorized events</td>
<td>Successful login attempts, firewall allow events, etc.</td>
</tr>
<tr>
<td>Level 4</td>
<td>System low priority errors</td>
<td>Errors related to bad configurations or unused devices/applications. They have no security relevance and are usually caused by default installations or software testing.</td>
</tr>
<tr>
<td>Level 5</td>
<td>User-generated errors</td>
<td>Missed passwords, denied actions, etc. These messages typically have no security relevance.</td>
</tr>
<tr>
<td>Level 6</td>
<td>Low relevance attacks</td>
<td>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.</td>
</tr>
<tr>
<td>Level 7</td>
<td>no predefined use</td>
<td></td>
</tr>
<tr>
<td>Level 8</td>
<td>no predefined use</td>
<td></td>
</tr>
<tr>
<td>Level 9</td>
<td>Error from invalid source</td>
<td>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.</td>
</tr>
<tr>
<td>Level 10</td>
<td>Multiple user generated errors</td>
<td>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.</td>
</tr>
<tr>
<td>Level</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>Level 11</td>
<td>no predefined use</td>
<td></td>
</tr>
<tr>
<td>Level 12</td>
<td>High-importance event</td>
<td>Include error or warning messages from the system, kernel, etc. They might indicate an attack against a specific application.</td>
</tr>
<tr>
<td>Level 13</td>
<td>Unusual error (high importance)</td>
<td>Common attack patterns such as a buffer overflow attempt, a larger than normal syslog message, or a larger than normal URL string.</td>
</tr>
<tr>
<td>Level 14</td>
<td>High importance security event</td>
<td>Typically the result of the correlation of multiple attack rules and indicative of an attack.</td>
</tr>
<tr>
<td>Level 15</td>
<td>Attack Successful</td>
<td>Very small chance of false positive. Immediate attention is necessary.</td>
</tr>
</tbody>
</table>

### strftime() Conversion Specifiers

<table>
<thead>
<tr>
<th>Specifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%a</td>
<td>Abbreviated weekday name (e.g., Thu)</td>
</tr>
<tr>
<td>%A</td>
<td>Full weekday name (e.g., Thursday)</td>
</tr>
<tr>
<td>%b</td>
<td>Abbreviated month name (e.g., Aug)</td>
</tr>
<tr>
<td>%B</td>
<td>Full month name (e.g., August)</td>
</tr>
<tr>
<td>%c</td>
<td>Date and time representation (e.g., Thu Sep 22 12:23:45 2007)</td>
</tr>
<tr>
<td>%d</td>
<td>Day of the month (01 - 31) (e.g., 20)</td>
</tr>
<tr>
<td>%H</td>
<td>Hour in 24 h format (00 - 23) (e.g., 13)</td>
</tr>
<tr>
<td>%I</td>
<td>Hour in 12 h format (01 - 12) (e.g., 02)</td>
</tr>
<tr>
<td>%j</td>
<td>Day of the year (001 - 366) (e.g., 235)</td>
</tr>
<tr>
<td>%m</td>
<td>Month as a decimal number (01 - 12) (e.g., 02)</td>
</tr>
<tr>
<td>%M</td>
<td>Minute (00 - 59) (e.g., 12)</td>
</tr>
<tr>
<td>%p</td>
<td>AM or PM designation (e.g., AM)</td>
</tr>
<tr>
<td>%S</td>
<td>Second (00 - 61) (e.g., 55)</td>
</tr>
<tr>
<td>%U</td>
<td>Week number with the first Sunday as the first day of week one (00 - 53) (e.g., 52)</td>
</tr>
<tr>
<td>%W</td>
<td>Weekday as a decimal number with Sunday as 0 (0 - 6) (e.g., 2)</td>
</tr>
<tr>
<td>%W</td>
<td>Week number with the first Monday as the first day of week one (00 - 53) (e.g., 21)</td>
</tr>
<tr>
<td>%x</td>
<td>Date representation (e.g., 02/24/79)</td>
</tr>
<tr>
<td>%X</td>
<td>Time representation (e.g., 04:12:51)</td>
</tr>
<tr>
<td>%y</td>
<td>Year, last two digits (00 - 99) (e.g., 76)</td>
</tr>
<tr>
<td>Specifier</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>%Y</td>
<td>Year (e.g., 2008)</td>
</tr>
<tr>
<td>%Z</td>
<td>Time zone name or abbreviation (e.g., EST)</td>
</tr>
<tr>
<td>%%</td>
<td>A % sign (e.g., %)</td>
</tr>
</tbody>
</table>

More information can be found at the following Web sites:

- [www.php.net/strftime](http://www.php.net/strftime)
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 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 tab of the Properties window](image)

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:
Examining a Log Inspection Rule
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

The Deep Security Virtual Appliance can perform Agentless Recommendation Scans on virtual machines but is limited to scanning:

- the operating system
- installed applications
- the Windows registry
- the file system

**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 certain computers.

**Note:** The Deep Security Relay has an embedded Agent and can therefore be instructed to perform Recommendation Scans on itself.

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 > Schedule 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:
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").
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).

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

<table>
<thead>
<tr>
<th>Note:</th>
<th>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 451).</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Note:</th>
<th>For more detailed information on SSL support, consult the release notes included with the Deep Security Agent software.</th>
</tr>
</thead>
</table>


Event Tagging

Event Tagging lets you annotate events with metadata "Tags". A Tag is a user-defined property which you can later use to identify or sort Events. For example, you might use Tags to identify Events that require further investigation.

For more information about Event Tagging, see *More About Event Tagging (page 447)*.

Standard Event Tagging

To tag a single Event:

1. Right-click on the Event in the Events list 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 **1 Selected System Event**. (You can select multiple Events at once from the Events list, in which case the number of selected Events will be displayed.) 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.

To tag multiple similar Events:

1. Right click on a representative Event from the Events list 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 similar Events**.

   **Note:** Depending on the type of Event (Firewall, Intrusion Prevention, Integrity Monitoring, etc.), you may be able to select **Display Advanced Settings**. Advanced settings will include further criteria for refining the selection of the Events you want to tag.

   Also select **Include Advanced Options**, if available. Click **Next**.

4. If you were able to select **Include Advanced Options** you will see a page that allows you to narrow your Event selection. For example, you could look for similar Events only on a specific computer, or group of computers. If this is the case, make your selections and click **Next**.

5. Select which attributes will be examined to determine whether Events are similar or not. 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. Select existing **Log Inspection Events** to identify and tag currently existing Events, and select **Update Now** to initiate the search for all similar Events (rather than have the search run in the background at a low priority).

**Note:** Notice the **Save Auto-Tag Rule** option. The selection criteria you have specified can be saved so that you can apply them again at a future date when new Events have accumulated. Saved auto-tag rules can be found on the Deep Security Manager's **Policies > Tags** page.

7. Review the Summary of your Event selection criteria and click **Finish**.

Looking at the Events list, you can see that your original Event and all similar Events have been tagged.

**To tag multiple similar Events as well as future similar Events:**

The procedure for tagging multiple similar as well as future Events is the same as above except for step 3, where you also select **New [Event Type] Events** (where "[Event Type]" depends on the type of Events you are tagging (Firewall, Intrusion Prevention, Integrity Monitoring, etc.)). Selecting **New [Event Type] Events** causes the Deep Security Manager to scan its database every five seconds (or more) for new Events and tag the appropriate ones.

**Note:** Event Tagging only occurs after Events have been retrieved from the Agents/Appliances to the Deep Security Manager's database.

**Trusted-Source-Based Event Tagging**

**Note:** Trusted-Source-Based Event Tagging can only be used with Events generated by the Integrity Monitoring protection module.

Trusted-Source-Based Event Tagging is based on either a single **Local Trusted Computer**, the **Trend Micro Certified Safe Software Service**, or a **Trusted Common Baseline** built from the states of files and systems from a group of computers. Trusted-Source-Based Event Tagging works by comparing the Integrity Monitoring Events generated on one computer to the Integrity Monitoring

**Local Trusted Computer**

Use the Local trusted Computer option to implement a "Golden Host" integrity model, where a trusted computer is used as the basis for comparison by other computers. The **before** and **after** states of an Integrity Monitoring Event on a computer are compared to events on the Trusted Computer. If there is a match, the tag is applied.

**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 the Deep Security Manager, go to Events & Reports > Integrity Monitoring Events and click on Auto-Tagging... in the toolbar. This will display the Auto-Tag Rules (Integrity Monitoring Events) window.
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 menu, 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 that match Events on this Trusted Source computer and 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 on the Trusted Source. Click Next.
9. Optionally give this Auto-Tagging 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 the Deep Security Manager, go to Events & Reports > Integrity Monitoring Events and click on Auto-Tagging... in the toolbar. This will display the Auto-Tag Rules (Integrity Monitoring Events) window.
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 that match the Certified Safe Software Service and click Next.
5. Identify the target computers whose Events will be matched to the Certified Safe Software Service. Click Next.
6. Optionally give this Auto-Tagging Rule a name and click Finish.
Trusted Common Baseline

This method of Event Tagging is applied to a group of computers. A group of computers is identified and a baseline is generated based on the files and system states targeted by the Integrity Monitoring Rules that are in effect on the computers in the group. When an Integrity Monitoring Event occurs within that group of computers, the after state of the Event is compared to the common baseline. If that after state is found to exist on any other computer in the group, the Tag is applied to the Event.

**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 the Deep Security Manager, go to Events & Reports > Integrity Monitoring Events and click on Auto-Tagging... in the toolbar. This will display the Auto-Tag Rules (Integrity Monitoring Events) window.
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 that have a match in the Trusted Common Baseline and click Next.
6. Identify the computers that will be included in the group that will be used to generate the Trusted Common baseline. Click Next.
7. Optionally give this Auto-Tagging Rule a name and click Finish.
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. 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.
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 (смотрите) 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 Updates 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.

When malware is detected, the Notifier displays a message in a system tray popup similar to the following:

![Malware Detected](image)

If the user clicks on the message, a dialog box with detailed information about Anti-Malware Events is displayed:
When a malicious web page is blocked, the Notifier displays a message in a system tray popup similar to the following:

![Web Page(s) Blocked](image)

If the user clicks on the message, a dialog box with detailed information about Web Reputation Events is displayed:

![Deep Security Notification](image)

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.
When the notifier is running on a 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.

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
- Oracle Database or Microsoft SQL Server
- The necessary database account privileges for database create/delete operations. (See [Multi-Tenancy (Advanced) (page 414)](#))
- 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 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). Tenants are created on the database with the least amount of load when multiple database servers are available.
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.

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 (you).
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 UI for that Tenancy.
5. Time Zone. Although time is recorded throughout Deep Security in UT, all Tenant-related Events will be shown to the Tenant Users in the time zone of the Tenant account, not the server/machine where they occurred. Click Next.
6. Enter a username for the first User of the new Tenant account.
7. 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 the Tenant creator to generate a Tenant without knowing the password. This is most applicable when manually creating accounts for users...
where the creator does not need access to the Tenant account. Two emails will be sent. One to notify the Tenant that an account has been created, and a second one that contains the Tenant's password.

**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.

8. 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:

- **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 been clicked. (You can manually override this state.)
- **Active**: Fully online and managed
- **Suspended**: No longer accepting sign ins.
- **Pending Deletion**: Tenants can be deleted, however the process is not immediate. The Tenant will be in the pending deletion state for approximately 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

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
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 as 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 using the "Per Tenant" licensing by default only the licensed modules for each Tenant will be visible.

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**

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

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

Primary Contact

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:
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 (page 185).

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 the View Imported Software button on the Administration > Updates > Software Updates tab, right-clicking and Agent install package, and selecting Generate Deployment Scripts from the context menu:

As an example, the script for Agent-Initiated Activation on a Windows machine might look as follows:

```
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:

![Tenant-related widgets]

Some examples of Tenant-related widgets:
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 instance 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.

<table>
<thead>
<tr>
<th></th>
<th>SQL Server</th>
<th>Oracle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process where multiple Tenants execute</td>
<td>Database Server</td>
<td>Database</td>
</tr>
<tr>
<td>One Tenant's set of data</td>
<td>Database</td>
<td>Tablespace/User</td>
</tr>
</tbody>
</table>

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:

![SQL Server dbcreator role](image)

For the user role of the primary Tenant it is important to assign DB owner to the main database:
If desired, rights may be further refined to include only the ability to modify the schema and access the data.

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

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 it may be required a Primary Tenant to gain 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 happened 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 ESX 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.

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 of 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](image-url)

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 Instructions (page 437)**.

---

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
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 505).

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.
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 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 471) and **Intrusion Prevention Events** (page 467). |

**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.
Reference

The Reference section contains further information on the following topics:

- **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* (page 434) modes.
- **Command-Line Instructions**: Information on the *Command-Line Instructions* (page 437) available for the Deep Security manager, Agent, and Relay, including information on Agent-Initiated Activation options.
- **Communication**: A diagram illustrating how the various components of Deep Security and Trend Micro communicate (page 446) with each other.
- **Disabling Diffie-Hellman in Apache**: The Diffie-Hellman (DH) public key cryptography protocol is not supported by the Deep Security Agent and must be disabled (page 451) on an Apache Web server for SSL filtering to work.
- **Encrypting DSM to DB Communication**: How to encrypt *Deep Security Manager to database communications* (page 452).
- **Event Lists**:
  - *Agent/Appliance Events* (page 454) A list of possible Agent/Appliance Events.
  - *Firewall Events* (page 471) A list of possible Firewall Events.
  - *Intrusion Prevention Events* (page 467) A list of possible Intrusion Prevention Events.
  - *System Events* (page 474) A list of possible System Events.
- **Policies, Inheritance and Overrides**: An explanation of how settings can be inherited or overridden (page 505) at various levels of the Policy hierarchy.
- **Integrity Monitoring Rules Language**: A description of the *Integrity Monitoring Rules language* (page 510) so you can write your own custom Integrity Monitoring Rules.
- **Manually deactivating, Starting, or Stopping the Agent or Appliance**: Information on how to *Manually Deactivate/Stop/Start the Agent/Appliance* (page 556).
- **Manually Upgrade the Agent on a Computer**: How to manually upgrade (page 558) the Agent on a computer.
- **More about Event Tagging**: More information (page 447) about the event tagging mechanism.
- **Multi Node Manager**: How to set up multiple *Deep Security Manager nodes* (page 560) to provide load balancing and redundancy.
- **Performance Requirements**: Guidelines (page 563) providing a general idea of the infrastructure requirements for Deep Security deployments of different scales.
- **Ports Used by Deep Security**: Information about the *ports* (page 565) used by Deep Security to communicate with various components of the system.
- **Teamed NICs**: Information on installing an Agent in a *teamed NIC environment* (page 571).
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:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Ignored Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stateful and Normalization Suppression</td>
<td>Out Of Connection</td>
</tr>
<tr>
<td></td>
<td>Invalid Flags</td>
</tr>
<tr>
<td></td>
<td>Invalid Sequence</td>
</tr>
<tr>
<td></td>
<td>Invalid ACK</td>
</tr>
<tr>
<td></td>
<td>Unsolicited UDP</td>
</tr>
<tr>
<td></td>
<td>Unsolicited ICMP</td>
</tr>
<tr>
<td></td>
<td>Out Of Allowed Policy</td>
</tr>
<tr>
<td></td>
<td>Dropped Retransmit</td>
</tr>
<tr>
<td>Stateful, Normalization, and Frag Suppression</td>
<td>Out Of Connection</td>
</tr>
<tr>
<td></td>
<td>Invalid Flags</td>
</tr>
<tr>
<td></td>
<td>Invalid Sequence</td>
</tr>
<tr>
<td></td>
<td>Invalid ACK</td>
</tr>
<tr>
<td></td>
<td>Unsolicited UDP</td>
</tr>
<tr>
<td></td>
<td>Unsolicited ICMP</td>
</tr>
<tr>
<td></td>
<td>Out Of Allowed Policy</td>
</tr>
<tr>
<td></td>
<td>CE Flags</td>
</tr>
<tr>
<td></td>
<td>Invalid IP</td>
</tr>
<tr>
<td></td>
<td>Invalid IP Datagram Length</td>
</tr>
<tr>
<td></td>
<td>Fragmented</td>
</tr>
<tr>
<td></td>
<td>Invalid Fragment Offset</td>
</tr>
<tr>
<td></td>
<td>First Fragment Too Small</td>
</tr>
<tr>
<td></td>
<td>Fragment Out Of Bounds</td>
</tr>
<tr>
<td></td>
<td>Fragment Offset Too Small</td>
</tr>
<tr>
<td></td>
<td>IPv6 Packet</td>
</tr>
<tr>
<td></td>
<td>Max Incoming Connections</td>
</tr>
<tr>
<td></td>
<td>Max Outgoing Connections</td>
</tr>
<tr>
<td></td>
<td>Max SYN Sent</td>
</tr>
<tr>
<td></td>
<td>License Expired</td>
</tr>
<tr>
<td></td>
<td>IP Version Unknown</td>
</tr>
<tr>
<td></td>
<td>Invalid Packet Info</td>
</tr>
<tr>
<td>Mode</td>
<td>Ignored Events</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Maximum ACK Retransmit</td>
</tr>
<tr>
<td></td>
<td>Packet on Closed Connection</td>
</tr>
<tr>
<td></td>
<td>Dropped Retransmit</td>
</tr>
<tr>
<td></td>
<td>Out Of Connection</td>
</tr>
<tr>
<td></td>
<td>Invalid Flags</td>
</tr>
<tr>
<td></td>
<td>Invalid Sequence</td>
</tr>
<tr>
<td></td>
<td>Invalid ACK</td>
</tr>
<tr>
<td></td>
<td>Unsolicited UDP</td>
</tr>
<tr>
<td></td>
<td>Unsolicited ICMP</td>
</tr>
<tr>
<td></td>
<td>Out Of Allowed Policy</td>
</tr>
<tr>
<td></td>
<td>CE Flags</td>
</tr>
<tr>
<td></td>
<td>Invalid IP</td>
</tr>
<tr>
<td></td>
<td>Invalid IP Datagram Length</td>
</tr>
<tr>
<td></td>
<td>Fragmented</td>
</tr>
<tr>
<td></td>
<td>Invalid Fragment Offset</td>
</tr>
<tr>
<td></td>
<td>First Fragment Too Small</td>
</tr>
<tr>
<td></td>
<td>Fragment Out Of Bounds</td>
</tr>
<tr>
<td></td>
<td>Fragment Offset Too Small</td>
</tr>
<tr>
<td></td>
<td>IPv6 Packet</td>
</tr>
<tr>
<td></td>
<td>Max Incoming Connections</td>
</tr>
<tr>
<td></td>
<td>Max Outgoing Connections</td>
</tr>
<tr>
<td></td>
<td>Max SYN Sent</td>
</tr>
<tr>
<td></td>
<td>License Expired</td>
</tr>
<tr>
<td></td>
<td>IP Version Unknown</td>
</tr>
<tr>
<td></td>
<td>Invalid Packet Info</td>
</tr>
<tr>
<td></td>
<td>Invalid Data Offset</td>
</tr>
<tr>
<td></td>
<td>No IP Header</td>
</tr>
<tr>
<td></td>
<td>Unreadable Ethernet Header</td>
</tr>
<tr>
<td></td>
<td>Undefined</td>
</tr>
<tr>
<td></td>
<td>Same Source and Destination IP</td>
</tr>
<tr>
<td></td>
<td>Invalid TCP Header Length</td>
</tr>
<tr>
<td></td>
<td>Unreadable Protocol Header</td>
</tr>
<tr>
<td></td>
<td>Unreadable IPv4 Header</td>
</tr>
<tr>
<td></td>
<td>Unknown IP Version</td>
</tr>
<tr>
<td></td>
<td>Maximum ACK Retransmit</td>
</tr>
<tr>
<td></td>
<td>Packet on Closed Connection</td>
</tr>
<tr>
<td></td>
<td>Dropped Retransmit</td>
</tr>
<tr>
<td>Stateful, Frag, and Verifier Suppression</td>
<td>Out Of Connection</td>
</tr>
<tr>
<td></td>
<td>Invalid Flags</td>
</tr>
<tr>
<td>Tap Mode</td>
<td>Invalid Sequence</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>Ignored Events</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td></td>
<td>Invalid ACK</td>
</tr>
<tr>
<td></td>
<td>Maximum ACK Retransmit</td>
</tr>
<tr>
<td></td>
<td>Packet on Closed Connection</td>
</tr>
<tr>
<td></td>
<td>Dropped Retransmit</td>
</tr>
</tbody>
</table>
Command-Line Instructions

Deep Security Agent (also applies to the Agent on a Deep Security Relay)

dsa_control

Usage

[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/
- /H <num>, --harden=<num> Harden Agent. (1: enable, 0: disable)
- /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.
- /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. This is intended for use in cases where an Agent is installed

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.
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]:[port]/` 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:

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dsa_control /x &quot;dsm_proxy://&lt;proxyURL&gt;/&quot;</code></td>
<td>Sets the address of the proxy server which the Agent uses to communicate with the DSM.</td>
</tr>
<tr>
<td><code>dsa_control /x &quot;&quot;</code></td>
<td>Clears the proxy server address.</td>
</tr>
<tr>
<td><code>dsa_control /u &quot;&lt;username:password&gt;&quot;</code></td>
<td>Sets the proxy username and password.</td>
</tr>
<tr>
<td><code>dsa_control /u &quot;&quot;</code></td>
<td>Clears the proxy username and password.</td>
</tr>
</tbody>
</table>

**Examples**

```
dsa_control.exe /x "dsm_proxy://172.21.3.184:808/"
```

Proxy uses IPv4.
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/"

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.
<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Examples</th>
<th>Can be performed during Activation</th>
<th>Can be performed after activation during Heartbeat</th>
<th>Value Format</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Sets description value.</td>
<td>&quot;description:Extra information about the host&quot;</td>
<td>yes</td>
<td>yes</td>
<td>string</td>
<td>Maximum length 2000 characters.</td>
</tr>
<tr>
<td>displayname</td>
<td>Sets displayname value. (Shown in parentheses next to the hostname.)</td>
<td>&quot;displayname:the_name&quot;</td>
<td>yes</td>
<td>yes</td>
<td>string</td>
<td>Maximum length 2000 characters.</td>
</tr>
<tr>
<td>externalid</td>
<td>&quot;externalid:15&quot;</td>
<td>yes</td>
<td>yes</td>
<td>integer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 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 Deep Security 9 SP1 Administrator’s Guide Command-Line Instructions 440
<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Examples</th>
<th>Can be performed during Activation</th>
<th>Can be performed after activation during Heartbeat</th>
<th>Value Format</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupid</td>
<td></td>
<td>&quot;groupid:33&quot;</td>
<td>yes</td>
<td>yes</td>
<td>integer</td>
<td>Cloud Provider accounts.</td>
</tr>
<tr>
<td>hostname</td>
<td></td>
<td>&quot;hostname:ABWebServer1&quot;</td>
<td>yes</td>
<td>no</td>
<td>string</td>
<td>Maximum length 254 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>policy</td>
<td></td>
<td>&quot;policy:Policy Name&quot;</td>
<td>yes</td>
<td>yes</td>
<td>string</td>
<td>Maximum length 254 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The Policy name is a case-insensitive match to the Policy list. If the Policy is not found, no Policy will be assigned. The Policy will be assigned.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A policy assigned by an Event-based Task will override a Policy assigned during Agent-Initiated Activation.</td>
</tr>
<tr>
<td>policyid</td>
<td></td>
<td>&quot;policyid:12&quot;</td>
<td>yes</td>
<td>yes</td>
<td>integer</td>
<td>Maximum length 254 characters.</td>
</tr>
<tr>
<td>relaygroup</td>
<td></td>
<td>&quot;relaygroup:Custom Relay Group&quot;</td>
<td>yes</td>
<td>yes</td>
<td>string</td>
<td>Maximum length 254 characters.</td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Examples</td>
<td>Can be performed during Activation</td>
<td>Can be performed after activation during Heartbeat</td>
<td>Value Format</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>------------------------------------</td>
<td>---------------------------------------------------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>relaygroupid</td>
<td>a specific Relay Group.</td>
<td></td>
<td>yes</td>
<td>yes</td>
<td>integer</td>
<td>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.</td>
</tr>
<tr>
<td>relayid</td>
<td></td>
<td></td>
<td>yes</td>
<td>yes</td>
<td>integer</td>
<td>This does not affect Relay Groups assigned during Event-based tasks. Use either this option or Event-based tasks, not both.</td>
</tr>
<tr>
<td>tenantID and tenantPassword</td>
<td></td>
<td></td>
<td>yes</td>
<td>yes</td>
<td>string</td>
<td>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.</td>
</tr>
<tr>
<td>RecommendationScan</td>
<td></td>
<td></td>
<td>no</td>
<td>yes</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>UpdateComponent</td>
<td>Instructs the Deep Security Manager to perform a</td>
<td></td>
<td>no</td>
<td>yes</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Examples</td>
<td>Can be performed during Activation</td>
<td>Can be performed after activation during Heartbeat</td>
<td>Value Format</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>-------------------------------------</td>
<td>--------------------------------------------------</td>
<td>------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Security Update operation.</td>
<td></td>
<td></td>
<td>no</td>
<td>yes</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>UpdateConfiguration</td>
<td>Instructs the Deep Security Manager to perform a &quot;Send Policy&quot; operation.</td>
<td>&quot;UpdateConfiguration:true&quot;</td>
<td>no</td>
<td>yes</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>AntiMalwareManualScan</td>
<td></td>
<td>&quot;AntiMalwareManualScan:true&quot;</td>
<td>no</td>
<td>yes</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>AntiMalwareCancelManualScan</td>
<td></td>
<td>&quot;AntiMalwareCancelManualScan:true&quot;</td>
<td>no</td>
<td>yes</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>IntegrityScan</td>
<td></td>
<td>&quot;IntegrityScan:true&quot;</td>
<td>no</td>
<td>yes</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>RebuildBaseline</td>
<td></td>
<td>&quot;RebuildBaseline:true&quot;</td>
<td>no</td>
<td>yes</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

**dsa_config**

**Usage**


- /h, --help: shows help message
- --verbose: generate verbose log messages
- /a, --agent=<str>: agent name (default is "ds_agent")
- /c, --cert=<str>: certificate file
- /x, --hex-width=<num>: number of characters per line in hex displays (4 to 32, default value is 8)
- /e, --enable: enable the agent
- /f, --fw:
- /p, --password=<str>: password for authentication

**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 hardening 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: wildcard 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

<table>
<thead>
<tr>
<th>Action Name</th>
<th>Description</th>
<th>Usage with Parameters (if any)</th>
</tr>
</thead>
<tbody>
<tr>
<td>changesetting</td>
<td>Change a setting</td>
<td>dsm_c -action changesetting -name NAME -value VALUE [-computerid COMPUTERID] [-computename COMPUTERNAME] [-policyid POLICYID] [-policyname POLICYNAME] [-tenantname TENANTNAME]</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Command Line</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>viewsetting</td>
<td>View a setting value</td>
<td><code>dsm_c -action viewsetting -name NAME [-computerid COMPUTERID] [-computername COMPUTERNAME] [-policyid POLICYID] [-policyname POLICYNAME] [-tenantname TENANTNAME]</code></td>
</tr>
<tr>
<td>createinsertstatements</td>
<td>Create insert statements (for export to a different database)</td>
<td>`dsm_c -action createinsertstatements [-file FILEPATH] [-generateDDL] [-databaseType sqlserver</td>
</tr>
<tr>
<td>diagnostic</td>
<td>Create a diagnostic package for the system</td>
<td><code>dsm_c -action diagnostic</code></td>
</tr>
<tr>
<td>fullaccess</td>
<td>Give an administrator the full access role</td>
<td><code>dsm_c -action fullaccess -username USERNAME [-tenantname TENANTNAME]</code></td>
</tr>
<tr>
<td>reindexhelp</td>
<td>Reindex help system</td>
<td><code>dsm_c -action reindexhelp</code></td>
</tr>
<tr>
<td>resetcounters</td>
<td>Reset counter tables (resets back to an empty state)</td>
<td><code>dsm_c -action resetcounters [-tenantname TENANTNAME]</code></td>
</tr>
<tr>
<td>resetevents</td>
<td>Reset the events tables (resets back to an empty state)</td>
<td>`dsm_c -action resetevents -type all</td>
</tr>
<tr>
<td>setports</td>
<td>Set Deep Security Manager port(s)</td>
<td><code>dsm_c -action setports [-managerPort port] [-heartbeatPort port]</code></td>
</tr>
<tr>
<td>trustdirectorycert</td>
<td>Trust the certificate of a directory</td>
<td><code>dsm_c -action trustdirectorycert -directoryaddress DIRECTORYADDRESS -directoryport DIRECTORYPORT [-username USERNAME] [-password PASSWORD] [-tenantname TENANTNAME]</code></td>
</tr>
<tr>
<td>unlockout</td>
<td>Unlock a User account</td>
<td><code>dsm_c -action unlockout -username USERNAME [-newpassword NEWPASSWORD] [-tenantname TENANTNAME]</code></td>
</tr>
</tbody>
</table>
More About Event Tagging

In Deep Security, a **Tag** is a unit of meta-data that you can apply to a Deep Security 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 sort, group, and otherwise organize Events in order to simplify the task of Event monitoring and management. A typical use of tagging is to distinguish between Events that have been investigated and found to be benign and those that require action.

Events can be manually tagged on an ad hoc basis, or they can be automatically tagged using one of two available auto-tagging systems:

- **Standard 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 Auto-Tagging** lets you auto-tag Events based on their similarity to known-good Events that occur on one or more trusted computers or to a whitelist of known-good software maintained by Trend Micro (the Certified Safe Software Service).

**Note:** An important difference between standard tagging and Trusted Source-based tagging is that "Run on Existing Events Now" can only be done in standard event-tagging model.

Although Event tagging can be used for a variety of purposes, it was designed to ease the burden of Event-management. Once an Event has been analyzed and assessed as benign, it is convenient to look through the Event logs of the computer (and any other similarly configured and tasked computers) to find similar Events and label them all as such, thereby eliminating the need to analyze each Event individually.

**Standard Event Tagging**

**Event Tagging** lets you apply one or more tags to an Event. You can tag Events with predefined tags ("attack", "suspicious", "patch", "acceptable change", "false positive", "high priority", etc.) or you can define and apply custom tags.

For example, you could create and apply a tag to a Intrusion Prevention Event indicating that you have assessed the Event as a false positive.

**Auto-Tagging**

Once you have tagged a single Event, **Auto-Tagging** lets you instruct Deep Security Manager to apply the same tag to all similar existing and/or future Events on the current or any other computers (where you define the properties and criteria for determining similarity). (When you use Auto-Tagging, you create an Auto-
tagging Rule. To view existing Auto-Tagging Rules, click Auto-Tagging... in the menu bar on any Events page. You can run any Auto-Tagging Rule again manually at a later date.)

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.

---

**Note:** You can set the Precedence value of an Auto-Tagging Rule by going to an Events page, clicking Auto-Tagging... in the toolbar to display the existing Auto-Tagging Rules associated with the Events, and editing the Properties window of the Auto-Tagging Rule.

---

Tags can be used as sorting criteria just like any other Event properties. You can use them to create customized dashboards and reports. You can use Tags to control analysis workflow by hiding already analyzed Events or identifying Events that require further analysis.

---

**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.

---

All the tagging and auto-tagging mentioned thus far applies to all Deep Security Events: Anti-Malware, Firewall, Intrusion Prevention, Integrity Monitoring, Log Inspection, and System Events. The following section describes how the Integrity Monitoring module lets you tag Events based on a Trusted Source.

**Trusted-Source-Based Event Tagging**

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 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.

**Trusted Computer**

A Trusted Computer is a computer which will be used as a "model" computer.

A Trusted Computer is a computer on which are running a set of integrity Monitoring Rules which generate Integrity Monitoring Events just as they do on any other computer. In Trusted-Source-Based Event Tagging, an auto-Tagging rules examines Events on target computers (computers that you are protecting) 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.

A Trusted Computer is a computer on which are running a set of Integrity Monitoring Rules. The Integrity Monitoring module works by creating a baseline of known good events.

The Trusted Computer is a computer which you know will only generate benign or harmless Events. A "target" computer is a computer that you are monitoring for unauthorized or unexpected changes.

You can establish auto-tagging rules which 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 if 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.

It's important to keep this in mind when scheduling scans of source and target computers.

(This also applies to creation and deletion events.)

---

**Note:** Remember that when using a Trusted Computer for Trusted-Source-Based 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 which regularly make modifications to the content of files on a system (prelinking on Linux, for example) can interfere with Trusted-Computer-based Auto-Tagging.

---

**Trend Micro 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.

**Trusted Common Baseline**

The Trusted Common Baseline method compares Events within a group of computers. A common baseline is generated from all the computers within a group of computers. When an Integrity Monitoring event occurs on a computer within that 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.

---

**Note:** Whereas in the Trusted Computer method the before and after states of an Integrity Monitoring Event are compared, in the Trusted Common Baseline method, only the after state is compared.
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

| 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](http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite).
Encrypting DSM 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](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.
Agent/Appliance Events

**Note:** Agent/Appliance Events are displayed within a System Event in the **System Events** page. For example, double-clicking the "Events Retrieved" System Event will display a window listing all the Agent/Appliance Events that were retrieved.

**Note:** Events annotated as "Deprecated" are no longer generated by the most recent Agents/Appliances but may still appear if you are running older versions.

<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Event</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Error</td>
<td>Unknown Agent/Appliance Event</td>
<td></td>
</tr>
<tr>
<td>1000</td>
<td>Error</td>
<td>Unable To Open Engine</td>
<td></td>
</tr>
<tr>
<td>1001</td>
<td>Error</td>
<td>Engine Command Failed</td>
<td></td>
</tr>
<tr>
<td>1002</td>
<td>Warning</td>
<td>Engine List Objects Error</td>
<td></td>
</tr>
<tr>
<td>1003</td>
<td>Warning</td>
<td>Remove Object Failed</td>
<td></td>
</tr>
<tr>
<td>1004</td>
<td>Warning</td>
<td>Engine Returned Bad Rule Data</td>
<td>Deprecated.</td>
</tr>
<tr>
<td>1005</td>
<td>Warning</td>
<td>Upgrading Driver</td>
<td></td>
</tr>
<tr>
<td>1006</td>
<td>Warning</td>
<td>Driver Upgrade Requires Reboot</td>
<td></td>
</tr>
<tr>
<td>1007</td>
<td>Warning</td>
<td>Driver Upgrade Succeeded</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration-Related Events**

<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Event</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>Info</td>
<td>Policy Sent</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>2001</td>
<td>Warning</td>
<td>Invalid Firewall Rule Assignment</td>
<td></td>
</tr>
<tr>
<td>2002</td>
<td>Warning</td>
<td>Invalid Firewall Stateful Configuration</td>
<td></td>
</tr>
<tr>
<td>2003</td>
<td>Error</td>
<td>Save Security Configuration Failed</td>
<td></td>
</tr>
<tr>
<td>2004</td>
<td>Warning</td>
<td>Invalid Interface Assignment</td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td>Warning</td>
<td>Invalid Interface Assignment</td>
<td></td>
</tr>
<tr>
<td>2006</td>
<td>Warning</td>
<td>Invalid Action</td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td>Warning</td>
<td>Invalid Packet Direction</td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>Warning</td>
<td>Invalid Rule Priority</td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td>Warning</td>
<td>Unrecognized IP Format</td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td>Warning</td>
<td>Invalid Source IP List</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>Warning</td>
<td>Invalid Source Port List</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Warning</td>
<td>Invalid Destination IP List</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>Warning</td>
<td>Invalid Destination Port List</td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>Warning</td>
<td>Invalid Schedule</td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>Warning</td>
<td>Invalid Source MAC List</td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>Warning</td>
<td>Invalid Destination MAC List</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>2017</td>
<td>Warning</td>
<td>Invalid Schedule Length</td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td>Warning</td>
<td>Invalid Schedule String</td>
<td></td>
</tr>
<tr>
<td>2019</td>
<td>Warning</td>
<td>Invalid Intrusion Prevention Rule</td>
<td>XML Rule</td>
</tr>
<tr>
<td>2020</td>
<td>Warning</td>
<td>Object Not Found</td>
<td></td>
</tr>
<tr>
<td>2021</td>
<td>Warning</td>
<td>Object Not Found</td>
<td></td>
</tr>
<tr>
<td>2022</td>
<td>Warning</td>
<td>Invalid Rule Assignment</td>
<td></td>
</tr>
<tr>
<td>2050</td>
<td>Warning</td>
<td>Firewall Rule Not Found</td>
<td></td>
</tr>
<tr>
<td>2075</td>
<td>Warning</td>
<td>Traffic Stream Not Found</td>
<td></td>
</tr>
<tr>
<td>2076</td>
<td>Warning</td>
<td>Intrusion Prevention Rule Not Found</td>
<td></td>
</tr>
<tr>
<td>2077</td>
<td>Warning</td>
<td>Pattern List Not Found</td>
<td></td>
</tr>
<tr>
<td>2078</td>
<td>Warning</td>
<td>Intrusion Prevention Rule Conversion Error</td>
<td></td>
</tr>
<tr>
<td>2080</td>
<td>Warning</td>
<td>Conditional Firewall Rule Not Found</td>
<td></td>
</tr>
<tr>
<td>2081</td>
<td>Warning</td>
<td>Conditional Intrusion Prevention Rule Not Found</td>
<td></td>
</tr>
<tr>
<td>2082</td>
<td>Warning</td>
<td>Empty Intrusion Prevention Rule</td>
<td></td>
</tr>
<tr>
<td>2083</td>
<td>Warning</td>
<td>Intrusion Prevention Rule</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Notes</td>
</tr>
<tr>
<td>----</td>
<td>----------</td>
<td>---------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>2085</td>
<td>Error</td>
<td>XML Rule Conversion Error</td>
<td></td>
</tr>
<tr>
<td>2086</td>
<td>Warning</td>
<td>Security Configuration Error</td>
<td></td>
</tr>
<tr>
<td>2087</td>
<td>Warning</td>
<td>Unsupported IP Match Type</td>
<td></td>
</tr>
<tr>
<td>2088</td>
<td>Warning</td>
<td>Unsupported MAC Match Type</td>
<td></td>
</tr>
<tr>
<td>2089</td>
<td>Warning</td>
<td>Invalid SSL Credential</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Missing SSL Credential</td>
<td></td>
</tr>
</tbody>
</table>

**Hardware-Related Events**

<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Event</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>3000</td>
<td>Warning</td>
<td>Invalid MAC Address</td>
<td></td>
</tr>
<tr>
<td>3001</td>
<td>Warning</td>
<td>Get Event Data Failed</td>
<td></td>
</tr>
<tr>
<td>3002</td>
<td>Warning</td>
<td>Too Many Interfaces</td>
<td></td>
</tr>
<tr>
<td>3003</td>
<td>Error</td>
<td>Unable To Run External Command</td>
<td></td>
</tr>
<tr>
<td>3004</td>
<td>Error</td>
<td>Unable To Read External Command Output</td>
<td></td>
</tr>
<tr>
<td>3005</td>
<td>Error</td>
<td>Operating System Call Error</td>
<td></td>
</tr>
<tr>
<td>3006</td>
<td>Error</td>
<td>Operating System Call Error</td>
<td></td>
</tr>
<tr>
<td>3007</td>
<td>Error</td>
<td>File Error</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>3008</td>
<td>Error</td>
<td>Machine-Specific Key Error</td>
<td></td>
</tr>
<tr>
<td>3009</td>
<td>Error</td>
<td>Unexpected Agent/Appliance Shutdown</td>
<td></td>
</tr>
<tr>
<td>3010</td>
<td>Error</td>
<td>Agent/Appliance Database Error</td>
<td></td>
</tr>
<tr>
<td>3300</td>
<td>Warning</td>
<td>Get Event Data Failed</td>
<td>Linux error.</td>
</tr>
<tr>
<td>3302</td>
<td>Warning</td>
<td>Get Security Configuration Failed</td>
<td>Linux error.</td>
</tr>
<tr>
<td>3303</td>
<td>Error</td>
<td>File Mapping Error</td>
<td>Linux error. File type error.</td>
</tr>
<tr>
<td>3600</td>
<td>Error</td>
<td>Get Windows System Directory Failed</td>
<td></td>
</tr>
<tr>
<td>3601</td>
<td>Warning</td>
<td>Read Local Data Error</td>
<td>Windows error.</td>
</tr>
<tr>
<td>3602</td>
<td>Warning</td>
<td>Windows Service Error</td>
<td>Windows error.</td>
</tr>
<tr>
<td>3700</td>
<td>Warning</td>
<td>Abnormal Restart Detected</td>
<td>Windows error.</td>
</tr>
<tr>
<td>3701</td>
<td>Info</td>
<td>System Last Boot Time Change</td>
<td>Windows error.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Communication-Related Events</strong></td>
<td></td>
</tr>
<tr>
<td>4000</td>
<td>Warning</td>
<td>Invalid Protocol Header</td>
<td>Content length out of range.</td>
</tr>
<tr>
<td>4001</td>
<td>Warning</td>
<td>Invalid Protocol Header</td>
<td>Content length missing.</td>
</tr>
<tr>
<td>4002</td>
<td>Info</td>
<td>Command Session Initiated</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>4003</td>
<td>Info</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Session Initiated</td>
<td></td>
</tr>
<tr>
<td>4004</td>
<td>Info</td>
<td>Command</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Received</td>
<td></td>
</tr>
<tr>
<td>4011</td>
<td>Warning</td>
<td>Failure to Contact Manager</td>
<td></td>
</tr>
<tr>
<td>4012</td>
<td>Warning</td>
<td>Heartbeat Failed</td>
<td></td>
</tr>
</tbody>
</table>

**Agent-Related Events**

<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Event</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5000</td>
<td>Info</td>
<td>Agent/Appliance Started</td>
<td></td>
</tr>
<tr>
<td>5001</td>
<td>Error</td>
<td>Thread Exception</td>
<td></td>
</tr>
<tr>
<td>5002</td>
<td>Error</td>
<td>Operation Timed Out</td>
<td></td>
</tr>
<tr>
<td>5003</td>
<td>Info</td>
<td>Agent/Appliance Stopped</td>
<td></td>
</tr>
<tr>
<td>5004</td>
<td>Warning</td>
<td>Clock Changed</td>
<td></td>
</tr>
<tr>
<td>5005</td>
<td>Info</td>
<td>Agent/Appliance Auditing Started</td>
<td></td>
</tr>
<tr>
<td>5006</td>
<td>Info</td>
<td>Agent/Appliance Auditing Stopped</td>
<td></td>
</tr>
<tr>
<td>5007</td>
<td>Info</td>
<td>Appliance Protection Change</td>
<td></td>
</tr>
<tr>
<td>5008</td>
<td>Warning</td>
<td>Filter Driver Connection Failed</td>
<td></td>
</tr>
<tr>
<td>5009</td>
<td>Info</td>
<td>Filter Driver Connection Success</td>
<td></td>
</tr>
<tr>
<td>5010</td>
<td>Warning</td>
<td>Filter Driver Informational Event</td>
<td></td>
</tr>
</tbody>
</table>

**Logging-Related Events**
<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Event</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>6000</td>
<td>Info</td>
<td>Log Device Open Error</td>
<td></td>
</tr>
<tr>
<td>6001</td>
<td>Info</td>
<td>Log File Open Error</td>
<td></td>
</tr>
<tr>
<td>6002</td>
<td>Info</td>
<td>Log File Write Error</td>
<td></td>
</tr>
<tr>
<td>6003</td>
<td>Info</td>
<td>Log Directory Creation Error</td>
<td></td>
</tr>
<tr>
<td>6004</td>
<td>Info</td>
<td>Log File Query Error</td>
<td></td>
</tr>
<tr>
<td>6005</td>
<td>Info</td>
<td>Log Directory Open Error</td>
<td></td>
</tr>
<tr>
<td>6006</td>
<td>Info</td>
<td>Log File Delete Error</td>
<td></td>
</tr>
<tr>
<td>6007</td>
<td>Info</td>
<td>Log File Rename Error</td>
<td></td>
</tr>
<tr>
<td>6008</td>
<td>Info</td>
<td>Log Read Error</td>
<td></td>
</tr>
<tr>
<td>6009</td>
<td>Warning</td>
<td>Log File Deleted Due To Insufficient Space</td>
<td></td>
</tr>
<tr>
<td>6010</td>
<td>Warning</td>
<td>Events Were Suppressed</td>
<td></td>
</tr>
<tr>
<td>6011</td>
<td>Warning</td>
<td>Events Truncated</td>
<td></td>
</tr>
<tr>
<td>6012</td>
<td>Error</td>
<td>Insufficient Disk Space</td>
<td></td>
</tr>
<tr>
<td>6013</td>
<td>Warning</td>
<td>Agent Configuration Package Too Large</td>
<td></td>
</tr>
</tbody>
</table>

**Attack/Scan/Probe-Related Events**

<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Event</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>7000</td>
<td>Warning</td>
<td>Computer OS Fingerprint Probe</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>7001</td>
<td>Warning</td>
<td>Network or Port Scan</td>
<td></td>
</tr>
<tr>
<td>7002</td>
<td>Warning</td>
<td>TCP Null Scan</td>
<td></td>
</tr>
<tr>
<td>7003</td>
<td>Warning</td>
<td>TCP SYNFIN Scan</td>
<td></td>
</tr>
<tr>
<td>7004</td>
<td>Warning</td>
<td>TCP Xmas Scan</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Integrity Monitoring Events</strong></td>
<td></td>
</tr>
<tr>
<td>8000</td>
<td>Info</td>
<td>Full Baseline Created</td>
<td>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.</td>
</tr>
<tr>
<td>8001</td>
<td>Info</td>
<td>Partial Baseline Created</td>
<td>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.</td>
</tr>
<tr>
<td>8002</td>
<td>Info</td>
<td>Scan for Changes Completed</td>
<td>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.)</td>
</tr>
<tr>
<td>8003</td>
<td>Error</td>
<td>Unknown Environment Variable in Integrity Monitoring Rule</td>
<td>Created when a rule uses a ${env.EnvironmentVar} and &quot;EnvironmentVar&quot; 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.</td>
</tr>
<tr>
<td>8004</td>
<td>Error</td>
<td>Bad Base in Integrity Monitoring Rule</td>
<td>Created when a rule contains an invalid base directory/key. For example, specifying a FileSet with a base of &quot;c:\foo\d:\bar&quot; 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.</td>
</tr>
<tr>
<td>8005</td>
<td>Error</td>
<td>Unknown Entity in Integrity Monitoring Rule</td>
<td>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.</td>
</tr>
<tr>
<td>8006</td>
<td>Error</td>
<td>Unsupported Entity in Integrity Monitoring Rule</td>
<td>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.</td>
</tr>
<tr>
<td>8007</td>
<td>Error</td>
<td>Unknown Feature in Integrity Monitoring Rule</td>
<td>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 &quot;whereBaseInOtherSet&quot;, &quot;status&quot;, and &quot;executable&quot;.</td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Notes</td>
</tr>
<tr>
<td>--------</td>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>8008</td>
<td>Error</td>
<td>Unsupported Feature in Integrity Monitoring Rule</td>
<td>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 &quot;status&quot; (used for Windows service states) are platform-specific.</td>
</tr>
<tr>
<td>8009</td>
<td>Error</td>
<td>Unknown Attribute in Integrity Monitoring Rule</td>
<td>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 unsupported Attribute names encountered. Examples of valid Attribute values are &quot;created&quot;, &quot;lastModified&quot; and &quot;inodeNumber&quot;.</td>
</tr>
<tr>
<td>8010</td>
<td>Error</td>
<td>Unsupported Attribute in Integrity Monitoring Rule</td>
<td>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 &quot;inodeNumber&quot; are platform-specific.</td>
</tr>
<tr>
<td>8011</td>
<td>Error</td>
<td>Unknown EntitySet XML attribute in Integrity Monitoring Rule</td>
<td>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 <code>&lt;FileSet dir=&quot;c:\foo&quot;&gt;</code> instead of <code>&lt;FileSet base=&quot;c:\foo&quot;&gt;</code></td>
</tr>
<tr>
<td>8012</td>
<td>Error</td>
<td>Unknown Registry String in Integrity Monitoring Rule</td>
<td>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.</td>
</tr>
<tr>
<td>8013</td>
<td>Error</td>
<td>Invalid WQLSet was used. Namespace or WQL query was missing.</td>
<td>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.</td>
</tr>
<tr>
<td>8014</td>
<td>Error</td>
<td>Invalid WQLSet was used. An unknown provider value was used.</td>
<td>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.</td>
</tr>
<tr>
<td>8015</td>
<td>Warning</td>
<td>Inapplicable Integrity Monitoring Rule</td>
<td>Can be caused by a number of reasons, such as platform mismatch, nonexistent target directories or files, or unsupported functionality.</td>
</tr>
<tr>
<td>8050</td>
<td>Error</td>
<td>Regular expression could not be compiled.</td>
<td>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.</td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>8100</td>
<td>Error</td>
<td>Log Inspection Engine Error</td>
<td></td>
</tr>
<tr>
<td>8101</td>
<td>Warning</td>
<td>Log Inspection Engine Warning</td>
<td></td>
</tr>
<tr>
<td>8102</td>
<td>Info</td>
<td>Log Inspection Engine Initialized</td>
<td></td>
</tr>
</tbody>
</table>

**Log Inspection Events**

| 9001 | Info     | Malware Scan Started          |                                |
| 9002 | Info     | Malware Scan Completed        |                                |
| 9003 | Info     | Malware Scan Terminated       | Abnormally                     |
| 9004 | Info     | Malware Scan Paused           |                                |
| 9005 | Info     | Malware Scan Resumed          |                                |
| 9006 | Info     | Malware Scan Cancelled        |                                |
| 9007 | Warning  | Malware Scan Cancel Failed    |                                |
| 9008 | Warning  | Malware Scan Start Failed     |                                |
| 9009 | Warning  | Malware Scan Stalled          |                                |
| 9010 | Error    | Malware Quarantine Failed (VM limit exceeded) | |
| 9011 | Error    | Malware Quarantine            |                                |

**Anti-Malware Events**
<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Event</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>9012</td>
<td>Warning</td>
<td>Failed</td>
<td>(Appliance limit exceeded)</td>
</tr>
<tr>
<td>9013</td>
<td>Info</td>
<td>Smart Protection Server Disconnected</td>
<td>for Smart Scan</td>
</tr>
<tr>
<td>9014</td>
<td>Warning</td>
<td>Computer reboot is required for Anti-Malware protection</td>
<td></td>
</tr>
</tbody>
</table>

**Download Security Update Events**

<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Event</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>9050</td>
<td>Info</td>
<td>Installation/ Upgrade of Anti-Malware Component on Agent Succeeded</td>
<td></td>
</tr>
<tr>
<td>9051</td>
<td>Error</td>
<td>Installation/ Upgrade of Anti-Malware Component on Agent Failed</td>
<td></td>
</tr>
<tr>
<td>9100</td>
<td>Info</td>
<td>Security Update Successful</td>
<td></td>
</tr>
<tr>
<td>9101</td>
<td>Error</td>
<td>Security Update Failure</td>
<td></td>
</tr>
<tr>
<td>9102</td>
<td>Error</td>
<td>Security Update Failure</td>
<td>Specific information recorded in error message.</td>
</tr>
</tbody>
</table>

**Relay Events**

<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Event</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>9103</td>
<td>Info</td>
<td>Relay Web Server Disabled</td>
<td></td>
</tr>
</tbody>
</table>

Deep Security 9 SP1 Administrator's Guide

Agent/Appliance Events
<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Event</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>9104</td>
<td>Info</td>
<td>Relay Web Server Enabled</td>
<td></td>
</tr>
<tr>
<td>9105</td>
<td>Error</td>
<td>Enable Relay Web Server Failed</td>
<td></td>
</tr>
<tr>
<td>9106</td>
<td>Error</td>
<td>Disable Relay Web Server Failed</td>
<td></td>
</tr>
<tr>
<td>9107</td>
<td>Error</td>
<td>Relay Web Server Failed</td>
<td></td>
</tr>
<tr>
<td>9108</td>
<td>Info</td>
<td>Unable to Connect to Update Source</td>
<td></td>
</tr>
<tr>
<td>9109</td>
<td>Error</td>
<td>Component Update Failure</td>
<td></td>
</tr>
<tr>
<td>9110</td>
<td>Error</td>
<td>Anti-Malware License is Expired</td>
<td></td>
</tr>
<tr>
<td>9111</td>
<td>Info</td>
<td>Security Update Rollback Success</td>
<td></td>
</tr>
<tr>
<td>9112</td>
<td>Error</td>
<td>Security Update Rollback Failure</td>
<td></td>
</tr>
</tbody>
</table>

### Integrity Scan Status Events

<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Event</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>9201</td>
<td>Info</td>
<td>Integrity Scan Started</td>
<td></td>
</tr>
<tr>
<td>9203</td>
<td>Info</td>
<td>Integrity Scan Terminated Abnormally</td>
<td></td>
</tr>
<tr>
<td>9204</td>
<td>Info</td>
<td>Integrity Scan Paused</td>
<td></td>
</tr>
<tr>
<td>9205</td>
<td>Info</td>
<td>Integrity Scan Resumed</td>
<td></td>
</tr>
<tr>
<td>9208</td>
<td>Warning</td>
<td>Integrity Scan Start Failed to Start</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Notes</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>9209</td>
<td>Warning</td>
<td>Integrity Scan</td>
<td>Stalled</td>
</tr>
</tbody>
</table>

### Smart Protection Server Status Events

<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Event</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>9300</td>
<td>Warning</td>
<td>Smart Protection Server</td>
<td>Disconnected for Web Reputation</td>
</tr>
<tr>
<td>9301</td>
<td>Info</td>
<td>Smart Protection Server</td>
<td>Connected for Web Reputation</td>
</tr>
</tbody>
</table>
## Intrusion Prevention Events

<table>
<thead>
<tr>
<th>ID</th>
<th>Event</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Normal (Filter)</td>
<td></td>
</tr>
<tr>
<td>200</td>
<td>Region Too Big (Filter)</td>
<td>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.</td>
</tr>
<tr>
<td>201</td>
<td>Memory Allocation Failure</td>
<td>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.</td>
</tr>
<tr>
<td>202</td>
<td>Maximum Edits Exceeded</td>
<td>The maximum number of edits (32) in a single region of a packet was exceeded.</td>
</tr>
<tr>
<td>203</td>
<td>Edit Too Large</td>
<td>Editing attempted to increase the size of the region above the maximum allowed size (8188 bytes).</td>
</tr>
<tr>
<td>204</td>
<td>Max Matches in Packet Exceeded</td>
<td>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.</td>
</tr>
<tr>
<td>205</td>
<td>Engine Call Stack Too Deep</td>
<td></td>
</tr>
<tr>
<td>206</td>
<td>Runtime Error</td>
<td>Runtime error.</td>
</tr>
<tr>
<td>207</td>
<td>Packet Read Error</td>
<td>Low level problem reading packet data.</td>
</tr>
<tr>
<td>300</td>
<td>Unsupported Cipher Error</td>
<td>An unknown or unsupported Cipher Suite has been requested.</td>
</tr>
<tr>
<td>301</td>
<td>Error Generating Master Key(s)</td>
<td>Unable to derive the cryptographic keys, Mac secrets, and initialization vectors from the master secret.</td>
</tr>
<tr>
<td>302</td>
<td>Record Layer Message (not ready)</td>
<td>The SSL state engine has encountered an SSL record before initialization of the session.</td>
</tr>
<tr>
<td>303</td>
<td>Handshake Message (not ready)</td>
<td>The SSL state engine has encountered a handshake message after the handshake has been negotiated.</td>
</tr>
<tr>
<td>ID</td>
<td>Event</td>
<td>Notes</td>
</tr>
<tr>
<td>----</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>304</td>
<td>Out Of Order Handshake Message</td>
<td>A well formatted handshake message has been encountered out of sequence.</td>
</tr>
<tr>
<td>305</td>
<td>Memory Allocation Error</td>
<td>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.</td>
</tr>
<tr>
<td>306</td>
<td>Unsupported SSL Version</td>
<td>A client attempted to negotiate an SSL V2 session.</td>
</tr>
<tr>
<td>307</td>
<td>Error Decrypting Pre-master Key</td>
<td>Unable to un-wrap the pre-master secret from the ClientKeyExchange message.</td>
</tr>
<tr>
<td>308</td>
<td>Client Attempted to Rollback</td>
<td>A client attempted to rollback to an earlier version of the SSL protocol than that which was specified in the ClientHello message.</td>
</tr>
<tr>
<td>309</td>
<td>Renewal Error</td>
<td>An SSL session was being requested with a cached session key that could not be located.</td>
</tr>
<tr>
<td>310</td>
<td>Key Exchange Error</td>
<td>The server is attempting to establish an SSL session with temporarily generated key.</td>
</tr>
<tr>
<td>311</td>
<td>Error Generating Pre-Master Request</td>
<td>An error occurred when trying to queue the pre-master secret for decryption.</td>
</tr>
<tr>
<td>312</td>
<td>Key Too Large</td>
<td>The master secret keys are larger than specified by the protocol identifier.</td>
</tr>
<tr>
<td>313</td>
<td>Invalid Parameters In Handshake</td>
<td>An invalid or unreasonable value was encountered while trying to decode the handshake protocol.</td>
</tr>
<tr>
<td>314</td>
<td>No Sessions Available</td>
<td></td>
</tr>
<tr>
<td>315</td>
<td>Compression Method Unsupported</td>
<td></td>
</tr>
<tr>
<td>500</td>
<td>URI Path Depth Exceeded</td>
<td>too many &quot;/&quot; separators, max 100 path depth.</td>
</tr>
<tr>
<td>501</td>
<td>Invalid Traversal</td>
<td>Tried to use &quot;.../.&quot; above root.</td>
</tr>
<tr>
<td>ID</td>
<td>Event</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>--------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>502</td>
<td>Illegal Character in URI</td>
<td>Illegal character used in uri.</td>
</tr>
<tr>
<td>503</td>
<td>Incomplete UTF8 Sequence</td>
<td>URI ended in middle of utf8 sequence.</td>
</tr>
<tr>
<td>504</td>
<td>Invalid UTF8 encoding</td>
<td>Invalid/non-canonical encoding attempt.</td>
</tr>
<tr>
<td>505</td>
<td>Invalid Hex Encoding</td>
<td>%nn where nn are not hex digits.</td>
</tr>
<tr>
<td>506</td>
<td>URI Path Length Too Long</td>
<td>path length is greater than 512 characters.</td>
</tr>
<tr>
<td>507</td>
<td>Invalid Use of Character</td>
<td>use of disabled char</td>
</tr>
<tr>
<td>508</td>
<td>Double Decoding Exploit</td>
<td>Double decoding exploit (%25xx, %25%xxd, etc).</td>
</tr>
<tr>
<td>700</td>
<td>Invalid Base64 Content</td>
<td>Packet content that was expected to be encoded in Base64 format was not encoded correctly.</td>
</tr>
<tr>
<td>710</td>
<td>Corrupted Deflate/GZIP Content</td>
<td>Corrupted Deflate/GZIP Content</td>
</tr>
<tr>
<td>711</td>
<td>Incomplete Deflate/GZIP Content</td>
<td>Incomplete Deflate/GZIP Content</td>
</tr>
<tr>
<td>712</td>
<td>Deflate/GZIP Checksum Error</td>
<td>Deflate/GZIP Checksum Error.</td>
</tr>
<tr>
<td>714</td>
<td>Unsupported GZIP Header Format/Method</td>
<td>Unsupported GZIP Header Format/Method.</td>
</tr>
<tr>
<td>ID</td>
<td>Event</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>801</td>
<td>Protocol Decoding</td>
<td>A protocol decoding rule defined a limit for a search or pdu object but the object was not found before the limit was reached.</td>
</tr>
<tr>
<td></td>
<td>Search Limit Exceeded</td>
<td></td>
</tr>
<tr>
<td>802</td>
<td>Protocol Decoding</td>
<td>A protocol decoding rule decoded data that did not meet the protocol content constraints.</td>
</tr>
<tr>
<td></td>
<td>Constraint Error</td>
<td></td>
</tr>
<tr>
<td>803</td>
<td>Protocol Decoding</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Engine Internal Error</td>
<td></td>
</tr>
<tr>
<td>804</td>
<td>Protocol Decoding</td>
<td>A protocol decoding rule encountered a type definition and packet content that caused the maximum type nesting depth (16) to be exceeded.</td>
</tr>
<tr>
<td></td>
<td>Structure Too Deep</td>
<td></td>
</tr>
<tr>
<td>805</td>
<td>Protocol Decoding</td>
<td>A rule programming error attempted to cause recursion or use to many nested procedure calls.</td>
</tr>
<tr>
<td></td>
<td>Stack Error</td>
<td></td>
</tr>
<tr>
<td>806</td>
<td>Infinite Data Loop</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Loop Error</td>
<td></td>
</tr>
</tbody>
</table>
## Firewall Events

<table>
<thead>
<tr>
<th>ID</th>
<th>Event</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Normal (Filter)</td>
<td>A packet was received that was not associated with an existing connection.</td>
</tr>
<tr>
<td>100</td>
<td>Out Of Connection</td>
<td>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.)</td>
</tr>
<tr>
<td>101</td>
<td>Invalid Flags</td>
<td>A packet with an invalid sequence number or out-of-window data size was encountered.</td>
</tr>
<tr>
<td>102</td>
<td>Invalid Sequence</td>
<td>A packet with an invalid acknowledgement number was encountered.</td>
</tr>
<tr>
<td>103</td>
<td>Invalid ACK</td>
<td>A packet with an invalid acknowledgement number was encountered.</td>
</tr>
<tr>
<td>104</td>
<td>Internal Error</td>
<td></td>
</tr>
<tr>
<td>105</td>
<td>CE Flags</td>
<td>The CWR or ECE flags were set and the Firewall Stateful Configuration specifies that these packets should be denied.</td>
</tr>
<tr>
<td>106</td>
<td>Invalid IP</td>
<td>Packets source IP was not valid.</td>
</tr>
<tr>
<td>107</td>
<td>Invalid IP Datagram Length</td>
<td>The length of the IP datagram is less than the length specified in the IP header.</td>
</tr>
<tr>
<td>108</td>
<td>Fragmented</td>
<td>A fragmented packet was encountered with deny fragmented packets disallowed enabled.</td>
</tr>
<tr>
<td>109</td>
<td>Invalid Fragment Offset</td>
<td></td>
</tr>
<tr>
<td>110</td>
<td>First Fragment Too Small</td>
<td>A fragmented packet was encountered, the size of the fragment was less than the size of a TCP packet (no data).</td>
</tr>
<tr>
<td>111</td>
<td>Fragment Out Of Bounds</td>
<td>The offsets specified in a fragmented packet sequence is outside the range of the maximum size of a datagram.</td>
</tr>
<tr>
<td>112</td>
<td>Fragment Offset Too Small</td>
<td>A fragmented packet was encountered, the size of the fragment was less than the size of a TCP packet (no data).</td>
</tr>
<tr>
<td>113</td>
<td>IPv6 Packet</td>
<td>An IPv6 Packet was encountered, and IPv6 blocking is enabled.</td>
</tr>
<tr>
<td>114</td>
<td>Max Incoming Connections</td>
<td>The number of incoming connections has exceeded the maximum number of connections allowed.</td>
</tr>
<tr>
<td>115</td>
<td>Max Outgoing Connections</td>
<td>The number of outgoing connections has exceeded the maximum number of connections allowed.</td>
</tr>
<tr>
<td>ID</td>
<td>Event</td>
<td>Notes</td>
</tr>
<tr>
<td>----</td>
<td>------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>116</td>
<td>Max SYN Sent</td>
<td>The number of half open connections from a single computer exceeds that specified in the Firewall Stateful Configuration.</td>
</tr>
<tr>
<td>117</td>
<td>License Expired</td>
<td></td>
</tr>
<tr>
<td>118</td>
<td>IP Version Unknown</td>
<td>An IP packet other than IPv4 or IPv6 was encountered.</td>
</tr>
<tr>
<td>119</td>
<td>Invalid Packet Info</td>
<td></td>
</tr>
<tr>
<td>120</td>
<td>Internal Engine Error</td>
<td>Insufficient resources.</td>
</tr>
<tr>
<td>121</td>
<td>Unsolicited UDP</td>
<td>Incoming UDP packets that were not solicited by the computer are rejected.</td>
</tr>
<tr>
<td>122</td>
<td>Unsolicited ICMP</td>
<td>ICMP stateful has been enabled (in Firewall Stateful Configuration) and an unsolicited packet that does not match any Force Allow rules was received.</td>
</tr>
<tr>
<td>123</td>
<td>Out Of Allowed Policy</td>
<td>The packet does not meet any of the Allow or Force Allow rules and so is implicitly denied.</td>
</tr>
<tr>
<td>124</td>
<td>Invalid Port Command</td>
<td>An invalid FTP port command was encountered in the FTP control channel data stream.</td>
</tr>
<tr>
<td>125</td>
<td>SYN Cookie Error</td>
<td>The SYN cookies protection mechanism encountered an error.</td>
</tr>
<tr>
<td>126</td>
<td>Invalid Data Offset</td>
<td>Invalid data offset parameter.</td>
</tr>
<tr>
<td>127</td>
<td>No IP Header</td>
<td></td>
</tr>
<tr>
<td>128</td>
<td>Unreadable Ethernet Header</td>
<td>Data contained in this Ethernet frame is smaller than the Ethernet header.</td>
</tr>
<tr>
<td>129</td>
<td>Undefined</td>
<td></td>
</tr>
<tr>
<td>130</td>
<td>Same Source and Destination IP</td>
<td>Source and destination IPs were identical.</td>
</tr>
<tr>
<td>131</td>
<td>Invalid TCP Header Length</td>
<td></td>
</tr>
<tr>
<td>132</td>
<td>Unreadable Protocol Header</td>
<td>The packet contains an unreadable TCP, UDP or ICMP header.</td>
</tr>
<tr>
<td>ID</td>
<td>Event</td>
<td>Notes</td>
</tr>
<tr>
<td>----</td>
<td>------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>133</td>
<td>Unreadable IPv4 Header</td>
<td>The packet contains an unreadable IPv4 header.</td>
</tr>
<tr>
<td>134</td>
<td>Unknown IP Version</td>
<td>Unrecognized IP version.</td>
</tr>
<tr>
<td>135</td>
<td>Invalid Adapter</td>
<td>An invalid adapter configuration has been received.</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>136</td>
<td>Overlapping Fragment</td>
<td>This packet fragment overlaps a previously sent fragment.</td>
</tr>
<tr>
<td>137</td>
<td>Maximum ACK Retransmit</td>
<td>This retransmitted ACK packet exceeds the ACK storm protection threshold.</td>
</tr>
<tr>
<td>138</td>
<td>Packet on Closed</td>
<td>A packet was received belonging to a connection already closed.</td>
</tr>
<tr>
<td></td>
<td>Connection Initiated</td>
<td></td>
</tr>
<tr>
<td>139</td>
<td>Dropped Retransmit</td>
<td>Dropped Retransmit.</td>
</tr>
<tr>
<td>140</td>
<td>Undefined</td>
<td></td>
</tr>
<tr>
<td>141</td>
<td>Out of Allowed Policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Open Port)</td>
<td></td>
</tr>
<tr>
<td>142</td>
<td>New Connection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Initiated</td>
<td></td>
</tr>
</tbody>
</table>
# System Events

The following table lists the System Events that can be recorded by Deep Security and their default settings. (Notifications cannot be sent for Events that are not recorded.)

<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Event</th>
<th>Record</th>
<th>Notify</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Error</td>
<td>Unknown Error</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>Info</td>
<td>Deep Security Manager Started</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>101</td>
<td>Info</td>
<td>License Changed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>102</td>
<td>Info</td>
<td>Trend Micro Deep Security Customer Account Changed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>103</td>
<td>Warning</td>
<td>Check For Updates Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>104</td>
<td>Warning</td>
<td>Automatic Software Download Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>105</td>
<td>Warning</td>
<td>Scheduled Rule Update Download and Apply Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>106</td>
<td>Info</td>
<td>Scheduled Rule Update Downloaded and Applied</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>107</td>
<td>Info</td>
<td>Rule Update Downloaded and Applied</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>108</td>
<td>Info</td>
<td>Script Executed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>109</td>
<td>Error</td>
<td>Script Execution Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>110</td>
<td>Info</td>
<td>System Events Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>111</td>
<td>Info</td>
<td>Firewall Events Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>112</td>
<td>Info</td>
<td>Intrusion Prevention Events Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>----</td>
<td>----------</td>
<td>--------------------------------------------</td>
<td>--------</td>
<td>-------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>113</td>
<td>Warning</td>
<td>Scheduled Rule Update Download Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>114</td>
<td>Info</td>
<td>Scheduled Rule Update Downloaded</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>115</td>
<td>Info</td>
<td>Rule Update Downloaded</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>116</td>
<td>Info</td>
<td>Rule Update Applied</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>117</td>
<td>Info</td>
<td>Deep Security Manager Shutdown</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>118</td>
<td>Warning</td>
<td>Deep Security Manager Offline</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>119</td>
<td>Info</td>
<td>Deep Security Manager Back Online</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>120</td>
<td>Error</td>
<td>Heartbeat Server Failed</td>
<td>On</td>
<td>On</td>
<td>The server within DSM that listens for incoming Agent Heartbeats has failed to start. Check that the DSM's incoming heartbeat port (by default 4120) is not in use by another application on the DSM server. Once it is free, the DSM should bind to it and this error should be fixed.</td>
</tr>
<tr>
<td>121</td>
<td>Error</td>
<td>Scheduler Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>122</td>
<td>Error</td>
<td>Manager Message Thread Failed</td>
<td>On</td>
<td>On</td>
<td>An internal thread has failed. There is no resolution for this error. If it persists, contact customer support.</td>
</tr>
<tr>
<td>123</td>
<td>Info</td>
<td>Deep Security Manager Forced Shutdown</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>124</td>
<td>Info</td>
<td>Rule Update Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>130</td>
<td>Info</td>
<td>Credentials Generated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>131</td>
<td>Warning</td>
<td>Credential Generation Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>140</td>
<td>Info</td>
<td>Discover Computers</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>141</td>
<td>Warning</td>
<td>Discover Computers Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>142</td>
<td>Info</td>
<td>Discover Computers Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>-------------------------------</td>
<td>---------</td>
<td>--------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>143</td>
<td>Info</td>
<td>Discover Computers Cancelled</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>150</td>
<td>Info</td>
<td>System Settings Saved</td>
<td>On (cannot be turned off)</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>151</td>
<td>Info</td>
<td>Software Added</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>152</td>
<td>Info</td>
<td>Software Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>153</td>
<td>Info</td>
<td>Software Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>154</td>
<td>Info</td>
<td>Software Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>155</td>
<td>Info</td>
<td>Software Platforms Changed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>160</td>
<td>Info</td>
<td>Authentication Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>161</td>
<td>Info</td>
<td>Rule Update Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>162</td>
<td>Info</td>
<td>Log Inspection Events Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>163</td>
<td>Info</td>
<td>Anti-Malware Event Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>164</td>
<td>Info</td>
<td>Security Update Successful</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>165</td>
<td>Error</td>
<td>Security Update Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>166</td>
<td>Info</td>
<td>Check for New Software Success</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>167</td>
<td>Error</td>
<td>Check for New Software Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>168</td>
<td>Info</td>
<td>Manual Security Update Successful</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>169</td>
<td>Error</td>
<td>Manual Security Update Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>170</td>
<td>Error</td>
<td>Manager Available Disk Space Too Low</td>
<td>On</td>
<td>On</td>
<td>The DSM has determined that there is not enough disk space available to continue to function and will shutdown. When this error occurs the DSM will shutdown. The resolution is to free up disk space and restart the DSM.</td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>---------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>171</td>
<td>Info</td>
<td>Anti-Malware Spyware Item Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>172</td>
<td>Info</td>
<td>Web Reputation Events Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>173</td>
<td>Info</td>
<td>Anti-Malware Quarantined File List</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>180</td>
<td>Info</td>
<td>Alert Type Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>190</td>
<td>Info</td>
<td>Alert Started</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>191</td>
<td>Info</td>
<td>Alert Changed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>192</td>
<td>Info</td>
<td>Alert Ended</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>197</td>
<td>Info</td>
<td>Alert Emails Sent</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>198</td>
<td>Warning</td>
<td>Alert Emails Failed</td>
<td>On</td>
<td>On</td>
<td>An Alert was raised which had been configured to generate an email</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>notification to one or more users but the email could not be sent. Make</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>sure SMTP setting are properly configured. See *Administration &gt; System</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Settings &gt; SMTP (page 203).*</td>
</tr>
<tr>
<td>199</td>
<td>Error</td>
<td>Alert Processing Failed</td>
<td>On</td>
<td>On</td>
<td>Processing of the Alerts has failed. This may mean that the current</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Alert status is inaccurate. There is no resolution for this error. If</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>it persists, contact customer support.</td>
</tr>
<tr>
<td>250</td>
<td>Info</td>
<td>Computer Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>251</td>
<td>Info</td>
<td>Computer Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>252</td>
<td>Info</td>
<td>Computer Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>253</td>
<td>Info</td>
<td>Policy Assigned to Computer</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>254</td>
<td>Info</td>
<td>Computer Moved</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>255</td>
<td>Info</td>
<td>Activation Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>256</td>
<td>Info</td>
<td>Send Policy Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>257</td>
<td>Info</td>
<td>Locked</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>258</td>
<td>Info</td>
<td>Unlocked</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>259</td>
<td>Info</td>
<td>Deactivation Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>260</td>
<td>Info</td>
<td>Scan for Open Ports</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>----</td>
<td>----------</td>
<td>--------------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>261</td>
<td>Warning</td>
<td>Scan for Open Ports Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>262</td>
<td>Info</td>
<td>Scan for Open Ports Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>263</td>
<td>Info</td>
<td>Scan for Open Ports Cancelled</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>264</td>
<td>Info</td>
<td>Agent Software Upgrade Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>265</td>
<td>Info</td>
<td>Agent Software Upgrade Cancelled</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>266</td>
<td>Info</td>
<td>Warnings/Errors Cleared</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>267</td>
<td>Info</td>
<td>Check Status Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>268</td>
<td>Info</td>
<td>Get Events Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>270</td>
<td>Error</td>
<td>Computer Creation Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>273</td>
<td>Info</td>
<td>Security Update Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>274</td>
<td>Info</td>
<td>Security Update Rollback Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>275</td>
<td>Warning</td>
<td>Duplicate Computer</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>276</td>
<td>Info</td>
<td>Security Updates Downloaded</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>280</td>
<td>Info</td>
<td>Computers Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>281</td>
<td>Info</td>
<td>Computers Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>286</td>
<td>Info</td>
<td>Computer Log Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>287</td>
<td>Info</td>
<td>Relay Group Assigned to Computer</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>290</td>
<td>Info</td>
<td>Group Added</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>291</td>
<td>Info</td>
<td>Group Removed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>292</td>
<td>Info</td>
<td>Group Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>-------------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>----------------</td>
</tr>
<tr>
<td>293</td>
<td>Info</td>
<td>Interface Renamed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>294</td>
<td>Info</td>
<td>Computer Bridge Renamed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>295</td>
<td>Info</td>
<td>Interface Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>296</td>
<td>Info</td>
<td>Interface IP Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>297</td>
<td>Info</td>
<td>Scan for Recommendations Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>298</td>
<td>Info</td>
<td>Recommendations Cleared</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>299</td>
<td>Info</td>
<td>Asset Value Assigned to Computer</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>Info</td>
<td>Scan for Recommendations Completed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>301</td>
<td>Info</td>
<td>Agent Software Deployment Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>302</td>
<td>Info</td>
<td>Agent Software Removal Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>303</td>
<td>Info</td>
<td>Computer Renamed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>304</td>
<td>Info</td>
<td>Scan for Integrity Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>305</td>
<td>Info</td>
<td>Rebuild Baseline Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>306</td>
<td>Info</td>
<td>Cancel Update Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>307</td>
<td>Info</td>
<td>Integrity Monitoring Rule Compile Issue</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>308</td>
<td>Info</td>
<td>Integrity Monitoring Rule Compile Issue</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>309</td>
<td>Info</td>
<td>Directory Added</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>310</td>
<td>Info</td>
<td>Directory Removed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>311</td>
<td>Info</td>
<td>Directory Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>320</td>
<td>Info</td>
<td>Directory Synchronization</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>321</td>
<td>Info</td>
<td>Directory Synchronization</td>
<td>On</td>
<td>On</td>
<td>Finished</td>
</tr>
<tr>
<td>322</td>
<td>Error</td>
<td>Directory Synchronization</td>
<td>On</td>
<td>On</td>
<td>Failed</td>
</tr>
<tr>
<td>323</td>
<td>Info</td>
<td>Directory Synchronization</td>
<td>On</td>
<td>On</td>
<td>Requested</td>
</tr>
<tr>
<td>324</td>
<td>Info</td>
<td>Directory Synchronization</td>
<td>On</td>
<td>On</td>
<td>Cancelled</td>
</tr>
<tr>
<td>325</td>
<td>Info</td>
<td>User Synchronization</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>326</td>
<td>Info</td>
<td>User Synchronization</td>
<td>On</td>
<td>On</td>
<td>Finished</td>
</tr>
<tr>
<td>327</td>
<td>Error</td>
<td>User Synchronization</td>
<td>On</td>
<td>On</td>
<td>Failed</td>
</tr>
<tr>
<td>328</td>
<td>Info</td>
<td>User Synchronization</td>
<td>On</td>
<td>On</td>
<td>Requested</td>
</tr>
<tr>
<td>329</td>
<td>Info</td>
<td>User Synchronization</td>
<td>On</td>
<td>On</td>
<td>Cancelled</td>
</tr>
<tr>
<td>330</td>
<td>Info</td>
<td>SSL Configuration</td>
<td>On</td>
<td>On</td>
<td>Created</td>
</tr>
<tr>
<td>331</td>
<td>Info</td>
<td>SSL Configuration</td>
<td>On</td>
<td>On</td>
<td>Deleted</td>
</tr>
<tr>
<td>332</td>
<td>Info</td>
<td>SSL Configuration</td>
<td>On</td>
<td>On</td>
<td>Updated</td>
</tr>
<tr>
<td>350</td>
<td>Info</td>
<td>Policy Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>351</td>
<td>Info</td>
<td>Policy Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>352</td>
<td>Info</td>
<td>Policy Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>353</td>
<td>Info</td>
<td>Policies Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>354</td>
<td>Info</td>
<td>Policies Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>360</td>
<td>Info</td>
<td>VMware vCenter Added</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>----</td>
<td>----------</td>
<td>--------------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>361</td>
<td>Info</td>
<td>VMware vCenter Removed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>362</td>
<td>Info</td>
<td>VMware vCenter Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>363</td>
<td>Info</td>
<td>VMware vCenter Synchronization</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>364</td>
<td>Info</td>
<td>VMware vCenter Synchronization Finished</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>365</td>
<td>Error</td>
<td>VMware vCenter Synchronization Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>366</td>
<td>Info</td>
<td>VMware vCenter Synchronization Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>367</td>
<td>Info</td>
<td>VMware vCenter Synchronization Cancelled</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>368</td>
<td>Warning</td>
<td>Interfaces Out of Sync</td>
<td>On</td>
<td>On</td>
<td>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.</td>
</tr>
<tr>
<td>369</td>
<td>Info</td>
<td>Interfaces in Sync</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>370</td>
<td>Info</td>
<td>ESX Server Prepared</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>371</td>
<td>Info</td>
<td>ESX Server Restored</td>
<td>On</td>
<td>On</td>
<td>The ESX has been restored to the state it was in before the Filter Driver software was installed.</td>
</tr>
<tr>
<td>372</td>
<td>Info</td>
<td>Filter Driver Upgraded</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>373</td>
<td>Info</td>
<td>Virtual Appliance Deployed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>374</td>
<td>Info</td>
<td>Virtual Appliance Upgraded</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>375</td>
<td>Warning</td>
<td>Virtual Appliance Upgrade Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>376</td>
<td>Warning</td>
<td>Virtual Machine Moved to Unprotected ESX</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>------------------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>377</td>
<td>Info</td>
<td>Virtual Machine Moved to Protected ESX</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>378</td>
<td>Warning</td>
<td>Virtual Machine unprotected after move to another ESX</td>
<td>On</td>
<td>On</td>
<td>A VM was moved to an unprotected ESX.</td>
</tr>
<tr>
<td>379</td>
<td>Info</td>
<td>Virtual Machine unprotected after move to another ESX Resolved</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>380</td>
<td>Error</td>
<td>Filter Driver Offline</td>
<td>On</td>
<td>On</td>
<td>The Filter Driver on a given ESX is offline. Use the VMware vCenter console to troubleshoot problems with the hypervisor and/or the ESX.</td>
</tr>
<tr>
<td>381</td>
<td>Info</td>
<td>Filter Driver Back Online</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>382</td>
<td>Info</td>
<td>Filter Driver Upgrade Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>383</td>
<td>Info</td>
<td>Appliance Upgrade Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>384</td>
<td>Warning</td>
<td>Prepare ESX Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>385</td>
<td>Warning</td>
<td>Filter Driver Upgrade Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>386</td>
<td>Warning</td>
<td>Restore ESX Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>387</td>
<td>Error</td>
<td>Connection to Filter Driver Failure</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>388</td>
<td>Info</td>
<td>Connection to Filter Driver Success</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>389</td>
<td>Error</td>
<td>Multiple Activated Appliances Detected</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>390</td>
<td>Info</td>
<td>Multiple Activated Appliances Detected Resolved</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>391</td>
<td>Error</td>
<td>Network Settings Out of Sync With vCenter Global Settings</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>------------------------------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>392</td>
<td>Info</td>
<td>Network Settings in Sync With vCenter Global Settings</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>393</td>
<td>Error</td>
<td>Anti-Malware Engine Offline</td>
<td>On</td>
<td>On</td>
<td>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.</td>
</tr>
<tr>
<td>394</td>
<td>Info</td>
<td>Anti-Malware Engine Back Online</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>395</td>
<td>Error</td>
<td>Virtual Appliance is Incompatible With Filter Driver</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>396</td>
<td>Info</td>
<td>Virtual Appliance is Incompatible With Filter Driver</td>
<td>On</td>
<td>On</td>
<td>Resolved</td>
</tr>
<tr>
<td>410</td>
<td>Info</td>
<td>Firewall Rule Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>411</td>
<td>Info</td>
<td>Firewall Rule Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>412</td>
<td>Info</td>
<td>Firewall Rule Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>413</td>
<td>Info</td>
<td>Firewall Rule Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>414</td>
<td>Info</td>
<td>Firewall Rule Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>420</td>
<td>Info</td>
<td>Firewall Stateful Configuration Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>421</td>
<td>Info</td>
<td>Firewall Stateful Configuration Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>422</td>
<td>Info</td>
<td>Firewall Stateful Configuration Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>423</td>
<td>Info</td>
<td>Firewall Stateful Configuration Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>424</td>
<td>Info</td>
<td>Firewall Stateful Configuration</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Imported</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>460</td>
<td>Info</td>
<td>Application Type Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>461</td>
<td>Info</td>
<td>Application Type Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>462</td>
<td>Info</td>
<td>Application Type Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>463</td>
<td>Info</td>
<td>Application Type Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>464</td>
<td>Info</td>
<td>Application Type Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>470</td>
<td>Info</td>
<td>Intrusion Prevention Rule Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>471</td>
<td>Info</td>
<td>Intrusion Prevention Rule Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>472</td>
<td>Info</td>
<td>Intrusion Prevention Rule Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>473</td>
<td>Info</td>
<td>Intrusion Prevention Rule Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>474</td>
<td>Info</td>
<td>Intrusion Prevention Rule Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>480</td>
<td>Info</td>
<td>Integrity Monitoring Rule Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>481</td>
<td>Info</td>
<td>Integrity Monitoring Rule Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>482</td>
<td>Info</td>
<td>Integrity Monitoring Rule Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>483</td>
<td>Info</td>
<td>Integrity Monitoring Rule Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>484</td>
<td>Info</td>
<td>Integrity Monitoring Rule Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>490</td>
<td>Info</td>
<td>Log Inspection Rule Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event Description</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>----</td>
<td>----------</td>
<td>-----------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>491</td>
<td>Info</td>
<td>Log Inspection Rule Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>492</td>
<td>Info</td>
<td>Log Inspection Rule Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>493</td>
<td>Info</td>
<td>Log Inspection Rule Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>494</td>
<td>Info</td>
<td>Log Inspection Rule Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>495</td>
<td>Info</td>
<td>Log Inspection Decoder Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>496</td>
<td>Info</td>
<td>Log Inspection Decoder Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>497</td>
<td>Info</td>
<td>Log Inspection Decoder Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>498</td>
<td>Info</td>
<td>Log Inspection Decoder Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>499</td>
<td>Info</td>
<td>Log Inspection Decoder Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>505</td>
<td>Info</td>
<td>Context Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>506</td>
<td>Info</td>
<td>Context Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>507</td>
<td>Info</td>
<td>Context Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>508</td>
<td>Info</td>
<td>Context Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>509</td>
<td>Info</td>
<td>Context Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>510</td>
<td>Info</td>
<td>IP List Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>511</td>
<td>Info</td>
<td>IP List Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>512</td>
<td>Info</td>
<td>IP List Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>513</td>
<td>Info</td>
<td>IP List Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>514</td>
<td>Info</td>
<td>IP List Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>520</td>
<td>Info</td>
<td>Port List Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>521</td>
<td>Info</td>
<td>Port List Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>522</td>
<td>Info</td>
<td>Port List Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>523</td>
<td>Info</td>
<td>Port List Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>524</td>
<td>Info</td>
<td>Port List Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>525</td>
<td>Info</td>
<td>Scan Cache Configuration Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>526</td>
<td>Info</td>
<td>Scan Cache Configuration Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>530</td>
<td>Info</td>
<td>MAC List Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>531</td>
<td>Info</td>
<td>MAC List Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>532</td>
<td>Info</td>
<td>MAC List Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>533</td>
<td>Info</td>
<td>MAC List Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>534</td>
<td>Info</td>
<td>MAC List Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>540</td>
<td>Info</td>
<td>Proxy Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>541</td>
<td>Info</td>
<td>Proxy Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>542</td>
<td>Info</td>
<td>Proxy Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>543</td>
<td>Info</td>
<td>Proxy Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>544</td>
<td>Info</td>
<td>Proxy Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>550</td>
<td>Info</td>
<td>Schedule Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>551</td>
<td>Info</td>
<td>Schedule Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>552</td>
<td>Info</td>
<td>Schedule Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>553</td>
<td>Info</td>
<td>Schedule Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>554</td>
<td>Info</td>
<td>Schedule Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>560</td>
<td>Info</td>
<td>Scheduled Task Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>561</td>
<td>Info</td>
<td>Scheduled Task Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>562</td>
<td>Info</td>
<td>Scheduled Task Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>563</td>
<td>Info</td>
<td>Scheduled Task Manually Executed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>564</td>
<td>Info</td>
<td>Scheduled Task Started</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>565</td>
<td>Info</td>
<td>Backup Finished</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>566</td>
<td>Error</td>
<td>Backup Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>567</td>
<td>Info</td>
<td>Sending Outstanding Alert Summary</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>568</td>
<td>Warning</td>
<td>Failed To Send Outstanding Alert Summary</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>569</td>
<td>Warning</td>
<td>Email Failed</td>
<td>On</td>
<td>On</td>
<td>An email notification could not be sent. Make sure SMTP setting are properly configured (Administration &gt; System Settings &gt; SMTP).</td>
</tr>
<tr>
<td>570</td>
<td>Info</td>
<td>Sending Report</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>571</td>
<td>Warning</td>
<td>Failed To Send Report</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>572</td>
<td>Error</td>
<td>Invalid Report Jar</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>573</td>
<td>Info</td>
<td>Asset Value Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>574</td>
<td>Info</td>
<td>Asset Value Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>575</td>
<td>Info</td>
<td>Asset Value Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>576</td>
<td>Error</td>
<td>Report Uninstall Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>577</td>
<td>Error</td>
<td>Report Uninstalled</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>580</td>
<td>Warning</td>
<td>Application Type Port List Misconfiguration</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>581</td>
<td>Warning</td>
<td>Application Type Port List Misconfiguration Resolved</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>582</td>
<td>Warning</td>
<td>Intrusion Prevention Rules Require</td>
<td>On</td>
<td>On</td>
<td>Configuration</td>
</tr>
<tr>
<td>583</td>
<td>Info</td>
<td>Intrusion Prevention Rules Require</td>
<td>On</td>
<td>On</td>
<td>Configuration Resolved</td>
</tr>
<tr>
<td>584</td>
<td>Warning</td>
<td>Integrity Monitoring Rules Require</td>
<td>On</td>
<td>On</td>
<td>Configuration</td>
</tr>
<tr>
<td>585</td>
<td>Info</td>
<td>Integrity Monitoring Rules Require</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>----</td>
<td>----------</td>
<td>-------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>586</td>
<td>Warning</td>
<td>Log Inspection Rules Require Configuration Resolved</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>587</td>
<td>Info</td>
<td>Log Inspection Rules Require Configuration Resolved</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>588</td>
<td>Warning</td>
<td>Log Inspection Rules Require Log Files</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>589</td>
<td>Info</td>
<td>Log Inspection Rules Require Log Files Resolved</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>590</td>
<td>Warning</td>
<td>Scheduled Task Unknown Type</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>591</td>
<td>Info</td>
<td>Relay Group Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>592</td>
<td>Info</td>
<td>Relay Group Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>593</td>
<td>Info</td>
<td>Relay Group Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>600</td>
<td>Info</td>
<td>User Signed In</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>601</td>
<td>Info</td>
<td>User Signed Out</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>602</td>
<td>Info</td>
<td>User Timed Out</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>603</td>
<td>Info</td>
<td>User Locked Out</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>604</td>
<td>Info</td>
<td>User Unlocked</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>608</td>
<td>Error</td>
<td>User Session Validation Failed</td>
<td>On</td>
<td>On</td>
<td>DSM is unable to confirm that the User session is the one that was initiated by a successful User sign-in/authentication. DSM will return the User to the sign-in page. User will be forced to re-authenticate.</td>
</tr>
<tr>
<td>609</td>
<td>Error</td>
<td>User Made Invalid Request</td>
<td>On</td>
<td>On</td>
<td>DSM received invalid request to access the audit data (Events). Access to the audit data is denied.</td>
</tr>
<tr>
<td>610</td>
<td>Info</td>
<td>User Session Validated</td>
<td>Off</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>611</td>
<td>Info</td>
<td>User Viewed Firewall Event</td>
<td>Off</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>----</td>
<td>----------</td>
<td>--------------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>613</td>
<td>Info</td>
<td>User Viewed Intrusion Prevention Event</td>
<td>Off</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>615</td>
<td>Info</td>
<td>User Viewed System Event</td>
<td>Off</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>616</td>
<td>Info</td>
<td>User Viewed Integrity Monitoring Event</td>
<td>Off</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>617</td>
<td>Info</td>
<td>User Viewed Log Inspection Event</td>
<td>Off</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>618</td>
<td>Info</td>
<td>User Viewed Quarantined File Detail</td>
<td>Off</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>619</td>
<td>Info</td>
<td>User Viewed Anti-Malware Event</td>
<td>Off</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>620</td>
<td>Info</td>
<td>User Viewed Web Reputation Event</td>
<td>Off</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>650</td>
<td>Info</td>
<td>User Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>651</td>
<td>Info</td>
<td>User Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>652</td>
<td>Info</td>
<td>User Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>653</td>
<td>Info</td>
<td>User Password Set</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>660</td>
<td>Info</td>
<td>Role Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>661</td>
<td>Info</td>
<td>Role Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>662</td>
<td>Info</td>
<td>Role Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>663</td>
<td>Info</td>
<td>Roles Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>664</td>
<td>Info</td>
<td>Roles Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>670</td>
<td>Info</td>
<td>Contact Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>671</td>
<td>Info</td>
<td>Contact Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>672</td>
<td>Info</td>
<td>Contact Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>700</td>
<td>Info</td>
<td>Agent Software Installed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>701</td>
<td>Error</td>
<td>Agent Software Installation Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>702</td>
<td>Info</td>
<td>Credentials Generated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>703</td>
<td>Error</td>
<td>Credential Generation Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>704</td>
<td>Info</td>
<td>Activated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>705</td>
<td>Error</td>
<td>Activation Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>706</td>
<td>Info</td>
<td>Agent Software Upgraded</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>707</td>
<td>Warning</td>
<td>Agent Software Upgrade Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>708</td>
<td>Info</td>
<td>Deactivated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>709</td>
<td>Error</td>
<td>Deactivation Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>710</td>
<td>Info</td>
<td>Events Retrieved</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>711</td>
<td>Info</td>
<td>Agent Software Deployed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>712</td>
<td>Error</td>
<td>Agent Software Deployment Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>713</td>
<td>Info</td>
<td>Agent Software Removed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>714</td>
<td>Error</td>
<td>Agent Software Removal Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>715</td>
<td>Info</td>
<td>Agent/Appliance Version Changed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>720</td>
<td>Info</td>
<td>Updated</td>
<td>On</td>
<td>On</td>
<td>Agent/Appliance updated.</td>
</tr>
<tr>
<td>721</td>
<td>Error</td>
<td>Update Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>722</td>
<td>Warning</td>
<td>Get Interfaces Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>723</td>
<td>Info</td>
<td>Get Interfaces Failure Resolved</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>724</td>
<td>Warning</td>
<td>Insufficient Disk Space</td>
<td>On</td>
<td>On</td>
<td>An Agent has reported low disk space. Free space on the Agent's host.</td>
</tr>
<tr>
<td>725</td>
<td>Warning</td>
<td>Events Suppressed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>726</td>
<td>Warning</td>
<td>Get Agent/Appliance Events Failed</td>
<td>On</td>
<td>On</td>
<td>DSM 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 &quot;Check Status&quot; to retry the operation.</td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>727</td>
<td>Info</td>
<td>Get Agent/Appliance Events Failure Resolved</td>
<td>On</td>
<td>On</td>
<td>DSM 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 &quot;Get Events Now&quot; to retry the operation.</td>
</tr>
<tr>
<td>728</td>
<td>Error</td>
<td>Get Events Failed</td>
<td>On</td>
<td>On</td>
<td><strong>DSM 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 &quot;Get Events Now&quot; to retry the operation.</strong></td>
</tr>
<tr>
<td>729</td>
<td>Info</td>
<td>Get Events Failure Resolved</td>
<td>On</td>
<td>On</td>
<td><strong>DSM 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 &quot;Get Events Now&quot; to retry the operation.</strong></td>
</tr>
<tr>
<td>730</td>
<td>Error</td>
<td>Offline</td>
<td>On</td>
<td>On</td>
<td>DSM 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 (page 60) for more information.</td>
</tr>
<tr>
<td>731</td>
<td>Info</td>
<td>Back Online</td>
<td>On</td>
<td>On</td>
<td>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.</td>
</tr>
<tr>
<td>732</td>
<td>Error</td>
<td>Firewall Rule Engine Offline</td>
<td>On</td>
<td>On</td>
<td>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.</td>
</tr>
<tr>
<td>733</td>
<td>Info</td>
<td>Firewall Rule Engine Back Online</td>
<td>On</td>
<td>On</td>
<td>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.</td>
</tr>
<tr>
<td>734</td>
<td>Warning</td>
<td>Computer Clock Change</td>
<td>On</td>
<td>On</td>
<td>A clock change has occurred on the Computer which exceeds the maximum allowed specified in Policy/Computer Editor &gt; Settings &gt; Computer &gt; Heartbeat area. Investigate what has caused the clock change on the computer.</td>
</tr>
<tr>
<td>735</td>
<td>Warning</td>
<td>Misconfiguration Detected</td>
<td>On</td>
<td>On</td>
<td>The Agent's configuration does not match the configuration indicated in the DSM's records. This is typically because of a recent backup restoration of the DSM or the DSA. Unanticipated misconfiguration warnings should be investigated.</td>
</tr>
<tr>
<td>736</td>
<td>Info</td>
<td>Check Status Failure Resolved</td>
<td>On</td>
<td>On</td>
<td>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.</td>
</tr>
<tr>
<td>737</td>
<td>Error</td>
<td>Check Status Failed</td>
<td>On</td>
<td>On</td>
<td>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.</td>
</tr>
<tr>
<td>738</td>
<td>Error</td>
<td>Intrusion Prevention Rule Engine Offline</td>
<td>On</td>
<td>On</td>
<td>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.</td>
</tr>
<tr>
<td>739</td>
<td>Info</td>
<td>Intrusion Prevention Rule Engine Back Online</td>
<td>On</td>
<td>On</td>
<td>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.</td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>740</td>
<td>Error</td>
<td>Agent/Appliance Error</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>741</td>
<td>Warning</td>
<td>Abnormal Restart Detected</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>742</td>
<td>Warning</td>
<td>Communications Problem</td>
<td>On</td>
<td>On</td>
<td>The DSA is having problems communicating its status to DSM. It usually indicates network or load congestion in the DSA -&gt; DSM direction. Further investigation is warranted if the situation persists.</td>
</tr>
<tr>
<td>743</td>
<td>Info</td>
<td>Communications Problem Resolved</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>744</td>
<td>Warning</td>
<td>Events Truncated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>745</td>
<td>Error</td>
<td>Log Inspection Engine Offline</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>746</td>
<td>Info</td>
<td>Log Inspection Engine Back Online</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>747</td>
<td>Warning</td>
<td>Last Automatic Retry</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>748</td>
<td>Info</td>
<td>Deep Security Manager Version</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>749</td>
<td>Warning</td>
<td>Deep Security Manager Upgrade</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>750</td>
<td>Warning</td>
<td>Incompatible Agent/Appliance Version</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>751</td>
<td>Info</td>
<td>Deep Security Manager Version</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>752</td>
<td>Warning</td>
<td>Deep Security Manager Upgrade</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>753</td>
<td>Info</td>
<td>Deep Security Manager Upgrade</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>754</td>
<td>Warning</td>
<td>Deep Security Manager Upgrade</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>755</td>
<td>Info</td>
<td>Agent/Appliance Version</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>756</td>
<td>Warning</td>
<td>Agent/Appliance Version</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>757</td>
<td>Info</td>
<td>Agent/Appliance Version</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>758</td>
<td>Warning</td>
<td>Agent/Appliance Version</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>759</td>
<td>Info</td>
<td>Agent/Appliance Version</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>760</td>
<td>Warning</td>
<td>Agent/Appliance Version</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>761</td>
<td>Info</td>
<td>Agent/Appliance Version</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>762</td>
<td>Warning</td>
<td>Agent/Appliance Version</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>763</td>
<td>Warning</td>
<td>Incompatible Agent/Appliance Version</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>764</td>
<td>Warning</td>
<td>Agent/Appliance Upgrade Recommended (Incompatible Security Component(s))</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>765</td>
<td>Warning</td>
<td>Computer Reboot Required</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>766</td>
<td>Warning</td>
<td>Network Engine Mode Configuration Incompatibility</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>767</td>
<td>Warning</td>
<td>Network Engine Mode Version Incompatibility</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>768</td>
<td>Warning</td>
<td>Network Engine Mode Incompatibility Resolved</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>770</td>
<td>Warning</td>
<td>Agent/Appliance Heartbeat Rejected</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>771</td>
<td>Warning</td>
<td>Contact by Unrecognized Client</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>780</td>
<td>Info</td>
<td>Scan for Recommendations Failure Resolved</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>781</td>
<td>Warning</td>
<td>Scan for Recommendations Failure</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>782</td>
<td>Info</td>
<td>Rebuild Baseline Failure Resolved</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>783</td>
<td>Warning</td>
<td>Rebuild Baseline Failure</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>784</td>
<td>Info</td>
<td>Security Update Successful</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>785</td>
<td>Warning</td>
<td>Security Update Failure</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>786</td>
<td>Info</td>
<td>Scan For Change Failure Resolved</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>787</td>
<td>Warning</td>
<td>Scan For Change Failure</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>790</td>
<td>Info</td>
<td>Agent-Initiated Activation Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>791</td>
<td>Warning</td>
<td>Agent-Initiated Activation Failure</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>792</td>
<td>Info</td>
<td>Manual Malware Scan Failure</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>793</td>
<td>Warning</td>
<td>Manual Malware Scan Failure</td>
<td>On</td>
<td>On</td>
<td>A Malware Scan has failed. Use the Vmware vCenter console to check the status of the VM on which the scan failed.</td>
</tr>
<tr>
<td>794</td>
<td>Info</td>
<td>Scheduled Malware Scan Failure</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>795</td>
<td>Warning</td>
<td>Scheduled Malware Scan Failure</td>
<td>On</td>
<td>On</td>
<td>A scheduled Malware Scan has failed. Use the Vmware vCenter console to check the status of the VM on which the scan failed.</td>
</tr>
<tr>
<td>796</td>
<td>Warning</td>
<td>Scheduled Malware Scan Task has been</td>
<td>On</td>
<td>On</td>
<td>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.</td>
</tr>
<tr>
<td>797</td>
<td>Info</td>
<td>Malware Scan Cancellation Failure</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>798</td>
<td>Warning</td>
<td>Malware Scan Cancellation Failure</td>
<td>On</td>
<td>On</td>
<td>A Malware Scan cancellation has failed. Use the Vmware vCenter console to check the status of the VM on which the scan failed.</td>
</tr>
<tr>
<td>799</td>
<td>Warning</td>
<td>Malware Scan Stalled</td>
<td>On</td>
<td>On</td>
<td>A Malware Scan has stalled. Use the Vmware vCenter console to check the status of the VM on which the scan stalled.</td>
</tr>
<tr>
<td>800</td>
<td>Info</td>
<td>Alert Dismissed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>801</td>
<td>Info</td>
<td>Error Dismissed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>850</td>
<td>Warning</td>
<td>Reconnaissance Detected: Computer OS Fingerprint Probe</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>851</td>
<td>Warning</td>
<td>Reconnaissance Detected: Network or Port Scan</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>852</td>
<td>Warning</td>
<td>Reconnaissance Detected: TCP Null Scan</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>853</td>
<td>Warning</td>
<td>Reconnaissance Detected: TCP SYNFIN Scan</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>854</td>
<td>Warning</td>
<td>Reconnaissance Detected: TCP Xmas Scan</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>900</td>
<td>Info</td>
<td>Deep Security Manager Audit Started</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>901</td>
<td>Info</td>
<td>Deep Security Manager Audit Shutdown</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>902</td>
<td>Info</td>
<td>Deep Security Manager Installed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>903</td>
<td>Warning</td>
<td>License Related Configuration Change</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>910</td>
<td>Info</td>
<td>Diagnostic Package Generated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>911</td>
<td>Info</td>
<td>Diagnostic Package Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>912</td>
<td>Info</td>
<td>Diagnostic Package Uploaded</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>913</td>
<td>Error</td>
<td>Automatic Diagnostic Package Error</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>914</td>
<td>Info</td>
<td>Quarantined File Deletion Succeeded</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>915</td>
<td>Info</td>
<td>Quarantined File Deletion Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>916</td>
<td>Info</td>
<td>Quarantined File Download Succeeded</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>917</td>
<td>Info</td>
<td>Quarantined File Download Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>918</td>
<td>Info</td>
<td>Quarantined File Administration Utility Download Succeeded</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>919</td>
<td>Info</td>
<td>Quarantined File Not Found</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>920</td>
<td>Info</td>
<td>Usage Information Generated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>921</td>
<td>Info</td>
<td>Usage Information Package Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>922</td>
<td>Info</td>
<td>Usage Information Package Uploaded</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>923</td>
<td>Error</td>
<td>Usage Information Package Error</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>924</td>
<td>Warning</td>
<td>Anti-Malware Quarantine Failed (VM limit exceeded)</td>
<td>On</td>
<td>On</td>
<td>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.</td>
</tr>
<tr>
<td>925</td>
<td>Warning</td>
<td>Anti-Malware Quarantine Failed (Quarantine limit exceeded)</td>
<td>On</td>
<td>On</td>
<td>An infected file could not be quarantined. The maximum space allocated on the Virtual Appliance for storing all quarantined files was exceeded.</td>
</tr>
<tr>
<td>926</td>
<td>Warning</td>
<td>Smart Protection Server Disconnected for Smart Scan</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>927</td>
<td>Info</td>
<td>Smart Protection Server Connected for Smart Scan</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>928</td>
<td>Info</td>
<td>Quarantined File Restoration Succeeded</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>929</td>
<td>Warning</td>
<td>Quarantined File Restoration Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>930</td>
<td>Info</td>
<td>Certificate Accepted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>931</td>
<td>Info</td>
<td>Certificate Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>932</td>
<td>Warning</td>
<td>Smart Protection Server Disconnected for Web Reputation</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>--------------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>933</td>
<td>Info</td>
<td>Smart Protection Server Connected for Web Reputation</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>934</td>
<td>Info</td>
<td>Installation/Upgrade of Anti-Malware Component on Agent Succeeded</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>935</td>
<td>Error</td>
<td>Installation/Upgrade of Anti-Malware Component on Agent Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>940</td>
<td>Info</td>
<td>Auto-Tag Rule Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>941</td>
<td>Info</td>
<td>Auto-Tag Rule Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>942</td>
<td>Info</td>
<td>Auto-Tag Rule Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>943</td>
<td>Info</td>
<td>Tag Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>944</td>
<td>Info</td>
<td>Tag Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>970</td>
<td>Info</td>
<td>Command Line Utility Started</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>978</td>
<td>Info</td>
<td>Command Line Utility Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>979</td>
<td>Info</td>
<td>Command Line Utility Shutdown</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>980</td>
<td>Info</td>
<td>System Information Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>990</td>
<td>Info</td>
<td>Manager Node Added</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>991</td>
<td>Info</td>
<td>Manager Node Decommissioned</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>992</td>
<td>Info</td>
<td>Manager Node Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>995</td>
<td>Info</td>
<td>Connection to the Certified Safe</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>996</td>
<td>Warning</td>
<td>Unable to connect to the Certified Safe</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Software Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>997</td>
<td>Error</td>
<td>Tagging Error</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>998</td>
<td>Error</td>
<td>System Event Notification Error</td>
<td>On</td>
<td></td>
<td>On (Cannot be turned on)</td>
</tr>
<tr>
<td>999</td>
<td>Error</td>
<td>Internal Software Error</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1101</td>
<td>Error</td>
<td>Plug-in Installation Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1102</td>
<td>Info</td>
<td>Plug-in Installed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1103</td>
<td>Error</td>
<td>Plug-in Upgrade Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1104</td>
<td>Info</td>
<td>Plug-in Upgraded</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1105</td>
<td>Error</td>
<td>Plug-in Start Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1106</td>
<td>Error</td>
<td>Plug-in Uninstall Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1107</td>
<td>Info</td>
<td>Plug-in Uninstalled</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1108</td>
<td>Info</td>
<td>Plug-in Started</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1109</td>
<td>Info</td>
<td>Plug-in Stopped</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1500</td>
<td>Info</td>
<td>Malware Scan Configuration Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1501</td>
<td>Info</td>
<td>Malware Scan Configuration Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1502</td>
<td>Info</td>
<td>Malware Scan Configuration Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>----------------------------</td>
<td>--------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>1503</td>
<td>Info</td>
<td>Malware Scan Configuration Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1504</td>
<td>Info</td>
<td>Malware Scan Configuration Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1505</td>
<td>Info</td>
<td>Directory List Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1506</td>
<td>Info</td>
<td>Directory List Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1507</td>
<td>Info</td>
<td>Directory List Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1508</td>
<td>Info</td>
<td>Directory List Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1509</td>
<td>Info</td>
<td>Directory List Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1510</td>
<td>Info</td>
<td>File Extension List Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1511</td>
<td>Info</td>
<td>File Extension List Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1512</td>
<td>Info</td>
<td>File Extension List Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1513</td>
<td>Info</td>
<td>File Extension List Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1514</td>
<td>Info</td>
<td>File Extension List Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1515</td>
<td>Info</td>
<td>File List Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1516</td>
<td>Info</td>
<td>File List Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1517</td>
<td>Info</td>
<td>File List Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1518</td>
<td>Info</td>
<td>File List Exported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1519</td>
<td>Info</td>
<td>File List Imported</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1520</td>
<td>Info</td>
<td>Manual Malware Scan Pending</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1521</td>
<td>Info</td>
<td>Manual Malware Scan Started</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>1522</td>
<td>Info</td>
<td>Manual Malware Scan Completed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1523</td>
<td>Info</td>
<td>Scheduled Malware Scan Started</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1524</td>
<td>Info</td>
<td>Scheduled Malware Scan Completed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1525</td>
<td>Info</td>
<td>Manual Malware Scan Cancellation In Progress</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1526</td>
<td>Info</td>
<td>Manual Malware Scan Cancellation Completed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1527</td>
<td>Info</td>
<td>Scheduled Malware Scan Cancellation In Progress</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1528</td>
<td>Info</td>
<td>Scheduled Malware Scan Cancellation Completed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1529</td>
<td>Info</td>
<td>Manual Malware Scan Paused</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1530</td>
<td>Info</td>
<td>Manual Malware Scan Resumed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1531</td>
<td>Info</td>
<td>Scheduled Malware Scan Paused</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1532</td>
<td>Info</td>
<td>Scheduled Malware Scan Resumed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1533</td>
<td>Info</td>
<td>Computer reboot required for Anti-Malware cleanup task</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1534</td>
<td>Info</td>
<td>Computer reboot required for Anti-Malware protection</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1536</td>
<td>Info</td>
<td>Quick Malware Scan Pending</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1537</td>
<td>Info</td>
<td>Quick Malware Scan Started</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>1538</td>
<td>Info</td>
<td>Quick Malware Scan Completed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1539</td>
<td>Info</td>
<td>Quick Malware Scan Cancellation In Progress</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1540</td>
<td>Info</td>
<td>Quick Malware Scan Cancellation Completed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1541</td>
<td>Info</td>
<td>Quick Malware Scan Paused</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1542</td>
<td>Info</td>
<td>Quick Malware Scan Resumed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1543</td>
<td>Warning</td>
<td>Quick Malware Scan Failure</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1550</td>
<td>Info</td>
<td>Web Reputation Settings Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1551</td>
<td>Info</td>
<td>Malware Scan Configuration Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1552</td>
<td>Info</td>
<td>Integrity Configuration Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1553</td>
<td>Info</td>
<td>Log Inspection Configuration Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1554</td>
<td>Info</td>
<td>Firewall Stateful Configuration Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1555</td>
<td>Info</td>
<td>Intrusion Prevention Configuration Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1600</td>
<td>Info</td>
<td>Relay Group Update Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1601</td>
<td>Info</td>
<td>Relay Group Update Success</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1602</td>
<td>Error</td>
<td>Relay Group Update Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>-------------------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>1603</td>
<td>Info</td>
<td>Security Update Rollback Success</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1604</td>
<td>Warning</td>
<td>Security Update Rollback Failure</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1650</td>
<td>Warning</td>
<td>Anti-Malware protection is absent or out of date</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1651</td>
<td>Info</td>
<td>Anti-Malware module is ready</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1660</td>
<td>Info</td>
<td>Rebuild Baseline Started</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1661</td>
<td>Info</td>
<td>Rebuild Baseline Paused</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1662</td>
<td>Info</td>
<td>Rebuild Baseline Resumed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1663</td>
<td>Warning</td>
<td>Rebuild Baseline Failure</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1664</td>
<td>Warning</td>
<td>Rebuild Baseline Stalled</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1665</td>
<td>Info</td>
<td>Rebuild Baseline Completed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1666</td>
<td>Info</td>
<td>Scan for Integrity Started</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1667</td>
<td>Info</td>
<td>Scan for Integrity Paused</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1668</td>
<td>Info</td>
<td>Scan for Integrity Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1669</td>
<td>Warning</td>
<td>Scan for Integrity Failure</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1670</td>
<td>Warning</td>
<td>Scan for Integrity Stalled</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1671</td>
<td>Info</td>
<td>Scan for Integrity Completed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1675</td>
<td>Error</td>
<td>Integrity Monitoring Engine Offline</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>----------------</td>
</tr>
<tr>
<td>1676</td>
<td>Info</td>
<td>Integrity Monitoring Engine Back Online</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1677</td>
<td>Error</td>
<td>Trusted Platform Module Error</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1678</td>
<td>Info</td>
<td>Trusted Platform Module Register Values Loaded</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1679</td>
<td>Warning</td>
<td>Trusted Platform Module Register Values Changed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1680</td>
<td>Info</td>
<td>TPM Checking Disabled</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1700</td>
<td>Info</td>
<td>Expected Activation Failure</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1800</td>
<td>Error</td>
<td>Deep Security Protection Module Failure</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1900</td>
<td>Info</td>
<td>Cloud Provider Added</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1901</td>
<td>Info</td>
<td>Cloud Provider Removed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1902</td>
<td>Info</td>
<td>Cloud Provider Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1903</td>
<td>Info</td>
<td>Cloud Provider Synchronization In Progress</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1904</td>
<td>Info</td>
<td>Cloud Provider Synchronization Finished</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1905</td>
<td>Error</td>
<td>Cloud Provider Synchronization Failed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1906</td>
<td>Info</td>
<td>Cloud Provider Synchronization Requested</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Severity</td>
<td>Event</td>
<td>Record</td>
<td>Notify</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>1907</td>
<td>Info</td>
<td>Cloud provider Synchronization Cancelled</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1950</td>
<td>Info</td>
<td>Tenant Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1951</td>
<td>Info</td>
<td>Tenant Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1952</td>
<td>Info</td>
<td>Tenant Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1953</td>
<td>Info</td>
<td>Tenant Database Server Created</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1954</td>
<td>Info</td>
<td>Tenant Database Server Deleted</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1955</td>
<td>Info</td>
<td>Tenant Database Server Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>1957</td>
<td>Error</td>
<td>Tenant Initialization Failure</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>2000</td>
<td>Info</td>
<td>Scan Cache Configuration Object Added</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>2001</td>
<td>Info</td>
<td>Scan Cache Configuration Object Removed</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>2002</td>
<td>Info</td>
<td>Scan Cache Configuration Object Updated</td>
<td>On</td>
<td>On</td>
<td></td>
</tr>
</tbody>
</table>
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:

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):
This means that the setting is inherited from the parent **Base** Policy, and that if you were to change the Anti-Malware setting in the **Base** Policy from **Off** to **On**, the setting would change in the **Windows** Policy as well. (The **Windows** Policy setting would then read **Inherited (On)**. The value in parentheses always shows you what the current inherited setting is.)

**Overrides**

The **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**:
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:
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.

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:

![Overrides page screenshot]

Overrides are displayed by protection module. You can revert system or module overrides by clicking the Remove button.
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 (page 80).

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 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 522), FileSet (page 525), GroupSet (page 529),
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:
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:

```xml
<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:

```xml
base="C:\program files\CompanyName * Web Server"
```

but this is not:

```xml
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:
"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:

```xml
<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.

```xml
<include>
  <key pattern="**/*.exe"/>
  <key pattern="**/sample*"/>
</include>
```

The following is another way to express the same requirements:

```xml
<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.

```xml
<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:

```xml
<FileSet base="C:\Program Files\MySQL">
  <include key="**/*.exe"/>
  <include key="**/*.dll"/>
</FileSet>
```
Like the "include" tag, the "exclude" tag can be written to require multiple criteria. The following example shows a multi-criteria "exclude" tag.

```xml
<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:

```xml
<FileSet base="C:\Program Files\MySQL">
  <include key="**/*Sample*"/>
</FileSet>
```

In this example, only "Sample.txt" would be returned on Windows and Unix:

```xml
<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.
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/":
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:

```xml
<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:

```xml
<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:

```xml
<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":

```xml
<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:

```xml
<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":

```xml
<FileSet base="C:\Program Files\MySQL" >
  <attributes>
    <permissions/>
    <owner/>
</FileSet>
```
In the following example, the STANDARD set of attributes will be monitored. (See Shorthand Attributes, below)

```xml
<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.

```xml
<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:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>STANDARD</td>
<td>The set of attributes to monitor for the Entity Set. This is different than &quot;every possible attribute&quot; for the Entity Set. For example, it would not include every possible hash algorithm, just the ones deemed sufficient. For the list of &quot;standard&quot; attributes for each Entity Set, see sections for the individual Entity Sets.</td>
</tr>
<tr>
<td>CONTENTS</td>
<td>This is Shorthand for the hash, or set of hashes, of the contents of the file. Defaults to SHA-1.</td>
</tr>
</tbody>
</table>

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:

```xml
<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:

```xml
<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:

```xml
<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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Required</th>
<th>Default Value</th>
<th>Allowed Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>base</td>
<td>Sets the base directory of the DirectorySet. Everything else in the tag is relative to this directory</td>
<td>Yes</td>
<td>N/A</td>
<td>String values resolving to syntactically valid path (Path is not required to exist) <strong>Note:</strong> UNC paths are allowed by Windows Agents, but require that the remote system allow access by the &quot;LocalSystem&quot; 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\MACHINES. The access token presented to the remote computer also contains the &quot;Administrators&quot; 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 &quot;Everyone&quot;. For testing access to UNC paths, use <a href="#">this technique</a> to launch a Windows command prompt running as a service under the LocalSystem account. With that you can try accessing network &amp; 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.</td>
</tr>
<tr>
<td>onChange</td>
<td>Whether the directories returned should be monitored in real time.</td>
<td>No</td>
<td>false</td>
<td>true, false</td>
</tr>
<tr>
<td>followLinks</td>
<td>Will this DirectorySet follow symbolic links.</td>
<td>No</td>
<td>false</td>
<td>true, false</td>
</tr>
</tbody>
</table>
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 510) 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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Required</th>
<th>Default Value</th>
<th>Allowed Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>base</td>
<td>Sets the base directory of the FileSet. Everything else in the tag is relative to this directory.</td>
<td>Yes</td>
<td>N/A</td>
<td>String values resolving to syntactically valid path (Path is not required to exist). <strong>Note:</strong> UNC paths are allowed by Windows Agents, but require that the remote system allow access by the &quot;LocalSystem&quot; 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\MACHINES. The access token presented to the remote computer also contains the &quot;Administrators&quot; 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 &quot;Everyone&quot;. For testing access to UNC paths, use <a href="#">this technique</a> to launch a Windows command prompt running as a service under the LocalSystem account. With that you can try accessing network &amp; 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.</td>
</tr>
<tr>
<td>onChange</td>
<td>Whether the files returned should be monitored in real time.</td>
<td>No</td>
<td>false</td>
<td>true, false</td>
</tr>
<tr>
<td>followLinks</td>
<td>Will this FileSet follow symbolic links.</td>
<td>No</td>
<td>false</td>
<td>true, false</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Note:</th>
<th>To demonstrate this, type the following at the command prompt:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>echo plain &gt; sample.txt</td>
</tr>
<tr>
<td></td>
<td>echo alternate &gt; sample.txt:s</td>
</tr>
<tr>
<td></td>
<td>more &lt; sample.txt</td>
</tr>
<tr>
<td></td>
<td>more &lt; sample.txt:s</td>
</tr>
</tbody>
</table>

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:
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:5" />
<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 510)](page 510) 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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Required</th>
<th>Default Value</th>
<th>Allowed Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>onChange</td>
<td>Will be monitored in real time</td>
<td>No</td>
<td>false</td>
<td>true, false</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Required</th>
<th>Default Value</th>
<th>Allowed Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>onChange</td>
<td>Will be monitored in real time</td>
<td>No</td>
<td>false</td>
<td>true, false</td>
</tr>
</tbody>
</table>

 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.

```xml
<InstalledSoftwareSet>
  <include key="*
  </attributes/>
</InstalledSoftwareSet>
```

**Sub Elements**

- **Include**
- **Exclude**

See the *general description (page 510)* 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:

```xml
<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:

```xml
<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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Required</th>
<th>Default Value</th>
<th>Allowed Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>onChange</td>
<td>Will be monitored in real time</td>
<td>No</td>
<td>false</td>
<td>true, false</td>
</tr>
</tbody>
</table>

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:


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 510)* 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:

```xml
<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:

```xml
<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):

```xml
<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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Required</th>
<th>Default Value</th>
<th>Allowed Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>onChange</td>
<td>Will be monitored in real time</td>
<td>No</td>
<td>false</td>
<td>true, false</td>
</tr>
</tbody>
</table>

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 510) 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:

```xml
<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 wildcards 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 *":

```xml
<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:

```xml
<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:

```xml
<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):

```xml
<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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Required</th>
<th>Default Value</th>
<th>Allowed Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>base</td>
<td>Sets the base key of the RegistryKeySet. Everything else in the tag is</td>
<td>Yes</td>
<td>N/A</td>
<td>String values resolving to syntactically valid registry key path</td>
</tr>
<tr>
<td></td>
<td>relative to this key. The base must begin with one of the following registry</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>branch names:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HKEY_CLASSES_ROOT (or HKCR),</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HKEY_LOCAL_MACHINE (or HKLM),</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HKEY_USERS (or HKU),</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HKEY_CURRENT_CONFIG (or HKCC)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 510) 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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Required</th>
<th>Default Value</th>
<th>Allowed Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>base</td>
<td>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)</td>
<td>Yes</td>
<td>N/A</td>
<td>String values resolving to syntactically valid registry key</td>
</tr>
</tbody>
</table>

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](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".

<table>
<thead>
<tr>
<th>Value</th>
<th>Escaped Form</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>Hello</td>
<td>HKLM\Software\Sample\Hello</td>
</tr>
<tr>
<td>&quot;Quotes&quot;</td>
<td>&quot;Quotes&quot;</td>
<td>HKLM\Software\Sample&quot;Quotes&quot;</td>
</tr>
<tr>
<td>back\slash</td>
<td>back\slash</td>
<td>HKLM\Software\Sample\back\slash</td>
</tr>
<tr>
<td>trailing.</td>
<td>trailing.</td>
<td>HKLM\Software\Sample\trailing.</td>
</tr>
<tr>
<td>@</td>
<td>@</td>
<td>HKLM\Software\Sample@</td>
</tr>
</tbody>
</table>

**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.

Sub Elements

- Include
- Exclude
See the *general description (page 510)* 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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Required</th>
<th>Default Value</th>
<th>Allowed Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>onChange</td>
<td>Will be monitored in real time</td>
<td>No</td>
<td>false</td>
<td>true, false</td>
</tr>
</tbody>
</table>

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 510)* 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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Required</th>
<th>Default Value</th>
<th>Allowed Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>onChange</td>
<td>Will be monitored in real time</td>
<td>No</td>
<td>false</td>
<td>true, false</td>
</tr>
</tbody>
</table>

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):

```xml
<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):

```xml
<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":

```xml
<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".

```xml
```
<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 (WMI) 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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Required</th>
<th>Default Value</th>
<th>Allowed Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>namespace</td>
<td>Sets the namespace of the WMI query.</td>
<td>Yes</td>
<td>N/A</td>
<td>String values representing a valid WMI namespace. The &quot;root\cimv2&quot; namespace is the one most commonly used when querying Windows operating system objects, but others such as &quot;root\directory\LDAP&quot; and &quot;root\Microsoft\SqlServer\ComputerManagement&quot; can be used. See here for a small script called GetNamespaces.vbs that enumerates the available WMI namespaces on a given host.</td>
</tr>
<tr>
<td>wql</td>
<td>A WQL query string.</td>
<td>Yes</td>
<td>N/A</td>
<td>A valid WQL string. The query must include the __Path attribute for each return 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 &quot;SELECT * FROM ...&quot; the __Path attribute will be available, but if using a more selective query such as &quot;SELECT Name FROM ...&quot; you must explicitly include __Path by writing the query as &quot;SELECT __Path,Name FROM ...&quot;.</td>
</tr>
<tr>
<td>onChange</td>
<td>Whether the files returned should be monitored in real time.</td>
<td>No</td>
<td>false</td>
<td>true, false</td>
</tr>
<tr>
<td>provider</td>
<td>Optionally specifies an alternative WMI namespace</td>
<td>No</td>
<td>none</td>
<td>RsopLoggingModeProvider</td>
</tr>
</tbody>
</table>

Note:

Deep Security 9 SP1 Administrator's Guide
A WMI 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".

### 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:

### Table: WQLSet Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Required</th>
<th>Default Value</th>
<th>Allowed Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>provider</td>
<td>provider to use.</td>
<td>No</td>
<td></td>
<td>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=&quot;RsopLoggingModeProvider&quot; 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&quot;. Specify namespace=&quot;Computer&quot; to query &quot;\Root\Rsop\NS71EF4AA3_FB96_465F_AC1C_DFCF9A3E9010\Computer&quot;.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies a per-row timeout in milliseconds.</td>
<td>No</td>
<td>5000</td>
<td>1-60000</td>
</tr>
</tbody>
</table>
will return attributes such as:

- AdapterType
- AdapterTypeId
- Availability
- Caption
- ConfigManagerError Code
- ConfigManagerUserConfig
- CreationClassName
- Description
- DeviceID
- Index
- Installed
- MACAddress
- 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:

```xml
<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:

```plaintext
\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: /etc/init.d/ds_agent reset

To deactivate the Appliance:

- Log into vCenter using the vSphere Client.
- From the Virtual Agents tab, select the DSVA and view the console
- Login by pressing F2 and entering the DSVA 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`
Manually Upgrade the Agent on a Computer

The occasion may arise where you are not able to upgrade the Agent software on a computer from the Manager interface because of connectivity restrictions between the Manager computer and the Agent computer. In such cases, upgrading the Agent software on a Computer has to be performed manually.

The new Agent software has to be downloaded manually from the Trend Micro Download Center or it can be done through the Deep Security Manager and then exported.

---

**Note:** Agent Self-Protection must be disabled on computers that you want to upgrade. To configure Agent Self-Protection, go to Policy/Computer Editor > Settings > Computer > Agent Self-Protection.

---

To download and export the new Agent software:

1. In the Deep Security Manager, go to Administration > Updates > Software Updates.
2. Make sure the most recent Deep Security Agents have been downloaded to the Deep Security Manager from Trend Micro Download Center.
3. On the Software Updates tab, click View Imported Software... The Software window appears.
4. Select the required Agent software and click Export in the menu bar.
5. Specify the location to which you want to export the Agent software.

Windows

To manually upgrade the Agent on a Windows computer, copy the Agent installer to the computer and run it. It will detect the previous Agent and perform the upgrade.

Linux

To manually upgrade the Agent on a Linux computer:

1. Copy the Agent installer to the computer
2. Run the following command:
   
   ```
   rpm -U <new agent installer rpm>
   ```

   (The "-U" argument instructs the installer to perform an upgrade.)

Solaris

To manually upgrade the Agent on a Solaris computer:
1. Copy the Agent installer to the computer
2. Unzip the package using gunzip
3. Run the following command:
   
   pkgadd -v -a /opt/ds_agent/ds_agent.admin -d <new agent package>
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)
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.

**Note:**

Jobs by Node

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

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.

![Chart Image]

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 505).)

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 DSVA on a single ESX 4.0 Update 1 server (ESXi 4.1 for Anti-Malware support). 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:

\(<\text{number of VMs}> \times <512 \text{ Bytes}> \times <\text{number of connections (default 10000)>}\)

So for 32 VMs with 10000 connections:

\(32 \times 512\text{Bytes} \times 10000 = 163840000 \text{ Bytes}\)

And the command to set the value is:

% esxcfg-module -s DSAFILTER_HEAP_MAX_SIZE=163840000 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 ESX 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 ESX(i) and the DVSA to shutdown.
Ports Used by Deep Security

A number of ports must be accessible for the Deep Security Manager and the Agents/Appliances to function as expected. The following is a list of the ports used, the description of the function for which the port is used, the related protocols, the application which initializes the connection, the application to which the connection is made, whether the use of a proxy is possible (and what type of proxy), and whether and where the port can be configured:

**Deep Security Manager**

**Port: 4119 (default)**

- **Use:**
- **Protocol:** TCP
- **Initiated By:**
  - Web Browser
  - ESX 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.

ESX Server

Port: 443

- Use: the Deep Security Manager communicates with the ESX host on port 443 when you deploy an Virtual Appliance to the ESX
- Protocol: HTTPS
- Initiated by: Deep Security Manager
- Connected to: ESX server
- Proxy: No
- Configuration: No configuration required.
- Notes: The vCenter provides three URLs on the ESX 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 ESX.
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](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.
Support

Please visit the Trend Micro customer support Web site for assistance with any of your Trend micro Products:

Trend Micro Customer Support