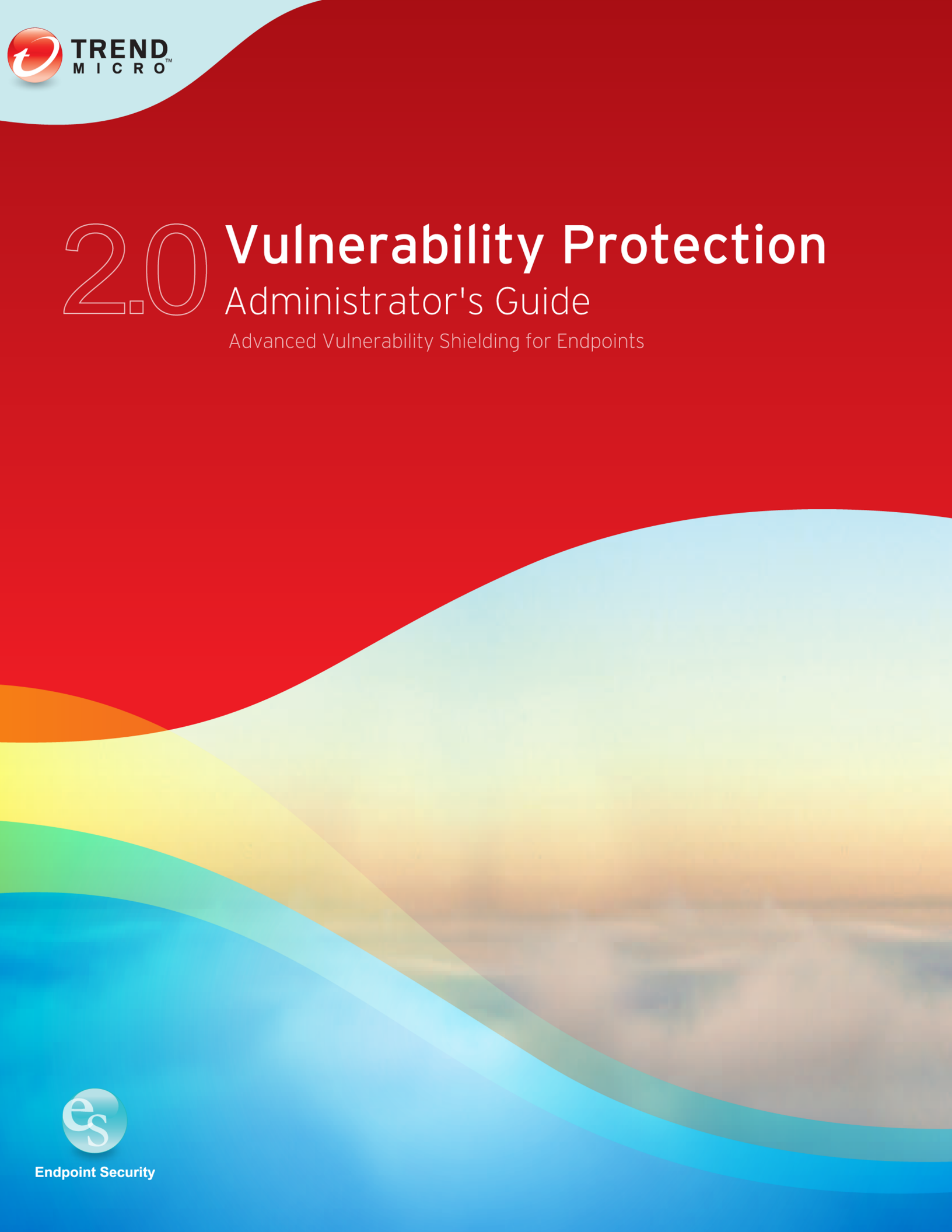
TREND MICRO™

2.0 Vulnerability Protection

Administrator's Guide

Advanced Vulnerability Shielding for Endpoints



Endpoint Security

Document version: 1.0
Document number: APEM26309/140218
Release date: April 2014
Document generated: May 8, 2014 (22:01:57)

Table of Contents

Introduction

This Introduction describes the main features and basic system requirements of Vulnerability Protection.

- **Overview:** A brief ***overview (page 6)*** of Trend Micro Vulnerability Protection.
- **System Requirements:** A basic overview of the Vulnerability Protection ***system requirements (page 7)*** and supported platforms. For more detailed information, see the Installation Guide.
- **Features:** A description of the major ***components and Protection Modules (page 8)*** that comprise the Vulnerability Protection system.

Overview

Trend Micro Vulnerability Protection provides advanced vulnerability shielding against zero-day threats and blocks exploits before a patch can even be deployed. Vulnerability Protection is a standalone product replacement for the Intrusion Defense Firewall (OfficeScan module) and works in conjunction with other complete user protection solutions including Control Manager for central management. Vulnerability Protection provides agent-based protection for your computers.

Protection includes:

- Firewall
- Intrusion Detection and Prevention

System Requirements

Vulnerability Protection

- **Memory:** 4GB (8GB recommended)
- **Disk Space:** 1.5GB (5GB recommended)

> *Note: Trend Micro recommends allocating 13 GB of disk space when installing Vulnerability Protection Manager with the embedded Microsoft SQL Server Express database.*

- **Operating System:**
  - Microsoft Windows 2012 R2 (64-bit)
  - Microsoft Windows 2012 (64-bit)
  - Windows Server 2008 R2 (64-bit)
  - Windows Server 2008 (32 and 64-bit)
  - Windows 2003 Server SP2 (32 and 64-bit)
  - Windows 2003 Server R2 SP2 (32 and 64-bit)
- **Database:**
  - Oracle 11g
  - Oracle 10g
  - Microsoft SQL Server 2012 (All Service Packs)
  - Microsoft SQL Server 2008 (All Service Packs)
  - Microsoft SQL Express 2008 R2 SP2 embedded

> *Note: Microsoft SQL Express 2008 R2 SP2 is supported with .NET Framework 2.0 SP2 and Windows installer 4.5. On Windows 2008 and above, use .NET Framework 3.5 SP1.*

- **Web Browser:** Firefox 12+, Internet Explorer 9.x, Internet Explorer 10.x, Internet Explorer 11.x, Chrome 20+. (Cookies must be enabled in all browsers.)

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

Vulnerability Protection Agent

- **Memory:** 128MB
- **Disk Space:** 500MB
- **Supported Platforms:** Windows

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

Product Features

Vulnerability Protection provides advanced server security for your computers. 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. The following tightly integrated modules easily expand the platform to ensure server, application, and data security across your computers.

Protection Modules

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 servers.

Centralizes management of server firewall policy using a bidirectional stateful firewall. 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.

Vulnerability Protection Components

Vulnerability Protection consists of the following set of components that work together to provide protection:

- **Vulnerability Protection Manager**, the centralized Web-based management console which administrators use to configure security policy and deploy protection to the Vulnerability Protection Agent, which is the enforcement component.

- **Vulnerability Protection Agent** is a security agent deployed directly on a computer which can provide Intrusion Prevention, Firewall, Web Application Protection, and Application Control.

Vulnerability Protection Manager

Vulnerability Protection 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. Vulnerability Protection Manager integrates with different aspects of the datacenter including 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.

Vulnerability Protection Agent

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

User's Guide

The User's Guide describes how to configure and manage the components of Vulnerability Protection from the system in general to configuration of the individual protection modules.

- **Quick Start: System Configuration:** A guide to configuring the basic Vulnerability Protection ***system settings (page 12)*** from from enabling regular automatic Security Updates to setting up email notifications.
- **Quick Start: Protecting a Computer:** A guide to ***protecting a standard Windows computer (page 14)*** with Vulnerability Protection.
- **System:** Describes the functionality and configuration of Vulnerability Protection system settings:
    - ***Communication (page 21)*** describes how the different Vulnerability Protection components communicate with each other.
    - ***Customize the Dashboard (page 23)*** describes how to create and save customized dashboard layouts.
    - ***Event Logging and Data Collection (page 26)*** describes how Vulnerability Protectioncollects events from the Agents.
    - ***Email Notifications (page 27)*** describes how to configure Vulnerability Protection to send email notifications of important Vulnerability Protection Events to various users.
    - ***Alerts (page 29)*** describes how to configure which Events will raise Alerts, what the severity of those Alerts will be, and whether to send email notifications of the Alerts.
    - ***Syslog Integration (SIEM) (page 31)*** describes how to configure Vulnerability Protection to send Events to a SIEM via Syslog.
    - ***Security Updates (page 39)*** describes how to manage Vulnerability Protection Security Updates.
    - ***User Management (page 40)*** describes how to manage Users of Vulnerability Protection including how to use role-based access control to restrict the access of Users specific areas of Vulnerability Protection and your network.
    - ***Database Backup and Recovery (page 46)*** describes how to perform (and automate) a backup of your Vulnerability Protection data.
- **Adding Computers:** To protect computers with Vulnerability Protection, they must first be added to the **Computers** list in the Vulnerability Protection Manager. New computers can be added to your Computers List by:
    - ***Importing computers from a local network (page 50)*** 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 Vulnerability Protection Manager.
    - ***Importing a Directory (page 52)*** You can import a Microsoft Active Directory or any other LDAP-based directory service.
    - ***Using a deployment script (page 56)*** 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 Vulnerability Protection 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 ***Vulnerability Protection Agent (page 58)***.
- **Protection Modules:** Describes configuration of the Vulnerability Protection protection modules.
  - The ***Firewall (page 61)*** is a bidirectional, stateful firewall that is responsible for making sure that packets originating from unauthorized sources do not reach the applications on its host.
  - The ***Intrusion Prevention (page 73)*** 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.
- **SSL Data Streams:** How to configure filtering of ***SSL traffic (page 78)***.
- **Events, Alerts, and Reports:** The functionality and configuration of Vulnerability Protection ***Events, Alerts, and Reports (page 81)***.
- **Protecting a Mobile Laptop:** How to ***protect a mobile laptop (page 87)***, with information about using the location awareness of Vulnerability Protection.
- **Load Balancers:** How to ***use a load balancer (page 97)*** with Vulnerability Protection.

Quick Start: System Configuration

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

To complete basic Vulnerability Protection system configuration, you will need to:

1. Configure Vulnerability Protection's ability to retrieve Updates from Trend Micro
2. Check that you have a Scheduled Task to perform regular Updates
3. Set up email notification of important events

Configure Vulnerability Protection's ability to retrieve Updates from Trend Micro

Next, check that you can retrieve updates from Trend Micro.

Go to the **Administration > Updates > Security Updates** tab and click the **Download Security Updates ...** button.

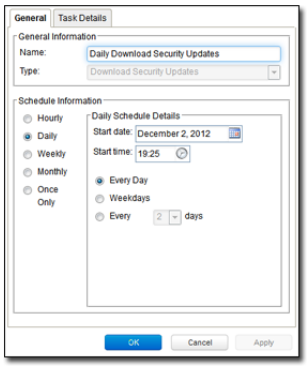
This will display the **Security Update** Wizard which contacts the Trend Micro Update Servers and downloads the latest Security Updates and distributes them to your computers. If upon completion the wizard displays the success message it means your can communicate with the Update servers:

Check that you have a Scheduled Task to perform regular Updates

Next, 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

Vulnerability Protection Alerts are raised when situations occur that require special attention. Alerts can be raised due to security Events such as an abnormal restart on a protected computer, or they can be system events like the Vulnerability Protection Manager running low on disk space. Vulnerability Protection 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 Vulnerability Protection Alerts.

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

Now you need to configure your User account to receive the email notifications Vulnerability Protection 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 Vulnerability Protection 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 Vulnerability Protection 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.

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

Basic Configuration is complete

This completes the basic Vulnerability Protection system configuration. Vulnerability Protection 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 Vulnerability Protection protection to your computers. See ***QuickStart: Protecting a Computer (page 14)*** or ***Protecting a Mobile Laptop (page 87)*** for a quick guide to protecting those two kinds of computer resources.

Quick Start: Protecting a Computer

The following describes the steps involved in using Vulnerability Protection to protect a Windows 7 Desktop computer.

It will involve the following steps:

1. Adding the computer to the Vulnerability Protection 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 Vulnerability Protection Manager

---

Note: *We will assume that you have already installed the Vulnerability Protection Manager on the computer from which you intend to manage the Vulnerability Protection Agents throughout your network. We will also assume that* ***you have installed (but not activated) Vulnerability Protection Agent on the computer you wish to protect****. 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 Vulnerability Protection Manager

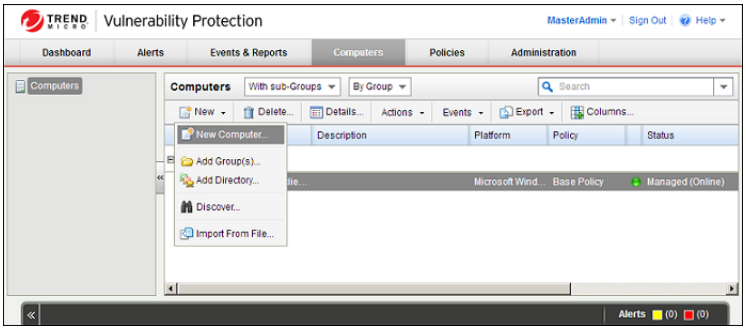
There are several ways of adding computers to the Vulnerability Protection Manager's **Computers** page. You can add computers by:

- Adding computers individually from a local network by specifying their IP addresses or hostnames
- Discovering computers on a local network by scanning the network

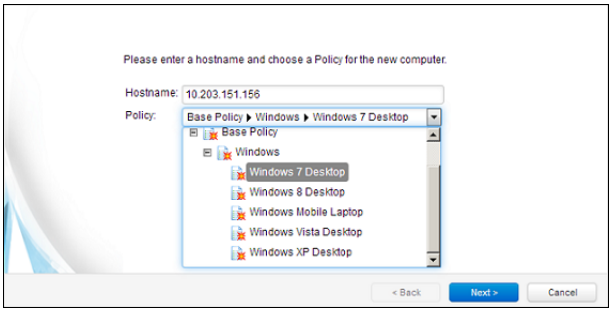
For the purposes of this exercise, we will add a computer from a local network but once a computer is added to the Manager, the protection procedures are the same regardless of where the computer is located.

To add a computer from a local network:

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



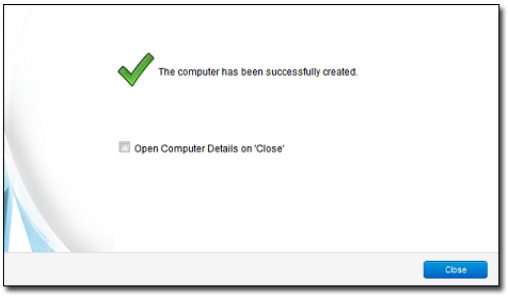
2. In the **New Computer** wizard, enter the hostname or IP address of the computer and select an appropriate security Policy to apply from the Policy tree in the drop-down menu. (In this case we will select the **Windows 7 Desktop** Policy.) Click **Next**.



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**.

> *Note: An Agent can be configured to automatically initiate its own activation upon installation. For details, see* ***Command-Line Instructions (page 101)****.*

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



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

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

Vulnerability Protection will automatically download the latest Security Updates to the computer after activation.

Once Vulnerability Protection 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 Vulnerability Protection 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 Desktop 7 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 Vulnerability Protection protection module updates to see if the current security Policy needs to be updated.

Recommendation Scans make recommendations for the Intrusion Prevention module.

To run a Recommendation Scan on your computer:

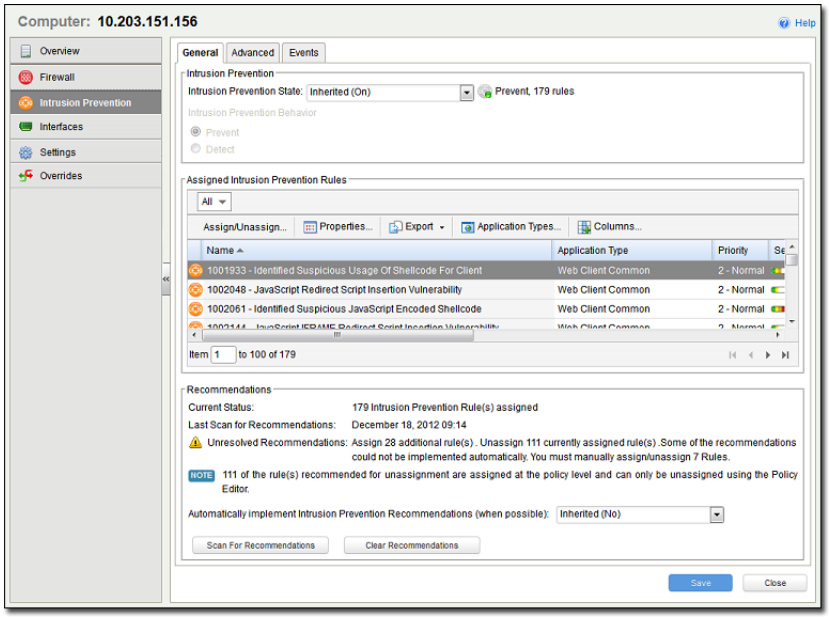
1. Go to the Computers page in the mainVulnerability Protection Manager console window.
2. Right-click on your computer and select **Actions > Scan for Recommendations**.

During the Recommendation Scan, your computer's Status will display **Scanning for Recommendations**. When the scan is finished, if Vulnerability Protection 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.



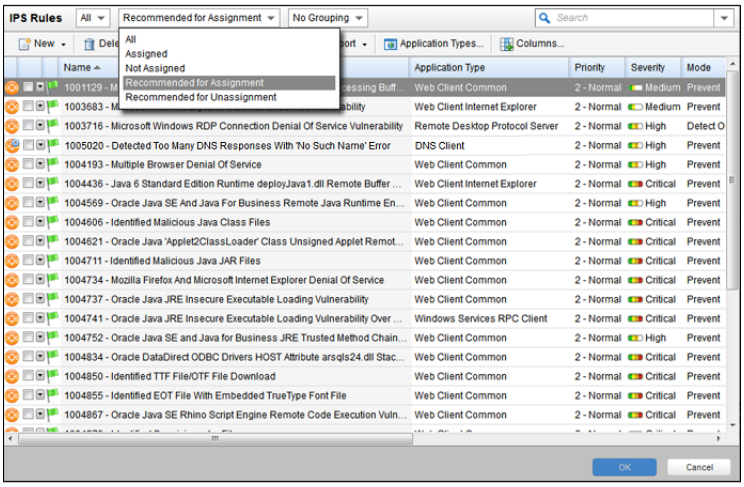
The **Current Status** tells us that there are currently 179 Intrusion Prevention Rules assigned to this computer.

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, Vulnerability Protection 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 7 Desktop Policy. (If we had opened the **Windows 7 Desktop** 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 list. To unassign a Rule, deselect the checkbox next to its name.

Note: *Rules that are in effect on a computer because they have been assigned in a Policy higher up the policy tree can't be unassigned locally. The only way to unassign such Rules is to edit the Policy where they were originally assigned and unassign them from there. For more information on this kind of Rule inheritance, see* ***Policies, Inheritance and Overrides (page 150)****.*

Automatically implement scan recommendations

You can configure Vulnerability Protection to automatically assign and unassign Rules after a Recommendation Scan. To do so, open the computer or Policy editor and go to **Intrusion Prevention**. In the Recommendations area on the General tab, set **Automatically implement Intrusion Prevention Recommendations (when possible):** to Yes.

Create a Scheduled task to perform regular Recommendation Scans

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

To create a Scheduled Task:

1. In the main Vulnerability Protection 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 7 Desktop 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, Vulnerability Protection 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 12)***, your computer will now be regularly updated with the latest protection from Trend Micro.

Monitor Activity Using the Vulnerability Protection 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 Vulnerability Protection 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.

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 Vulnerability Protection Manager to Users, by logging into the system and consulting the dashboard, by performing detailed investigations by drilling-down to specific logs, and by configuring Alerts to notify Users of critical events, you can remain apprised of the health and status of your network.

System

- ***Communication (page 21)*** describes how the different Vulnerability Protection components communicate with each other.
- ***Customize the Dashboard (page 23)*** describes how to create custom dashboard layout for yourself or other Users.
- ***Events, Alerts, and Reports (page 81)*** describes how to stay abreast of Vulnerability Protection events by monitoring Events, configuring and generating Alerts, and producing periodic customized Reports.
- ***Set Up Email Alerts (page 27)*** describes how to configure Vulnerability Protection to send email notifications of important Vulnerability Protection Events to various users.
- ***Alerts (page 29)*** 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.
- ***Syslog Integration (SIEM) (page 31)*** describes how to configure Vulnerability Protection to send Events to a SIEM via Syslog.
- ***Security Updates (page 39)*** describes how to manage Vulnerability Protection Security Updates.
- ***User Management (page 40)*** describes how to manage Users of Vulnerability Protection including how to use role-based access control to restrict the access of Users specific areas of Vulnerability Protection and your network.
- ***Database Backup and Recovery (page 46)*** describes how to perform (and automate) a backup of your Vulnerability Protection data.

Communication

Who Initiates Communication

At the default setting (**Bidirectional**), the Agent will initiate the heartbeat but will still listen on the Agent port for Manager connections and the Manager is free to contact the Agent 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 itself periodically check for updates and control heartbeat operations. If this is the case, select **Agent Initiated** .

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

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

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

To configure Communication Direction in a Policy:

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

To configure Communication Direction on a specific computer:

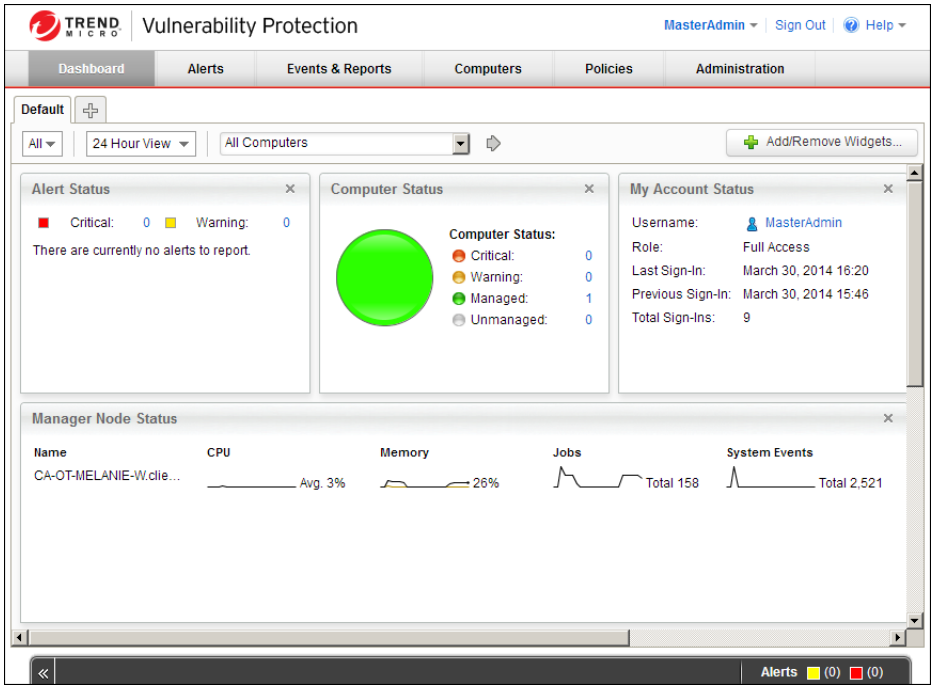
1. Open the Computer Editor(the **Details** window) of the computer whose communications settings you want to configure.
2. Go to **Settings > Computer > Communication Direction.**
3. In the "Direction of Vulnerability Protection Manager to Agent communication: "drop-down menu, select one of the three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

4. Click **Save** to apply the changes.

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

Customize the Dashboard

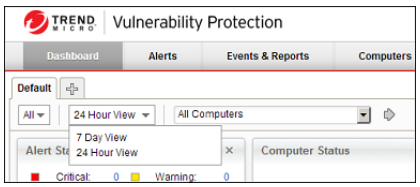
The Dashboard is the first page that comes up after you sign in to the Vulnerability Protection Manager. Several aspects of the dashboard can be configured and customized, and layouts can be saved and displayed when you sign in. (The dashboard will be displayed as you left it when you logged out, regardless 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.

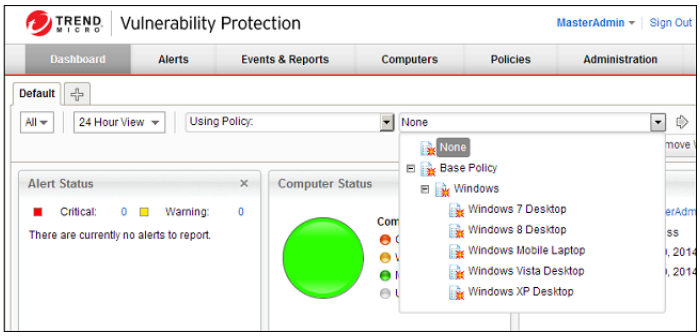
Date/Time Range

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



Computers and Computer Groups

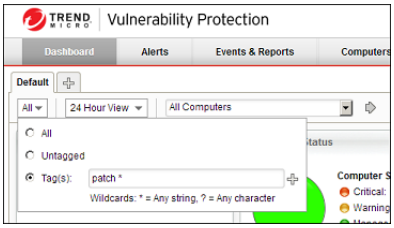
Use the **Computer:** drop-down menu to filter the displayed data to display only data from specific computers.



Filter by Tags

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

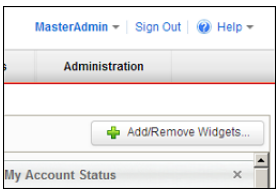
The data displayed in the Dashboard can be filtered by tags:



For more information on tagging see ***Event Tagging (page 85)***.

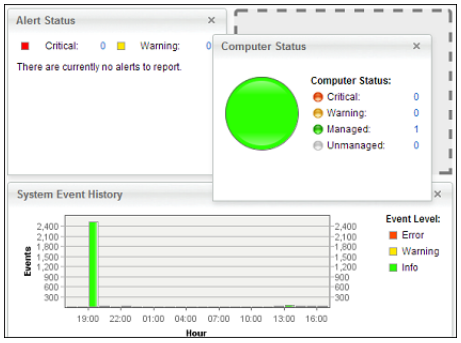
Select Dashboard Widgets

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



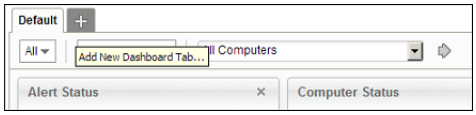
Changing the Layout

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:



Event Logging and Data Collection

By default, Vulnerability Protection Manager collects Events from the Agents 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 Vulnerability Protection 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, Vulnerability Protection 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 Vulnerability Protection 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.**

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

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

Email Notifications

Vulnerability Protection Manager can send emails to specific Users when selected Alerts are triggered. To enable the email system, you must give Vulnerability Protection 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 and the Manager can be instructed to forward Events to a SIEM system. The Agent 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 Vulnerability Protection Manager.

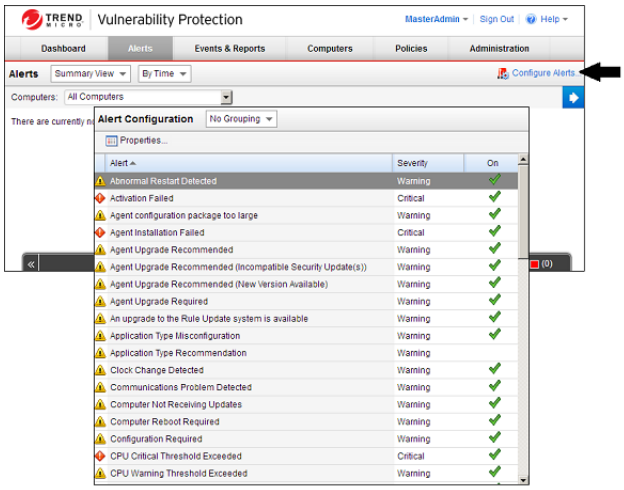
Protection module security Events can be forwarded from the Agents via Syslog. To configure the Protection module security Events Syslog settings, go to the **Policy/Computer Editor > Settings > SIEM** tab.

For information on configuring Syslog, see ***Syslog Integration (SIEM) (page 31)***.

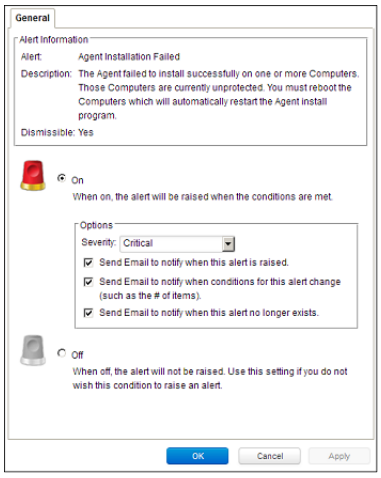
Alerts

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.



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

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

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

Note:	*For the emails to be sent, you must configure the SMTP settings on the **Administration > System Settings > SMTP** tab.*

Syslog Integration (SIEM)

Vulnerability Protection 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 Vulnerability Protection 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 Vulnerability Protection Agents.

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 Vulnerability Protection Manager logs to VPM.log`
    - `Local4.* /var/log/VPM.log`
5. Save the file and exit
6. Create the `/var/log/VPM.log` file by typing `touch /var/log/VPM.log`
7. Set the permissions on the VPM 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/VPM.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 Vulnerability Protection Agents.

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 Vulnerability Protection Manager logs to VPM.log`
    - `Local4.* /var/log/VPM.log`
4. Save the file and exit
5. Create the `/var/log/VPM.log` file by typing `touch /var/log/VPM.log`
6. Set the permissions on the VPM 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/VPM.log`

Vulnerability Protection Manager Settings

You can configure Vulnerability Protection 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 Vulnerability Protection 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. The second option (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 "Vulnerability Protection 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 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 Vulnerability Protection Manager or a Vulnerability Protection Agent, look at the "Device Product" field:

Sample Log Entry: Jan 18 11:07:53 vpmhost CEF:0|Trend Micro|**Vulnerability Protection Manager**|2.0|600|Administrator Signed In|4|suser=Master...

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|Vulnerability Protection Agent|2.0|**123**|**Out Of Allowed Policy**|5|cn1=1...

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

Signature IDs	Description
10	Custom Intrusion Prevention Rule
20	Log-Only Firewall Rule
21	Deny Firewall Rule
100-299	Out of "Allowed" Policy Firewall Rule
300-399	SSL Events
500-899	Firewall Stateful Configuration Events
1,000,000-1,999,999	Trend Micro Intrusion Prevention Rule

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|Vulnerability Protection Agent|2.0|20|Log for TCP Port 80|0|cn1=1 cn1Label=Host ID dvc=hostname act=Log dmac=00:50:56:F5:7F:47 smac=00:0C:29:EB:35:DE TrendMicroDsFrameType=IP src=192.168.126.150 dst=72.14.204.147 out=1019 cs3=DF 0 cs3Label=Fragmentation Bits proto=TCP spt=49617 dpt=80 cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=1 TrendMicroDsPacketData=AFB...

Extension Field	Name	Description	Examples
act	Action	The action taken by the Firewall rule. Can contain: Log or Deny. If the rule or the network engine is operating in tap mode, the action value will be proceeded by "IDS:".	act=Log act=Deny
cn1	Host Identifier	The Agent Computer internal identifier which can be used to uniquely identify the Agent Computer from a given syslog event.	cn1=113
cn1Label	Host ID	The friendly name label for the field cn1.	cn1Label=Host ID
cnt	Repeat Count	The number of times this event was sequentially repeated.	cnt=8
cs2	TCP Flags	(For the TCP protocol only) The raw TCP flag byte followed by the URG, ACK, PSH, RST, SYN and FIN fields may be present if the TCP header was set. If "Relay via Manager" is selected, the output of this extension contains only the flag names.	cs2=0x10 ACK cs2=0x14 ACK RST
cs2Label	TCP Flags	The friendly name label for the field cs2.	cs2Label=TCP Flags
cs3	Packet Fragmentation Information	The "DF" field will be present if the IP "Don't Fragment" bit is set. The "MF" field will be present if the "IP More Fragments" bit is set.	cs3=MF cs3=DF MF
cs3Label	Fragmentation Bits	The friendly name label for the field cs3.	cs3Label=Fragmentation Bits
cs4	ICMP Type and Code	(For the ICMP protocol only) The ICMP type and code stored in their respective order delimited by a space.	cs4=11 0 cs4=8 0
cs4Label	ICMP	The friendly name label for the field cs4.	cs4Label=ICMP Type and Code

Extension Field	Name	Description	Examples
dmac	Destination MAC Address	Destination computer network interface MAC address.	dmac= 00:0C:29:2F:09:B3
dpt	Destination Port	(For TCP and UDP protocol only) Destination computer connection port.	dpt=80 dpt=135
dst	Destination IP Address	Destination computer IP Address.	dst=192.168.1.102 dst=10.30.128.2
in	Inbound Bytes Read	(For inbound connections only) Number of inbound bytes read.	in=137 in=21
out	Outbound Bytes Read	(For outbound connections only) Number of outbound bytes read.	out=216 out=13
proto	Transport protocol	Name of the connection transportation protocol used.	proto=tcp proto=udp proto=icmp
smac	Source MAC Address	Source computer network interface MAC address.	smac= 00:0E:04:2C:02:B3
spt	Source Port	(For TCP and UDP protocol only) Source computer connection port.	spt=1032 spt=443
src	Source IP Address	Source computer IP Address.	src=192.168.1.105 src=10.10.251.231
TrendMicroDsFrameType	Ethernet frame type	Connection Ethernet frame type.	TrendMicroDsFrameType=IP TrendMicroDsFrameType=ARP TrendMicroDsFrameType=RevARP TrendMicroDsFrameType=NetBEUI
TrendMicroDsPacketData	Packet data	(If include packet data is set) A Base64 encoded copy of the packet data. The "equals" character is escaped. E.g. "\=" This extension is not included when the "Relay via the Manager" option is selected.	TrendMicroDsPacketData=AA...BA\=

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|Vulnerability Protection Agent|2.0|1001111|Test Intrusion Prevention Rule|3|cn1=1 cn1Label=Host ID dvchost=hostname dmac=00:50:56:F5:7F:47 smac=00:0C:29:EB:35:DE TrendMicroDsFrameType=IP src=192.168.126.150 dst=72.14.204.105 out=1093 cs3=DF 0 cs3Label=Fragmentation Bits proto=TCP spt=49786 dpt=80 cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=1 act=IDS:Reset cn3=10 cn3Label=Intrusion Prevention Packet Position cs5=10 cs5Label=Intrusion Prevention Stream Position cs6=8 cs6Label=Intrusion Prevention Flags TrendMicroDsPacketData=R0VUIC9zP3...

Extension Field	Name	Description	Examples
act	Action	The action taken by the Intrusion Prevention rule. Can contain: Block, Reset, or Log. If the rule or the network engine is operating in detect-only mode, the action value will be	act=Block

Extension Field	Name	Description	Examples
		preceded by "IDS:". (IPS Rules written before Vulnerability Protection version 7.5 SP1 could additionally perform Insert, Replace, and Delete actions. These actions are no longer performed. If an older IPS Rule is triggered which still attempts to perform those actions, the Event will indicate that the Rule was applied in detect-only mode.)	
cn1	Host Identifier	The Agent Computer internal identifier which can be used to uniquely identify the Agent Computer from a given syslog event.	cn1=113
cn1Label	Host ID	The friendly name label for the field cn1.	cn1Label=Host ID
cn3	Intrusion Prevention Packet Position	Position within packet of data that triggered the event.	cn3=37
cn3Label	Intrusion Prevention Packet Position	The friendly name label for the field cn3.	cn3Label=Intrusion Prevention Packet Position
cnt	Repeat Count	The number of times this event was sequentially repeated.	cnt=8
cs1	Intrusion Prevention Filter Note	(Optional) A note field which can contain a short binary or text note associated with the payload file. If the value of the note field is all printable ASCII characters, it will be logged as text with spaces converted to underscores. If it contains binary data, it will be logged using Base-64 encoding.	cs1=Drop_data
cs1Label	Intrusion Prevention Note	The friendly name label for the field cs1.	cs1Label=Intrusion Prevention Note
cs2	TCP Flags	(For the TCP protocol only) The raw TCP flag byte followed by the URG, ACK, PSH, RST, SYN and FIN fields may be present if the TCP header was set.	cs2=0x10 ACK cs2=0x14 ACK RST
cs2Label	TCP Flags	The friendly name label for the field cs2.	cs2Label=TCP Flags
cs3	Packet Fragmentation Information	The "DF" field will be present if the IP "Don't Fragment" bit is set. The "MF" field will be present if the "IP Mote Fragments" bit is set.	cs3=MF cs3=DF MF
cs3Label	Fragmentation Bits	The friendly name label for the field cs3.	cs3Label=Fragmentation Bits
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

Extension Field	Name	Description	Examples
cs5	Intrusion Prevention Stream Position	Position within stream of data that triggered the event.	cs5=128 cs5=20
cs5Label	Intrusion Prevention Stream Position	The friendly name label for the field cs5.	cs5Label=Intrusion Prevention Stream Position
cs6	Intrusion Prevention Filter Flags	A combined value that includes the sum of the following flag values: 1 - Data truncated - Data could not be logged. 2 - Log Overflow - Log overflowed after this log. 4 - Suppressed - Logs threshold suppressed after this log. 8 - Have Data - Contains packet data 16 - Reference Data - References previously logged data.	The following example would be a summed combination of 1 (Data truncated) and 8 (Have Data): cs6=9
cs6Label	Intrusion Prevention Flags	The friendly name label for the field cs6.	cs6=Intrusion Prevention Filter Flags
dmac	Destination MAC Address	Destination computer network interface MAC address.	dmac= 00:0C:29:2F:09:B3
dpt	Destination Port	(For TCP and UDP protocol only) Destination computer connection port.	dpt=80 dpt=135
dst	Destination IP Address	Destination computer IP Address.	dst=192.168.1.102 dst=10.30.128.2
in	Inbound Bytes Read	(For inbound connections only) Number of inbound bytes read.	in=137 in=21
out	Outbound Bytes Read	(For outbound connections only) Number of outbound bytes read.	out=216 out=13
proto	Transport protocol	Name of the connection transportation protocol used.	proto=tcp proto=udp proto=icmp
Smac	Source MAC Address	Source computer network interface MAC address.	smac= 00:0E:04:2C:02:B3
Spt	Source Port	(For TCP and UDP protocol only) Source computer connection port.	spt=1032 spt=443
Src	Source IP Address	Source computer IP Address.	src=192.168.1.105 src=10.10.251.231
TrendMicroDsFrameType	Ethernet frame type	Connection Ethernet frame type.	TrendMicroDsFrameType=IP TrendMicroDsFrameType=ARP TrendMicroDsFrameType=RevARP TrendMicroDsFrameType=NetBEUI

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

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|Vulnerability Protection Manager|2.0|600|User Signed In|3|src=10.52.116.160 suser=admin target=admin msg=User signed in from fe80:0:0:0:2d02:9870:beaa:fd41

Extension Field	Name	Description	Examples
src	Source IP Address	Source Vulnerability Protection Manager IP Address.	src=10.52.116.23
suser	Source User	Source Vulnerability Protection Manager user account.	suser=MasterAdmin
target	Target entity	The event target entity. The target of the event maybe the administrator account logged into Vulnerability Protection Manager, or a Computer.	target=MasterAdmin target=server01
msg	Details	Details of the System event. May contain a verbose description of the event.	msg=User password incorrect for username MasterAdmin on an attempt to sign in from 127.0.0.1 msg=A Scan for Recommendations on computer (localhost) has completed...

Security Updates

Vulnerability Protection periodically needs to be updated with the latest Security and Software Updates. The update packages are retrieved from Trend Micro in the form of **Security Updates**.

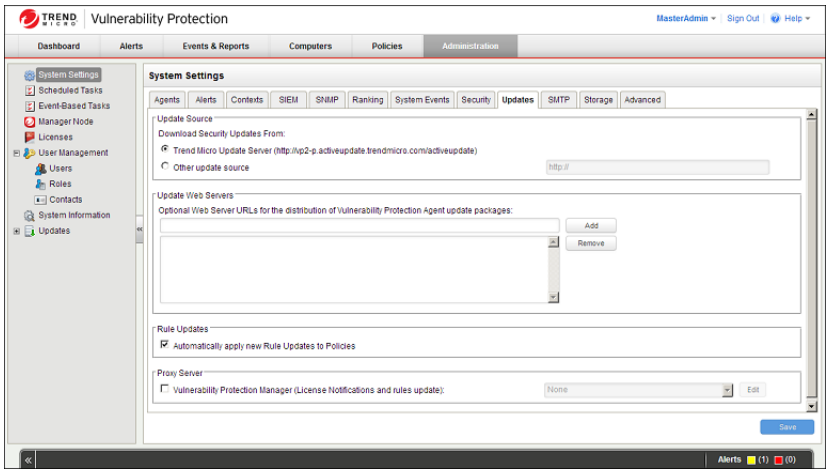
Security Updates

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

To configure Security Updates, you will need to configure your Security Update source.

Configure your Security Update Source

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



User Management

Vulnerability Protection has **Users**, **Roles**, and **Contacts**.

A **User** is a Vulnerability Protection account holder who can sign in to the Vulnerability Protection 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 Vulnerability Protection Manager. **Contacts** do not have a User account and cannot sign in to Vulnerability Protection Manager but they can be designated as the recipients of email notifications and scheduled Reports.

Note: Although Contacts cannot sign in to Vulnerability Protection 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

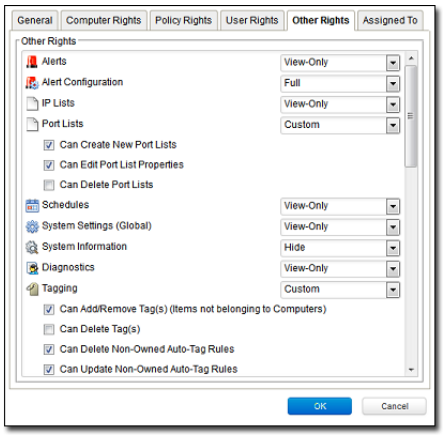
Access rights and editing privileges are attached to Roles and not to Users. To change the access rights and editing privileges of an individual User, the User must be assigned a different Role, or the Role itself must be edited.

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.

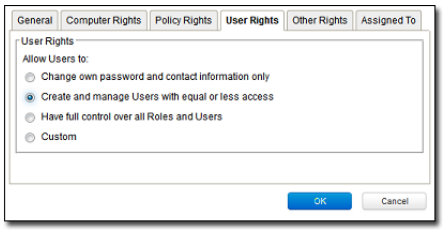
Role-Based Editing Privileges

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.

RIGHTS	**SETTINGS BY ROLE**		
General	**Full Access Role**	**Auditor Role**	**New Role Defaults**
Access to VPM User Interface	Allowed	Allowed	Allowed
Access to Web Service API	Allowed	Allowed	Not allowed
Computer Rights	Full Access Role	Auditor Role	New Role Defaults
View	Allowed, All Computers	Allowed, All Computers	Allowed, All Computers
Edit	Allowed, All Computers	Not allowed, All Computers	Not allowed, All Computers
Delete	Allowed, All Computers	Not allowed, All Computers	Not allowed, All Computers
Dismiss Alerts for	Allowed, All Computers	Not allowed, All Computers	Not allowed, All Computers
Tag Items for	Allowed, All Computers	Not allowed,	Not allowed,

RIGHTS	SETTINGS BY ROLE		
		All Computers	All Computers
View non-selected computers and data (e.g. events, reports)	Allowed	Allowed	Allowed, All Computers
View events and Alerts not related to computers	Allowed	Allowed	Allowed, All Computers
Create new computers in selected groups	Allowed	Not allowed	Not allowed
Add or remove sub-groups in selected groups	Allowed	Not Allowed	Not allowed
Import computer files	Allowed	Not allowed	Not allowed
Add, remove, and synchronize Directories	Allowed	Not allowed	Not allowed
Policy Rights	Full Access Role	Auditor Role	New Role Defaults
View	Allowed, All Policies	Allowed, All Policies	Allowed, All Policies
Edit	Allowed, All Policies	Not allowed, All Policies	Not allowed, All Policies
Delete	Allowed, All Policies	Not allowed, All Policies	Not allowed, All Policies
View non-selected Policies	Allowed	Allowed	Allowed
Create new Policies	Allowed	Not allowed	Not allowed
Import Policies	Allowed	Not allowed	Not allowed
User Rights (See note on User rights below)	Full Access Role	Auditor Role	New Role Defaults
View Users	Allowed	Allowed	Not allowed
Create Users	Allowed	Not allowed	Not allowed
Edit User Properties	Allowed	Not allowed	Not allowed
Delete Users	Allowed	Not allowed	Not allowed

RIGHTS	SETTINGS BY ROLE		
View Roles	Allowed	Allowed	Not allowed
Create Roles	Allowed	Not allowed	Not allowed
Edit Role Properties	Allowed	Not allowed	Not allowed
Delete Roles	Allowed	Not allowed	Not allowed
Delegate Authority			
Other Rights	Full Access Role	Auditor Role	New Role Defaults
Alerts	Full (Can Dismiss Global Alerts)	View-Only	View-Only
Alert Configuration	Full (Can Edit Alert Configurations)	View-Only	View-Only
Firewall Rules	Full (Can Create, Edit, Delete Firewall Rules)	View-Only	View-Only
Firewall Stateful Configurations	Full (Can Create, Edit, Delete Firewall Stateful Configurations)	View-Only	View-Only
Intrusion Prevention Rules	Full (Can Create, Edit, Delete)	View-Only	View-Only
Application Types	Full (Can Create, Edit, Delete)	View-Only	View-Only
IP Lists	Full (Can Create, Edit, Delete)	View-Only	View-Only
MAC Lists	Full (Can Create, Edit, Delete)	View-Only	View-Only
Port Lists	Full (Can Create, Edit, Delete)	View-Only	View-Only
Contexts	Full (Can Create, Edit, Delete)	View-Only	View-Only
Schedules	Full (Can Create, Edit, Delete)	View-Only	View-Only
System Settings (Global)	Full (Can View, Edit System Settings (Global))	View-Only	Hide
System Information	Full (Can View System Information, Can Edit and Decommission Manager Nodes, Can Manage System Extensions)	View-Only	Hide
Diagnostics	Full (Can Create Diagnostic Packages)	View-Only	View-Only
Tagging (Advanced)	Full (Can Tag (Items not belonging to Computers), Can Delete Tags, Can Update Non-Owned Auto-Tag Rules, Can Run Non-Owned Auto-Tag Rules, Can Delete Non-Owned Auto-Tag Rules)	View-Only	View-Only
Tasks	Full (Can View, Add, Edit, Delete Tasks, Execute Tasks)	View-Only	Hide
Contacts	Full (Can View, Create, Edit, Delete Contacts)	View-Only	Hide
Licenses	Full (Can View, Change License)	View-Only	Hide
Updates	Full (Can Add, Edit, Delete Software; Can View Update For Components; Can Download, Import, Apply Update Components; Can Delete Vulnerability Protection Rule Updates)	View-Only	Hide
Asset Values	Full (Can Create, Edit, Delete Asset Values)	View-Only	View-Only
Certificates	Full (Can Create, Delete SSL Certificates)	View-Only	View-Only

Note on User Rights

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

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

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

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

Custom settings corresponding to "Create and manage users with equal or less access" option	
Users	
Can View Users	Allowed
Can Create New Users	Allowed
Can Edit User Properties (User can always edit select properties of own account)	Allowed
Can Delete Users	Allowed
Roles	
Can View Roles	Not allowed

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

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

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

Database Backup and Recovery

Backup

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

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

Internal Database or MS SQL Server Database

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

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

If you are using a Microsoft SQL Server or SQL Server Express database, a 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 database, refer to your SQL Server or SQL Server Express documentation.)

Restore

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

Database Only

1. Stop the Vulnerability Protection 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

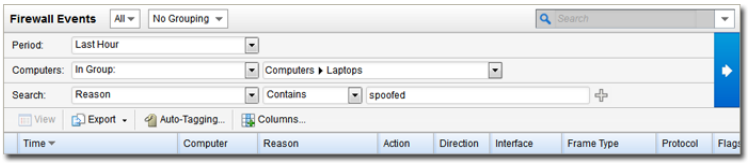
Both Vulnerability Protection Manager and Database

- Remove any remnants of the lost/corrupted Manager and database
- Install a fresh Vulnerability Protection Manager using a fresh/empty database
- Stop the Vulnerability Protection 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 Vulnerability Protection Manager service
- Verify contents restored
- Update all of the computers to ensure they have the proper configuration

Export

You can export various Vulnerability Protection 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 Vulnerability Protection Manager and are planning to set up a second Manager to manage a collection of computers. Exporting a list of selected computers will save you the trouble of re-discovering all the computers again and arranging them into groups.

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

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

Note:	*When you export a selected Policy to XML, any child Policies the Policy may have are included in the exported package. The export package contains all the actual objects associated with the policy except: Intrusion Prevention Rules 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.
- **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 Vulnerability Protection, 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 Vulnerability Protection, they must first be added to the **Computers** list in the Vulnerability Protection Manager. New computers can be added to your Computers List by:

- ***Importing computers from a local network (page 50)*** 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 Vulnerability Protection Manager.
- ***Importing a Directory (page 52)*** You can import a Microsoft Active Directory or any other LDAP-based directory service.
- ***Using a deployment script (page 56)*** 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 Vulnerability Protection 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 Vulnerability Protection 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 Vulnerability Protection Agent on the computer and then run a set of command-line instructions which tell the Agent to communicate with the Vulnerability Protection Manager. During the communication, the Vulnerability Protection 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 Vulnerability Protection 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 101)***.

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. 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 Vulnerability Protection 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.

If the computer is detected but no Vulnerability Protection 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 in a Directory/Active directory.

Active Directory

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

To import a Microsoft Active Directory:

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

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

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

   *Note: The **Details** window of each computer in the Vulnerability Protection 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 Vulnerability Protection 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 Vulnerability Protection 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 Vulnerability Protection Manager with the Active Directory Server.

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

Vulnerability Protection can leverage Active Directory information for computer discovery and User account and Contact creation.

Port Requirements

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

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

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

Server Certificate Usage

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

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

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

Filtering Active Directory Objects

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

Importing Users and Contacts

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

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

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

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

To import Users or Contacts:

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

Once imported, these accounts can be differentiated from organic Vulnerability Protection 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 Vulnerability Protection Manager. To keep the Active Directory objects that have been imported to the Vulnerability Protection 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 Vulnerability Protection Manager

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

Removing Active Directory from the Computers List

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

- Remove Directory and all subordinate computers/groups from Vulnerability Protection 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 Vulnerability Protection Manager console with an imported user account. Doing so will result in an error.

To remove users and contacts:

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

Deployment Scripts

Adding a computer to your list of protected resources in Vulnerability Protection 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 Vulnerability Protection 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 selecting **Deployment Scripts** from the Vulnerability Protection Manager's Help menu (at the top right of the Vulnerability Protection Manager window).
2. Select the platform to which you are deploying the software. (Platforms listed in the drop-down menu will correspond to the software that you have imported into the Vulnerability Protection Manager from the Trend Micro Download Center.)
3. Select **Activate the Agent Automatically**. (Agents must be activated by the Vulnerability Protection Manager before a protection Policy can be implemented.)
4. Select the Policy you wish to implement on the computer (optional)
5. Select the Computer Group (optional)

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

Note: The deployment scripts generated by Vulnerability Protection Manager for Windows Agent deployments require Windows Powershell version 2.0 or later.

Deploying Protection

- **Agent-based Protection:** The Vulnerability Protection Agent provides protection on the computer. This small software component is deployed on the computer and implements the security Policy you have applied to it.

Agent-Based Protection

Manual Deployment

You can manually install any of the Vulnerability Protection 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 49)***.

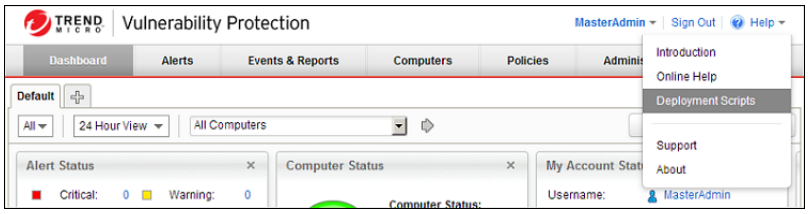
Deployment Scripts

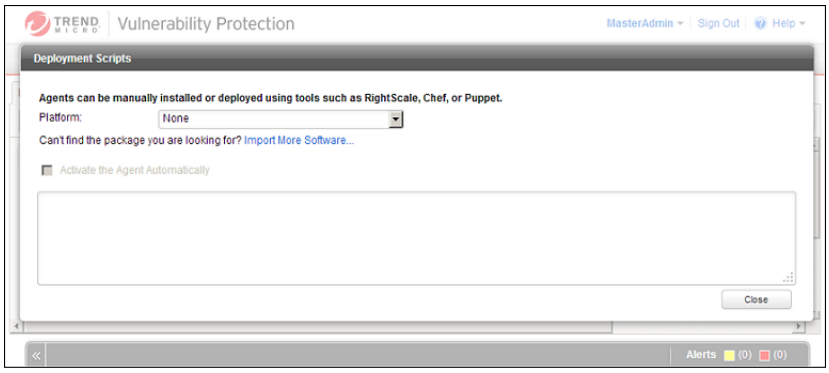
Adding a computer to your list of protected resources in Vulnerability Protection and implementing protection is a multi-step process. Almost all of these steps can be performed from the command line on the computer and can therefore be scripted. The Vulnerability Protection Manager contains a deployment 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 Vulnerability Protection Manager's Help menu at the top right of the page.
2. Select the platform to which you are deploying the software. (Platforms listed in the drop-down menu will correspond to the software that you have imported into the Vulnerability Protection Manager from the Trend Micro Download Center.
3. Select **Activate the Agent Automatically**. (Agents must be activated by the Vulnerability Protection Manager before a protection Policy can be implemented.)
4. Select the Policy you wish to implement on the computer.
5. Select the computer Group

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


TREND MICRO
Vulnerability Protection
MasterAdmin
Sign Out
Help
Dashboard
Alerts
Events & Reports
Computers
Policies
Introduction
Online Help
Deployment Scripts
Support
About
Default
All
24 Hour View
All Computers
Alert Status
Critical: 0
Warning: 0
Computer Status
My Account
Username:
MasterAdmin


TREND MICRO
Vulnerability Protection
MasterAdmin
Sign Out
Help
Deployment Scripts
Agents can be manually installed or deployed using tools such as RightScale, Chef, or Puppet.
Platform:
None
Can't find the package you are looking for? Import More Software...
Activate the Agent Automatically
Close
Alerts (0) (0)

Protection Modules

Describes configuration of the Vulnerability Protection protection modules.

- The ***Firewall (page 61)*** is a bidirectional, stateful firewall that is responsible for making sure that packets originating from unauthorized sources do not reach the applications on its host.
- The ***Intrusion Prevention (page 73)*** 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.

Firewall

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

Basic configuration

To enable Firewall functionality on a computer:

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

Inline vs. Tap Mode

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

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

In Tap Mode, the live stream is not modified. All operations are performed on the replicated stream. When in Tap Mode, Vulnerability Protection 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**
- **Othe**r (for which you must provide a protocol number)

Direction

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

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

TCP Header Flags

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

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

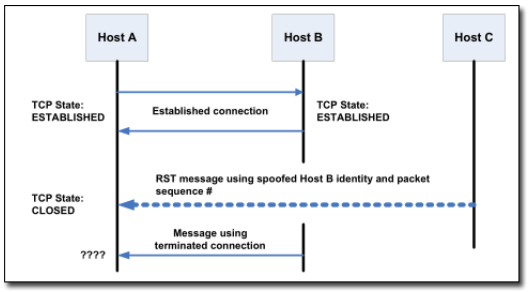
There are a number of ways these flags can be used in different attacks. Only a selection will be discussed here.

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

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

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

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



Frame Types

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

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

Firewall Rule Actions

Firewall Rules can take the following actions:

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

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

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

More about "Allow" Rules

Allow rules have two functions:

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

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

Commonly applied **Allow** rules include:

- **ARP**: Permits incoming Address Resolution Protocol (ARP) traffic .

- **Allow solicited TCP/UDP replies**: Ensures that the host computer is able to receive replies to its own TCP and UDP messages. This works in conjunction with TCP and UDP stateful configuration.
- **Allow solicited ICMP replies**: Ensures that the host computer is able to receive replies to its own ICMP messages. This works in conjunction with ICMP stateful configuration.

More about "Bypass" Rules

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

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

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

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

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

If the Vulnerability Protection Manager uses a remote database that is protected by a Vulnerability Protection Agent, Intrusion Prevention-related false alarms may occur when the Vulnerability Protection 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 Vulnerability Protection Manager to the database host.

Default Bypass Rule for Vulnerability Protection Manager Traffic

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

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

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

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

More about "Force Allow" Rules

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

- Allow
- Deny
- Force Allow

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

Vulnerability Protection 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, Vulnerability Protection Firewall Rules are run in a deterministic order based on the rule action and the rule priority, which is independent of the order in which they are defined or assigned.

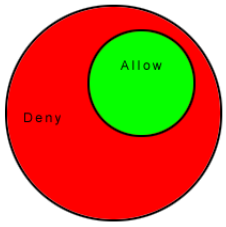
Rule Action

Each rule can have one of four actions.

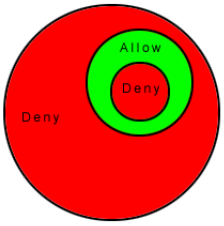
1. **Bypass:** if a packet matches a **bypass** rule, it is passed through both the firewall *and the Intrusion Prevention Engine* regardless of any other rule (at the same priority level).
2. **Log Only:** if a packet matches a **log only** rule it is passed and the event is logged.

3. **Force Allow:** if a packet matches a **force allow** rule it is passed regardless of any other rules (at the same priority level).
4. **Deny:** if a packet matches a **deny** rule it is dropped.
5. **Allow:** if a packet matches an **allow** rule, it is passed. Any traffic not matching one of the **allow** rules is denied.

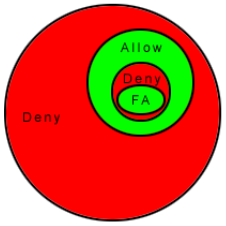
Implementing an ALLOW rule will cause all other traffic not specifically covered by the Allow rule to be denied:



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



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



Rule Priority

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

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

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

Putting Rule Action and Priority together

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

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

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

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

Stateful Filtering

When 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. 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 was not there (See below for more information)

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 Vulnerability Protection Network Engine which can operate in one of two modes:

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

In Tap Mode, the live stream is not modified. All operations are performed on the replicated stream. When in Tap Mode, Vulnerability Protection 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 Vulnerability Protection 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.

Recommendation Scans

Vulnerability Protection 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, Vulnerability Protection will recommend security Rules that should be applied.

During a Recommendation Scan, Vulnerability Protection Agents scan:

- the operating system
- installed applications
- the Windows registry
- open ports
- the directory listing
- the file system
- running processes and services
- users

Note: For large deployments, Trend Micro recommends managing Recommendations at the Policy level. That is, all computers that are to be scanned should already have a Policy assigned to them. This way, you can make all your rule assignments from a single source (the Policy) rather than having to manage individual rules on individual computers.

Recommendation Scans can be initiated manually or you can create a Scheduled Task to periodically run scans on specified computers.

Running Recommendation Scans

To launch a Recommendation Scan manually:

1. In the Vulnerability Protection 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 Vulnerability Protection Manager, go to the **Administration > Scheduled Tasks** page.
2. Click **New** on the toolbar and select "New Scheduled Task" to display the **New Scheduled Task** wizard.
3. Select "Scan Computers for Recommendations" from the **Type** menu and select how often you want the scan to occur. Click **Next**.
4. The next page will let you be more specific about the scan frequency, depending on your choice in step 3. Make your selection and click **Next**.
5. Now select which computer(s) will be scanned and click **Next**.

Note: As usual, for large deployments it's best to perform all actions through Policies.

6. Finally, give a name to your new Scheduled Task, select whether or not to "Run Task on 'Finish'", click **Finish**.

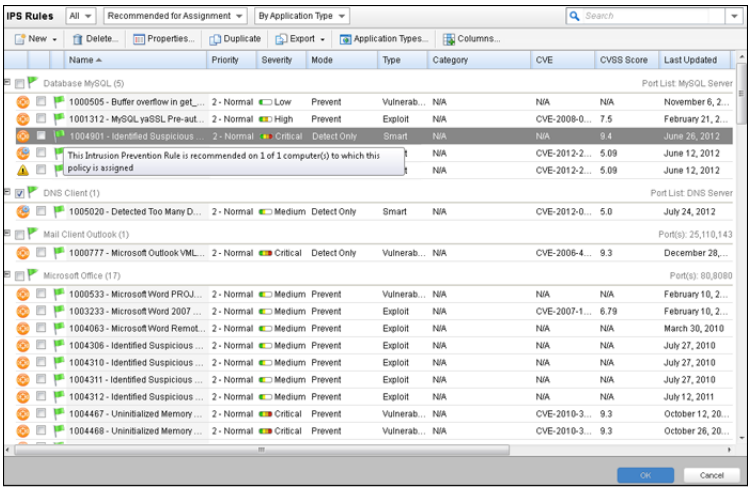
Managing Recommendation Scan Results

Vulnerability Protection 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 Vulnerability Protection 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.

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. 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: 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

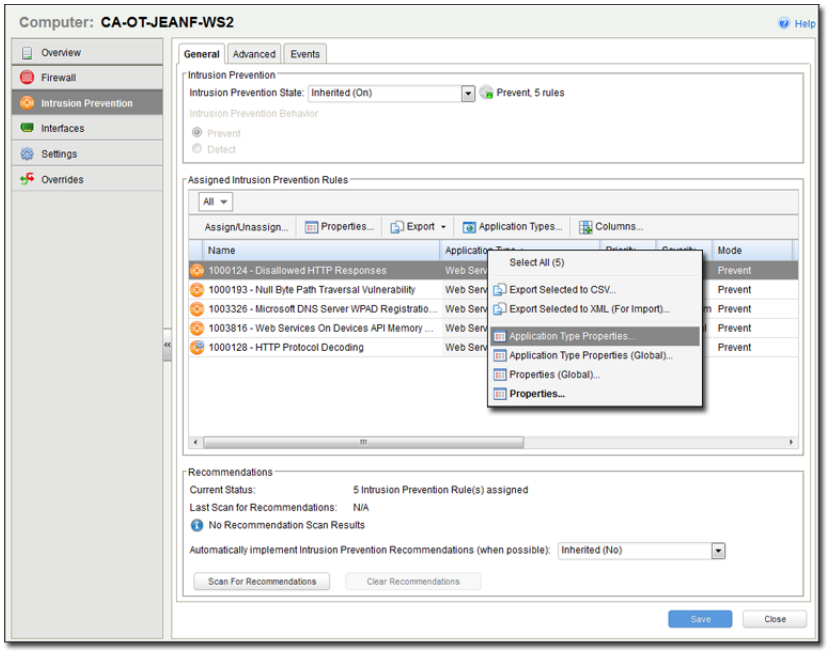
Give a name to and provide a description of this SSL configuration.

8. Look Over the Summary and Close the SSL Configuration Wizard

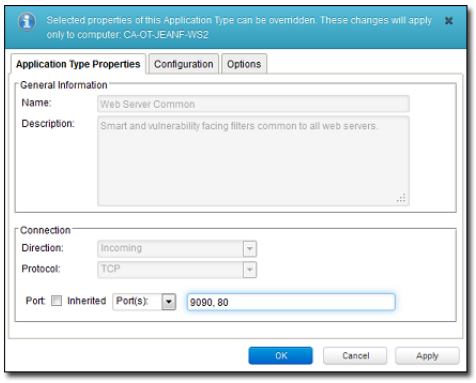
Read the summary of the configuration operation and click **Finish** to close the wizard.

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

Note: *The Vulnerability Protection 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 111)****.*

Events, Alerts, and Reports

Events

Vulnerability Protection will record security Events when a protection module Rule or condition is triggered, and System Events when administrative or system-related Events occur (like a User signing in or Agent software being upgraded.) Events can occur many times on a daily basis and do not necessarily require individual attention.

Most Events that take place on a computer are sent to the Vulnerability Protection Manager during the next heartbeat operation except the following which will be sent right away if ***Communication (page 21)*** settings allow Agents to initiate communication:

- Abnormal restart detected
- Low disk space warning

By default, the Vulnerability Protection Manager collects Event logs from the Agents at every heartbeat. The Event data is used to populate the various reports, graphs, and charts in the Vulnerability Protection Manager.

Once collected by the Vulnerability Protection 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 147)***.)
- **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 147)***.

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...

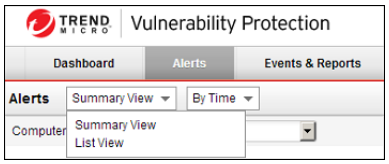
Clicking **Auto-Tagging...** displays a list of existing Auto-Tagging Rules. (See ***Event Tagging (page 147)***.)

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 Vulnerability Protection 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 and Firewall Rules. Alerts can be configured by clicking **Configure Alerts...** ().

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

Reports

Vulnerability Protection 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**.

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 147)***.

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. (Vulnerability Protection 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. (Vulnerability Protection 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), 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. 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)). Selecting **New [Event Type] Events** causes the Vulnerability Protection 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 to the Vulnerability Protection Manager's database.

Protecting a Mobile Laptop

The following describes the steps involved in using Vulnerability Protection 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
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 Vulnerability Protection Agents throughout your network. We will also assume that **you have installed (but not activated) Vulnerability Protection 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 Vulnerability Protection **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

Adding computers individually by specifying their IP addresses or hostnames

To add an individual computer by specifying its IP address or hostname, go to the **Computers** page and click **New** in the toolbar.

Type the hostname or IP address of the new computer in the **Hostname** text box. The **New Computer** wizard also lets you specify a Policy which it will apply to the new computer if it finds the computer and determines that an unactivated Agent is present. (For now, don't select a Policy.) When you click **Next**, the wizard will find the computer and activate the Agent. When Agent activation has completed, the wizard will give you the option of

opening the **Computer Editor** window (the Details window) which lets you configure many the Agent's settings. Skip the **Details** window for now.

Adding computers by scanning the network (Discovery)

To discover computers by scanning the network:

1. Go to the **Computers** page.
2. Click **Discover...** in the toolbar to display the **Discover Computers** dialog.
3. Type a range of IP addresses you want to scan for computers. If you wish, you can enter a masked IP address to do the same thing.
4. Select **Automatically resolve IPs to hostnames** to instruct the Manager to automatically resolve hostnames as it performs the discovery.
5. You have the option to add discovered computers to a computer group you have created. For now, leave the **Add Discovered Computers to Group** drop-down list choice set to "Computers".
6. Finally, clear the **Automatically perform a port scan of discovered computers** checkbox. (Port scanning detects which ports are open on the discovered computers.)
7. Click **OK**. The dialog box will disappear and "Discovery in progress..." will appear in the Manager's status bar at the bottom of your browser. (The discovery process can be cancelled by clicking the "X".)

In a few minutes, all visible computers on the network will have been detected and the Manager will have identified those with Vulnerability Protection 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 Vulnerability Protection 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 Vulnerability Protection 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 Vulnerability Protection 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 Vulnerability Protection 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 Vulnerability Protection 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 101)**.*

To manually activate an Agent on a computer, right-click one or more selected computers and select **Actions > Activate/Reactivate**.

Create a Policy for a Windows laptop

Now that the Agents are activated, it's time to assign some rules to protect the computer. Although you can assign rules directly to a computer, it's more useful to create a Policy which contains these rules and which can then be assigned to multiple computers.

Creating the Policy will involve the following steps:

1. Creating and naming the new Policy
2. Setting which interfaces to monitor
3. Setting the network engine to Inline Mode
4. Assigning Firewall Rules (including some with location awareness) and enable Stateful Inspection
5. Assigning Intrusion Prevention Rules
6. Assigning the Policy to the computer

Creating and naming the New Policy

To create and name the new Policy:

1. Go to the **Policies** section, click on Policies in the navigation panel on the left to go to the **Policies** page.
2. Click **New** in the toolbar to display the **New Policy** wizard.
3. Name the new Policy "My New Laptop Policy" and select **Base Policy** from the **Inherit from:** menu. Click **Next.**
4. The next page asks if you would like to base the Policy on an existing computer's current configuration. If you were to select **Yes**, you would be asked to pick an existing managed computer and the wizard

would take all the configuration information from that computer and create a new Policy based on it. This can be useful if, for instance, you have fine-tuned the security configuration of an existing computer over a period of time and now wish to create a Policy based on it so that you can apply it to other functionally identical computers. For now, select **No** and click **Next**.

5. The last page confirms that the new Policy has been created. Select the **Open Policy Details on 'Close'** option and click **Close**.

Setting which interfaces to monitor

To set which interfaces to monitor:

1. Because you set the **Open Policy Details on 'Close'** option, the new Policy editor window is displayed.
2. The laptops to which this Policy will be assigned are equipped with two network interfaces (a local area connection and a wireless connection) and we intend to tune the security configuration to take into account which interface is being used. Click **Interface Types** in the navigation panel and select the **Rules can apply to specific interfaces** option. Enter names for the interfaces and strings (with optional wildcards) which the Agent will use to match to interface names on the computer: "LAN Connection" and "Local Area Connection *", and "Wireless" and "Wireless Network Connection *" in the first two Interface Type areas. Click **Save** at the bottom right of the page.

Setting the network engine to Inline Mode

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

For now, we will configure our Policy to direct the engine to operate Inline.

To set the network engine to Inline Mode:

1. Still in the My New Laptop Policy editor, go to **Settings** and click on the **Network Engine** tab.
2. Set the Network Engine Mode to **Inline**. By default, the setting should already be set to "Inherited (Inline)" since the **Base** policy default mode is **Inline** and your new Policy inherits its settings from there.

Assigning Firewall Rules (including some with location awareness) and turn on Stateful Inspection

To assign Firewall Rules:

1. Click **Firewall** in the navigation panel and in the **Firewall** area of the **General** tab, select **On** from the **Firewall State** drop-down menu.

Note:	*Selecting "Inherit" will cause this setting on this Policy to be inherited from its parent Policy. This setting in the parent Policy may already be "On" but for now you will enforce the*

setting at the level of this Policy regardless of any parent Policy settings. For information on Inheritance, see ***Policies, Inheritance and Overrides (page 150)****.*

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 Vulnerability Protection 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
    - Microsoft Office
    - Web Client Common
    - Web Client Internet Explorer
    - Web Client Mozilla Firefox
    - Windows Services RPC Client
    - Windows Services RPC Server

Note:	*Make sure the first two drop-down filter menus are showing **All** and that the third sorting filter menu is sorting **By Application Type**. It's easier to page through the Application*

	*Types if you right-click in the Rules list and select **Collapse All**. There are many Application Types (and Intrusion Prevention Rules), so you will have to have to use the pagination controls at the bottom right of the page to find them all, or use the search feature at the top right of the page. Select an Application Type by putting a check next to the Application Type name.*

Note:	*Some Intrusion Prevention Rules are dependent on others. If you assign a rule that requires another rule to also be assigned (which has not yet been assigned) a popup window will appear letting you assign the required rule.*

Note:	*When assigning any kinds of Rules to a computer, do not let yourself be tempted to be "extra secure" and assign all available rules to your computer. The Rules are designed for a variety of operating systems, applications, vulnerabilities and may not be applicable to your computer. The traffic filtering engine would just be wasting CPU time looking for patterns that will never appear. Be selective when securing your computers!*

6. Click **OK** and then **Save** to assign the Application Types to the Policy.

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 Vulnerability Protection 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 Vulnerability Protection 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 Vulnerability Protection 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 Vulnerability Protection 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 Vulnerability Protection Manager and the computers that it is managing.

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

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

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

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

- The **Firewall Computer Activity (Prevented)** widget displays a list of the most common reasons for packets to be denied (that is, blocked from reaching a computer by the Agent on that computer) along with the number of packets that were denied. Items in this list will be either types of Packet Rejections or Firewall Rules. Each "reason" is a link to the corresponding logs for that denied packet.

- The **Firewall Event History [2x1]** widget displays a bar graph indicating how many packets were blocked in the last 24 hour period or seven day period (depending on the view selected). Clicking a bar will display the corresponding logs for the period represented by the bar.
- The **Firewall IP Activity (Prevented)** widget displays a list of the most common source IPs of denied packets.

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

Logs of Firewall and Intrusion Prevention Events

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

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

Note: *For the meaning of the different packet rejection reasons, see **Firewall Events (page 118)** and **Intrusion Prevention Events (page 124)**.*

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 Vulnerability Protection 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.

Load Balancers

When the Vulnerability Protection Manager is deployed without load balancers, Agents are provided with the list of Manager hostnames and will automatically contact those hostnames.

If your Vulnerability Protection Manager is located in a DMZ or behind a NAT, you may choose to put a load balancer in front of the Manager so that Agents can access the Manager's public IP address or FQDN. You can enter the load balancer settings at **Administration** > **System Settings** > **Advanced**. The hostnames and ports you supply here will override those currently used by the Agents.

Note:	*The Manager web console 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.*

Reference

The Reference section contains further information on the following topics:

- **Advanced Logging Policy Modes**: To reduce the number of events being logged, the Vulnerability Protection Manager can be configured to operate in one of several ***Advanced Logging Policy (page 99)*** modes.
- **Command-Line Instructions:** Information on the ***Command-Line Instructions (page 101)*** available for the Vulnerability Protection Manager and Agent, including information on Agent-Initiated Activation options.
- **Disabling Diffie-Hellman in Apache:** The Diffie-Hellman (DH) public key cryptography protocol is not supported by the Vulnerability Protection Agent and must be ***disabled (page 111)*** on an Apache Web server for SSL filtering to work.
- **Encrypting Manager to DB Communication:** How to encrypt ***Vulnerability Protection Manager to database communications (page 112)***.
- **Event Lists:**
  - ***Agent Events (page 115)*** A list of possible Agent Events.
  - ***Firewall Events (page 118)*** A list of possible Firewall Events.
  - ***Intrusion Prevention Events (page 124)*** A list of possible Intrusion Prevention Events.
  - ***System Events (page 128)*** A list of possible System Events.
- **Manually deactivating, Starting, or Stopping the Agent:** Information on how to ***Manually Deactivate/Stop/Start the Agent (page 145)***.
- **Manually Upgrade the Agent on a Computer:** How to ***manually upgrade (page 146)*** the Agent on a computer.
- **More about Event Tagging:** More ***information (page 147)*** about the event tagging mechanism.
- **Performance Requirements:** ***Guidelines (page 149)*** providing a general idea of the infrastructure requirements for Vulnerability Protection deployments of different scales.
- **Policies, Inheritance and Overrides:** An explanation of how settings can be ***inherited or overridden (page 150)*** at various levels of the Policy hierarchy.
- **Ports Used by Vulnerability Protection:** Information about the ***ports (page 152)*** used by Vulnerability Protection to communicate with various components of the system.
- **Teamed NICs:** Information on installing an Agent in a ***teamed NIC environment (page 156)***.

Advanced Logging Policy Modes

To reduce the number of events being logged, the Vulnerability Protection Manager can be configured to operate in one of several **Advanced Logging Policy** modes. These modes are set in the Policy and Computer Editors on the **Settings > Network Engine > Advanced Network Engine Settings** area.

The following table lists the types of Events are ignored in four of the more complex Advanced Logging Policy modes:

Mode	Ignored Events
Stateful and Normalization Suppression	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Unsolicited UDP Unsolicited ICMP Out Of Allowed Policy Dropped Retransmit
Stateful, Normalization, and Frag Suppression	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Unsolicited UDP Unsolicited ICMP Out Of Allowed Policy CE Flags Invalid IP Invalid IP Datagram Length Fragmented Invalid Fragment Offset First Fragment Too Small Fragment Out Of Bounds Fragment Offset Too Small IPv6 Packet Max Incoming Connections Max Outgoing Connections Max SYN Sent License Expired IP Version Unknown Invalid Packet Info Maximum ACK Retransmit Packet on Closed Connection Dropped Retransmit
Stateful, Frag, and Verifier Suppression	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Unsolicited UDP Unsolicited ICMP

Mode	Ignored Events
	Out Of Allowed Policy CE Flags Invalid IP Invalid IP Datagram Length Fragmented Invalid Fragment Offset First Fragment Too Small Fragment Out Of Bounds Fragment Offset Too Small IPv6 Packet Max Incoming Connections Max Outgoing Connections Max SYN Sent License Expired IP Version Unknown Invalid Packet Info Invalid Data Offset No IP Header Unreadable Ethernet Header Undefined Same Source and Destination IP Invalid TCP Header Length Unreadable Protocol Header Unreadable IPv4 Header Unknown IP Version Maximum ACK Retransmit Packet on Closed Connection Dropped Retransmit
Tap Mode	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Maximum ACK Retransmit Packet on Closed Connection Dropped Retransmit

Command-Line Instructions

Vulnerability Protection Agent

dsa_control

Usage

dsa_control [-a <str>] [-b] [-c <str>] [-d] [-g <str>] [-s <num>] [-m] [-p <str>] [-r] [-R <str>] [-t <num>] [Additional keyword:value data to send to Manager during activation/heartbeat...]

- **-a <str>, --activate=<str>** Activate agent with Manager at specified URL. URL format must be 'dsm://hostOrIp:port/' where port is the Manager's heartbeat port (default 4120).
- **-b, --bundle** Create update bundle.
- **-c <str>, --cert=<str>** Identify the certificate file.
- **-d, --diag** Generate an agent diagnostic package.
- **-g <str>, --agent=<str>** Agent URL. Defaults to 'https://localhost:4118/'
- **-m, --heartbeat** Ask the Agent to contact the Manager now.
- **-p <str>, --passwd=<str>** Authentication password.
- **-r, --reset** Reset agent configuration.
- **-s <num>, --selfprotect=<num>** enable self-protection on the Agent by preventing local end-users from uninstalling, stopping, or otherwise controlling the Agent. Command-line instructions must include the authentication password when self-protection is enabled. (1: enable, 0: disable)
- **-t <num>, --retries=<num>** If dsa_control cannot contact the Vulnerability Protection 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.

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 Vulnerability Protection Manager (or one of its Manager Nodes) can send instructions to and communicate with the Agent.

You can manually activate an Agent from the Vulnerability Protection Manager by right-clicking on the computer in the Computers screen and selecting **Actions > Activate/Reactivate**.

Vulnerability Protection 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 Vulnerability Protection installation and you want to write a script to automate the activation process.

Note: *For Agent-Initiated Activation to work, the **Allow Agent-Initiated Activation** option must be enabled on the **Administration > System Settings > Agents** tab.*

The minimum activation instruction contains the activation command and the Manager's URL (including the port number):

```
dsa_control -a dsm://[managerurl]:[port]/
```

where:

- **-a** is the command to activate the Agent , and
- **dsm://managerurl:4120/** is the parameter that points the Agent to the Vulnerability Protection Manager. ("managerurl" is the URL of the Vulnerability Protection 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 Vulnerability Protection Manager through a proxy server. Use the following command-line options to instruct the Agent to communicate with the Vulnerability Protection Manager through a proxy server:

Syntax	Notes
`dsa_control -x "dsm_proxy://<proxyURL>/"`	Sets the address of the proxy server which the Agent uses to communicate with the Manager.
`dsa_control -x ""`	Clears the proxy server address.
`dsa_control -u "<username:password>"`	Sets the proxy username and password.
`dsa_control -u ""`	Clears the proxy username and password.
Examples	
`dsa_control.exe -x "dsm_proxy://172.21.3.184:808/"`	Proxy uses IPv4.
`dsa_control.exe -x "dsm_proxy://winsrv2k3-0:808/"`	Proxy uses hostname.
`dsa_control.exe -x "dsm_proxy://[fe80::340a:7671:64e7:14cc]:808/"`	Proxy uses IPv6.
`dsa_control.exe -u "root:Passw0rd!"`	Proxy authentication is "root" and password is "Passw0rd!" (basic authentication only, digest and NTLM are not supported).

When used in the context of Agent-initiated activation, the proxy commands must be issued first, followed by the Agent-initiated activation commands. The following example shows a complete sequence for setting a proxy address, setting proxy credentials, and activating the Agent:

```
dsa_control.exe -x "dsm_proxy://172.21.3.184:808/"
dsa_control.exe -u "root:Passw0rd!"
dsa_control -a "dsm://seg-dsm-1:4120/"
Required Setting in Vulnerability Protection Manager
```

The Vulnerability Protection 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 Vulnerability Protection 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 Vulnerability Protection 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 Vulnerability Protection Manager.

The following table lists the parameters that are available to the activation and heartbeat commands. Note that some parameters can only be used with either the activation or heartbeat exclusively.

Key	Description	Examples	Can be performed during Activation	Can be performed after activation during Heartbeat	Value Format	Notes
description	Sets **description** value.	"description:Extra information about the host"	yes	yes	string	Maximum length 2000 characters.
displayname	Sets **displayname** value. (Shown in parentheses next to the hostname.)	"displayname:the_name"	yes	yes	string	Maximum length 2000 characters.
externalid		"externalid:15"	yes	yes	integer	
group	Sets the computers page	"group:Zone A/Webservers"	yes	yes	string	Maximum length 254 characters per group

Key	Description	Examples	Can be performed during Activation	Can be performed after activation during Heartbeat	Value Format	Notes
	Group the computer belongs in.					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) accounts.
groupid		"groupid:33"	yes	yes	integer	
hostname		"hostname:ABWebServer1"	yes	no	string	Maximum length 254 characters. The hostname can specify an IP address, hostname or FQDN that is best used to contact the computer in the **Computers** list in Vulnerability Protection Manager.
policy		"policy:Policy Name"	yes	yes	string	Maximum length 254 characters. The Policy name is a case-insensitive match to the Policy list. If the Policy is not found, no Policy will be assigned. A policy assigned by an Event-based Task

Key	Description	Examples	Can be performed during Activation	Can be performed after activation during Heartbeat	Value Format	Notes
						will override a Policy assigned during Agent-Initiated Activation.
policyid		"policyid:12"	yes	yes	integer	
RecommendationScan	Initiate a Recommendation Scan on the computer.	"RecommendationScan:true"	no	yes	boolean	
UpdateComponent	Instructs the Vulnerability Protection Manager to perform a Security Update operation.	"UpdateComponent:true"	no	yes	boolean	
UpdateConfiguration	Instructs the Vulnerability Protection Manager to perform a "Send Policy" operation.	"UpdateConfiguration:true"	no	yes	boolean	

dsa_query

The dsa_query tool provides the following information :

- License-status of each component
- Scan progress
- Version information of Security Update components

Usage

dsa_query [-c <str>] [-p <str>] [-r <str]

- -p,--passwd <string>: authentication password. Required when agent self-protection is enabled.

> *Note:* *For some query-commands, authentication can be bypassed directly, in such case, password is not required.*

- -c,--cmd <string>: execute query-command against ds_agent. The following commands are supported:
  - "GetHostInfo": to query which identity is returned to the Vulnerability Protection during a heartbeat
  - "GetAgentStatus": to query which protection modules are enabled and other miscellaneous information
- -r,--raw <string>: returns the same query-command information as "-c" but in raw data format for third party software interpretation.

pattern: wildchar pattern to filter result, optional.

These keys are organized in nested namespace because the response from ds_agent are formed in XML-format. If users's key mapped to an leaf-node, we would return string-value directly. In other cases, we would return xml-formatted result, contains all information under that matched node.

Example:
dsa_query -c "GetComponentInfo" -r "au" "AM*"

Vulnerability Protection Manager

vp_c

Usage

vp_c -action actionname

Action Name	Description	Usage with Parameters (if any)
changesetting	Change a setting	vp_c -action changesetting -name NAME -value VALUE [-computerid COMPUTERID] [-computername COMPUTERNAME] [-policyid POLICYID] [-policyname POLICYNAME] [-tenantname TENANTNAME]
viewsetting	View a setting value	vp_c -action viewsetting -name NAME [-computerid COMPUTERID] [-computername COMPUTERNAME] [-policyid POLICYID] [-policyname POLICYNAME] [-tenantname TENANTNAME]
createinsertstatements	Create insert statements (for export to a different database)	vp_c -action createinsertstatements [-file FILEPATH] [-generateDDL] [-databaseType sqlserver|oracle] [-maxresultfromdb count] [-tenantname TENANTNAME]
diagnostic	Create a diagnostic package for the system	vp_c -action diagnostic
fullaccess	Give an administrator the full access role	vp_c -action fullaccess -username USERNAME [-tenantname TENANTNAME]
reindexhelp	Reindex help system	vp_c -action reindexhelp
resetcounters	Reset counter tables (resets back to an empty state	vp_c -action resetcounters [-tenantname TENANTNAME]

resetevents	Reset the events tables (resets back to an empty state)	vp_c -action resetevents -type all|am|wrs|fw|dpi|im|li [-tenantname TENANTNAME]
setports	Set Vulnerability Protection Manager port(s)	vp_c -action setports [-managerPort port] [-heartbeatPort port]
trustdirectorycert	Trust the certificate of a directory	vp_c -action trustdirectorycert -directoryaddress DIRECTORYADDRESS -directoryport DIRECTORYPORT [-username USERNAME] [-password PASSWORD] [-tenantname TENANTNAME]
unlockout	Unlock a User account	vp_c -action unlockout -username USERNAME [-newpassword NEWPASSWORD] [-tenantname TENANTNAME]

Computer and Agent Status

The **status** column of the Vulnerability Protection Manager's **Computers** page displays the current state of the computer and its Agent. The status column will usually display the state of the computer on the network followed by the state (in parentheses) of the Agent providing protection, if one is present. If the computer or Agent 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 Events (page 115)** and **System Events (page 128)** in the Reference section.*

Computer States

Computer State	Description	Notes
Discovered	Computer has been added to the Computers List via the Discovery process.	
Unmanaged	Unmanaged by this Vulnerability Protection Manager, unactivated, and can't be communicated with until activated.	
Managed	An Agent is present and activated with no pending operations or errors.	
Updating	The Agent is being updated with a combination of new configuration settings and Security Updates.	
Update Pending (Schedule)	The Agent will be updated with a combination of new configuration settings and Security Updates once the computer's access schedule permits.	
Update Pending (Heartbeat)	An update will be performed at the next heartbeat.	
Update Pending (Offline)	The Manager cannot currently communicate with the Agent. An update is ready to be applied once the Agent comes back online.	
Scanning for Open Ports	The Manager is scanning the Computer for open ports.	
Activating	The Manager is activating the Agent.	
Activating (Delayed)	The activation of the Agent is delayed by the amount of time specified in the relevant event-based task.	
Activated	The Agent is activated.	
Deactivating	The Manager is deactivating the Agent. This means that the Agent is available for activation and management by another Vulnerability Protection Manager.	
Deactivate Pending (Heartbeat)	A deactivate instruction will be sent from the Manager during the next heartbeat.	
Locked	The computer is in a locked state. While in in a locked state the Manager will not communicate with the Agent or generate any computer-related Alerts. Existing computer Alerts are not affected.	

Computer State	Description	Notes
Multiple Errors	Multiple errors have occurred on this computer. See the computer's system events for details.	
Multiple Warnings	Multiple warnings are in effect on this computer. See the computer's system events for details.	
Upgrading Agent	The Agent software on this computer is in the process of being upgraded to a newer version.	
Scanning for Recommendations	A Recommendation Scan is underway.	
Scan for Recommendations Pending (Schedule)	A Recommendation Scan will be initiated once the computer's Access Schedule permits.	
Scan for Recommendations Pending (Heartbeat)	The Manager will initiate a Recommendation Scan at the next heartbeat.	
Scan for Recommendations Pending (Offline)	The Agent is currently offline. The Manager will initiate a Recommendation Scan when communication is reestablished.	
Checking Status	The agent state is being checked.	
Getting Events	The Manager is retrieving Events from the Agent.	
Upgrade Recommended	A newer version of the Agent is available. An software upgrade is recommended.	

Agent States

Agent State	Description	Notes
Activated	The Agent has been successfully activated and is ready to be managed by the Vulnerability Protection Manager.	
Activation Required	An unactivated Agent has been detected on the target machine. It must be activated before it can be managed by the Vulnerability Protection Manager.	
No Agent	No Agent was detected on the computer.	
Unknown	No attempt has been made to determine whether an Agent is present.	
Deactivation Required	The Manager has attempted to activate an Agent that has already been activated by another Vulnerability Protection Manager. The original Vulnerability Protection Manager must deactivate the Agent before it can be activated by the new Manager.	
Reactivation Required	The Agent is installed and listening and is waiting to be reactivated a Vulnerability Protection Manager.	
Online	The Agent is online and operating as expected.	
Offline	No contact has been made with the Agent for the number of heartbeats specified in **Policy/Computer Editor > Settings > Computers** tab.	

Computer Errors

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

Protection Module Status

When you hover over a computer name on the **Computers** page, the state of its protection modules is displayed.

On/Off State:

State	Description
On	Module is configured in Vulnerability Protection Manager and is installed and operating on the Vulnerability Protection Agent.
Off	Module is either not configured in VVulnerability Protection Manager, not installed and operating on the Vulnerability Protection Agent, or both.
Unknown	Indicates an error with the Firewall or Intrusion Prevention modules.

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 Vulnerability Protection Agent and must be disabled on an Apache Web server for SSL filtering to work.

The "Key Exchange Algorithm" and "Authentication Method" parameters are the first two fields of the " `SSLCipherSuite` " variable present in the `httpd-ssl.conf` file. To instruct Apache to not use Diffie-Hellman, " `!ADH` " must be added to these fields.

The following example shows the syntax required to disable DH key exchange and authentication methods in Apache:

```
SSLCipherSuite !ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
```

Note: *Only the first two fields are of concern with regards to disabling ADH. The " `!` " tells Apache to "Not" use ADH.*

The config files may be located in different places depending on your Apache build. For example:

- **Default installation on RHEL4:** `/etc/httpd/conf.d/ssl.conf`
- **Apache 2.2.2:** `/usr/local/apache2/conf/extra/httpd-ssl.conf`

References

For more information, visit the Apache Documentation of `SSLCipherSuite` at http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite.

Encrypting Manager to DB Communication

Communication between the Vulnerability Protection 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 Vulnerability Protection Manager and the database is not secure, you should encrypt the communications between them. Do this by editing the `dsm.properties` file located in `\Vulnerability Protection Manager\webclient\webapps\ROOT\WEB-INF\`

MS SQL Server

To encrypt communication between the Vulnerability Protection Manager and an MS SQL Server database:

1. Add the following line to `dsm.properties`:

   ```
   database.SqlServer.ssl=require
   ```

2. Stop and restart the Vulnerability Protection Manager service.

Oracle Database

To encrypt communication between the Vulnerability Protection 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 Vulnerability Protection Manager service.

(All parameters prefixed with database.Oracle. will be passed to the Oracle driver.)

Possible values for the `encryption_types_client` are:

- AES256
- AES192
- AES128
- 3DES168
- 3DES112
- DES56C

- DES40C
- RC4_256
- RC4_128
- RC4_40
- RC4_56

Possible values for `crypto_checksum_types_client` are:

- MD5
- SHA1

For additional options consult: http://docs.oracle.com/cd/B28359_01/java.111/b31224/clntsec.htm

Running an Agent on the Database Server

Encryption should be enabled if you are using an Agent to protect the database. When you perform a Security Update, the Vulnerability Protection 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.

Event Lists

Agent Events

*Note: Agent 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 Events that were retrieved.*

Note: Events annotated as "Deprecated" are no longer generated by the most recent Agents but may still appear if you are running older versions.

ID	Severity	Event	Notes
Special Events			
0	Error	Unknown Agent Event	
Driver-Related Events			
1000	Error	Unable To Open Engine	
1001	Error	Engine Command Failed	
1002	Warning	Engine List Objects Error	
1003	Warning	Remove Object Failed	
1004	Warning	Engine Returned Bad Rule Data	Deprecated.
1005	Warning	Upgrading Driver	
1006	Warning	Driver Upgrade Requires Reboot	
1007	Warning	Driver Upgrade Succeeded	
Configuration-Related Events			
2000	Info	Policy Sent	
2001	Warning	Invalid Firewall Rule Assignment	
2002	Warning	Invalid Firewall Stateful Configuration	
2003	Error	Save Security Configuration Failed	
2004	Warning	Invalid Interface Assignment	
2005	Warning	Invalid Interface Assignment	
2006	Warning	Invalid Action	
2007	Warning	Invalid Packet Direction	
2008	Warning	Invalid Rule Priority	
2009	Warning	Unrecognized IP Format	
2010	Warning	Invalid Source IP List	
2011	Warning	Invalid Source Port List	
2012	Warning	Invalid Destination IP List	
2013	Warning	Invalid Destination Port List	
2014	Warning	Invalid Schedule	
2015	Warning	Invalid Source MAC List	
2016	Warning	Invalid Destination MAC List	

ID	Severity	Event	Notes
2017	Warning	Invalid Schedule Length	
2018	Warning	Invalid Schedule String	
2019	Warning	Invalid Intrusion Prevention Rule XML Rule	
2020	Warning	Object Not Found	
2021	Warning	Object Not Found	
2022	Warning	Invalid Rule Assignment	
2050	Warning	Firewall Rule Not Found	
2075	Warning	Traffic Stream Not Found	
2076	Warning	Intrusion Prevention Rule Not Found	
2078	Warning	Intrusion Prevention Rule Conversion Error	
2080	Warning	Conditional Firewall Rule Not Found	
2081	Warning	Conditional Intrusion Prevention Rule Not Found	
2082	Warning	Empty Intrusion Prevention Rule	
2083	Warning	Intrusion Prevention Rule XML Rule Conversion Error	
2085	Error	Security Configuration Error	
2086	Warning	Unsupported IP Match Type	
2087	Warning	Unsupported MAC Match Type	
2088	Warning	Invalid SSL Credential	
2089	Warning	Missing SSL Credential	
Hardware-Related Events			
3000	Warning	Invalid MAC Address	
3001	Warning	Get Event Data Failed	
3002	Warning	Too Many Interfaces	
3003	Error	Unable To Run External Command	
3004	Error	Unable To Read External Command Output	
3005	Error	Operating System Call Error	
3006	Error	Operating System Call Error	
3007	Error	File Error	
3008	Error	Machine-Specific Key Error	
3009	Error	Unexpected Agent Shutdown	
3010	Error	Agent Database Error	
3600	Error	Get Windows System Directory Failed	
3601	Warning	Read Local Data Error	Windows error.
3602	Warning	Windows Service Error	Windows error.
3603	Error	File Mapping Error	Windows error. File size error.
3700	Warning	Abnormal Restart Detected	Windows error.
3701	Info	System Last Boot Time Change	Windows error.
Communication-Related Events			
4000	Warning	Invalid Protocol Header	Content length out of range.

ID	Severity	Event	Notes
4001	Warning	Invalid Protocol Header	Content length missing.
4002	Info	Command Session Initiated	
4003	Info	Configuration Session Initiated	
4004	Info	Command Received	
4011	Warning	Failure to Contact Manager	
4012	Warning	Heartbeat Failed	
Agent-Related Events			
5000	Info	Agent Started	
5001	Error	Thread Exception	
5002	Error	Operation Timed Out	
5003	Info	Agent Stopped	
5004	Warning	Clock Changed	
5005	Info	Agent Auditing Started	
5006	Info	Agent Auditing Stopped	
5100	Info	Protection Module Deployment Started	
5101	Info	Protection Module Deployment Succeeded	
5102	Error	Protection Module Deployment Failed	
5103	Info	Protection Module Download Succeeded	
Logging-Related Events			
6000	Info	Log Device Open Error	
6001	Info	Log File Open Error	
6002	Info	Log File Write Error	
6003	Info	Log Directory Creation Error	
6004	Info	Log File Query Error	
6005	Info	Log Directory Open Error	
6006	Info	Log File Delete Error	
6007	Info	Log File Rename Error	
6008	Info	Log Read Error	
6009	Warning	Log File Deleted Due To Insufficient Space	
6010	Warning	Events Were Suppressed	
6011	Warning	Events Truncated	
6012	Error	Insufficient Disk Space	
6013	Warning	Agent Configuration Package Too Large	
Download Security Update Events			
9100	Info	Security Update Successful	
9101	Error	Security Update Failure	
9102	Error	Security Update Failure	Specific information recorded in error message.

Firewall Events

ID	Event	Notes
1	Normal (Filter)	
100	Out Of Connection	A packet was received that was not associated with an existing connection.
101	Invalid Flags	Flag(s) set in packet were invalid. This could be due to a flag that does not make sense within the context of a current connection (if any), or due to a nonsensical combination of flags. (Firewall Stateful Configuration must be On for connection context to be assessed.)
102	Invalid Sequence	A packet with an invalid sequence number or out-of-window data size was encountered.
103	Invalid ACK	A packet with an invalid acknowledgement number was encountered.
104	Internal Error	
105	CE Flags	The CWR or ECE flags were set and the Firewall Stateful Configuration specifies that these packets should be denied.
106	Invalid IP	Packet's source IP was not valid.
107	Invalid IP Datagram Length	The length of the IP datagram is less than the length specified in the IP header.
108	Fragmented	A fragmented packet was encountered with deny fragmented packets disallowed enabled.
109	Invalid Fragment Offset	
110	First Fragment Too Small	A fragmented packet was encountered, the size of the fragment was less than the size of a TCP packet (no data).
111	Fragment Out Of Bounds	The offsets(s) specified in a fragmented packet sequence is outside the range of the maximum size of a datagram.
112	Fragment Offset Too Small	A fragmented packet was encountered, the size of the fragment was less than the size of a TCP packet (no data).
113	IPv6 Packet	An IPv6 Packet was encountered, and IPv6 blocking is enabled.
114	Max Incoming Connections	The number of incoming connections has exceeded the maximum number of connections allowed.
115	Max Outgoing Connections	The number of outgoing connections has exceeded the maximum number of connections allowed.
116	Max SYN Sent	The number of half open connections from a single computer exceeds that specified in the Firewall Stateful Configuration.
117	License Expired	
118	IP Version Unknown	An IP packet other than IPv4 or IPv6 was encountered.
119	Invalid Packet Info	

ID	Event	Notes
120	Internal Engine Error	Insufficient resources.
121	Unsolicited UDP	Incoming UDP packets that were not solicited by the computer are rejected.
122	Unsolicited ICMP	ICMP stateful has been enabled (in Firewall Stateful Configuration) and an unsolicited packet that does not match any Force Allow rules was received.
123	Out Of Allowed Policy	The packet does not meet any of the Allow or Force Allow rules and so is implicitly denied.
124	Invalid Port Command	An invalid FTP port command was encountered in the FTP control channel data stream.
125	SYN Cookie Error	The SYN cookies protection mechanism encountered an error.
126	Invalid Data Offset	Invalid data offset parameter.
127	No IP Header	
128	Unreadable Ethernet Header	Data contained in this Ethernet frame is smaller than the Ethernet header.
129	Undefined	
130	Same Source and Destination IP	Source and destination IPs were identical.
131	Invalid TCP Header Length	
132	Unreadable Protocol Header	The packet contains an unreadable TCP, UDP or ICMP header.
133	Unreadable IPv4 Header	The packet contains an unreadable IPv4 header.
134	Unknown IP Version	Unrecognized IP version.
135	Invalid Adapter Configuration	An invalid adapter configuration has been received.
136	Overlapping Fragment	This packet fragment overlaps a previously sent fragment.
137	Maximum ACK Retransmit	This retransmitted ACK packet exceeds the ACK storm protection threshold.
138	Packet on Closed Connection	A packet was received belonging to a connection already closed.
139	Dropped Retransmit	Dropped Retransmit.
140	Undefined	

ID	Event	Notes
141	Out of Allowed Policy (Open Port)	
142	New Connection Initiated	
143	Invalid Checksum	
144	Invalid Hook Used	
145	IP Zero Payload	
146	IPv6 Source Is Multicast	
147	Invalid IPv6 Address	
148	IPv6 Fragment Too Small	
149	Invalid Transport Header Length	
150	Out of Memory	
151	Max TCP Connections	
152	Max UDP Connections	
200	Region Too Big	
201	Insufficient Memory	
202	Maximum Edits Exceeded	
203	Edit Too Large	
204	Max Matches in Packet Exceeded	
205	Engine Call Stack Too Deep	
206	Runtime Error	
207	Packet Read Error	
300	Unsupported Cipher	

ID	Event	Notes
301	Error Generating Master Key(s)	
302	Record Layer Message (not ready)	
303	Handshake Message (not ready)	
304	Out Of Order Handshake Message	
305	Insufficient Memory	
306	Unsupported SSL Version	
307	Error Decrypting Pre-master Key	
308	Client Attempted to Rollback	
309	Renewal Error	
310	Key Exchange Error	
311	Error Generating Pre-Master Request	
312	Key Too Large	
313	Invalid Parameters In Handshake	
314	No Sessions Available	
315	Compression Method Unsupported	
500	URI Path Depth Exceeded	
501	Invalid Traversal	
502	Illegal Character in URI	

ID	Event	Notes
503	Incomplete UTF8 Sequence	
504	Invalid UTF8 encoding	
505	Invalid Hex Encoding	
506	URI Path Length Too Long	
507	Invalid Use of Character	
508	Double Decoding Exploit	
700	Invalid Base64 Content	
710	Corrupted Deflate/GZIP Content	
711	Incomplete Deflate/GZIP Content	
712	Deflate/GZIP Checksum Error	
713	Unsupported Deflate/GZIP Dictionary	
714	Unsupported GZIP Header Format/Method	
801	Protocol Decoding Search Limit Exceeded	
802	Protocol Decoding Constraint Error	
803	Protocol Decoding Engine Internal Error	
804	Protocol Decoding	

ID	Event	Notes
	Structure Too Deep	
805	Protocol Decoding Stack Error	
806	Infinite Data Loop Error	

Intrusion Prevention Events

ID	Event	Notes
0	Normal (Filter)	
200	Region Too Big	A region (edit region, uri etc) exceeded the maximum allowed buffering size (7570 bytes) without being closed. This is usually because the data does not conform to the protocol.
201	Insufficient Memory	The packet could not be processed properly because resources were exhausted. This can be because too many concurrent connections require buffering (max 2048) or matching resources (max 128) at the same time or because of excessive matches in a single IP packet (max 2048) or simply because the system is out of memory.
202	Maximum Edits Exceeded	The maximum number of edits (32) in a single region of a packet was exceeded.
203	Edit Too Large	Editing attempted to increase the size of the region above the maximum allowed size (8188 bytes).
204	Max Matches in Packet Exceeded	There are more than 2048 positions in the packet with pattern match occurrences. An error is returned at this limit and the connection is dropped because this usually indicates a garbage or evasive packet.
205	Engine Call Stack Too Deep	
206	Runtime Error	Runtime error.
207	Packet Read Error	Low level problem reading packet data.
300	Unsupported Cipher	An unknown or unsupported Cipher Suite has been requested.
301	Error Generating Master Key(s)	Unable to derive the cryptographic keys, Mac secrets, and initialization vectors from the master secret.
302	Record Layer Message (not ready)	The SSL state engine has encountered an SSL record before initialization of the session.
303	Handshake Message (not ready)	The SSL state engine has encountered a handshake message after the handshake has been negotiated.
304	Out Of Order Handshake Message	A well formatted handshake message has been encountered out of sequence.

ID	Event	Notes
305	Insufficient Memory	The packet could not be processed properly because resources were exhausted. This can be because too many concurrent connections require buffering (max 2048) or matching resources (max 128) at the same time or because of excessive matches in a single IP packet (max 2048) or simply because the system is out of memory.
306	Unsupported SSL Version	A client attempted to negotiate an SSL V2 session.
307	Error Decrypting Pre-master Key	Unable to un-wrap the pre-master secret from the ClientKeyExchange message.
308	Client Attempted to Rollback	A client attempted to rollback to an earlier version of the SSL protocol than that which was specified in the ClientHello message.
309	Renewal Error	An SSL session was being requested with a cached session key that could not be located.
310	Key Exchange Error	The server is attempting to establish an SSL session with temporarily generated key.
311	Error Generating Pre-Master Request	An error occurred when trying to queue the pre-master secret for decryption.
312	Key Too Large	The master secret keys are larger than specified by the protocol identifier.
313	Invalid Parameters In Handshake	An invalid or unreasonable value was encountered while trying to decode the handshake protocol.
314	No Sessions Available	
315	Compression Method Unsupported	
500	URI Path Depth Exceeded	too many "/" separators, max 100 path depth.
501	Invalid Traversal	Tried to use "../" above root.
502	Illegal Character in URI	Illegal character used in uri.
503	Incomplete UTF8 Sequence	URI ended in middle of utf8 sequence.
504	Invalid UTF8 encoding	Invalid/non-canonical encoding attempt.

ID	Event	Notes
505	Invalid Hex Encoding	%nn where nn are not hex digits.
506	URI Path Length Too Long	path length is greater than 512 characters.
507	Invalid Use of Character	use of disabled char
508	Double Decoding Exploit	Double decoding exploit attempt (%25xx, %25%xxd, etc).
700	Invalid Base64 Content	Packet content that was expected to be encoded in Base64 format was not encoded correctly.
710	Corrupted Deflate/ GZIP Content	Corrupted Deflate/GZIP Content
711	Incomplete Deflate/ GZIP Content	Incomplete Deflate/GZIP Content
712	Deflate/ GZIP Checksum Error	Deflate/GZIP Checksum Error.
713	Unsupported Deflate/ GZIP Dictionary	Unsupported Deflate/GZIP Dictionary.
714	Unsupported GZIP Header Format/ Method	Unsupported GZIP Header Format/Method.
801	Protocol Decoding Search Limit Exceeded	A protocol decoding rule defined a limit for a search or pdu object but the object was not found before the limit was reached.
802	Protocol Decoding Constraint Error	A protocol decoding rule decoded data that did not meet the protocol content constraints.
803	Protocol Decoding Engine Internal Error	

ID	Event	Notes
804	Protocol Decoding Structure Too Deep	A protocol decoding rule encountered a type definition and packet content that caused the maximum type nesting depth (16) to be exceeded.
805	Protocol Decoding Stack Error	A rule programming error attempted to cause recursion or use to many nested procedure calls.
806	Infinite Data Loop Error	

System Events

The following table lists the System Events that can be recorded by Vulnerability Protection and their default settings. (Notifications cannot be sent for Events that are not recorded.)

ID	Severity	Event	Record	Forward	Notes
0	Error	Unknown Error	On	On	
100	Info	Vulnerability Protection Manager Started	On	On	
101	Info	License Changed	On	On	
102	Info	Trend Micro Vulnerability Protection Customer Account Changed	On	On	
103	Warning	Check For Updates Failed	On	On	
105	Warning	Scheduled Rule Update Download and Apply Failed	On	On	
106	Info	Scheduled Rule Update Downloaded and Applied	On	On	
107	Info	Rule Update Downloaded and Applied	On	On	
108	Info	Script Executed	On	On	
109	Error	Script Execution Failed	On	On	
110	Info	System Events Exported	On	On	
111	Info	Firewall Events Exported	On	On	
112	Info	Intrusion Prevention Events Exported	On	On	
113	Warning	Scheduled Rule Update Download Failed	On	On	
114	Info	Scheduled Rule Update Downloaded	On	On	

ID	Severity	Event	Record	Forward	Notes
115	Info	Rule Update Downloaded	On	On	
116	Info	Rule Update Applied	On	On	
117	Info	Vulnerability Protection Manager Shutdown	On	On	
118	Warning	Vulnerability Protection Manager Offline	On	On	
119	Info	Vulnerability Protection Manager Back Online	On	On	
120	Error	Heartbeat Server Failed	On	On	The server within Manager that listens for incoming Agent Heartbeats has failed to start. Check that the Manager's incoming heartbeat port (by default 4120) is not in use by another application on the Manager server. Once it is free, the Manager should bind to it and this error should be fixed.
121	Error	Scheduler Failed	On	On	
122	Error	Manager Message Thread Failed	On	On	An internal thread has failed. There is no resolution for this error. If it persists, contact customer support.
123	Info	Vulnerability Protection Manager Forced Shutdown	On	On	
124	Info	Rule Update Deleted	On	On	
130	Info	Credentials Generated	On	On	
131	Warning	Credential Generation Failed	On	On	
140	Info	Discover Computers	On	On	
141	Warning	Discover Computers Failed	On	On	
142	Info	Discover Computers Requested	On	On	
143	Info	Discover Computers Cancelled	On	On	
150	Info	System Settings Saved	On (cannot be turned off)	On	

ID	Severity	Event	Record	Forward	Notes
151	Info	Software Added	On	On	
152	Info	Software Deleted	On	On	
153	Info	Software Updated	On	On	
154	Info	Software Exported	On	On	
155	Info	Software Platforms Changed	On	On	
160	Info	Authentication Failed	On	On	
161	Info	Rule Update Exported	On	On	
164	Info	Security Update Successful	On	On	
165	Error	Security Update Failed	On	On	
166	Info	Check for New Software Success	On	On	
167	Error	Check for New Software Failed	On	On	
168	Info	Manual Security Update Successful	On	On	
169	Error	Manual Security Update Failed	On	On	
170	Error	Manager Available Disk Space Too Low	On	On	The Manager has determined that there is not enough disk space available to continue to function and will shutdown. When this error occurs the Manager will shutdown. The resolution is to free up disk space and restart the Manager.
180	Info	Alert Type Updated	On	On	
190	Info	Alert Started	On	On	
191	Info	Alert Changed	On	On	
192	Info	Alert Ended	On	On	
197	Info	Alert Emails Sent	On	On	
198	Warning	Alert Emails Failed	On	On	An Alert was raised which had been configured to generate an email notification to one or more users but the email could not be sent. Make sure SMTP setting are properly configured.
199	Error	Alert Processing Failed	On	On	Processing of the Alerts has failed. This may mean that the current Alert status is inaccurate. There is no resolution for this error. If it persists, contact customer support.
250	Info	Computer Created	On	On	
251	Info	Computer Deleted	On	On	
252	Info	Computer Updated	On	On	
253	Info	Policy Assigned to Computer	On	On	
254	Info	Computer Moved	On	On	

ID	Severity	Event	Record	Forward	Notes
255	Info	Activation Requested	On	On	
256	Info	Send Policy Requested	On	On	
257	Info	Locked	On	On	
258	Info	Unlocked	On	On	
259	Info	Deactivation Requested	On	On	
260	Info	Scan for Open Ports	On	On	
261	Warning	Scan for Open Ports Failed	On	On	
262	Info	Scan for Open Ports Requested	On	On	
263	Info	Scan for Open Ports Cancelled	On	On	
264	Info	Agent Software Upgrade Requested	On	On	
265	Info	Agent Software Upgrade Cancelled	On	On	
266	Info	Warnings/Errors Cleared	On	On	
267	Info	Check Status Requested	On	On	
268	Info	Get Events Requested	On	On	
270	Error	Computer Creation Failed	On	On	
273	Info	Security Update Requested	On	On	
274	Info	Security Update Rollback Requested	On	On	
275	Warning	Duplicate Computer	On	On	
276	Info	Security Updates Downloaded	On	On	
280	Info	Computers Exported	On	On	
281	Info	Computers Imported	On	On	
286	Info	Computer Log Exported	On	On	
290	Info	Group Added	On	On	

ID	Severity	Event	Record	Forward	Notes
291	Info	Group Removed	On	On	
292	Info	Group Updated	On	On	
293	Info	Interface Renamed	On	On	
294	Info	Computer Bridge Renamed	On	On	
295	Info	Interface Deleted	On	On	
296	Info	Interface IP Deleted	On	On	
297	Info	Scan for Recommendations Requested	On	On	
298	Info	Recommendations Cleared	On	On	
299	Info	Asset Value Assigned to Computer	On	On	
300	Info	Scan for Recommendations Completed	On	On	
301	Info	Agent Software Deployment Requested	On	On	
302	Info	Agent Software Removal Requested	On	On	
303	Info	Computer Renamed	On	On	
310	Info	Directory Added	On	On	
311	Info	Directory Removed	On	On	
312	Info	Directory Updated	On	On	
320	Info	Directory Synchronization	On	On	
321	Info	Directory Synchronization Finished	On	On	
322	Error	Directory Synchronization Failed	On	On	
323	Info	Directory Synchronization Requested	On	On	
324	Info	Directory Synchronization Cancelled	On	On	

ID	Severity	Event	Record	Forward	Notes
325	Info	User Synchronization	On	On	Synchronization of the Users list with an Active Directory has been started.
326	Info	User Synchronization Finished	On	On	Synchronization of the Users list with an Active Directory has completed.
327	Error	User Synchronization Failed	On	On	
328	Info	User Synchronization Requested	On	On	
329	Info	User Synchronization Cancelled	On	On	
330	Info	SSL Configuration Created	On	On	
331	Info	SSL Configuration Deleted	On	On	
332	Info	SSL Configuration Updated	On	On	
350	Info	Policy Created	On	On	
351	Info	Policy Deleted	On	On	
352	Info	Policy Updated	On	On	
353	Info	Policies Exported	On	On	
354	Info	Policies Imported	On	On	
410	Info	Firewall Rule Created	On	On	
411	Info	Firewall Rule Deleted	On	On	
412	Info	Firewall Rule Updated	On	On	
413	Info	Firewall Rule Exported	On	On	
414	Info	Firewall Rule Imported	On	On	
420	Info	Firewall Stateful Configuration Created	On	On	
421	Info	Firewall Stateful Configuration Deleted	On	On	
422	Info	Firewall Stateful Configuration Updated	On	On	

ID	Severity	Event	Record	Forward	Notes
423	Info	Firewall Stateful Configuration Exported	On	On	
424	Info	Firewall Stateful Configuration Imported	On	On	
460	Info	Application Type Created	On	On	
461	Info	Application Type Deleted	On	On	
462	Info	Application Type Updated	On	On	
463	Info	Application Type Exported	On	On	
464	Info	Application Type Imported	On	On	
470	Info	Intrusion Prevention Rule Created	On	On	
471	Info	Intrusion Prevention Rule Deleted	On	On	
472	Info	Intrusion Prevention Rule Updated	On	On	
473	Info	Intrusion Prevention Rule Exported	On	On	
474	Info	Intrusion Prevention Rule Imported	On	On	
505	Info	Context Created	On	On	
506	Info	Context Deleted	On	On	
507	Info	Context Updated	On	On	
508	Info	Context Exported	On	On	
509	Info	Context Imported	On	On	
510	Info	IP List Created	On	On	
511	Info	IP List Deleted	On	On	
512	Info	IP List Updated	On	On	
513	Info	IP List Exported	On	On	
514	Info	IP List Imported	On	On	
520	Info	Port List Created	On	On	
521	Info	Port List Deleted	On	On	

ID	Severity	Event	Record	Forward	Notes
522	Info	Port List Updated	On	On	
523	Info	Port List Exported	On	On	
524	Info	Port List Imported	On	On	
525	Info	Scan Cache Configuration Created	On	On	
526	Info	Scan Cache Configuration Exported	On	On	
530	Info	MAC List Created	On	On	
531	Info	MAC List Deleted	On	On	
532	Info	MAC List Updated	On	On	
533	Info	MAC List Exported	On	On	
534	Info	MAC List Imported	On	On	
540	Info	Proxy Created	On	On	
541	Info	Proxy Deleted	On	On	
542	Info	Proxy Updated	On	On	
543	Info	Proxy Exported	On	On	
544	Info	Proxy Imported	On	On	
550	Info	Schedule Created	On	On	
551	Info	Schedule Deleted	On	On	
552	Info	Schedule Updated	On	On	
553	Info	Schedule Exported	On	On	
554	Info	Schedule Imported	On	On	
560	Info	Scheduled Task Created	On	On	
561	Info	Scheduled Task Deleted	On	On	
562	Info	Scheduled Task Updated	On	On	
563	Info	Scheduled Task Manually Executed	On	On	
564	Info	Scheduled Task Started	On	On	
565	Info	Backup Finished	On	On	
566	Error	Backup Failed	On	On	
567	Info	Sending Outstanding Alert Summary	On	On	
568	Warning	Failed To Send Outstanding Alert Summary	On	On	

ID	Severity	Event	Record	Forward	Notes
569	Warning	Email Failed	On	On	An email notification could not be sent. Make sure SMTP setting are properly configured (**Administration > System Settings > SMTP**).
570	Info	Sending Report	On	On	
571	Warning	Failed To Send Report	On	On	
572	Error	Invalid Report Jar	On	On	
573	Info	Asset Value Created	On	On	
574	Info	Asset Value Deleted	On	On	
575	Info	Asset Value Updated	On	On	
576	Error	Report Uninstall Failed	On	On	
577	Error	Report Uninstalled	On	On	
580	Warning	Application Type Port List Misconfiguration	On	On	
581	Warning	Application Type Port List Misconfiguration Resolved	On	On	
582	Warning	Intrusion Prevention Rules Require Configuration	On	On	
583	Info	Intrusion Prevention Rules Require Configuration Resolved	On	On	
590	Warning	Scheduled Task Unknown Type	On	On	
600	Info	User Signed In	On	On	
601	Info	User Signed Out	On	On	
602	Info	User Timed Out	On	On	
603	Info	User Locked Out	On	On	
604	Info	User Unlocked	On	On	
608	Error	User Session Validation Failed	On	On	Manager is unable to confirm that the User session is the one that was initiated by a successful User sign-in/authentication. Manager will return the User to the sign-in page. User will be forced to re-authenticate.

ID	Severity	Event	Record	Forward	Notes
609	Error	User Made Invalid Request	On	On	Manager received invalid request to access the audit data (Events). Access to the audit data is denied.
610	Info	User Session Validated	Off	Off	
611	Info	User Viewed Firewall Event	Off	Off	
613	Info	User Viewed Intrusion Prevention Event	Off	Off	
615	Info	User Viewed System Event	Off	Off	
650	Info	User Created	On	On	
651	Info	User Deleted	On	On	
652	Info	User Updated	On	On	
653	Info	User Password Set	On	On	
660	Info	Role Created	On	On	
661	Info	Role Deleted	On	On	
662	Info	Role Updated	On	On	
663	Info	Roles Imported	On	On	
664	Info	Roles Exported	On	On	
670	Info	Contact Created	On	On	
671	Info	Contact Deleted	On	On	
672	Info	Contact Updated	On	On	
700	Info	Agent Software Installed	On	On	
701	Error	Agent Software Installation Failed	On	On	
702	Info	Credentials Generated	On	On	
703	Error	Credential Generation Failed	On	On	
704	Info	Activated	On	On	
705	Error	Activation Failed	On	On	
706	Info	Agent Software Upgraded	On	On	
707	Warning	Agent Software Upgrade Failed	On	On	
708	Info	Deactivated	On	On	
709	Error	Deactivation Failed	On	On	
710	Info	Events Retrieved	On	On	
711	Info	Agent Software Deployed	On	On	

ID	Severity	Event	Record	Forward	Notes
712	Error	Agent Software Deployment Failed	On	On	
713	Info	Agent Software Removed	On	On	
714	Error	Agent Software Removal Failed	On	On	
715	Info	Agent Version Changed	On	On	
720	Info	Policy Sent	On	On	Agent updated.
721	Error	Send Policy Failed	On	On	
722	Warning	Get Interfaces Failed	On	On	
723	Info	Get Interfaces Failure Resolved	On	On	
724	Warning	Insufficient Disk Space	On	On	An Agent has reported low disk space. Free space on the Agent's host.
725	Warning	Events Suppressed	On	On	
726	Warning	Get Agent Events Failed	On	On	Manager was unable to retrieve Events from Agent. This error does not mean that the data was lost on the Agent. This error is normally caused by a network interruption while events are being transferred. Clear the error and run a "Check Status" to retry the operation.
727	Info	Get Agent Events Failure Resolved	On	On	
728	Error	Get Events Failed	On	On	Manager was unable to retrieve audit data from Agent. This error does not mean that the data was lost on the Agent. This error is normally caused by a network interruption while events are being transferred. Clear the error and run a "Get Events Now" to retry the operation.
729	Info	Get Events Failure Resolved	On	On	
730	Error	Offline	On	On	Manager cannot communicate with Computer. This error does not mean that protection being provided by an Agent is inactive. See ***Computer and Agent Status (page 108)*** for more information.
731	Info	Back Online	On	On	
732	Error	Firewall Rule Engine Offline	On	On	The Firewall Engine is offline and traffic is flowing unfiltered. This is normally due to an error during installation or verification of the driver on the computer's OS platform. Check the status of the network driver at the computer to ensure it is properly loaded.
733	Info	Firewall Rule Engine Back Online	On	On	
734	Warning	Computer Clock Change	On	On	A clock change has occurred on the Computer which exceeds the maximum allowed specified in **Policy/Computer Editor >**

ID	Severity	Event	Record	Forward	Notes
					Settings > Computer > Heartbeat area. Investigate what has caused the clock change on the computer.
735	Warning	Misconfiguration Detected	On	On	The Agent's configuration does not match the configuration indicated in the Manager's records. This is typically because of a recent backup restoration of the Manager or the Agent. Unanticipated misconfiguration warnings should be investigated.
736	Info	Check Status Failure Resolved	On	On	
737	Error	Check Status Failed	On	On	
738	Error	Intrusion Prevention Rule Engine Offline	On	On	The Intrusion Prevention Engine is offline and traffic is flowing unfiltered. This is normally due to an error during installation or verification of the driver on the computer's OS platform. Check the status of the network driver at the computer to ensure it is properly loaded.
739	Info	Intrusion Prevention Rule Engine Back Online	On	On	
740	Error	Agent Error	On	On	
741	Warning	Abnormal Restart Detected	On	On	
742	Warning	Communications Problem	On	On	The Agent is having problems communicating its status to Manager. It usually indicates network or load congestion in the Agent -> Manager direction. Further investigation is warranted if the situation persists.
743	Info	Communications Problem Resolved	On	On	
745	Warning	Events Truncated	On	On	
750	Warning	Last Automatic Retry	On	On	
755	Info	Vulnerability Protection Manager Version Compatibility Resolved	On	On	
756	Warning	Vulnerability Protection Manager Upgrade Recommended (Incompatible Security Update(s))	On	On	
760	Info	Agent Version Compatibility Resolved	On	On	

ID	Severity	Event	Record	Forward	Notes
761	Warning	Agent Upgrade Recommended	On	On	
762	Warning	Agent Upgrade Required	On	On	
763	Warning	Incompatible Agent Version	On	On	
764	Warning	Agent Upgrade Recommended (Incompatible Security Component(s))	On	On	
765	Warning	Computer Reboot Required	On	On	
766	Warning	Network Engine Mode Configuration Incompatibility	On	On	
767	Warning	Network Engine Mode Version Incompatibility	On	On	
768	Warning	Network Engine Mode Incompatibility Resolved	On	On	
770	Warning	Agent Heartbeat Rejected	On	On	
771	Warning	Contact by Unrecognized Client	On	On	
780	Info	Scan for Recommendations Failure Resolved	On	On	
781	Warning	Scan for Recommendations Failure	On	On	
784	Info	Security Update Successful	On	On	
785	Warning	Security Update Failure	On	On	
786	Info	Scan For Change Failure Resolved	On	On	
787	Warning	Scan For Change Failure	On	On	
790	Info	Agent-Initiated Activation Requested	On	On	

ID	Severity	Event	Record	Forward	Notes
791	Warning	Agent-Initiated Activation Failure	On	On	
800	Info	Alert Dismissed	On	On	
801	Info	Error Dismissed	On	On	
900	Info	Vulnerability Protection Manager Audit Started	On	On	
901	Info	Vulnerability Protection Manager Audit Shutdown	On	On	
902	Info	Vulnerability Protection Manager Installed	On	On	
903	Warning	License Related Configuration Change	On	On	
910	Info	Diagnostic Package Generated	On	On	
911	Info	Diagnostic Package Exported	On	On	
912	Info	Diagnostic Package Uploaded	On	On	
913	Error	Automatic Diagnostic Package Error	On	On	
920	Info	Usage Information Generated	On	On	
921	Info	Usage Information Package Exported	On	On	
922	Info	Usage Information Package Uploaded	On	On	
923	Error	Usage Information Package Error	On	On	
930	Info	Certificate Accepted	On	On	
931	Info	Certificate Deleted	On	On	
940	Info	Auto-Tag Rule Created	On	On	
941	Info	Auto-Tag Rule Deleted	On	On	
942	Info	Auto-Tag Rule Updated	On	On	
943	Info	Tag Deleted	On	On	
944	Info	Tag Created	On	On	

ID	Severity	Event	Record	Forward	Notes
970	Info	Command Line Utility Started	On	On	
978	Info	Command Line Utility Failed	On	On	
979	Info	Command Line Utility Shutdown	On	On	
980	Info	System Information Exported	On	On	
992	Info	Manager Node Updated	On	On	
997	Error	Tagging Error	On	On	
998	Error	System Event Notification Error	On	Off (Cannot be turned on)	
999	Error	Internal Software Error	On	On	
1101	Error	Plug-in Installation Failed	On	On	
1102	Info	Plug-in Installed	On	On	
1103	Error	Plug-in Upgrade Failed	On	On	
1104	Info	Plug-in Upgraded	On	On	
1105	Error	Plug-in Start Failed	On	On	
1106	Error	Plug-in Uninstall Failed	On	On	
1107	Info	Plug-in Uninstalled	On	On	
1108	Info	Plug-in Started	On	On	
1109	Info	Plug-in Stopped	On	On	
1505	Info	Directory List Created	On	On	
1506	Info	Directory List Deleted	On	On	
1507	Info	Directory List Updated	On	On	
1508	Info	Directory List Exported	On	On	
1509	Info	Directory List Imported	On	On	
1554	Info	Firewall Stateful Configuration Updated	On	On	

ID	Severity	Event	Record	Forward	Notes
1555	Info	Intrusion Prevention Configuration Updated	On	On	
1603	Info	Security Update Rollback Success	On	On	
1604	Warning	Security Update Rollback Failure	On	On	
1677	Error	Trusted Platform Module Error	On	On	
1678	Info	Trusted Platform Module Register Values Loaded	On	On	
1679	Warning	Trusted Platform Module Register Values Changed	On	On	
1680	Info	TPM Checking Disabled	On	On	
1700	Info	Expected Activation Failure	On	On	
1800	Error	Vulnerability Protection Protection Module Failure	On	On	
2000	Info	Scan Cache Configuration Object Added	On	On	
2001	Info	Scan Cache Configuration Object Removed	On	On	
2002	Info	Scan Cache Configuration Object Updated	On	On	
2400	Info	Firewall Installation Began	On	On	
2401	Info	Firewall Installation Succeeded	On	On	
2402	Warning	Firewall Installation Failed	On	On	
2403	Info	Firewall Download Succeeded	On	On	
2500	Info	Intrusion Prevention Installation Began	On	On	

ID	Severity	Event	Record	Forward	Notes
2501	Info	Intrusion Prevention Installation Succeeded	On	On	
2502	Warning	Intrusion Prevention Installation Failed	On	On	
2503	Info	Intrusion Prevention Download Succeeded	On	On	

Manually Deactivate/Stop/Start the Agent

Deactivating the Agent

Deactivation of the Agent can normally be done from the Vulnerability Protection Manager that is currently managing the Agent. If the Vulnerability Protection Manager cannot communicate with the Agent, 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\Vulnerability Protection Agent**)
2. Run the following: **dsa_control.exe -r**

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**

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 Vulnerability Protection 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 Vulnerability Protection Manager, go to **Administration > Updates > Software Updates** .
2. Make sure the most recent Vulnerability Protection Agents have been downloaded to the Vulnerability Protection 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.

More About Event Tagging

In Vulnerability Protection, a **Tag** is a unit of meta-data that you can apply to a Vulnerability Protection 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 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 Vulnerability Protection 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 Vulnerability Protection Events: Firewall, Intrusion Prevention, and System Events.

Performance Requirements

The following guidelines provide a general idea of the infrastructure requirements for Vulnerability Protection 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 150)***.)

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.

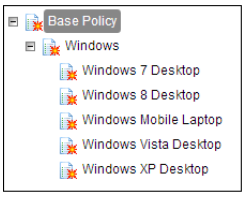
Dedicated Servers

The Vulnerability Protection 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 Vulnerability Protection Manager and the database should be installed on dedicated servers. It is also important that the database and the Vulnerability Protection Manager be co-located to ensure unhindered communication between the two. The same applies to additional Vulnerability Protection 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.*

Policies, Inheritance, and Overrides

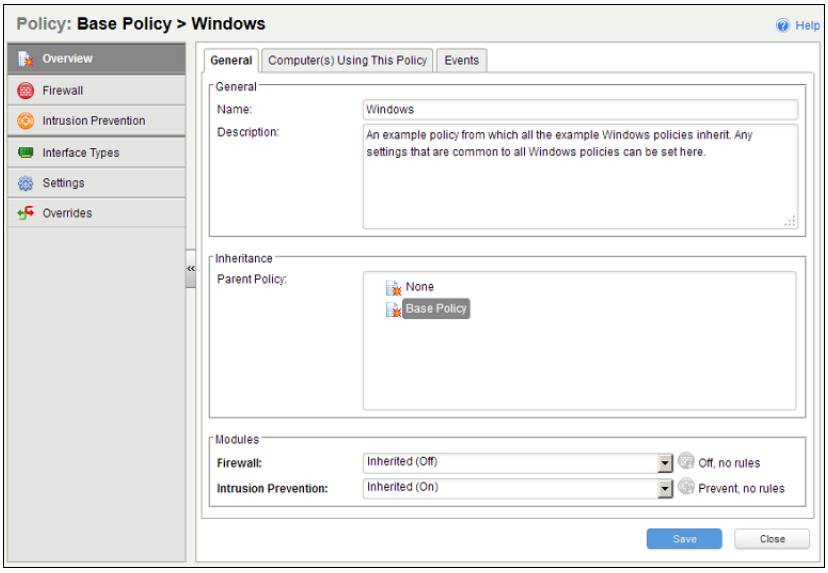
Most Vulnerability Protection elements and settings operate on multiple hierarchical levels starting a parent Base Policy level, going down through multiple levels of child Policies, and finishing at the level of the Computer to which the final Policy is assigned. Vulnerability Protection provides a 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. Vulnerability Protection also has branches designed for specific operating systems. 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.



This means that the setting is inherited from the parent **Base** Policy, and that if you were to change the Firewall setting in the **Base** Policy from **Off** to **On**, the setting would change in the **Windows** Policy as well. (The

Windows Policy setting setting would then read **Inherited (On)**. The value in parentheses always shows you what the current inherited setting is.)

Overriding Object Properties

The Intrusion Prevention Rules that are included in this Policy are copies of the Intrusion Prevention Rules stored by the Vulnerability Protection 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 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 Vulnerability Protection 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 are displayed by protection module. You can revert system or module overrides by clicking the **Remove** button.

Ports Used

Vulnerability Protection

Port: 4119 (default)

- Use:
  - Access to Vulnerability Protection Manager Web console browser interface.
- Protocol: TCP
- Initiated By:
  - Web Browser
- Connected To: Vulnerability Protection Manager
- Proxy: No
- Configuration: This port is configured during the Vulnerability Protection Manager installation process.

Port: 4120 (default)

- Use: Agent-initiated communication with the Manager. The Agent sends Events to the Manager, and the Manager sends Configuration Updates.
- Protocol: TCP
- Initiated By: Agent
- Connected To: Vulnerability Protection Manager
- Proxy: No
- Configuration: This port is configured during the Vulnerability Protection Manager installation process.

Agent

Port: 4118

- Use: Manager-to-Agent communication.
- Protocol: TCP
- Initiated By: Vulnerability Protection Manager
- Connected To: Agent
- Proxy: No
- Configuration: This port is not configurable. (Contact your support provider if this port assignment is problematic.)

SQL Server Database Server

Port: 1433, 1434

- Use: Manager-to-database communication (required to connect the database to the Vulnerability Protection Manager)
- Protocol: TCP for 1433, UDP for 1434
- Initiated By: Vulnerability Protection Manager
- Connected To: SQL database server
- Proxy: No
- Configuration: This port is configured during the Vulnerability Protection 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: Vulnerability Protection Manager
- Connected To: Oracle database server
- Proxy: No
- Configuration: This port is configured during the Vulnerability Protection Manager installation process.

Syslog Facility

Port: 514 (default)

- Use: Syslog
- Protocol: UDP
- Initiated By: Agent
- 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: Vulnerability Protection 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: Vulnerability Protection Manager
- 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 Vulnerability Protection Manager
- Protocol: TCP
- Initiated By: Vulnerability Protection Manager
- Connected To: LDAP server
- Proxy: No
- Configuration: This port can be configured in the **Add Directory** wizard on the **Computers** page.

Certified Safe Software Service

Port: 443

- Use: Certified Safe Software Service
- Protocol: TCP
- Initiated By: Vulnerability Protection 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: Vulnerability Protection Manager
- Connected to: DNS server
- Proxy: No
- Configuration: The port is randomly selected when the Vulnerability Protection Manager needs to lookup a hostname.

Teamed NICs

Installing the Windows 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 so that they are compatible with the Vulnerability Protection Agent. If you encounter difficulties, please contact your support provider.

Windows

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

Note:	*Using the Agent in a teamed NICs environment on Windows 2003 requires SP 2 or later, or the installation of the following patch: http://support.microsoft.com/kb/912222/article*

Note:	*Using the Agent in a teamed NICs environment on Windows 2000 is not supported.*

Note:	*The Agent's network driver is bound to the network interfaces only at install or upgrade time. After installation, it is not possible for the bindings to be automatically adjusted when you add or remove network interfaces to or from a Teamed NIC. Doing so can lead to network connectivity problems, or to the host system not being properly protected. After adding or removing a network interface in a teamed environment where the Agent's network driver is installed, you should verify that the driver is only bound to the virtual interface and not bound to any physical adapters.*

Support

Please visit the Trend Micro customer support Web site for assistance with any of your Trend Micro Products:

Trend Micro Customer Support

TREND MICRO INCORPORATED
10101 North De Anza Blvd. Cupertino, CA., 95014, USA
Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com
www.trendmicro.com
Item Code: APEM26309/140218