Administration Guide

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

Document Version: VBUS-AG-9.3.0

Last updated: Monday, April 25, 2016

Table of Contents

1 — Introduction

VIPRE is a scalable Endpoint Solution that protects your networked machines from all types of malware and viruses and includes a firewall (Premium and Endpoint only). Its Bad URL Blocking feature under web filtering prevents end users from accidentally opening known bad websites (Premium and Endpoint only). VIPRE Business can be installed at more than one physical location and still be centrally managed. Its policy-based architecture allows administrators to create multiple policies based on user and machine types.

You can get information about VIPRE Business from any of the following:

- The **Help** is your primary resource for answers to questions you may have while using VIPRE Business. Wherever you are in the application, you can press F1 to display context sensitive help with links to conceptual and procedural information.
- The **Administration Guide** offers the same information as the Help and is arranged in one document.

These are downloadable PDF files available at ThreatTrackSecurity.com.

1.1 — About this document

Note: This document applies to VIPRE® Antivirus Business, VIPRE® Business Premium, and VIPRE® Endpoint Security, except when noted for specific features. The features Anti-Phishing, Advanced Browser Protection, Firewall, and Patch Management apply to VIPRE Business Premium and VIPRE Endpoint Security. The Device Control feature applies only to VIPRE Endpoint Security.

1.2 — System Requirements

For the most up to date System Requirements, please visit our product website at threattracksecurity.com.

1.2.1 — Admin Console and VIPRE Site Service

Operating systems

- Windows Server 2012 (excluding Server 2012 Core)
- Windows Small Business Server 2011, 2008 and 2003
- Windows Server 2008 SP2 and 2008 R2 (excluding Server 2008 Core)
- Windows Server 2003 SP1+ (32- & 64-bit)
- Windows 10
- Windows 8 (32- & 64-bit)
- Windows 7 (32- & 64-bit)
- Windows Vista SP2 (32- & 64-bit)
- Windows XP Professional SP3 (32- & 64-bit)

Note: Embedded operating systems are not supported

Hardware

- Pentium III 400 MHz or higher
- 300 MB free disk space
- 512 MB memory
- 1024 x 768 monitor resolution

Miscellaneous

- MDAC 2.6 SP2 or later
- Internet Explorer 6 or later
- Microsoft .NET Framework 3.5 (if not already installed, .NET will automatically install during installation)

1.2.2 — VIPRE Agent (Windows)

Operating systems

- Windows 10
- Windows 8 (32- & 64-bit)
- Windows 7 (32- & 64-bit)
- Windows Vista, Vista SP1+(32- & 64-bit)
- Windows XP Professional SP2+ (32- & 64-bit)
- Windows Server 2012 (including R2)
- Windows Small Business Server 2011, 2008 and 2003
- Windows Server 2008 and 2008 R2 (excluding Server 2008 Core)
- Windows Server 2003 SP1+ (32- & 64-bit)
- Windows 2000 Server with SP4 RU1 or later (supports legacy 5.0 agents for upgrade only)
- Windows 2000 Professional with SP4 RU1 or later (supports legacy 5.0 agents for upgrade only)
- Windows Embedded for Point of Service (WEPOS) platforms

Hardware

- 300 MB free disk space
- 512 MB memory

Miscellaneous

- Internet Explorer 6 or later

Supported email applications

- Outlook 2000+
- Outlook Express 5.0+
- Windows Mail on Vista
- SMTP/POP3 (Thunderbird, IncrediMail, Eudora, etc.)
- SSL supported in Outlook and Outlook Express only

1.2.3 — VIPRE Agent (Mac)

Operating systems

- OSX 10.8 (Mountain Lion)
- OSX 10.9 (Mavericks)
- OSX 10.10 (Yosemite)

1.2.4 — VIPRE Business Mobile Security

Operating systems

- Android 2.2 and above
- iOS 5.1.1 and above

1.2.5 — Hyper-V Agent

Operating systems

- Windows Server
  - Windows Server 2012 R2
  - Windows Server 2012 R2 Core
  - Windows Server 2012
  - Windows Server 2012 Core
  - Windows Server 2008 R2 SP1
  - Windows Server 2008 R2 SP1 Core
- Microsoft Hyper-V Server
  - Microsoft Hyper-V Server 2012 R2
  - Microsoft Hyper-V Server 2012
  - Microsoft Hyper-V Server 2008 R2 SP1
  - Windows 8.1 with Hyper-V role enabled
  - Windows 8 with Hyper-V role enabled

1.3 — VIPRE Business Components

VIPRE Business consists of the following main components:

- The **VIPREAdmin Console** is the interface to centrally manage agent computers
- The **VIPRE Database** for new installations (up to 500 Agents) is a built-in database requiring zero-configuration. Microsoft SQL and SQL Express databases are configurable and recommended for users with over 500 Agents
- The **VIPRE Site Service (VSS)** is the VIPRE component that handles all communication between the VIPRE Database, the Admin Console, and the Agents
- A **Site** is a physical location where the VSS is installed. Additional sites can be configured as needed, and consist of all of the Policies and Agents unique to a site
- A **Policy** consists of a set of configurations. You create configured policies that fit your organization's needs and then assign Agents to those policies. A new policy is created based on one of the policies that are included with VIPRE Business:
  - The **Default Policy** includes basic configurations with most Remediation settings set to Quarantine

IMPORTANT: Active Protection, Email Protection, and the Firewall *(Premium and Endpoint users only)* are OFF by default in the Default Policy.

- The **Default policies** are designed for some commonly used configurations, including: Workstations, various server types, and remote users. Also, the Defaults are pre-populated with Microsoft's recommendations for antivirus scanning exclusions

- An **Agent** is installed on client machines (computers that you want to protect) which run periodic security scans, based on settings of the assigned policy. The following tabs are available for every Site or Policy that you create. They enable you to install, manage and configure your agents, network-wide:
  - **Unprotected Computers** - displays the computers that don't have an agent installed on them
  - **Protected Computers** - displays the computers that are running agent scans based on the assigned security policies
  - **Patch Management** - provides system patching status for every computer that is running an agent, ensuring that your systems are kept up to date
  - **Quarantine** - enables you to see quarantined items and provides details about each threat
  - **Pending Agent Installs** - displays the computers that initiated an agent install and are still in progress
  - **Agent Install History** - displays records of all the attempted agent installs
- The **Report Viewer** is a standalone application that is installed with the Console by default. Also, it can be installed by itself on separate machines to be used by administrators and managers who want to run various reports at their convenience
- **Update Servers** are optional; they can be created for Agents to receive updates locally and are configured at the Policy level.

1.4 — Registering VIPRE Business

To benefit from all the features and full performance of VIPRE, it is recommended to register the product immediately after installation. A license key is required for every site you are going to manage.

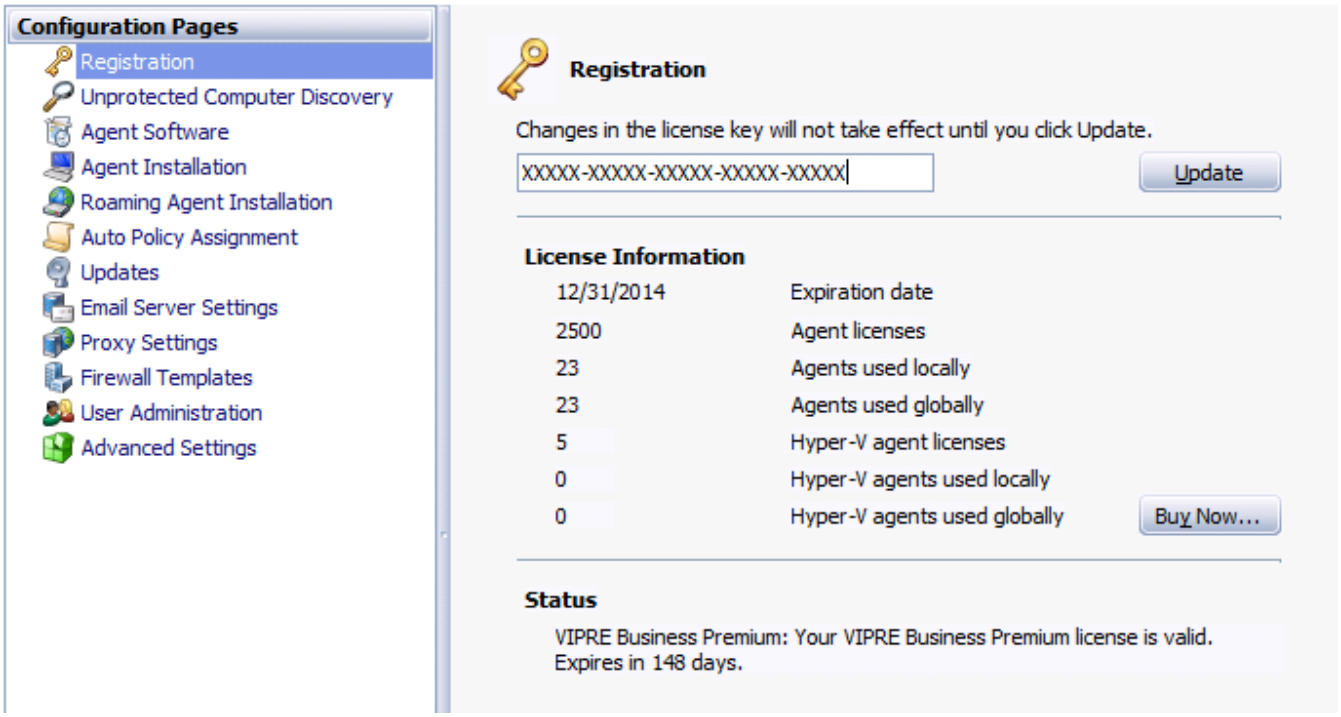
> **Note**: In the free trial mode, you can have up to 5 agents installed. A license key is not required for the free trial.

To purchase VIPRE Business

1. From the Admin Console, click **Help > Registration**.

> **Note**: Alternatively, from Site Navigator, right-click on the site you want to register and select **Properties**.

2. (Optional) From the top-right of the Site Properties dialog, select the site you want to register.
3. From the left pane, click **Registration** under **Configuration Pages**.



4. Click **Buy Now**. The ThreatTrack Security product page displays in your default browser.
5. After purchasing VIPRE Business, register your license following the procedure below.

To register VIPRE Business

1. From the Admin Console, click **Help > Registration**.

> **Note**: Alternatively, from Site Navigator, right-click on the site you want to register and select **Properties**.

2. (Optional) From the top-right of the Site Properties dialog, select the site you want to register.
3. From the left pane, click **Registration** under **Configuration Pages**.
4. Key in or paste the license key in the registration box and click **Update**.
5. Click **OK**.

2 — Installing Agents on Machines

This chapter on Installing Agents on Machines covers all the procedures for installing agents.

An **Agent** is the client software that is installed on workstations or other machines, running periodic scans for threats based on its assigned policy. The following tabs enable you to install, manage and configure your agents, network-wide:Unprotected ComputersProtected ComputersPatch ManagementQuarantine Pending Agent Installs Agent Install History

2.1 — Manually Installing Agents

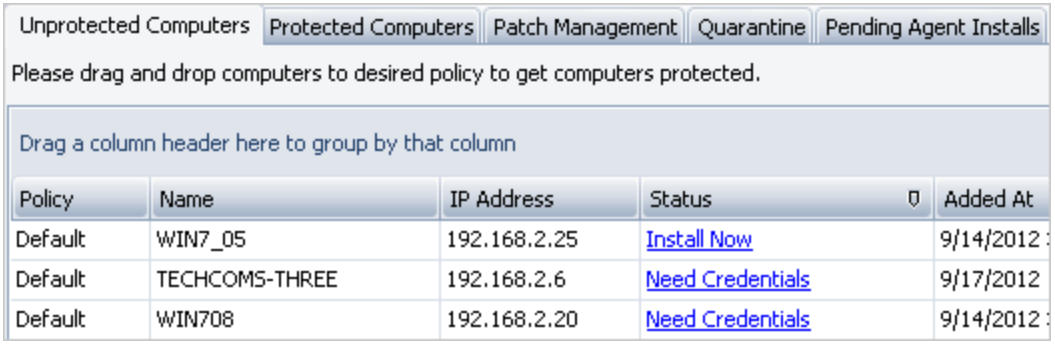
When VIPRE is installed, it automatically scans your network to detect online computers and lists them under the **Unprotected Computers** tab of your Default Policy. This tab shows the computers that do not have an agent installed on them. Through the Unprotected Computers tab, you are able to deploy agents on specific computers as well as assign security policies on agent by agent basis.

Note: In evaluation mode, you can have up to 5 agents installed.

Note: To deploy agents in large environments, it is recommended to use an automatic installation method, especially if the agents will share the same settings. This reduces configuration time and prevents manual configuration errors.

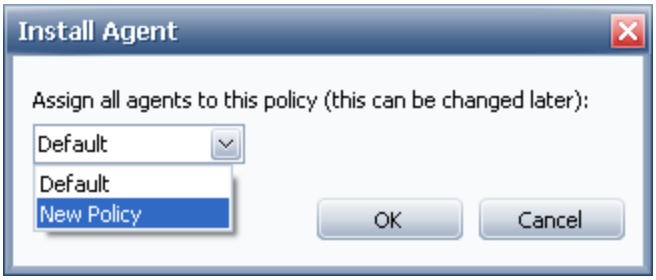
To manually install agents:

1. From the main menu, click **Install Agent**. This displays the **Unprotected Computers** tab of your default policy.

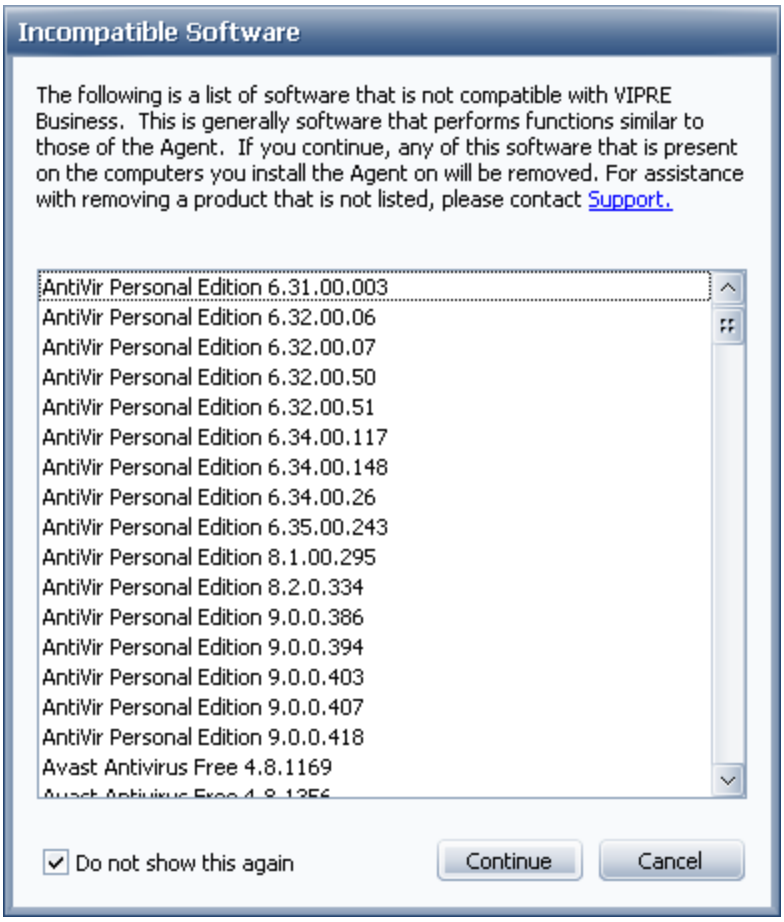


2. From the **Unprotected Computers** tab, you may install an agent in one of three ways, all with the same end result:
   a. From the **Status** column, click **Install Now** for each agent you want to install.
   b. Alternatively, use **Ctrl** or **Shift** to select multiple computers, right-click and select **Install Agent(s)...**
   c. You may also click the **Install Now** button in the **Install Column** on the left side of the display for each agent you wish to install.

Note: When VIPRE cannot connect to the selected computers using the pre-configured remote credentials, it displays **Need Credentials** instead of **Install Now**. Click **Need Credentials** and key in the required username and password.



3. Select the policy that you want to assign to the new agent(s) and click **OK**.



4. From the **Incompatible Software** dialog, review the software that can interfere or interrupt VIPRE's activity. Click **Continue** to begin installing the agent(s).

Note: After an agent is installed, the computer is automatically listed under the **Protected Computers** tab.

2.2 — Automatic Agent Installation

Automatic Agent Installation is a pre-configured process for each policy, whereby agents are automatically installed on newly discovered machines. You can select the locations where VIPRE scans for new machines, using any of the following methods (or in combination):

- Active Directory Queries
- Machine Lists
- IP Ranges and/or Subnets.

> **Note**: **Active Directory** is the **recommended** method because it will detect new machines as soon as they are joined to the domain.

Installing agents automatically consists of the following steps:

- Step 1: Configure a security policy
- Step 2: Configure the new policy Installation Management settings
- Step 3: Assign computers to the policy
- Step 4: Enable automatic agent installation at site level

Step 1: Configure a security policy

Agents are installed at policy-level, NOT at site-level. If you haven't configured a policy already, add a policy.

Step 2: Configure the new policy Agent Installation Management settings

1. From the **Admin Console > Site Navigator**, right-click on the policy to which you want to install agents and select **Properties**.
2. From the Policy Properties dialog, click **Agent Installation Management > Configuration** and configure the following:

Auto-Agent Installation Options:

- **Enabled**: select to enable Automatic Agent Installation at the policy level. The checkboxes below "Enabled" are grayed out until "Enabled" is selected.

> **Note**: You MUST enable scheduled automatic agent installation at both the policy and site level for a scheduled installation to occur. (*See Step 6*)

- **Only attempt to install to machines that respond to a ping**: when selected, the VSS tries to ping each machine first, then only installs to those that respond, reducing Agent Installation time considerably.

> **Note:** If you are blocking ICMP (Internet Control Message Protocol) traffic between VIPRE Business and the workstations, do NOT select this option. This will result in the pings failing and creating a large ping timeout value, thus increasing the deployment time considerably.

Step 3: Assign computers to the policy

1. From the Policy Properties dialog, select **Agent Installation Management > Computers**. You can select groups of machines using any of the methods below (or in combination):

   - **AD Queries**: (*recommended*) Active Directory queries run on the same directory as the VIPRE Site Service. You can run queries at the root level or by group level. If you select a group, then any new machine added to that group will have an agent installed the next time Automatic Agent Installation runs:

     i. Click **Add** to display the **Add AD Query Path(s)** dialog box.

     ii. Enter specific machine names or IP addresses to add to the query, or browse the appropriate domain, then select the sub-folder that you wish to query. Click **OK**.

   - **Machine List**: add one or more machines:

     i. Click **Add** to display the **Add Machines** dialog box.

     ii. Enter specific machine names or IP addresses to add to the list, or browse the appropriate domain, then select the machine or group of machines where you wish to install agents. Click **OK**.

   - **IP Ranges and Subnets**: in the IP Range section, enter a range of addresses and let the VIPRE Site Service resolve that list and find existing machines. The Subnet section allows you to get more specific, supporting up to a Class B address (such as 255.255.0.0):

     i. Click **Add** in either of these sections to display the **IP Range** or **Subnet** dialog box respectively.

     ii. Enter a range of IP addresses or a subnet Host Address and a Subnet Mask in the appropriate text boxes and click **OK**.

   - **Exclusion List**: after you have selected a group of machines you may find there are machines you wish to exclude from the Automatic Agent Installation. The **Exclusion List** takes precedence over all other lists. You can list the same machine in the **Machine List** area and the **Exclusion List** area. The final list will be resolved and that machine will be excluded. When Automatic Agent Installation runs, agents will not be installed on these listed machines:

     i. Click **Add** to display the **Add Exclusions** dialog box.

     ii. Enter specific machine names or IP addresses or browse to the appropriate domain, then select the machine or group of machines to which you wish to install agents. Click **OK**.

     iii. **Verify** the lists to combine the results of all queries into one list, thus removing any duplicates, as well as removing the machines listed in the **Exclusion List**:

     Once you have selected machines for Automatic Agent Installation, as well as any to be excluded, click **Verify**.

     After the computers are verified, a list of them displays. Select machines for further exclusion, if needed.

     Click **OK** to accept this list. Your Automatic Agent Installation list for this policy is now created and verified.

Step 4: Enable automatic agent installation at site level

1. From **Admin Console > Site Navigator**, right-click the site you want to configure and select **Properties**.
2. From the left pane, click **Agent Installation**.
3. Select **Enable automatic agents installation**, from under **Automatic Agent Installation**. This enables auto agent install for all the policies under the site.

4. In the space provided next to **Schedule Auto Installation start time**, specify the time when VIPRE scans your network for new machines and deploys agents on them.

Note: Time must be specified in 24-hour format.

5. Click **OK**.

Note: Each time Automatic Agent Installation runs, a "verify" automatically occurs; therefore, any machines added to the network will automatically be found if you are using an AD or IP range scope.

2.3 — Creating an Installer Package

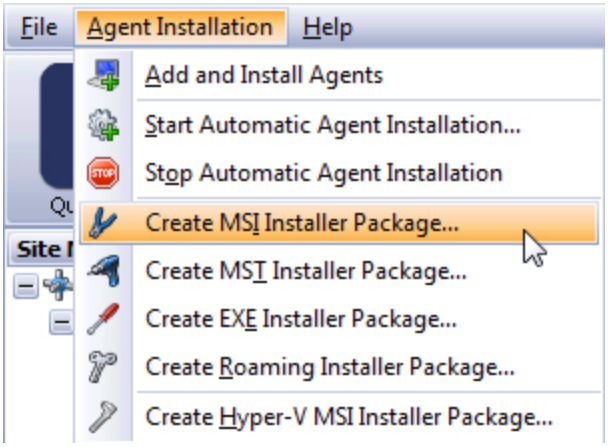
An **Installer Package** can consist of an MSI, MST, or EXE file. Once the package is created, you can distribute it on to machines manually or using a third-party application, such as Microsoft SMS.

Using an Installer Package is suitable for users who cannot use the "Push" manual installation method.

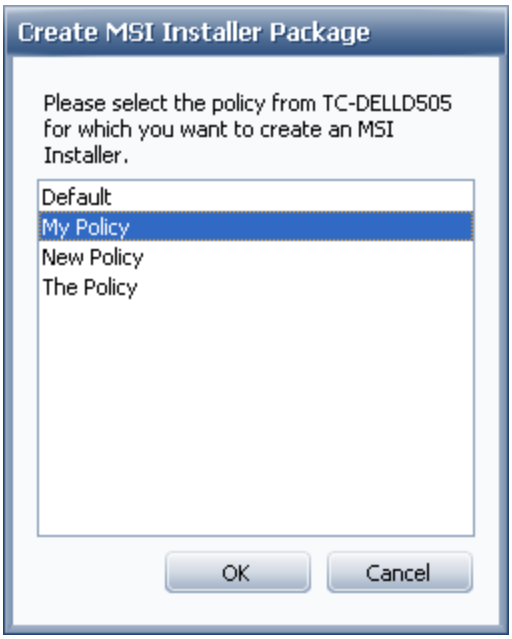
Note: Installation credentials are not relevant for Installer packages; they are only necessary for manual push and automatic installations.

To create an installer package:

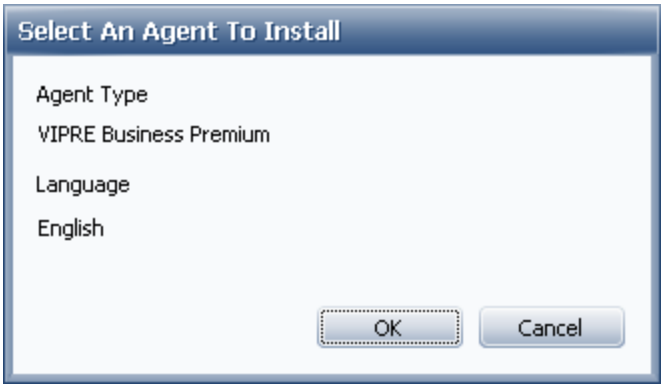
1. From the Admin Console, click **Agent Installation** and select one of the following installer package options:



- **Create MSI Installer Package** - creates an MSI installer that can be deployed across your network using Group Policy Objects (GPO)
- **Create MST Installer Package** - creates MST files that can be used to modify pre-installation settings of the MSI installer. This is used when an advanced deployment is selected in Group Policy Objects (GPO)
- **Create EXE Installer Package** - creates an executable file that can be used to install agents manually or automatically, using third-party tools.



2. Select the policy that is assigned to the agent when it is installed and click **OK**.



3. (Optional) Select the agent software that is installed when the installer package is executed. This applies for users who have a combination of VIPRE Business and VIPRE Business Premium or VIPRE Endpoint Security license keys.
4. Click **OK**.
5. Select a location where the package is saved and click **Save**.

Once the package is created, run the package on the workstation(s) manually or use a 3rd party application.

Note: In evaluation mode, you can have up to 5 agents installed.

2.4 — Agent Installation in a Workgroup Environment

Push vs. Installer Package

You can install agents in a Workgroup environment by either a "Push" method (see Manually Installing Agents) or by Creating an Installer Package.

Companies unable to use the Push method may find creating an MSI Installer Package is a good alternative.

Static IP Addresses

It's important to use a Static IP Address and NOT a Dynamic IP, because a Dynamic IP will change and then be unable to communicate to the server.

Enter the Static IP Address for each Policy, under **Policy Properties > Agent >** Communication **> Servers (Name or IP)** area.

2.5 — Connecting Agents over the WAN

VIPRE Business allows you to install and communicate with Agents across the Internet, even if they do not access the network via a VPN connection. This is done using Network Address Translation (NAT).

A policy for the remote agents has to be created; agents are deployed to that policy using an installer package.

Installing agents over WAN consists of the following steps:

- Step 1: Configure firewall settings
- Step 2: Create a policy for remote Agents
- Step 3: Create an installer package
- Step 4: Distribute the package
- Step 5: Install the package

Step 1: Configure firewall settings

1. If you are using a 3rd party (non-Microsoft) Business Router/Firewall:

> **Note**: If you are using the Microsoft Windows firewall, configuration is automatic. You will not need to do any further configuration.

2. Allow **Inbound** external traffic on port **TCP** and **UDP** port **18082** to the VIPRE Server.
3. Allow **SOAP** traffic (if your firewall blocks at the protocol level).
4. On your Remote Agents Router/Firewall:
   a. If the agent computer has a third-party firewall installed, you may need to allow **Outbound** traffic on **TCP** and **UDP** port **18082** so that it can communicate with the VIPRE Server.
   b. Allow **SOAP** traffic (if your firewall blocks at the protocol level).

Note: Some firewalls may block SOAP over HTTP. You will need to configure your firewall to allow this communication type.

Step 2: Create a policy for remote Agents

1. From **Site Navigator**, right-click on the site to which you want to add a policy and select **Add Policy**.
2. Enter a name for the remote agents policy, for example, "Remote Agents".
3. Double-click the policy to open the Policy Properties screen.
4. From the left pane, click **Agent > Communication**.
5. Under **Servers (Name or IP)**, key in the public IP and communication port for:
6. **Policy Server** - server that distributes security policy updates to machines running an agent
7. **Update Server** - server that distributes threat definitions updates to machines running an agent

Note: Usually, this is the address issued to you by your ISP and will not begin with **10**, **172**, or **192**.

Note: The Policy Server and Update Server can be two separate machines, situated in different geographical locations.

8. Click **OK**.

Step 3: Create an installer package

The recommended method of deploying agents over WAN, is using an Installer Package.

To create an installer package:

1. From the Admin Console, click **Agent Installation** and select one of the following installer package options:
   - **Create MSI Installer Package** - creates an MSI installer that can be deployed across your network using Group Policy Objects (GPO)
   - **Create MST Installer Package** - creates MST files that can be used to modify pre-installation settings of the MSI installer. This is used when an advanced deployment is selected in Group Policy Objects (GPO)
   - **Create EXE Installer Package** - creates an executable file that can be used to install agents manually or automatically, using third-party tools.
2. Select the "Remote Agents" policy (configured in Step 2: Create a policy for remote Agents). The selected policy is assigned to agents that are installed from this package. Click **OK**.
3. Save the installer package in a convenient location.

Step 4: Distribute the package

The package must be distributed to all the client machines that require an agent. This can be done using any of the following methods:

- Group Policy
- Network Shares
- Jump Drive
- CD / DVD
- Flash Drives.

Step 5: Install the package

Run the installer package while connected to the Internet. During installation, the agent needs to communicate with the VIPRE Site Service in order to receive threat definitions.

2.6 — Roaming Agents

When an agent can no longer talk directly with the Console, it becomes a roaming agent. Roaming agents communicate to the Console through the VIPRE Roaming Service (VRS).

Roaming allows for easier management of remote agents, as you no longer need to use firewall port forwarding to retain a remote agent connection.

The roaming service acts as a holding queue for messages between the Console and roaming agents. The Console checks the VIPRE Roaming Service every 5 minutes for incoming roaming agent messages.

When an agent is connected directly to the Console, it has a call in period of once every 5 minutes. If an agent is unable to connect directly to the Console, it is considered a roaming agent. When roaming, the call in period changes (by default) to once per hour. AP (Active Protection) events will still be handled immediately.

2.6.1 — Types of Roaming Agents

There are two distinct types of roaming agents:

- You may **configure a previously installed "regular" agent** as a roaming agent. This means any existing agent can be configured to roam, once it is installed locally on the network.
- You may **install a new agent on a remote machine** that has no direct VIPRE Console contact. This uses the Roaming Agent installation package, and allows for a full installation without direct contact with the VIPRE server.

See also:

Creating a Roaming Installer

Turning Roaming Agents On

Approving Roaming Agents

2.6.2 — Turning Roaming Agents On

Roaming is controlled on both the site level and policy level. You must enable both for roaming to function correctly.

To enable roaming agent installation at the site level

1. Select **Admin Console > Site Properties**.
2. From the left pane, click **Roaming Agent Installation**.

3. Select **Allow**, from under **Roaming Agent Installation**. This enables roaming agent installations to contact VIPRE Site Service for all the policies under the site.
4. Click **OK**.

To enable roaming agent installation at the policy level

1. Select **Admin Console > Site Navigator**.
2. From the left pane, click the policy you wish change.
3. Click the **Enable roaming for this policy** link.

2.6.3 — Approving Roaming Agents

When a roaming agent calls in for the first time, the admin must manually approve or reject the pending roaming installation. Alternatively, a policy can be set to auto-approve pending roaming installations.

To approve or reject a pending roaming installation

1. Select **Admin Console > Site Navigator**.
2. From the left pane, click the policy you wish change.
3. For the agent in question, in the Install column, click **Approve** or **Reject**.

Note: Some pending roaming installs may not immediately show as pending. To resolve this, select a different policy, and then click back to the policy in question.

To set a policy to auto-approve roaming installations

1. Select **Admin Console > Site Navigator**.
2. From the left pane, click the policy you wish change.
3. Click the **Settings** tab, then **Properties**. The Policy Properties window will display.
4. Select **Agent > Roaming Agents** from the left pane.
5. Click the **Automatically approve roaming installations for this policy** check box.
6. Click **OK**.

2.6.4 — Creating a Roaming Installer

You may create roaming agent installation packages to enable a remote machine to roam. This can be used to install the agent on laptops or in remote offices.

To create a roaming installation package

1. Select **Admin Console > Install Agent**. The Install Agent Wizard will launch.
2. From the drop down, choose the type of device you are installing to, and click **Continue**.
3. From the drop down, choose the policy this device will adhere to, and click **Continue**.
4. Select **Roaming Installation**.
5. **Optionally**, select the **Make the installer expire after ten days** check box to limit the amount of time the installer may be used,

   Or

Optionally, select the **Allow only "x" installations with this package** check box to limit the number of installations to a number of your choosing (10 by default).

6. Click **Continue**.
7. Enter or browse to the location where you would like the installation file to be saved, and then click **Continue**.
8. You should see a message confirming successful creation of the EXE package. Click **Finish**.
9. Distribute this file to your end-user.

Note: Roaming agents receive their definitions updates from ThreatTrack, not through the Console.

Note: Roaming agents will not auto-update their versions. An administrator must create a new roaming installation package and send it to the user for installation.

2.7 — Automatic Policy Assignment

VIPRE Business Premium and VIPRE Endpoint Security can automatically assign computers to a policy during installation. This only affects computers on the "Default" policy, or not in the catalog.

Auto Policy Assignment is divided by the three computer types: **Workstations**, **Laptops**, and **Servers**.

To enable Auto Policy Assignment

1. Under Site Properties, select **Auto Policy Assignment**.
2. Check the **Automatically assign my computers to a policy** check box.
3. For each type of computer, select a policy from the drop-down list.
4. Click **Apply** or **OK**.

Note: It's a good practice to ensure you have created specific policies for each type of machine, such as "Default for Workstations", "Default for Laptops", and so forth.

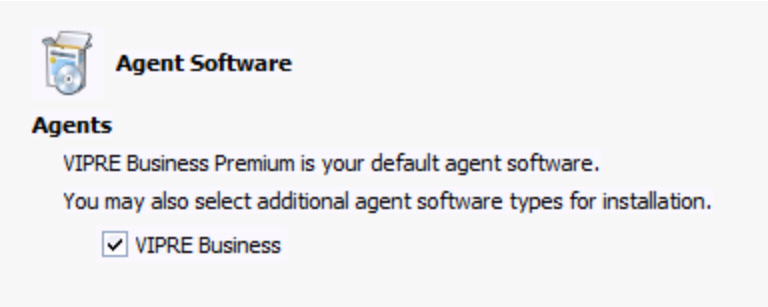
2.8 — Choosing Default Agent Type for Installations

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

If you are running VIPRE Business Premium or VIPRE Endpoint Security, you have the option to distribute Endpoint/Premium and non-Premium agents when you create an agent installation.

To enable agent type selection:

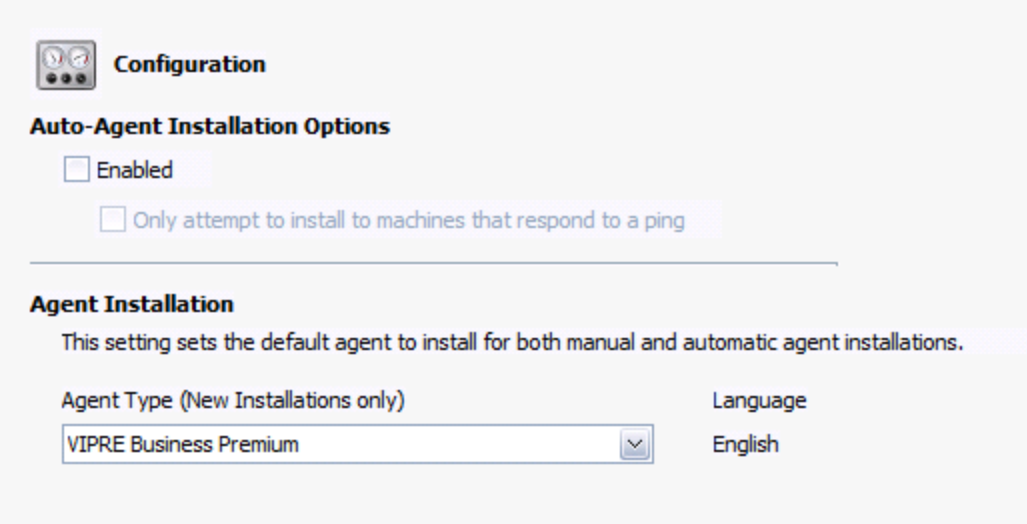
1. Open the **Site Properties > Agent Software**.
2. **Select the check box next to an agent type** to add it as an option for agent installation. This enables selecting a *default agent type* for each policy (see below).



Screenshot 1: Selecting additional agent types.

To select the default agent type for each policy:

1. Double-click on a policy, then select **Agent Installation Management > Configuration**.
2. Under **Agent Installation**, select the **Agent Type** you wish to use by default.
3. The Install Agent will now use your *default* agent for any new installations.



Screenshot 2: Selecting a default Agent Type for new installations.

3 — Managing Agents

3.1 — Agents Grid

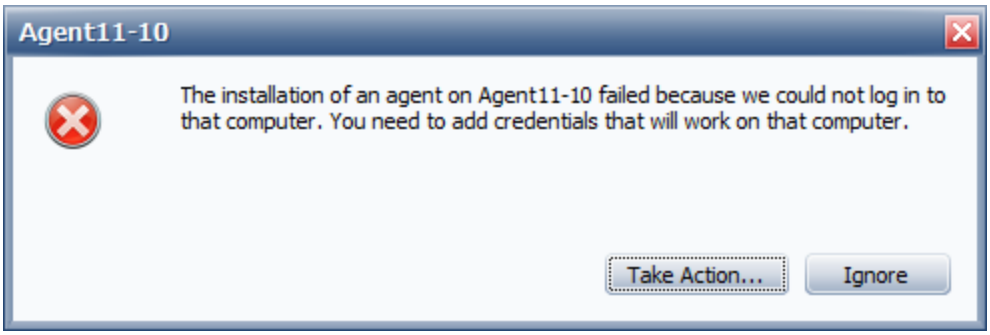
Information Column: The Protected Computers and Unprotected Computers grids contain a column with this icon: 

This column provides information about computer types and informs about alerts that require attention from an admin.

3.1.1 — Alerts:

The  icon appears when an admin attempts to install a VIPRE Business agent that fails due to missing credentials. This icon is displayed in the **Unprotected Computers** grid under individual Windows policies or the Windows policies group.

When the  icon is clicked, the following dialog box displays:

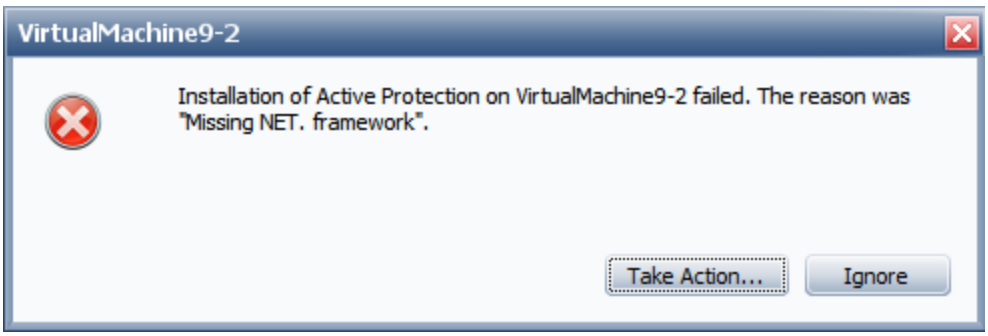


As an admin, you can

- Click **Take Action**, which displays the credentials dialog to enter valid credentials for that machine, or
- Click **Ignore**, which clears the icon and no action is taken.

The  icon also appears on the **Protected Computers grid** under individual Hyper-V policies, or on the Hyper-V policies group when an Active Protection installation fails for a Virtual Machine.

When the icon is clicked, a similar dialog box displays.



The admin can

- **Take Action**, which retries the AP installation, or
- **Ignore the alert**, which clears the icon and no action is taken.

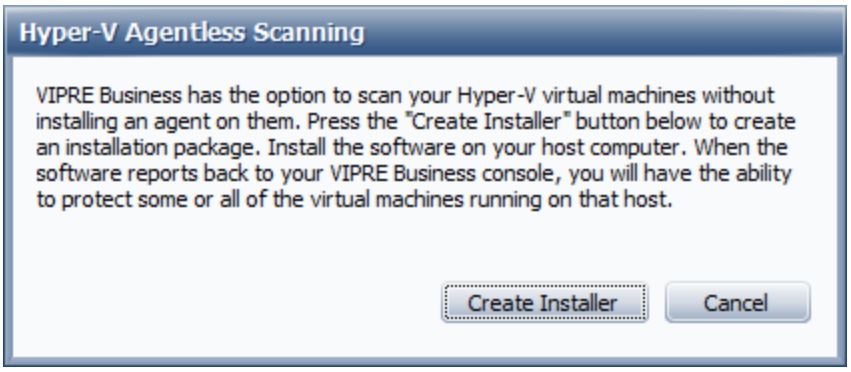
3.1.2 — Computer Types

When there are no alerts, the information column also displays machine types.

Under Windows policies or the Windows Policies group:

- This icon represents a workstation: 
- This icon represents a laptop: 
- This icon represents a server: 
- Hyper-V hosts also live under Windows policies. Their denotation is a clickable letter "H" in the information column.

When clicked, VIPRE shows the following dialog:



From here, the admin can create a Hyper-V installer package to install the Hyper-V agent on any host.

Under Hyper-V policies or the Hyper-V policy group

All computers on the protected and unprotected grids has a "VM" denotation in the information column if they do not have any other alerts associated with them. "VM" indicates a Hyper-V Virtual Machine.

Mac policies and policy group, iOS policies and policy group, and Android policies and policy group

These currently do not display any information in the information column.

3.2 — Unprotected Computers Tab

VIPRE automatically detects online computers that are reachable from the machine on which it is installed. These computers are listed under the **Unprotected Computers** tab of the selected security

policy. From this tab, you are able to deploy agents on single or multiple computers, as well as assign policies to the new agent(s).

The Unprotected Computers tab is suitable for deploying agents in small environments, where as in large environments, it is recommended to use an automatic method. VIPRE automatically scans your network for unprotected computers through Active Directory and NetBIOS once an hour, and agents that are unresponsive for three days are automatically removed from the list. For more information refer to Automatically Installing Agents.

On individual Windows policies or on the Windows policies group, the Unprotected Computers tab is hidden if:

- Endpoint discovery is disabled in the site settings, and
- The VSS has not already discovered unprotected machines on the network.

Therefore, if the VSS discovers an unprotected machine, after which the admin turns off endpoint discovery, the Unprotected Computers tab is still shown.

On individual Hyper-V policies and on the Hyper-V policies group, the Unprotected Computers tab is always shown, regardless if the endpoint discovery option is enabled or not.

Search button: The admin can click on the "Search" button in the lower right corner of the Unprotected Computers tab to force the VSS to search the network for new, unprotected machines. This search function honors the Unprotected Computer Discovery settings in site properties.

Regardless of whether the "Enable endpoint discovery" checkbox is checked, the VSS searches for new computers on the selected domains in the tree list. If no domains are checked, the VSS does not search when the search button is clicked, regardless of whether the "Enable endpoint discovery" checkbox is checked.

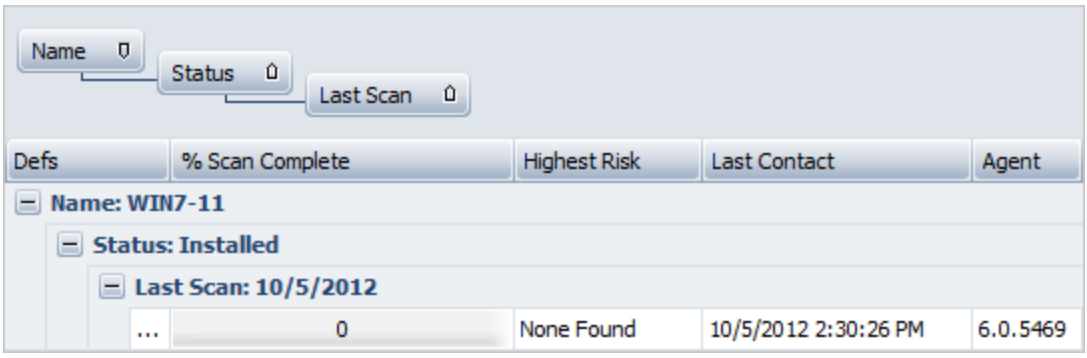
Newly discovered machines have a status of "Install Now" if the "Authenticate with unprotected computers using saved credentials" checkbox is unchecked. When the checkbox is checked, the machines' statuses change to "Not Installed" and the VSS tries to log in to those machines using the saved credentials. If the saved credentials don't work, the machines' status changes to "Need Credentials". If the credentials work, the status changes to "Install Now."

This topic contains information about:

- Grouping computer information
- Agents right-click menu
- Manually adding computers for agent installation
- Manually searching for unprotected computers
- Possible agent statuses

3.2.1 — Grouping computer information

The information in this tab can be grouped by any of the existing columns. Drag a column heading and drop it in the provided area above the headings row. You can add multiple column headings. Each heading that is added, becomes a sub-group of the preceding heading.



3.2.2 — Agents right-click menu

To interact with agents from the Unprotected Computers tab:

1. Select one or more agents. Use **Ctrl** or **Shift** for multiple selections.
2. Right-click one of the selected agents and select any of the following options:

- **Refresh**: select to refresh the data on the screen.
- **Print\Email\Export**: select to print, email, or export the entire contents of the grid. Once selected, a preview pane displays how the grid will be printed. From the preview pane, you can modify the background (including the color or watermark), change the print settings, export the grid as a PDF document, and send it via email in any of several formats, including PDF, MHT, RTF, Excel, CSV, TXT, or an image file.

Note: You can select the columns that will display and in what order before printing, emailing, or exporting.

- **Add to Agent Installation Scopes**: adds the selected computer(s) to the policy's Automatic Agent Installation list. This option is used when automatic agents installation is going to be set up or is already set up, and enables you to install the selected agent(s) at a scheduled time.
- **Install Agent(s)...**: starts downloading the micro installer on the target computer and attempts to install the agent.
- **Edit Note**: click to display a text box to enter a note for selected agent. You can only enter a note for one agent at a time.
- **Re-scan the selected computer(s)**: refreshes the information displayed under the **Status** column of each unprotected computer. In some cases, computers that go offline remain available under the Unprotected Computers tab. Use this option to updates computers statuses and display the most recent information.
- **Ping Computer**: select to send an ICMP ping to a computer. This enables you to determine if the target computer is online and responsive.
- **Restart the selected computer(s)**: restarts the selected computer(s).
- **Hide the selected computer(s):** hides the computer(s) until you choose to show them. To show them, select **View hidden computer(s)** on the top-right of the Unprotected Computers page, then select the computer(s) to 'unhide'.

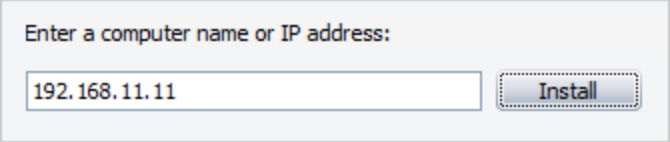
- **Remove the selected computer(s)**: removes the computer(s) if they are no longer on the network. If they become active again, they will be rediscovered during the next endpoint discovery.

3.2.3 — Manually adding computers for agent installation

If you have an unprotected computer on the network which is not listed under the Unprotected Computers tab, you are able to add that computer manually and install an agent on it.

To manually add an unprotected computer:

1. From **Site Navigator**, select the policy you want to configure.



2. Specify the computer to add, in the **Enter a computer name or IP address** field at the bottom of the **Unprotected Computers** tab.
3. Click **Install**.
4. (Optional) Review the list of incompatible software and click **OK** to add the computer and begin installing the agent.

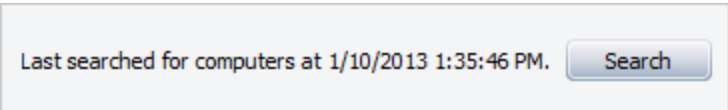
Note: Once the agent is installed, the computer is automatically moved to the Protected Computers tab.

3.2.4 — Manually searching for unprotected computers

VIPRE automatically scans the network to check for new unprotected computers that are not listed in the Unprotected Computers tab. Through this tab, you are able to force this scan and retrieve new machines before the scheduled scan starts.

To manually search for unprotected computers:

1. From **Site Navigator**, select the policy you want to configure.



2. From the bottom right of the **Unprotected Computers** tab, click **Search**.

Note: VIPRE scans your network for online computers that do not have an agent installed on them and adds them to the list.

3.2.5 — Possible agent statuses

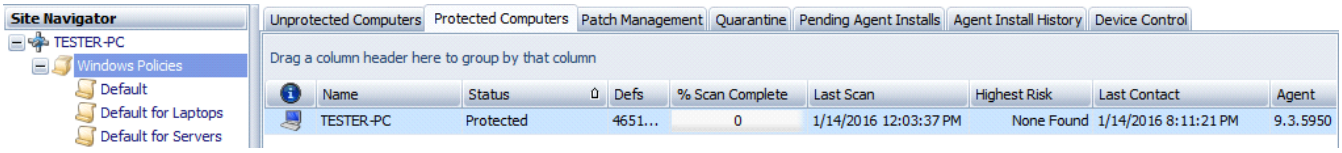
It is essential to check the **Status** column to monitor the availability and security state of an agent. For a full list of possible agent statuses, refer to Agent Status.

Defs	Name	Status	Last Scan	Highest Risk
13428	WIN7-11	Scanning Files	10/7/2012 9:58:32 PM	None Found
13428	WIN708	Patch Scanning	10/7/2012 9:40:25 PM	None Found
13428	WIN706	Protected	10/7/2012 9:41:20 PM	None Found

3.3 — Protected Computers Tab

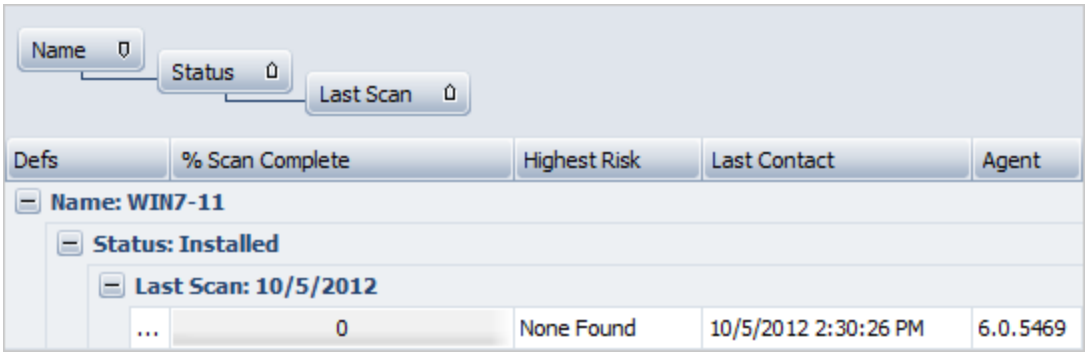
Computer that are being protected by an agent are displayed under the **Protected Computers** tab of any selected security policy. From this tab you can manage and interact with single or multiple agents at one go. The following sections contain information about:

- Grouping computer information
- Agents right-click menu
- Possible agent statuses



3.3.1 — Grouping computer information

The information in this tab can be grouped by any of the existing columns. Drag a column heading and drop it in the provided area above the headings row. You can add multiple column headings. Each heading that is added, becomes a sub-group of the preceding heading.



3.3.2 — Agents right-click menu

To interact with agents from the Protected Computers tab:

1. Select one or more agents. Use **Ctrl** or **Shift** for multiple selections.

2. Right-click one of the selected agents and select any of the following options:

- **Refresh**: select to refresh the data on the screen.

- **Print\Email\Export**: select to print, email, or export the entire contents of the grid. Once selected, a preview pane displays how the grid will be printed. From the preview pane, you can modify the

background (including the color or watermark), change the print settings, export the grid as a PDF document, and send it via email in any of several formats, including PDF, MHT, RTF, Excel, CSV, TXT, or an image file.

Note: You can select the columns that will display and in what order before printing, emailing, or exporting.

- **Expand All**: select to expand the outline and see more entries.
- **Collapse All**: select to collapse the outline and see fewer entries.

Agent Commands:

- **Purge Deferred Work Item(s)**: select to purge all work waiting to be sent to the agent from the VSS.
- **Say Hello**: select to force an agent to say hello. This can be used for agents that didn't get an update to pick up the deferred work.
- **Check for Policy Update**: click for the agent to check that it has the latest update to its assigned policy.
- **Ping Agent**: select to send an ICMP ping to the agent. This tells you that the VIPRE service on the agent machine is running or not.
- **Shutdown Agent(s)**: select to stop the selected agent(s). This applies to all versions of agents.
- **Start Agent(s):** select to start the selected agent(s). This only applies to agents that are version 3.x and higher.
- **Issue Remote Restart Command**: this can be used when an agent is showing that it needs to Reboot in the console and for non-agent related issues. This command does not require an agent to exist on the remote computer for the restart command to be issued.

Agent Updates:

- **Check for Agent Software Updates**: select to have the agent(s) check for—and get if available—the latest software updates for the selected agent(s).
- **Schedule Agent Upgrades**: allows you to tell end users to leave their computers on overnight or over a weekend and to schedule software updates during off-hours so that the end users won't be affected by the upgrade if a reboot is needed. Time is in military time.
- **Check for Threat Definitions Updates**: select to check for—and get if available—the latest threat definitions for the selected agent(s).
- **Force Full Threat Definitions Update**: select to force the agent to get the full threat database for the selected agent(s). This will take longer than a definition update.
- **Agent Details**: select to display Agent Details.
- **Edit Note**: click to display a text box to enter a note for selected agent. You can only enter a note for one agent at a time.

Scanning:

- **Full Scan**: immediately initiates a full scan for the selected agent(s).
- **Quick Scan**: immediately initiates a quick scan for the selected agent(s).
- **Abort Scan**: select to completely terminate the current scan for the selected agent(s).
- **Pause Scan**: select to temporarily pause the current scan for the selected agent(s).
- **Resume Scan**: select to continue the paused scan for the selected agent(s).
- **Patch Management**: (*Premium or Endpoint Security*)
  - **Install Approved Patches**: starts installing the approved patches related to the selected agent(s).

Note: If there are approved patches pending installation, the agent Status displays **Installing Patches**.

  - **Scan for Missing Patches**: starts scanning software applications installed on the selected agent(s) for missing patches

Note: To verify that the scan started, ensure the agent Status is **Patch Scanning**.

- **Reassign Agent to Policy**: select to assign the agent to a different policy.

- **Disposition**: select to clear the **Disposition Needed** column in the **Agent Catalog**.

- **Add and Install Agent(s)**: select to display the **Installing VIPRE to your Computers** dialog box and add agents to the Agent Catalog and install them on computers.
- **Uninstall Agent(s)**: select to uninstall an agent from a workstation. Click **Yes** when prompted. Click **No** to close the window and leave the agent installed.

- **Add to Agent Installation Scopes**: click to add an agent to the list of agents in the Automatic Agent Installation queue.

- **Remove Agent(s) from Catalog**: select and click **Yes** to remove the selected agents. Click **No** to close the **Remove Agents** dialog box without removing any agents.

- **Grid Colors**: select to open the Agent Grid Colors dialog box where you can modify the colors in the grid.

3.3.3 — Possible agent statuses

3.4 — Agent Statuses

Agents have the following status types:

- **Agent Download Failed**: Indicates that the Micro Installer was unable to download the agent software, and that the agent installation failed.
- **Agent Installation Failed**: Indicates that an agent was not installed successfully.
- **Agent Shutdown**: Indicates that the machine on which the agent resides has been shut down.

- **Begin Custom Scan**: Indicates that a custom scan is in progress. This can be a right-click scan, a USB drive scan or a custom scan that was configured on the agent.
- **Begin Scanning**: Indicates that a Quick Scan has begun.
- **Begin Scanning Full**: Indicates that a Full Scan has begun.
- **Cleaning**: Indicates that an agent is cleaning threats.
- **Defs Update Complete**: Indicates that an agent's definitions were successfully updated.
- **Downgrade Ignored**: Indicates that a user tried to install a downgrade version of VIPRE (for example, a VPE agent over a VEP agent) and that the downgrade is being ignored.
- **Downloading Admin Action**: Indicates that the admin action script (tool to remove 3rd party agents) is being downloaded onto the machine where the agent is going to be installed.
- **Downloading MSI**: Indicates that the MSI Installer package is being downloaded onto the machine where the agent is going to be installed.
- **Installing Agent**: Indicates that an agent is being installed.
- **Installing Micro Installer**: Indicates that the Micro Installer is being installed.
- **Installing Patches**: Indicates that missing patches are being installed.
- **Installation Complete**: Indicates that patch installation is complete.
- **Needs Credentials**: Indicates that none of the credentials specified in **Site Properties > Agent Installation** are valid for the computer.
- **Not Communicating**: Indicates that an agent is no longer communicating. The last contact time was an indeterminate amount of time.
- **Not Found**: Indicates that NetBIOS or Active Directory queries cannot find the computer on the network.
- **Protect Now**: Indicates that the agent is not installed on the computer.
- **Patch Scanning**: Indicates that a scan for missing patches is in progress.
- **Protected**: Indicates that an agent has successfully installed.
- **Reboot Required**: Indicates that the machine on which the agent is installed requires a reboot (usually after the agent was installed).
- **Running Admin Action**: Indicates that an admin action script is being run to remove 3rd party agent.
- **Scan Aborted**: Indicates that the scan was aborted by the user.
- **Scan Complete**: Indicates that the scan has completed.
- **Scan Failed**: Indicates that the scan failed for an unspecified reason.
- **Scan Paused**: Indicates that a scan was paused by the user.
- **Scanning Cookies**: Indicates that an agent is scanning cookies.
- **Scanning Files**: Indicates that an agent is scanning files.
- **Scanning Folders**: Indicates that an agent is scanning folders.
- **Scanning Memory**: Indicates that an agent is scanning the PC's memory, including its processes.
- **Scanning Registry**: Indicates that an agent is scanning the Windows registry.
- **Updating Defs**: Indicates that an agent is updating its definitions.
- **Updates Failed**: Indicates that updates for the agent failed.
- **Uploading MSI Log**: Indicates that the log of the installation is inserted into the database where the VSS is located.

- **Updating Software**: Indicates that an agent's software is being updated.
- **User Remediation**: Indicates that a user has selected to do something with a found threat (quarantine or remove).

3.5 — Hyper-V Protected Computer Information

Protected Hyper-V VMs have an agent details dialog that is similar to machines that are protected by VIPRE Business.

The **Agent Environment** tab contains:

- VM hostname
- VM domain
- VM agent GUID
- VM IP address
- VM OS name
- VM date protected (date added)
- VM status
- VM deferred work, if any
- Last time the host called in to the VSS
- Last time the VSS was scanned by the host
- Last time a threat was detected on the VM
- Host machine's Hyper-V agent version
- Threat db version

The agent note is on the bottom right of the dialog.

Last Scan Summary tab: on the upper left, the UI shows when the different severities of threats were detected last, if ever. The right side shows the summary of the last scan:

- When the scan was performed
- How long the scan took
- How many threats were found
- How many severe risks were found
- How many high risks were found
- How many elevated risks were found
- How many moderate and low risk threats were found

Below that Is the section for scanned traces, including:

- How traces were scanned and found
- The different types of traces:
  - Files
  - Registry
  - Cookies
  - Archives
  - Rootkits

Quarantine tab: displays all items quarantined for the selected VM in a table.

Scan History tab: displays a history of all scans performed, and the results from those scans for that VM. The length of time items remain in the scan history is admin-defined.

AP History tab: displays a list of all AP events that occurred on that VM.

4 — Scanning Agent Machines

This chapter on Scanning Agent Machines covers all configuration and procedures for running scans on the machines in your network.

4.1 — Configure Agent Scan Settings

Agent scan settings must be configured at policy level. These settings include on demand scanning, scanning USB devices, and start-up scanning.

To configure agent scan settings:

1. From **Site Navigator** double-click the policy that you want to configure.
2. In **Policy Properties**, expand **Scanning** and click **Settings**.
3. Configure user interaction for scanning:
   - **Allow user to scan files and folders via a right-click menu option in Windows Explorer**: once selected and applied, this feature is available after the Agent picks up the updated policy.
4. Configure USB Device settings:
   - **Scan USB drives upon insertion**: unselect this to turn off USB drive scanning. When selected *and* a scan is in progress, the USB drive performs your selected action below:
     - **Do not perform USB scan if another scan is already in progress**: if a scan is in progress, the USB device will not be scanned on insertion. The user will have to scan the device manually.
     - **Interrupt active scan for USB scan**: if a scan is in progress, it will be canceled, and then the USB device will be scanned. The interrupted scan will need to be run again manually by the user or the Administrator, or picked up automatically by a scheduled scan.
5. Configure scan settings on start-up:
   - **Randomize scheduled scan start times in minutes**: this randomizer setting allows you to manage update server traffic when Agents check for threat definitions updates before running a scan. This setting matters when the "Disable automatic definitions updates before scans" setting is unselected AND you have a large number of Agents.

     Enter a number of minutes based how many agents you have assigned to the policy. Agents will pick a random time to check for updates during the number of minutes entered. The default setting is 5 minutes, which is sufficient for most environments. You can enter between 0-180 minutes.
   - **Missed scan options at start-up**:
     - **Do not perform quick scan**: select to turn off make up missed scans on start up.
     - **Prompt user to perform quick scan**: select this option so that if a scheduled scan is missed, the end user will be prompted to perform a scan at their convenience.
     - **Perform quick scan after start-up in minutes**: select this option so that if a scheduled scan is missed, the machine will perform a quick scan at the entered interval, once it is online. The default setting is 5 minutes. You can enter between 1 and 60 minutes.
6. Click **Apply** to save settings.

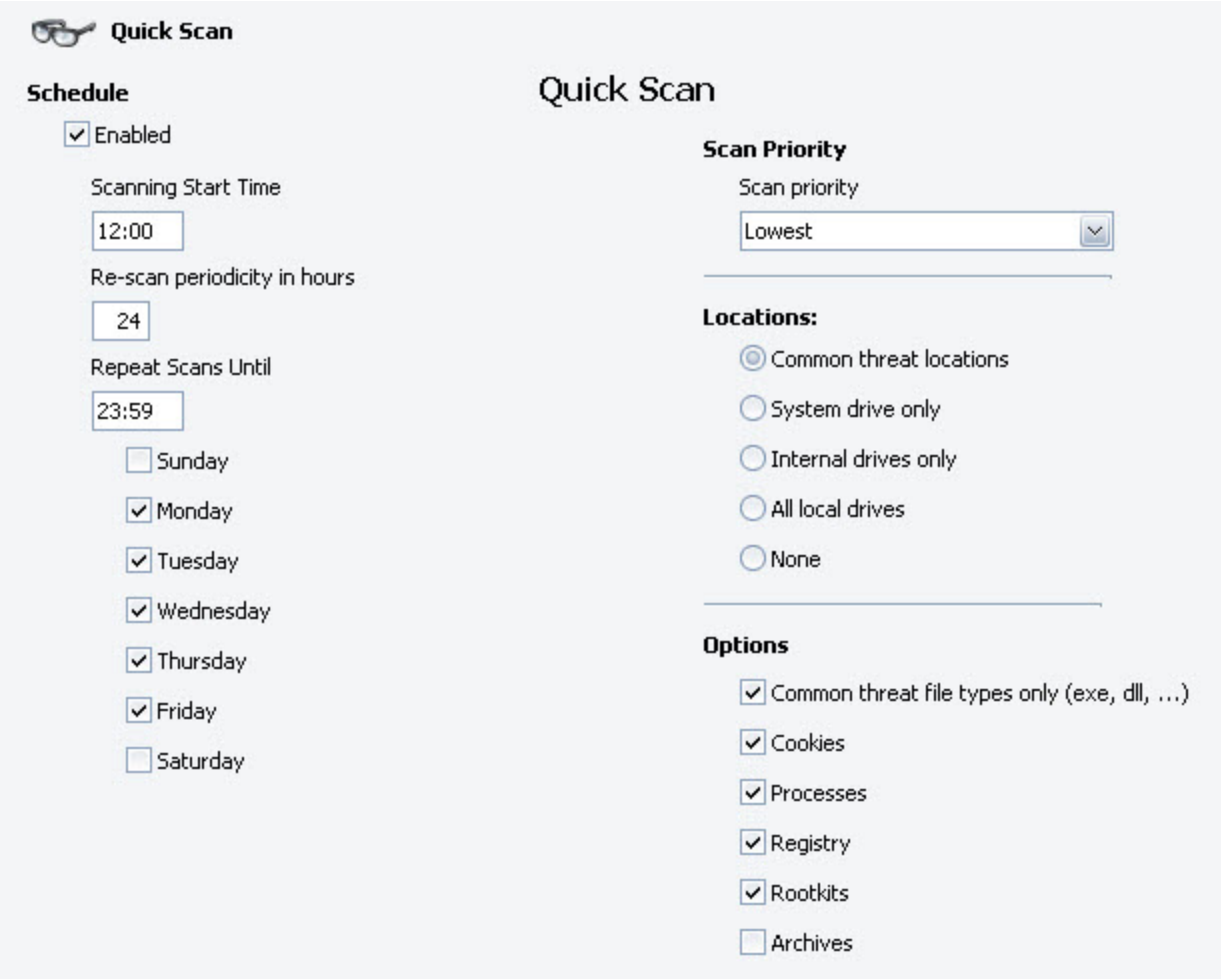
4.2 — Configure Automatic Scan Settings

Configure automatic scans for Agents. A "Quick Scan" typically focuses on the most vulnerable areas, while a "Full Scan" is a more thorough scan of the agent workstation.

You may also choose to run a "Custom Scan" which allows you to specify exact scan locations.

You configure how comprehensive a scan will be.

IMPORTANT: Before scheduling a scan, ensure that the "Allow user to manage scan schedules" setting on the Agent User Interaction screen is unselected.



To schedule 1 scan per day:

1. From **Site Navigator**, double-click the policy that you want to configure.
2. From **Policy Properties**, expand **Scanning** and select **Full Scan**, **Quick Scan**, or **Custom Scan**.
3. Select **Enabled**.
4. Enter a **Scanning Start Time**. For example, "21:00."
5. Enter a "zero" for **Re-scan periodicity in hours**.

Note: By entering a zero, the "Repeat Scans Until" field is ignored, therefore only 1 scan will occur for the selected day(s).

6. Select one or more days.
7. Select the **Scan Priority**, **Locations**, and **Options** as described in the Screen Descriptions area below.
8. Click **Apply** to accept changes.

To schedule multiple scans in 1 day:

> **Note**: It is a best practice to only schedule multiple Quick Scans on the same day. If you intend to run multiple Full Scans on the same day, take into account how long the full scan will run to avoid potential issues, especially a case where scans are running constantly on a machine. Poor system performance could result on the agent machine.

1. From **Site Navigator**, double-click the policy that you want to configure.
2. From **Policy Properties**, expand **Scanning** and select **Full Scan**, **Quick Scan**, or **Custom Scan**.
3. Select **Enabled**.
4. Enter a **Scanning Start Time**. For example, "21:00."
5. Under **Re-scan periodicity in hours**, enter a number between 1 and 23. The scan will run after this number of hours.

   Example: If you enter 09:00 for the "Scanning Start Time" and 2 for the "Repeat every," your agents will run the requested scan at 9 a.m. and every 2 hours after that, until the "Repeat Scans Until" time is reached.

> **Note**: If a scan is already in progress and the time comes for a scheduled scan, the scheduled scan will occur after the current scan completes.

6. Under **Repeat Scans Until**, enter a time for the repeated scans to stop running for that 24-hour period.
7. Select one or more days.
8. Select the **Scan Priority**, **Locations**, and **Options** as described in the Screen Descriptions area below.
9. Click **Apply** to accept changes.

Recommended Scanning:

If agent workstations are always powered on, the scheduled scans should run as indicated below. The "Default" is what is set in the Default Policy, and "Optional" is a best practice under slower network conditions.

- **Quick Scan**:
  - **Default**: 7 days per week at noon.
  - **Optional**: 7 days per week during non business operational hours.
- **Full Scan**:
  - **Default**: 7 days per week at 9:00 p.m. (21:00).
  - **Optional**: 7 days per week during non business hours, when possible, and after nightly backups.

For environments where agent workstations can only be scanned during working hours, the scheduled scans should be run as follows:

- **Quick Scan**: daily during lunch time and set the quick scan to run at a low priority during working hours.
- **Full Scan**: during lunch time on one or more days that scanning least impacts employee productivity. Set the full scan to run at a low priority during working hours.

4.2.1 — Screen Descriptions

Scan Priority:

Select one of the following priority options:

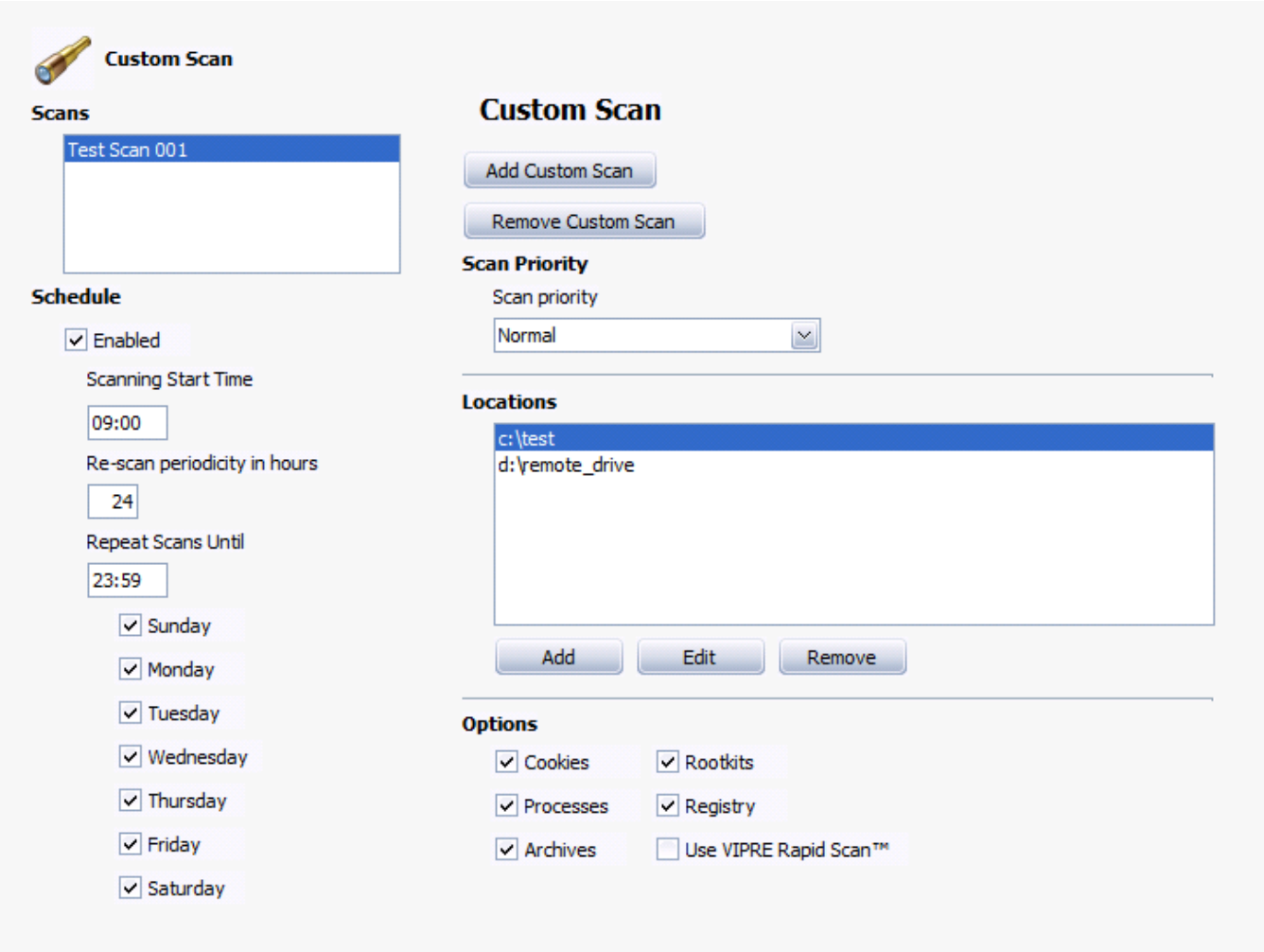
- **Lowest**: Set the priority to Lowest if you are going to be running the scans in the middle of the day. Windows will run other programs that are requesting to run before the scan. This should reduce the impact of end user performance when a scan runs during working hours.
- **Normal**: Set the priority to Normal when scanning at night or on multi-core machines where scanning at a higher priority won't affect user performance.
- **Highest**: Set the priority to Highest when it is important to have the scan run as quickly as possible, even if the end user is actively using the computer.

Locations:

The fields in this area set where on the workstations the scan will take place. You can select specific drives or none at all, and instead focus on key areas on the machine which you select in the Options area.

- **Common threat locations**: select for the scan to include the root of the drive, the program files directory, the system directory, and so forth
- **System drive only**: select for the scan to include the main drive (C:) only.
- **Internal drives only**: select for the scan to include internal drives only. This selection excludes USB, FireWire, and other external drives.
- **All local drives**: select for the scan to include all internal drives, partitions, plus any attached USB, FireWire, or other external devices.
- **None**: select for the scan to focus on only the selection(s) in the Options area. When selected, no drive or folder will receive scans.

Note: When creating a **Custom Scan**, use the *Add*, *Edit* and *Remove* buttons to specify exact locations you wish to scan (such as c:\Windows, d:\external\backup, etc.).



Screenshot 3: Custom Scan screen, showing specific scan Locations.

Options:

You can scan common threat types, the registry, cookies, and/or processes, of which are all separate from full drives and directories that are selected in the Locations area.

- **Cookies**: deselect for the scan to exclude cookies. This will prevent cookies from appearing in your reports if they may not be of large concern to you.
- **Processes**: select for the scan to include all running processes (applications).
- **Registry**: select for the scan to include the workstation's registry. Deselect if you want to scan only files, directories, or some other specific scan type without the registry being included in the scan.
- **Rootkits**: select for the scan to include rootkits.
- **Archives**: select for the scan to include archive files (such as .RAR or .ZIP). If a .RAR file is found to contain an infected file, the .RAR file will be quarantined. If a .ZIP file is found to contain an

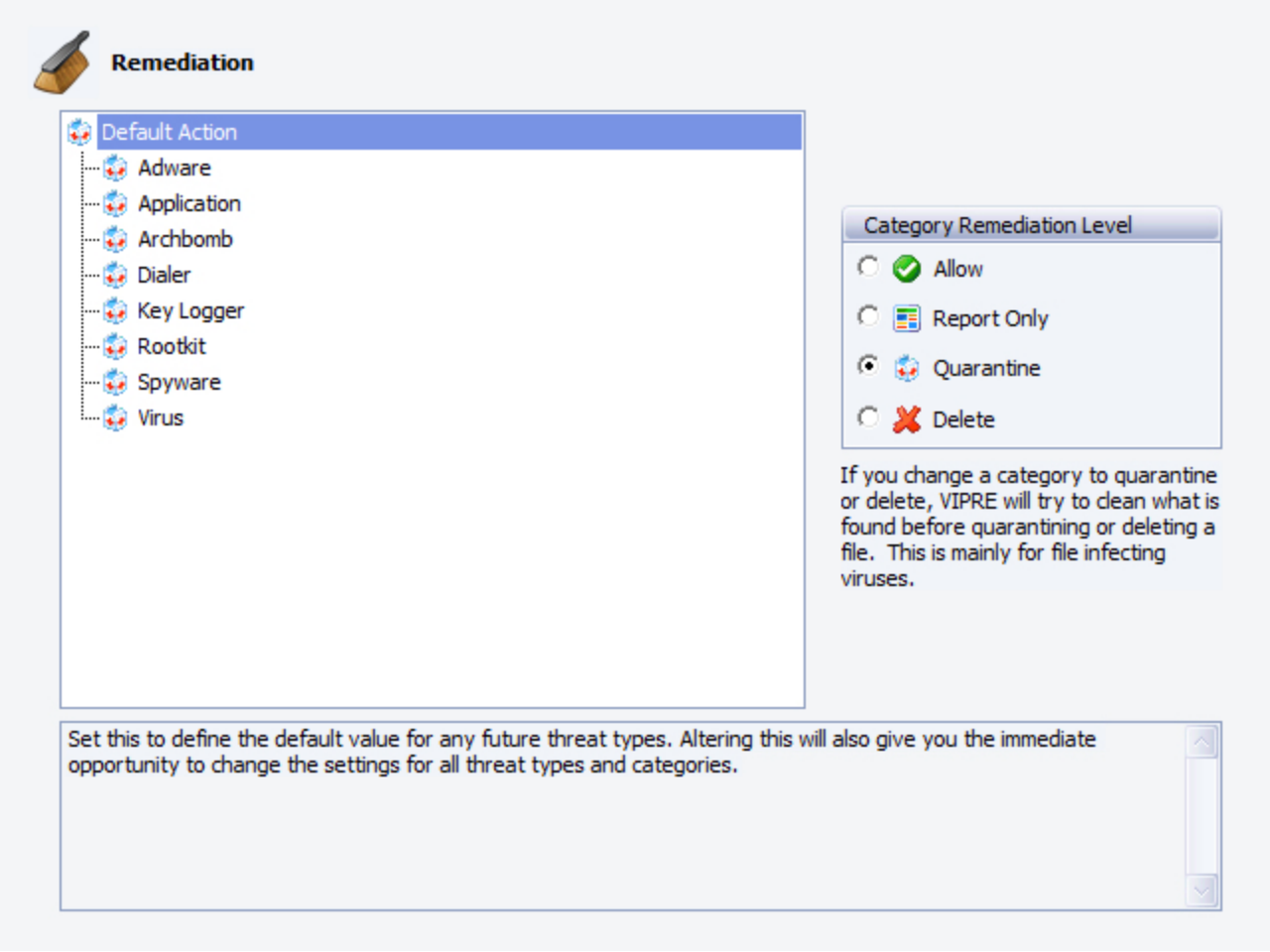
infected file, the infected file is quarantined and replaced by a .TXT file with text indicating that it was infected and that it has been quarantined.

- **Use VIPRE RapidScan**: select to enable previously scanned files to be checked much faster on subsequent scans. By keeping track of items already scanned, RapidScan quickly scans only files that have changed since the previous RapidScan, allowing for very quick successive scans. When a previously checked file is modified, RapidScan will re-scan it.

4.3 — Configure Scanning Remediation Settings

Configure how the results of scans are cleaned (remediated). Assign actions according to threat types, such as Adware, Viruses, Worms, and so forth. Actions include allow, report only, quarantine, and delete.

IMPORTANT: For the best results, ensure that you go through the list of threats and assign the appropriate action that best suits the needs of your organization. Select a category to display a detailed explanation below it.



To configure remediation settings:

1. In the **Policy Properties**, open **Remediation**.
2. Assign Category Remediation Levels for each of the threat types:
   a. Select a threat in the tree.
   b. Select one of the actions in the "Category Remediation Level." When that type of threat is detected, the assigned action will be taken.

   Allow: the threat is allowed to run on the machine. Threats with Allow remediation assigned cannot be tracked in reports.

   Report Only: the threat is allowed to run and can be tracked in reports.

   Quarantine: the threat is placed in quarantine, which resides on the agent machine.

   Delete: the threat is completely removed from the agent machine and unrecoverable.

Warning**:** As a safeguard, you may want to select Quarantine and not Delete. Items in Quarantine can be recovered, deleted items cannot.

3. Repeat Step 2a-b for each threat type listed.
4. Click **Apply** to save changes.

4.4 — Scanning Agent Workstations

After Agents are installed on workstations, they will be scanned based on the schedule configured in the policy's Scanning settings.

To scan an agent workstation:

1. From the policy's **Agents** screen, right-click on the agent and select **Scanning>Full Scan** or **Quick Scan**.
2. Select either a Quick or Full Scan and click **OK**.

Note: You can select more than one agent to scan.

Note: Manual scans initiated from the Console do not use the RapidScan setting, even if it is enabled in the policy.

5 — Monitoring Statuses

This chapter on Monitoring Statuses discusses UI screens that are used by Administrators to monitor the status of agents. The screens consist of dialog boxes, property pages, and tabs.

In addition to the primary purpose of monitoring, some of these screens contain right-click functionality to perform various actions.

5.1 — Agent Details Dialog Box

The **Agent Details** dialog box contains all detailed information for an agent to be viewed and analyzed. The agent name is displayed in upper left corner of the dialog box.

To display this dialog, right-click on an agent in the Agent Catalog and select **Agent Details**.

The dialog box contains the following tabs:

- **Agent Environment** displays the computer's environment, agent status, agent software and definitions information.
- **Last Scan Summary** details of the last scan performed on the machine.
- **Quarantine** tab displays all items quarantined for the selected agent in a table.
- **Scan History** displays a history of all scans performed, and the results from those scans for that workstation. The length of time items remain in the scan history is admin-defined.
- **AP History** displays a list of all AP events that occurred on that agent.
- **Email AV History** displays a list of all email AV events that occurred on that agent.
- Missing Patches
- Installed Patches

5.1.1 — Agent Details - Agent Environment Tab

Agent Environment displays the computer's environment, agent status, agent software and definitions information.

To access this tab, right-click on an agent from the Agents screen and select **Agent Details**.

> **Note:** You can right-click from anywhere on the tab to **Refresh** the displayed data.

This screen contains the following items:

Environment

The Environment section lists specific policy and agent information:

- **Agent Type**: displays whether the type is Business, Premium, or Endpoint Security.
- **Language**: displays the language of the agent.
- **Policy**: displays the policy to which the agent is assigned.
- **Domain**: displays the Agent's domain name.
- **Agent Guid**: displays a unique agent identifier used in the reporting database and Agent Catalog.
- **IP Address**: displays the Agent's IP address.
- **OS Name**: displays the name of the operating system on the agent's machine.

- **Date Added**: displays the date the agent was added to the catalog.
- **Policy Guid**: displays the Policy's unique alpha-numeric identifier.
- **Last User**: displays the last user ID used to log onto this agent machine.

Status

The Status section lists the last statuses, communications, scans, and any deferred work for the agent:

- **Status**: displays the agent's status. Status values can include Installed, Not Installed, Agent Shut-down, Scanning, Inactive, and so forth.
- **Deferred Work**: displays whether an agent has work pending. Pending is the only value. If there is no work pending, the column is left blank.
- **Dispositioning Needed**: displays whether a threat has been found. Columns are left blank for agents without found threats. The values can also be TRUE/FALSE.
- **Needs Reboot**: displays whether a reboot of the agent workstation is required with the values TRUE or FALSE.
- **Last Contact**: displays the date of the last heartbeat from the agent.
- **Last Scan**: displays the date of last scan.
- **Last Threat Detection**: displays the date of last threat found, regardless of severity.
- **Updated Data Last**: displays the date of last threat database update.

Software and Definitions

The Software section lists agent version information:

- **Agent Software Version**: displays the Agent version number.
- **Last Software Check**: displays the date of the last time the agent checked for software updates.
- **Software Update Available**: displays whether or not a newer agent is available. Agents for which newer versions are available are marked as True, and False for unavailable.
- **Threat Database Version**: displays the version of the threat database.
- **Last Threat Database Check**: displays the date the agent last checked for threat definitions.
- **Threat Update Available**: displays whether a newer threat database is available for that agent. Agents for which newer versions are available are marked as True, and False for unavailable.

Note

The Note box displays the user-entered notes for this agent.

To add a note for an agent, in the Agent Catalog, right-click on the agent that you want to enter a note for and select **Edit Note**.

5.1.2 — Agent Details - Last Scan Summary Tab

Last Scan Summary details of the last scan performed on the machine.

To access this tab, right-click on an agent from the Agents screen and select **Agent Details**.

> **Note:** You can right-click from anywhere on the tab to **Refresh** the displayed data.

This screen contains the following items:

Last Severity Level Detection

The Last Severity Level Detection section lists when threats of five varying severity levels were last detected by this agent.

Last Scan Summary

The Last Scan Summary section lists specific information about the last scan completed, including scan duration, threats found, and all processes and files scanned:

- **Last Scan Date**: displays the date and time of the last scan performed.
- **Duration**: displays the duration of the last scan performed.
- **Highest Risk**: displays the most severe threat level found during the last scan.
- **Threats Found**: displays the total number of threats found during the last scan.
- **Severe Found**: displays the number of *Severe* threats found on the agent machine during the last scan.
- **High Found**: displays the number of *High* threats found on the agent machine during the last scan.
- **Elevated Found**: displays the number of *Elevated* threats found on the agent machine during the last scan.
- **Moderate Found**: displays the number of *Moderate* threats found on the agent machine during the last scan.
- **Low Found**: displays the number of *Low* threats found on the agent machine during the last scan.
- **Traces**: The Traces area contains the traces **Scanned** and traces **Found** columns that correspond to specific scanned areas of the agent machine. The numbers in the **Scanned** column simply show the number of items in that area that were scanned during the last scan, while the **Found** column shows the number of threat traces that were found. The Total shows the total number of malware traces that were scanned and found on the agent machine during the last scan.

5.1.3 — Agent Details - Quarantine Tab

The **Quarantine** tab displays all items quarantined for the selected agent in a table. The listed items are expandable by clicking the plus sign next to a particular threat. The different traces detected, including files, registry items, folders, and so forth are displayed. Columns displayed include Type and Data.

To access this tab, right-click on an agent from the Agents screen and select **Agent Details>Quarantine** tab.

> **Note:** The column headings are dynamic, allowing you to move their order and sort by a category within that column. Click the filter icon  on a column heading to select a filtering option. See Filtering Views for more information on using the available filters.

This screen contains the following items:

Columns:

- **Quarantined Threat ID**: displays an ID number associated with that quarantined item.
- **Scan Date**: displays the date and time the scan was performed.
- **Scan Type**: displays the type of detection: quick scan, full scan, custom scan, email AV, or AP.

- **Name**: displays the name of the malware threat detected during the scan.
- **Category**: displays the type of malware threat that was discovered. For example, Trojan Downloader, Worm.Generic, and so forth
- **Status**: displays the status of the quarantined item and will either remain blank, display Unquarantine Pending, or Delete Pending.
- **Severity**: displays the level of severity of the malware threat discovered. Severity levels are measured as Low, Moderate, Elevated, High, or Severe.
- **Threat Type**: displays the type of threat. For example, Adware.

Right-click menu options:

Right-click anywhere in the **Quarantine** tab to display the right-click menu. The following options are available:

- **Refresh**: select to refresh the data on the screen.

- **Print\Email\Export**: select to print, email, or export the entire contents of the grid. Once selected, a preview pane displays how the grid will be printed. From the preview pane, you can modify the background (including the color or watermark), change the print settings, export the grid as a PDF document, and send it via email in any of several formats, including PDF, MHT, RTF, Excel, CSV, TXT, or an image file.

Note: You can select the columns that will display and in what order before printing, emailing, or exporting.

- **Expand All**: select to expand the outline and see more entries.
- **Collapse All**: select to collapse the outline and see fewer entries.

- **Threat Details**: select to display the details of the threat.

- **Delete from Quarantine**: select to delete the threat from the agent system. Selecting this option displays the **Delete Threat** dialog box. Click **Yes** if you are sure you want to delete the threat selected. Click **No** to close the dialog box without deleting the threat.
- **Unquarantine Threat**: select to remove the threat from the quarantined threats list for the selected policies.
- **Unquarantine and Send for Analysis**: same as the "Unquarantine Threat" listed above, and will then automatically send the item to ThreatTrack Security for analysis. A message of this action is generated in the System Messages screen.
- **Send for Analysis**: select to send the item to ThreatTrack Security for analysis. A message of this action is generated in the System Messages screen.

- **Allow Threat**: opens the Allow Threat dialog box where you can select the policies for which you want to allow this item. Once allowing, it will be displayed on the Allowed Threats screen for the policy. You can remove the threat from this page, as well.

5.1.4 — Agent Details - Scan History Tab

The **Scan History** tab **Scan History** displays a history of all scans performed, and the results from those scans for that workstation. The length of time items remain in the scan history is admin-defined. See Agent Actions for scheduling the length of time items stay in scan history.

To access this tab, right-click on an agent from the Agents screen and select **Agent Details>Scan History** tab.

> **Note:** The column headings are dynamic, allowing you to move their order and sort by a category within that column. Click the filter icon  on a column heading to select a filtering option. See Filtering Views for more information on using the available filters.

This screen contains the following items:

Columns:

- **Scan Date**: displays the date and time the scan was performed.
- **Agent**: displays the agent version number.
- **Threat DB**: displays the Threat database version number.
- **Total Found**: displays the total number of spyware and other unwanted applications and artifacts found on the agent machine during the last scan.
- **Cookies**: displays the number of cookies found during the last scan.
- **Registry**: displays the number of registry artifacts found during the last scan.
- **Files**: displays the number of file artifacts found during the last scan.
- **Processes**: displays the number of process artifacts found during the last scan.
- **Deleted**: displays the number of threats deleted from the system.
- **Report Only**: displays the number of threats in which the only action taken by the system is to report the threat.
- **Quarantined**: displays the number of threats placed in quarantine.
- **Type**: displays the type of scan that was performed.
- **Scan Duration**: displays how long the scan took to run in hours:minutes:seconds. For example, 00:36:23.

Expandable Rows

Entries in the **Scan History** tab are also expandable down to two different levels. Clicking the plus sign next to a scan date displays a sub-list detailing threats found.

The columns in the first sub-table displayed include:

- **Name**: displays the name of the particular spyware or other unwanted applications or artifacts found.
- **Category**: displays the type of spyware or other unwanted applications or artifacts.
- **Action**: displays action taken regarding the threat.
- **Severity**: displays the level of severity of the threat found. Severity levels are measured as Low, Moderate, Elevated, High, or Severe.

- **Threat ID**: displays the unique ID number of the threat.
- **Type**: displays the type of threat. For example, Adware.

The second level of expansion is for each particular threat. The columns in the second sub-table displayed include:

- **Type**: displays the specific artifact type found (such as files, registry items, and so forth).
- **Data**: displays specific location information about the artifact.

As with the main Scan History table, all columns are configurable, can be sorted, and can be filtered.

Scan History Right-Click Menu

Right-click anywhere in the tab to display the right-click menu. The following options are available:

- **Refresh**: select to refresh the data on the screen.

- **Print\Email\Export**: select to print, email, or export the entire contents of the grid. Once selected, a preview pane displays how the grid will be printed. From the preview pane, you can modify the background (including the color or watermark), change the print settings, export the grid as a PDF document, and send it via email in any of several formats, including PDF, MHT, RTF, Excel, CSV, TXT, or an image file.

Note: You can select the columns that will display and in what order before printing, emailing, or exporting.

- **Expand All**: select to expand the outline and see more entries.
- **Collapse All**: select to collapse the outline and see fewer entries.

- **Threat Details**: select to display details for the selected threat.

5.1.5 — Agent Details - AP History Tab

The **AP History** displays a list of all AP events that occurred on that agent.

To access this tab, right-click on an agent from the Agents screen and select **Agent Details>AP History** tab.

Note: The column headings are dynamic, allowing you to move their order and sort by a category within that column. Click the filter icon  on a column heading to select a filtering option. See Filtering Views for more information on using the available filters.

This screen contains the following items:

Columns:

- **Event Date**: displays the date and time the AP event was triggered.
- **Monitor**: displays the AP Monitor that triggered the event.
- **Monitor Type**: displays the type of monitor that triggered the event.

- **Executable**: displays the path and filename that triggered the event.
- **Known As**: displays whether the event was good or bad.
- **Event Type**: displays whether the event was a prompt or notification.
- **Disposition**: displays the result of the event.
- **User Name**: displays the user name that was logged in at the time of the event, only if the event was a Prompt.
- **Authority**: displays whether it was a known or unknown threat.

AP History Right-Click Menu

Right-click anywhere in the tab to display the right-click menu. The following options are available:

- **Refresh**: select to refresh the data on the screen.

- **Print\Email\Export**: select to print, email, or export the entire contents of the grid. Once selected, a preview pane displays how the grid will be printed. From the preview pane, you can modify the background (including the color or watermark), change the print settings, export the grid as a PDF document, and send it via email in any of several formats, including PDF, MHT, RTF, Excel, CSV, TXT, or an image file.

Note: You can select the columns that will display and in what order before printing, emailing, or exporting.

- **Expand All**: select to expand the outline and see more entries.
- **Collapse All**: select to collapse the outline and see fewer entries.

- **Event Details**: select to display the Event Details dialog box to view specific details of the event.

5.1.6 — Agent Details - Email AV History Tab

The **Email AV History** displays a list of all email AV events that occurred on that agent.

To access this tab, right-click on an agent from the Agents screen and select **Agent Details>Email AV History** tab.

Note: The column headings are dynamic, allowing you to move their order and sort by a category within that column. Click the filter icon  on a column heading to select a filtering option. See Filtering Views for more information on using the available filters.

This screen contains the following items:

Columns:

- **Event Date**: displays the date and time the event was detected.
- **Threat ID**: displays the unique ID number of the threat.

- **Attachment**: displays the attachment that triggered the event.
- **Description**: displays the action of the email event. For example, deleted, quarantined, or none.

Email History Right-Click Menu

Right-click anywhere in the tab to display the right-click menu. The following options are available:

- **Refresh**: select to refresh the data on the screen.

- **Print\Email\Export**: select to print, email, or export the entire contents of the grid. Once selected, a preview pane displays how the grid will be printed. From the preview pane, you can modify the background (including the color or watermark), change the print settings, export the grid as a PDF document, and send it via email in any of several formats, including PDF, MHT, RTF, Excel, CSV, TXT, or an image file.

Note: You can select the columns that will display and in what order before printing, emailing, or exporting.

- **Expand All**: select to expand the outline and see more entries.
- **Collapse All**: select to collapse the outline and see fewer entries.

5.1.7 — Agent Details - Missing Patches Tab

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

The **Missing Patches** tab displays software patches that are missing from applications that are installed on the agent machine. The following sections contain information about:

- Accessing the Missing Patches tab
- Columns of the Missing Patches tab
- Missing Patches tab right-click menu

5.1.7.1 — Accessing the Missing Patches tab

To access the Missing Patches tab:

1. From **Site Navigator**, select the policy which holds the agents you want to configure.
2. From the right pane, click the **Protected Computers** tab.
3. Right-click an agent from the list and select **Agent Details...**
4. From the Agent Details dialog, click **Missing Patches** tab.

Note: The column headings are dynamic, allowing you to move their order and sort by a category within that column. Click the filter icon  on a column heading to select a filtering option. See Filtering Views for more information on using the available filters.

5.1.7.2 — Columns of the Missing Patches tab

The Missing Patches tab provides the following information about each patch:

- **Manufacturer**: displays the software vendor of the application.
- **Product**: displays the application name.
- **Patch Name**: displays the patch that is missing from the application.
- **Severity**: displays the importance of the patch and the security risk that is imposed on the system if the patch remains uninstalled.
- **Status**: displays the Status of the missing patch.

5.1.7.3 — Missing Patches tab right-click menu

Right-click anywhere in the tab to display the right-click menu. The following options are available:

- **Refresh**: select to refresh the data on the screen.

- **Print\Email\Export**: select to print, email, or export the entire contents of the grid. Once selected, a preview pane displays how the grid will be printed. From the preview pane, you can modify the background (including the color or watermark), change the print settings, export the grid as a PDF document, and send it via email in any of several formats, including PDF, MHT, RTF, Excel, CSV, TXT, or an image file.

Note: You can select the columns that will display and in what order before printing, emailing, or exporting.

- **Expand All**: select to expand the outline and see more entries.
- **Collapse All**: select to collapse the outline and see fewer entries.

5.1.8 — Agent Details - Installed Patches Tab

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

The **Installed Patches** tab displays software patches that are installed on agent machines. When a missing patch is installed, it is automatically added to the Installed Patches tab. The following sections contain information about:

- Accessing the Installed Patches tab
- Columns of the Installed Patches tab
- Installed Patches tab right-click menu

Note: The column headings are dynamic, allowing you to move their order and sort by a category within that column. Click the filter icon  on a column heading to select a filtering option. See Filtering Views for more information on using the available filters.

5.1.8.1 — Accessing the Installed Patches tab

To access the Installed Patches tab:

1. From **Site Navigator**, select the policy which holds the agents you want to configure.
2. From the right pane, click the **Protected Computers** tab.

3. Right-click an agent from the list and select **Agent Details...**
4. From the Agent Details dialog, click **Installed Patches** tab.

5.1.8.2 — Columns of the Installed Patches tab

The Installed Patches tab provides the following information about each patch:

- **Manufacturer**: displays the software vendor of the application.
- **Product**: displays the application name.
- **Patch Name**: displays the patch that is missing from the application.
- **Severity**: displays the importance of the patch and the security risk that is imposed on the system if the patch remains uninstalled.
- **Released**: displays the date when the patch was released by the software vendor.

5.1.8.3 — Installed Patches tab right-click menu

Right-click anywhere in the tab to display the right-click menu. The following options are available:

- **Refresh**: select to refresh the data on the screen.

- **Print\Email\Export**: select to print, email, or export the entire contents of the grid. Once selected, a preview pane displays how the grid will be printed. From the preview pane, you can modify the background (including the color or watermark), change the print settings, export the grid as a PDF document, and send it via email in any of several formats, including PDF, MHT, RTF, Excel, CSV, TXT, or an image file.

Note: You can select the columns that will display and in what order before printing, emailing, or exporting.

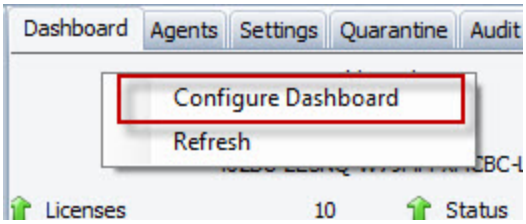
- **Expand All**: select to expand the outline and see more entries.
- **Collapse All**: select to collapse the outline and see fewer entries.

5.2 — Dashboard Property Page

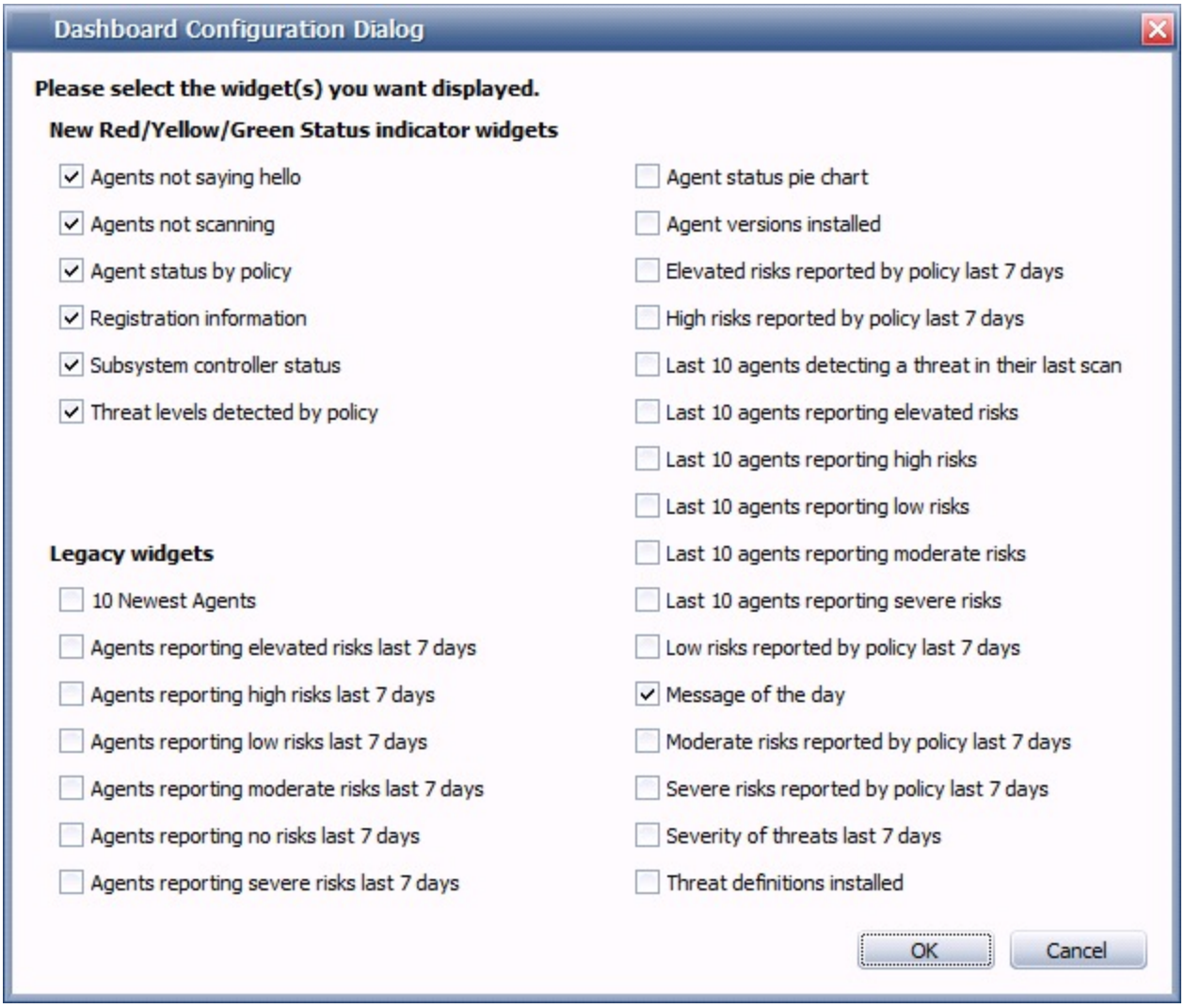
The **Dashboard** is only available when selecting a site in the site navigator window. It lists various types of statuses.

To configure the Dashboard

1. Select a site and click **Dashboard**.
2. Right-click in the Dashboard area and select **Configure Dashboard**.



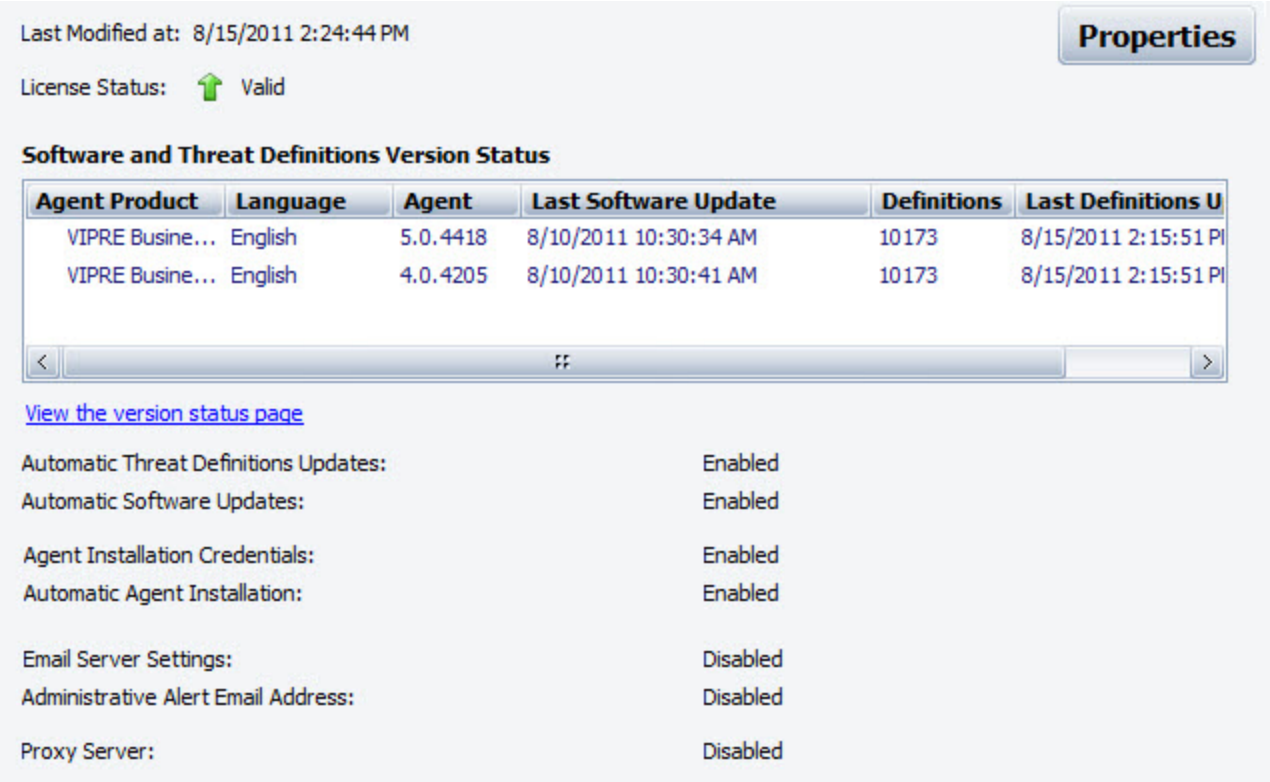
The Dashboard Configuration Dialog displays.



3. Make your selections and click **OK**. The widgets display in the Dashboard.

5.3 — Site Settings Property Page

The **Settings** property page displays the versions of the software and definitions, as well as whether the main site settings are enabled or disabled.



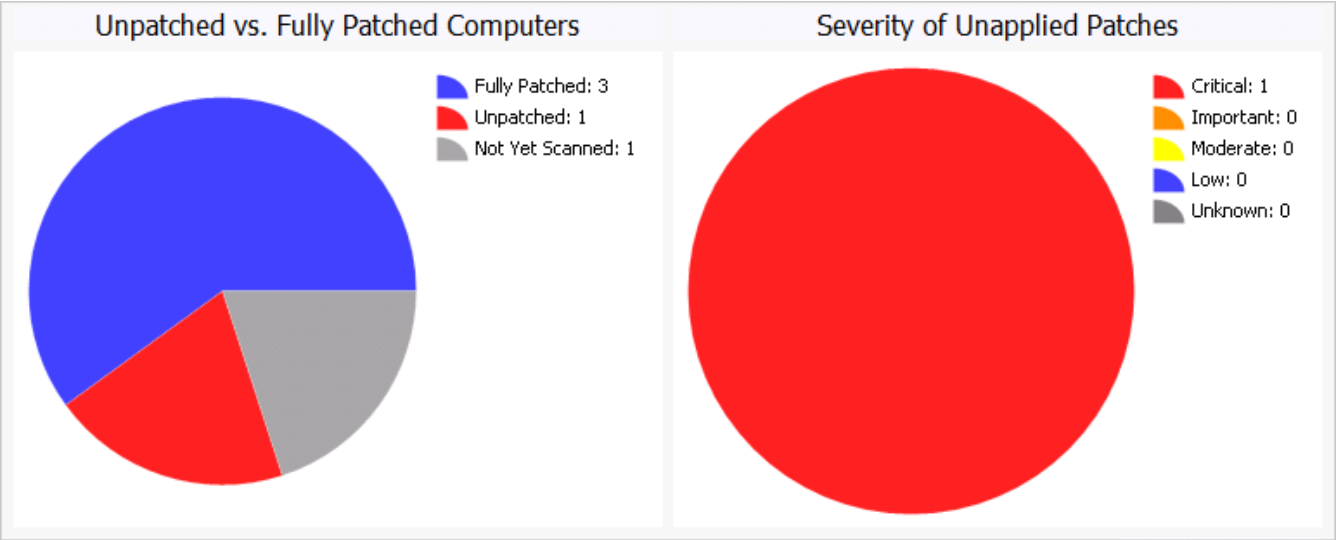
To edit the site settings, click the **Properties** button, which opens the Site Properties.

5.4 — Patch Management Property Page

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

The **Patch Management** screen displays software patch information for all the agents that are managed by the selected policy. It provides you with an overview of patch information and enables you to view patch details as well as configure patch management options.

> **Note**: Critical patch management alerts are displayed in the **Alerts** section of the screen.



The Patch Management screen displays patch information in the following pie-charts:

- **Unpatched vs. Fully Patched Computers** - displays the number of agents that are:
  - Fully Patched
  - Unpatched
  - Not Yet Scanned
- **Severity of Unapplied Patches** - displays ratings which represent the security risk that missing patches impose on agent machines:
  - Critical
  - Important
  - Moderate
  - Low
  - Unknown

To access the Patch Management screen:

1. From **Site Navigator**, select the policy you want to manage.
2. From the right pane, click the **Patch Management** tab.

5.4.1 — Viewing Patch Details

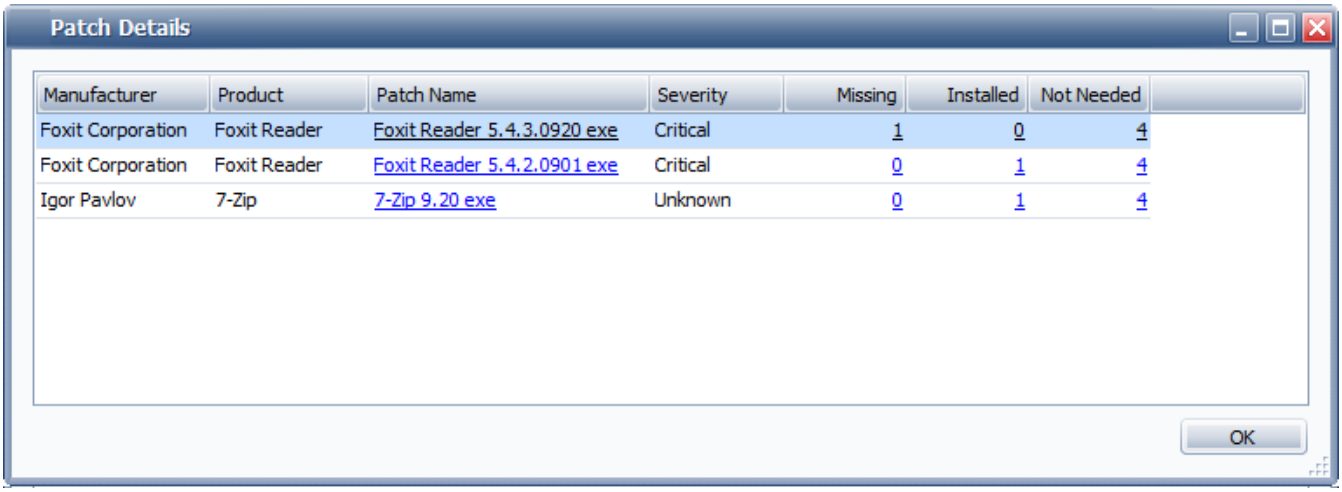
From the Patch Management screen, you are able to delve deeper in patching information. VIPRE provides you with a Patch Details dialog, which includes the following information for each missing patch:

- **Manufacturer**: name of the software vendor that published the unpatched software application
- **Product**: name of unpatched software application
- **Patch Name**: name used to identify the missing patch
- **Severity**: security risk imposed by missing patch
- **Missing**: Number of computers that require the missing patch

- **Installed**: Number of computers that already installed the missing patch
- **Not Needed**: Number of computers that do not require the missing patch.

To view patch details:

1. From **Site Navigator**, select the policy you want to manage.
2. From the right pane, click the **Patch Management** tab.
3. Click **Patch Details**.



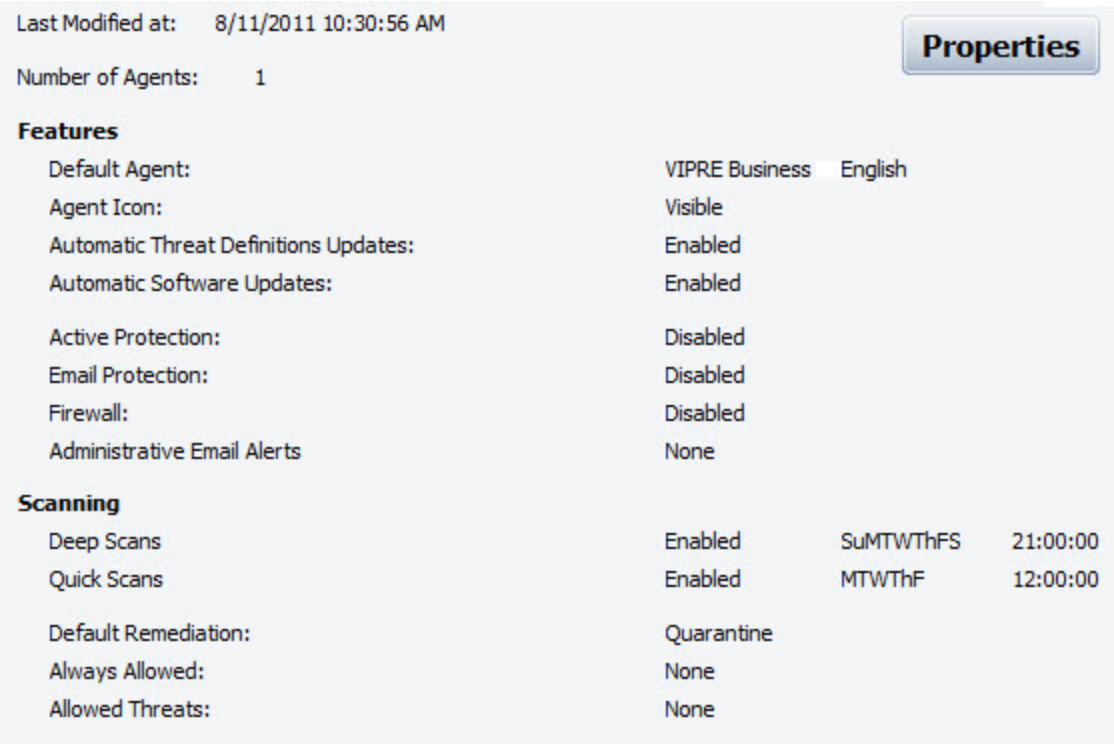
4. Click a Patch Name to view more information about the missing patch.

Note: An Internet connection is required since additional patch information is retrieved directly from the vendor's website.

5. Click a number from the **Missing**/**Installed**/**Not Needed** column, to view the computer name(s) associated with the Missing/Installed/Not Needed patch.
6. Click **OK**.

5.5 — Policy Settings Property Page

The **Policy Settings** property page displays whether the main features in the policy are enabled or disabled, and when the automatic scanning is scheduled.



To edit the policy settings, click the **Properties** button, which opens the Policy Properties.

5.6 — Quarantine Property Page

The **Quarantine** screen displays all quarantined items found by all agents for the selected policy or site. In the Admin Console, it is one of 6 available tabs when viewing a policy, and one of 8 tabs available when viewing a site. This page is used to view all characteristics associated with those quarantined items. Right-click on any Quarantine item to view options associated with that item.

Note: The column headings are dynamic, allowing you to move their order and sort by a category within that column. Click the filter icon on a column heading to select a filtering option. See Filtering Views for more information on using the available filters.

Tip: You can sort the information in the table by dragging a column header to the top area of the window.

The columns include:

- **Name**: displays the name of the malware threat detected during the scan.
- **Category**: displays the type of malware threat that was discovered. For example, Trojan Downloader, Worm.Generic, and so forth
- **Severity**: displays the level of severity of the malware threat discovered. Severity levels are measured as Low, Moderate, Elevated, High, or Severe.
- **Agent Count**: displays the number of agents that contain this quarantined threat for this policy.

- **Last Quarantined**: displays the date the threat was last quarantined under this policy.
- **Threat ID**: displays the ID number for the associated threat.

5.6.1 — Quarantine Right-Click Menu

The right-click menu options are listed below:

- **Refresh**: select to refresh the data on the screen.

- **Print\Email\Export**: select to print, email, or export the entire contents of the grid. Once selected, a preview pane displays how the grid will be printed. From the preview pane, you can modify the background (including the color or watermark), change the print settings, export the grid as a PDF document, and send it via email in any of several formats, including PDF, MHT, RTF, Excel, CSV, TXT, or an image file.

Note: You can select the columns that will display and in what order before printing, emailing, or exporting.

- **Expand All**: select to expand the outline and see more entries.
- **Collapse All**: select to collapse the outline and see fewer entries.

- **Details**: displays the **Details** dialog box with two tabs containing the following:
- **Quarantined Items**: displays all of the occurrences of each type of quarantined item.
- **Scan History**: displays every agent scan that detected the item.

- **Delete from Quarantine**: select to delete the threat from the agent system. Selecting this option displays the **Delete Threat** dialog box. Click **Yes** if you are sure you want to delete the threat selected. Click **No** to close the dialog box without deleting the threat.
- **Unquarantine Threat**: select to remove the threat from the quarantined threats list for the selected policies.
- **Unquarantine and Send for Analysis**: same as the "Unquarantine Threat" listed above, and will then automatically send the item to ThreatTrack Security for analysis. A message of this action is generated in the System Messages screen.
- **Send for Analysis**: select to send the item to ThreatTrack Security for analysis. A message of this action is generated in the System Messages screen.

- **Allow Threat**: opens the Allow Threat dialog box where you can select the policies for which you want to allow this item. Once allowing, it will be displayed on the Allowed Threats screen for the policy. You can remove the threat from this page, as well.

5.7 — Site Properties: Audit Trail Property Page

The **Audit Trail** property page allows you to monitor what configurations were made in VIPRE Business, who made them, and when they were made.

To print the audit trail, right-click in the grid area and select **Print\Email\Export**.

Columns:

- **Changed At**: displays the date and time that the command was changed.
- **Changed By**: displays who changed the command.
- **Command**: displays the changed VIPRE Business component where the field resides, such as Policy, VssConfig, VssLicense, and so forth
- **Target**: displays the sub-component where the field resides, such as the policy or site name.
- **Field**: displays the field/command that was changed.
- **Old Value**: displays the original setting.
- **New Value**: displays what the setting was changed to.

5.8 — Pending Agent Installs Property Page

The **Pending Agent Installs** screen lists all pending agent upgrades and installs. If an Automatic Agent Installation is running, both the pending auto-install and scheduled installs will display here.

Note: The column headings are dynamic, allowing you to move their order and sort by a category within that column. Click the filter icon  on a column heading to select a filtering option. See Filtering Views for more information on using the available filters.

This screen contains the following items:

Columns:

- **Policy**: displays the name of the policy to which the agent is based.
- **Agent**: displays the agent name where the Agent install attempt occurred.
- **Agent Guid**: displays a unique agent identifier used in the reporting database and Agent Catalog.
- **Last Install Attempt At**: displays the date and time the last install occurred for that agent.
- **Last Status Check At**: displays the date and time the last status check occurred for that agent.
- **Last Status**: displays the last status that was received for that agent.
- **Manual Push**: displays whether or not the install was a "Manual Push" or not.
- **Last Updated At**: displays the date and time the agent last received threat definition updates.
- **Install At**: displays the date and time that the Agent will be installed.

Right-click menu options:

- **Refresh**: select to refresh the data on the screen.

- **Print\Email\Export**: select to print, email, or export the entire contents of the grid. Once selected, a preview pane displays how the grid will be printed. From the preview pane, you can modify the background (including the color or watermark), change the print settings, export the grid as a PDF document, and send it via email in any of several formats, including PDF, MHT, RTF, Excel, CSV, TXT, or an image file.

Note: You can select the columns that will display and in what order before printing, emailing, or exporting.

- **Reschedule**: select to reschedule the Agent upgrade. Enter the date and time.
- **Cancel**: select to cancel the Agent upgrade.

5.9 — Agent Install History Property Page

The **Agent Install History** screen lists all manual and automatic agent installations that occurred per policy.

Note: The column headings are dynamic, allowing you to move their order and sort by a category within that column. Click the filter icon  on a column heading to select a filtering option. See Filtering Views for more information on using the available filters.

This screen contains the following items:

Columns:

- **Policy**: displays the name of the policy to which the agent is based.
- **Agent**: displays the agent name where the installation attempt occurred.
- **Agent Guid**: displays a unique agent identifier used in the reporting database and Agent Catalog.
- **Last Install Attempt At**: displays the date and time the last installation occurred for that agent.
- **Last Status Check At**: displays the date and time the last status check occurred for that agent.
- **Last Status**: displays the last status that was received for that agent.
- **Manual Push**: displays whether or not the installation was a "Manual Push" or not.
- **Last Updated At**: displays the date and time the agent last received threat definition updates.

Right-click menu options:

- **Refresh**: select to refresh the data on the screen.

- **Print\Email\Export**: select to print, email, or export the entire contents of the grid. Once selected, a preview pane displays how the grid will be printed. From the preview pane, you can modify the background (including the color or watermark), change the print settings, export the grid as a PDF document, and send it via email in any of several formats, including PDF, MHT, RTF, Excel, CSV, TXT, or an image file.

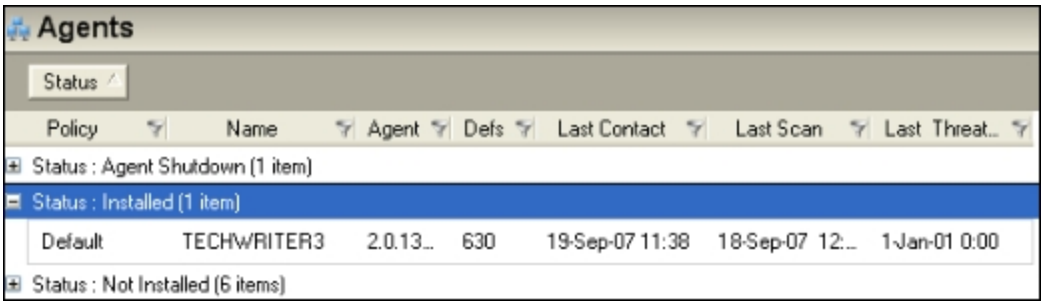
Note: You can select the columns that will display and in what order before printing, emailing, or exporting.

- **Delete History**: select to delete all deployment history.

5.10 — Grouping Views

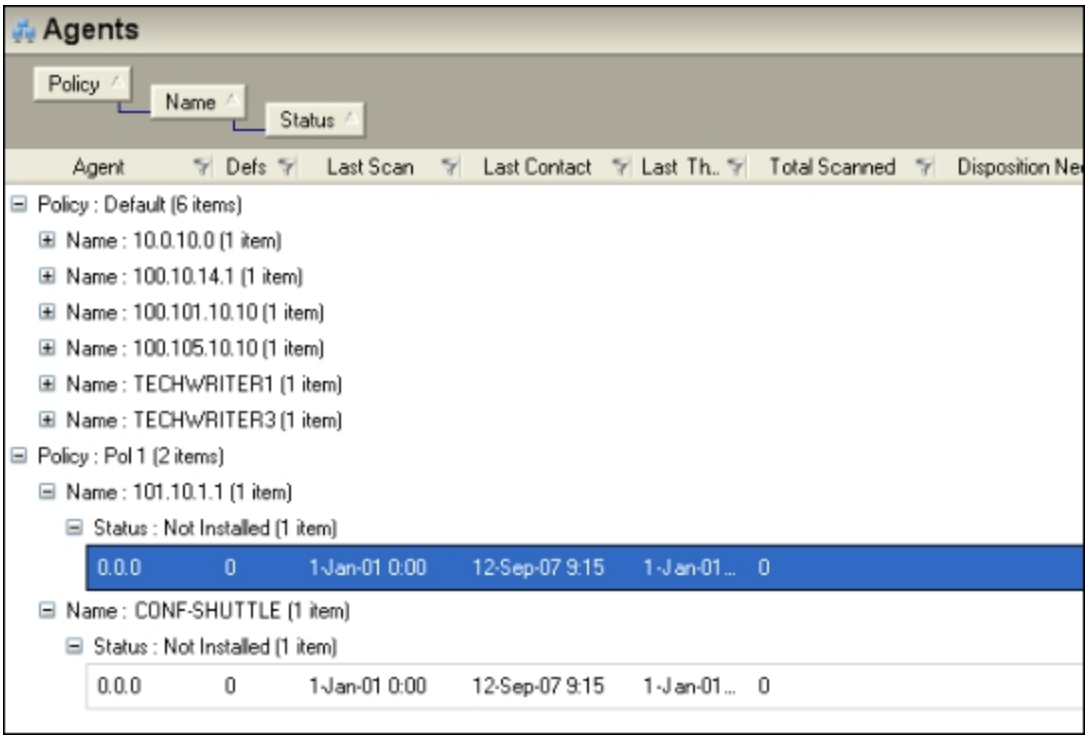
There are default views for the Agents, Quarantine, and System Messages screens, but the views are fully user-configurable. Along with resizing and dragging columns to different positions, you can also drag a column header into the grouping area above the table. This groups results by that column. Doing that enables you to narrow specific searches for information.

Using the Agents screen as an example, you can see in the view below that the **Status** column has been dragged into the sort area above the table. The screens sort the view by statuses, allowing you to expand particular choices. The Installed agents are expanded to show just what's in that category, with the other categories collapsed and showing how many items are in each.



5.10.1 — Nested Groups

You can drag multiple columns into the grouping area above the table to create nested groups, and you can click and drag the column headers in that space to any order you desire.



In the view above, the **Policy**, **Name**, and **Status** columns have all been dragged into the grouping area and have been placed in that order. This creates a view displaying each policy, all those agents assigned to those policies, and the status of each agent. The information displayed in the area below the last grouped item, in this case **Status**, corresponds to the columns remaining in the standard view. You can still drag those columns around to reorganize them, the information will move in the table according to how the remaining columns are arranged. You can also drag the three columns in the grouping area around, rearranging the view.

5.10.2 — Using the Right-Click Menu with Grouped Views

Select the display below the last grouped item, as shown in the image, to perform all listed actions in the right-click menu, such as expanding and collapsing entries, printing, checking **Agent Details** and running scans. If you select one of the grouped items instead, the agent specific actions in the right-click menu are disabled. These include **Agent Details...**, **Scan...**, **Purge Deferred Work Item(s)...**, **Reassign Agent to Policy...**, **Uninstall Agents...**, and **Remove Agent(s) from Catalog...**

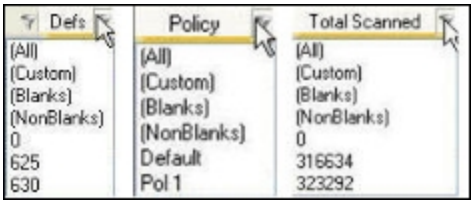
Note: You cannot filter columns that are in the grouping area above the table, but you can filter through any other columns you have displayed. See also Filtering Views for more information.

5.11 — Filtering Views

Filtering allows you to search for very specific information, making management of the system easier and more efficient. You can filter on a single column or on multiple columns to further refine your search. You cannot filter on a column if it has been dragged into the sort area above the table; that column must be dragged back into the table to be filtered.

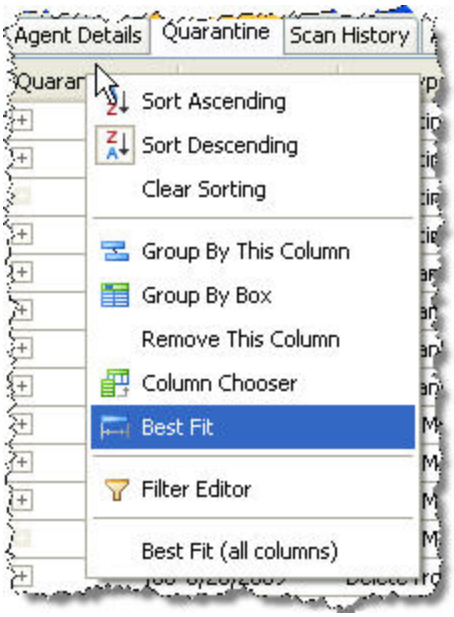
Filtering within a column:

To filter within each column click the filter icon  next to a column heading and select one of the options.

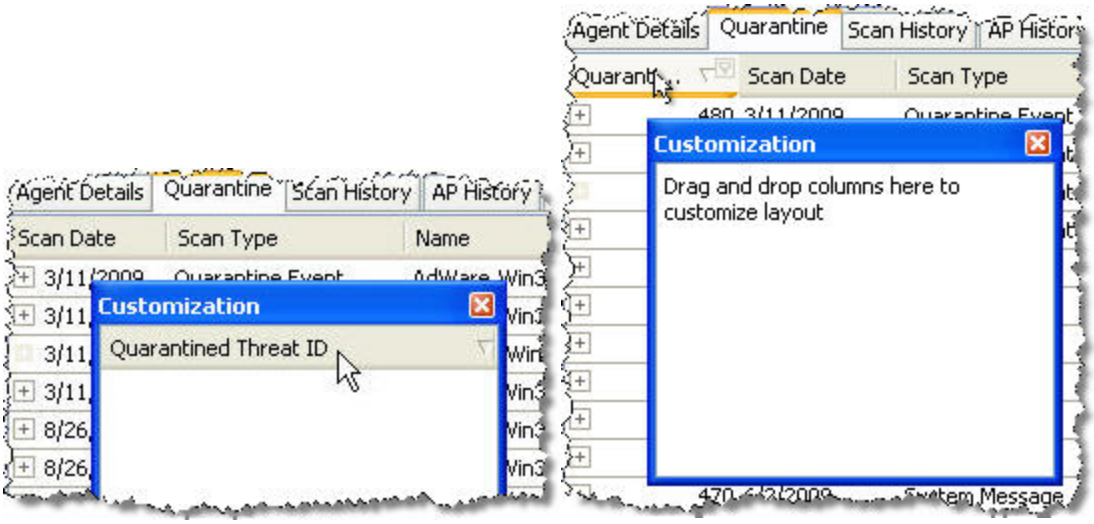


Filtering Right-Click Menu:

Right-click from anywhere in the header area to access additional filtering options:



The **Column Chooser** allows you to add or remove any column heading. Simply drag/drop from the Customization box to the desired location in the header, as pictured below.



The **Filter Editor** allows you to perform advanced search strings.

To use the Filter Editor:

1. Right-click on a column heading that you want to search by and select **Filter Editor**. The Filter Editor dialog box displays.
2. Choose a boolean operator by clicking on the default And operator.
3. Optionally, change the column name. The column name is displayed within brackets (for example, [Category]) under the operator.
4. Click [Begins with] to choose a boolean value.
5. Optionally, click <enter a value> to enter a custom boolean value.

6. Optionally, to add additional search strings, click the "plus sign" next to the boolean operator at the top.
7. To delete a search string, click its "x".

6 — Working with the Agents Catalog

The **Agents** screen (also known as the *Agent Catalog*) is a listing of agents, properties, and other information that can be accessed in multiple ways. You can access agent information by site or by policy from the **Agents** tab by viewing a site or policy, respectively, on the Admin Console.

Note: The column headings are dynamic, allowing you to move their order and sort by a category within that column. Click the filter icon  on a column heading to select a filtering option. See Filtering Views for more information on using the available filters.

Tip: You can sort the information in the table by dragging a column header to the top area of the window.

6.1 — Agent Status

The Agent Status column indicates all status types for the agents, located here.

6.2 — Right-Click Menu

Right-clicking anywhere in the agent catalog displays the right-click menu. The options in the menu are explained further in Agents - Right-Click Menu, and include basic viewing and printing options and the ability to perform various Agent commands for managing Agents.

6.3 — Adding Columns

You can choose the selection of columns to be displayed by right-clicking anywhere on the header of the catalog screen and selecting **Column Chooser**. The **Customization** box is displayed. The columns are listed alphabetically. Add columns to the agent catalog by dragging/dropping a listed heading to the desired location in the header.

6.4 — Agent Details

You can display the **Agent Details** dialog box two ways: right-click on an agent and select **Agent Details**, or double-click on an agent. This screen displays all information available on the particular agent selected. In addition to **Agent Details**, there are also tabs on this screen for displaying quarantined items, scan history, AP history, email AV history, and system messages for the particular agent selected.

See Agent Details screen for more information.

6.5 — Grouped Views

There are default views for the agent catalog, but the views are fully user-configurable. In addition to resizing and dragging columns you can group columns in the grouping area for different views. The agent catalog groups information by statuses, allowing you to expand particular choices.

See Grouped Views for more information.

6.6 — Filtered Views

You can also filter within each column by clicking the filter icon  next to a column heading and selecting one of the options. The agent catalog will only display those agents meeting the criteria selected. You can filter through the standard filtering options, or through column specific criteria. The most useful filtering option is the "Custom" option, which allows you to do a Boolean search. You can also filter through multiple columns, further refining you search.

See Filtering Views for more information.

6.7 — Agents - Right-Click Menu

The following right-click menu options are available for the Agents screen:

- **Refresh**: select to refresh the data on the screen.

- **Print\Email\Export**: select to print, email, or export the entire contents of the grid. Once selected, a preview pane displays how the grid will be printed. From the preview pane, you can modify the background (including the color or watermark), change the print settings, export the grid as a PDF document, and send it via email in any of several formats, including PDF, MHT, RTF, Excel, CSV, TXT, or an image file.

> **Note**: You can select the columns that will display and in what order before printing, emailing, or exporting.

- **Expand All**: select to expand the outline and see more entries.
- **Collapse All**: select to collapse the outline and see fewer entries.

6.7.1 — Agent Commands:

- **Purge Deferred Work Item(s)**: select to purge all work waiting to be sent to the agent from the VSS.
- **Say Hello**: select to force an agent to say hello. This can be used for agents that didn't get an update to pick up the deferred work.
- **Check for Policy Update**: click for the agent to check that it has the latest update to its assigned policy.
- **Ping Agent**: select to send an ICMP ping to the agent. This tells you that the VIPRE service on the agent machine is running or not.
- **Shutdown Agent(s)**: select to stop the selected agent(s). This applies to all versions of agents.
- **Start Agent(s)**: select to start the selected agent(s). This only applies to agents that are version 3.x and higher.
- **Issue Remote Restart Command**: this can be used when an agent is showing that it needs to Reboot in the console and for non-agent related issues. This command does not require an agent to exist on the remote computer for the restart command to be issued.
- **Agent Updates**:

- **Check for Agent Software Updates**: select to have the agent(s) check for—and get if available—the latest software updates for the selected agent(s).
- **Schedule Agent Upgrades**: allows you to tell end users to leave their computers on overnight or over a weekend and to schedule software updates during off-hours so that the end users won't be affected by the upgrade if a reboot is needed. Time is in military time.
- **Check for Threat Definitions Updates**: select to check for—and get if available—the latest threat definitions for the selected agent(s).
- **Force Full Threat Definitions Update**: select to force the agent to get the full threat database for the selected agent(s). This will take longer than a definition update.
- **Agent Details**: select to display Agent Details.
- **Edit Note**: click to display a text box to enter a note for selected agent. You can only enter a note for one agent at a time.

6.7.2 — Scanning

- **Full Scan**: immediately initiates a full scan for the selected agent(s).
- **Quick Scan**: immediately initiates a quick scan for the selected agent(s).
- **Abort Scan**: select to completely terminate the current scan for the selected agent(s).
- **Pause Scan**: select to temporarily pause the current scan for the selected agent(s).
- **Resume Scan**: select to continue the paused scan for the selected agent(s).
- **Patch Management**: (*Premium or Endpoint Security)*
  - **Install Approved Patches**: starts installing the approved patches related to the selected agent(s).

Note: If there are approved patches pending installation, the agent Status displays **Installing Patches**.

  - **Scan for Missing Patches**: starts scanning software applications installed on the selected agent(s) for missing patches

Note: To verify that the scan started, ensure the agent Status is **Patch Scanning**.

- **Reassign Agent to Policy**: select to assign the agent to a different policy.

- **Disposition**: select to clear the **Disposition Needed** column in the **Agent Catalog**.

- **Add and Install Agent(s)**: select to display the **Installing VIPRE to your Computers** dialog box and add agents to the Agent Catalog and install them on computers.
- **Uninstall Agent(s)**: select to uninstall an agent from a workstation. Click **Yes** when prompted. Click **No** to close the window and leave the agent installed.

- **Add to Agent Installation Scopes**: click to add an agent to the list of agents in the Automatic Agent Installation queue.

- **Remove Agent(s) from Catalog**: select and click **Yes** to remove the selected agents. Click **No** to close the **Remove Agents** dialog box without removing any agents.

- **Grid Colors**: select to open the Agent Grid Colors dialog box where you can modify the colors in the grid.

6.8 — Agent Statuses

Agents have the following status types:

- **Agent Download Failed**: Indicates that the Micro Installer was unable to download the agent software, and that the agent installation failed.
- **Agent Installation Failed**: Indicates that an agent was not installed successfully.
- **Agent Shutdown**: Indicates that the machine on which the agent resides has been shut down.
- **Begin Custom Scan**: Indicates that a custom scan is in progress. This can be a right-click scan, a USB drive scan or a custom scan that was configured on the agent.
- **Begin Scanning**: Indicates that a Quick Scan has begun.
- **Begin Scanning Full**: Indicates that a Full Scan has begun.
- **Cleaning**: Indicates that an agent is cleaning threats.
- **Defs Update Complete**: Indicates that an agent's definitions were successfully updated.
- **Downgrade Ignored**: Indicates that a user tried to install a downgrade version of VIPRE (for example, a VPE agent over a VEP agent) and that the downgrade is being ignored.
- **Downloading Admin Action**: Indicates that the admin action script (tool to remove 3rd party agents) is being downloaded onto the machine where the agent is going to be installed.
- **Downloading MSI**: Indicates that the MSI Installer package is being downloaded onto the machine where the agent is going to be installed.
- **Installing Agent**: Indicates that an agent is being installed.
- **Installing Micro Installer**: Indicates that the Micro Installer is being installed.
- **Installing Patches**: Indicates that missing patches are being installed.
- **Installation Complete**: Indicates that patch installation is complete.
- **Needs Credentials**: Indicates that none of the credentials specified in **Site Properties > Agent Installation** are valid for the computer.
- **Not Communicating**: Indicates that an agent is no longer communicating. The last contact time was an indeterminate amount of time.
- **Not Found**: Indicates that NetBIOS or Active Directory queries cannot find the computer on the network.
- **Protect Now**: Indicates that the agent is not installed on the computer.
- **Patch Scanning**: Indicates that a scan for missing patches is in progress.
- **Protected**: Indicates that an agent has successfully installed.
- **Reboot Required**: Indicates that the machine on which the agent is installed requires a reboot (usually after the agent was installed).
- **Running Admin Action**: Indicates that an admin action script is being run to remove 3rd party agent.
- **Scan Aborted**: Indicates that the scan was aborted by the user.
- **Scan Complete**: Indicates that the scan has completed.
- **Scan Failed**: Indicates that the scan failed for an unspecified reason.

- **Scan Paused**: Indicates that a scan was paused by the user.
- **Scanning Cookies**: Indicates that an agent is scanning cookies.
- **Scanning Files**: Indicates that an agent is scanning files.
- **Scanning Folders**: Indicates that an agent is scanning folders.
- **Scanning Memory**: Indicates that an agent is scanning the PC's memory, including its processes.
- **Scanning Registry**: Indicates that an agent is scanning the Windows registry.
- **Updating Defs**: Indicates that an agent is updating its definitions.
- **Updates Failed**: Indicates that updates for the agent failed.
- **Uploading MSI Log**: Indicates that the log of the installation is inserted into the database where the VSS is located.
- **Updating Software**: Indicates that an agent's software is being updated.
- **User Remediation**: Indicates that a user has selected to do something with a found threat (quarantine or remove).

7 — Managing Sites

This chapter on Managing Sites discusses the procedures associated with site management.

A **Site** is a physical location where the VSS is installed. Additional sites can be configured as needed, and consist of all of the Policies and Agents unique to a site

7.1 — Adding a Site

The Admin Console allows you to manage multiple site locations.

To add a site in the Admin Console:

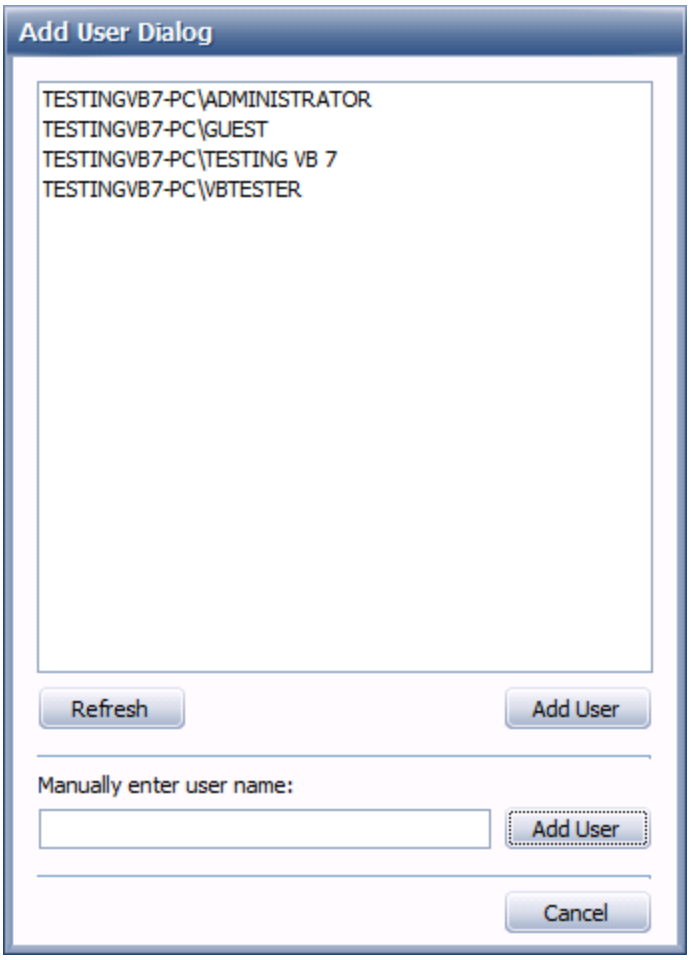
1. If there is a 3rd party firewall other than a Microsoft Firewall between your location and the site you wish to add, ensure that traffic on port 18088 is allowed to pass through.
2. From the **File** menu, select **Site Manager**. The Site Manager displays.
3. Click **Add**. The Add Site dialog box displays.
4. Enter the **Server** name for the other site. This can be the machine name, IP address, or host name.
5. If the remote server is on a different domain, you will need to unselect the "Use logged on user account" checkbox and enter the appropriate credentials of the remote network.
6. Optionally, enter any associated comments for this site and click **OK**.
7. To add additional sites to the Admin Console, repeat steps 2 - 6.

7.2 — Adding Administrators for Console Access

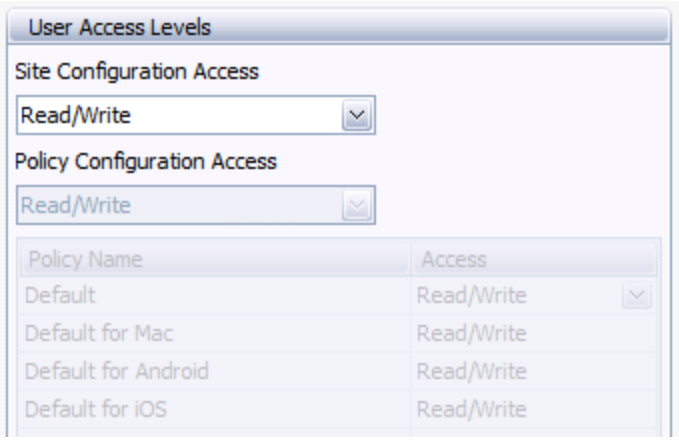
By default, Admin Console security is set to full access for domain and local administrators on the respective site. Optionally, you can add additional users to access the site and control the access they have to it and its policies.

To add an administrator to access the console:

1. From the **Site Properties**, open the **User Administration** screen.
2. Click **Add User** and select a user from the list.



3. Click **OK**. The new user displays in the "Users" area.
4. Under the **User Access Levels** area:



   a. Assign the **Site Configuration Access**.
   b. Assign the **Policy Configuration Access** for each applicable policy.

5. To add additional users, repeat Steps 3-4.
6. Click **Apply** or **OK** to save changes.

7.3 — Connecting a Remote Admin Console

VIPRE Business supports the ability to have multiple consoles connected to one VIPRE Site.

To add a LAN remote Admin Console:

1. Begin the VIPRE installation process and install the .NET 3.5 Framework, if necessary.

   During the "Select Features" screen of the installation, choose **VIPRE Business Admin Console and Report Viewer**.
2. Once installed, open VIPRE Business.
3. From the **File** menu, select **Site Manager**. The Site Manager displays.
4. Click **Add**.
5. Enter the **Server** name for the other site. This can be the machine name, IP address, or host name.
6. If the remote server is on a different domain, you will need to unselect the “Use logged on user account” checkbox and enter the appropriate credentials of the remote network.
7. Optionally, modify the refresh "update interval" in seconds. The default is 1 second and the values are 1-120 seconds.
8. Optionally, enter any associated comments for this site and click **OK**. Opening the console will now display the remote site.
9. To add additional sites to the Admin Console, repeat steps 4 - 8.

To add a WAN remote Admin Console:

1. Configure your firewall to forward Port 18088 to the VIPRE Site Service.
2. Begin the VIPRE installation process and install the .NET 3.5 Framework, if necessary.

   During the "Select Features" screen of the installation, choose **VIPRE Business Admin Console and Report Viewer**.
3. Once installed, open VIPRE Business.
4. From the **File** menu, select **Site Manager**. The Site Manager displays.
5. Click **Add**. The Add Site dialog box displays.
6. Enter the Public IP address for the name and Port 18088.
7. As needed, add credentials. Your site is added to the "Sites" list box and will appear in the Site Navigator.
8. Optionally, enter any associated comments for this site and click **OK**. Opening the console will now display the remote site.
9. To add additional sites to the Admin Console, repeat steps 4 - 8.

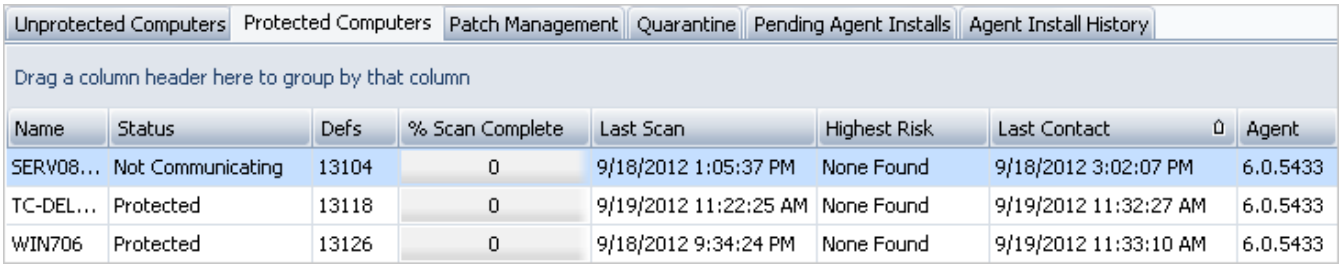
7.4 — Reusing Old Licenses

Over time, it is possible that some licenses remain assigned to decommissioned machines. You can free up unused licenses by deleting an agent from the Protected Computers list.

> **Note**: Removing unused agents is configurable on a per-policy basis.

To remove unused agents from the list:

1. From Site Navigator, select the site containing the agents you want to remove.
2. Click **Protected Computers** tab to display agents that are installed on your network computers.



3. Sort agents by the **Last Contact** column to group ones that have not been contacted for some time.
4. Select the agents you want to remove. You can use **Ctrl** or **Shift** for multiple selections. Keep in mind those agents that are assigned to laptops that may have not checked in for a while.

> **Note**: If you remove an agent that resides on a laptop that has not checked in for a while, it will reappear in the console once the laptop is reconnected to the network.

5. Right-click on the selected agent(s) and select **Remove Agent(s) from Catalog...**
6. Click **Yes**, when prompted. The pertaining license keys become reusable immediately.

8 — Configuring Site Properties

The **Site Properties** is used to configure all settings for a VIPRE Business Site.

8.1 — To open the Site Properties or Site Configuration Wizard:

From the Site Navigator in the Admin Console, right-click on your desired site and select one of the following:

- **Properties**: select to open the VIPRE Business Site Properties.
- **Site Configuration Wizard**: select to open the Site Configuration Wizard.

The screens are summarized here.

8.2 — Configuring a Site

It is important to configure your site(s) before installing Agents.

To configure a Site:

1. From the main Admin Console, click the **Site Properties** icon to open the Site Properties window.
2. Configure the following screens:

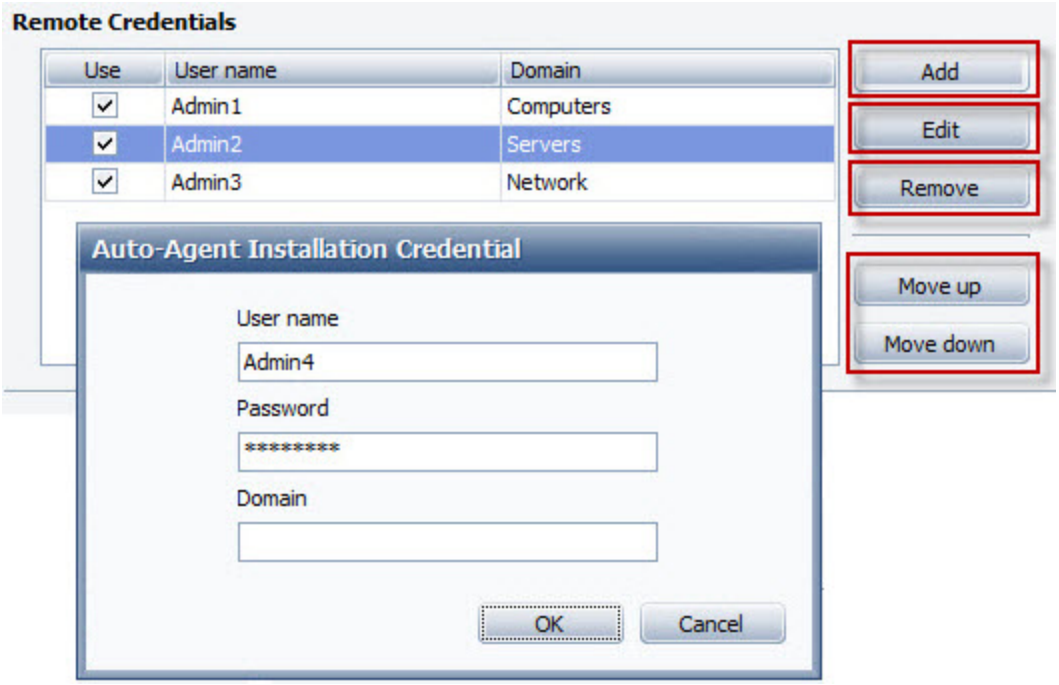
- **Registration**: register your copy of VIPRE Business, view information about your license, and view your license status. You can also purchase a license or update your existing license. *For more information*, see "Registering VIPRE Business".
- **Unprotected Computer Discovery**: manage settings for discovery unprotected computers and checking saved credentials to see if agent could be pushed to found computer. *For more information, see* "Managing Unprotected Computer Discovery".
- **Agent Software**: select the appropriate agent software for your site. *For more information*, see "Select Agent Software for the Site".
- **Agent Installation**: assign one or more credentials for administrative access rights to the machines, which is used for installing agents. At least one credential is required prior to installing an agent. Credentials are not applicable if you are running an installer package. *For more information*, see "Configuring Remote Credentials for Agent Installation".
- **Updates**: manage the updates for the site. *For more information*, see "Manage Site Updates".
- **Email Server Settings**: set up the email server and authentication for all notifications under this site. You can enter recipients to receive alerts that address issues with the VIPRE Site Service. You can set specific email alerts for scanning, Email Protection, and Active Protection from the Policy Properties. *For more information*, see "Configure Email Server Settings".
- **Proxy Settings**: configure the Site's **Proxy Settings** if your site requires a proxy to reach the Internet. *For more information*, see "Configure Site Proxy Settings".
- **Firewall Templates**: create templates that contain a set of firewall configurations that you later apply to agents at the Policy level. *For more information*, see "Manage Firewall Templates".
- **User Administration**: optionally, add additional users to access the site and control the access they have to it and its policies. *For more information*, see "Adding Administrators for Console Access".

- **Advanced Settings**: optionally, change the data repository location, set site service for agent interaction, and set database retention. Also, you can change the database VIPRE Business uses. *For more information*, see "Site Properties: Advanced Settings".

3. Click **Apply** or **OK** to save changes.

8.3 — Configuring Remote Credentials for Agent Installation

A "remote credential" is the administrative access to the machines for installing agents, which consists of a user name, password, and domain. At least one credential is required prior to installing an agent. Credentials are not applicable if you are running an installer package.



To configure a remote credential for agent installation:

1. In the **Site Properties**, open the **Agent Installation** screen.
2. Click **Add**. The Auto-Agent Installation Credential dialog box displays.
3. Enter the Administrative access credentials and click **OK**. The credential displays in the table.
4. Optionally, prioritize the credentials in the order that you want them to be used during an Agent installation with the Move up and Move down buttons.
5. Optionally to not use a credential, unselect the checkbox in the "Use" column for the corresponding credential.
6. Optionally to modify a credential, select the credential and click **Edit**.
7. Optionally to no longer use a credential, select the credential and click **Remove**.
8. Click **Apply** to accept changes.

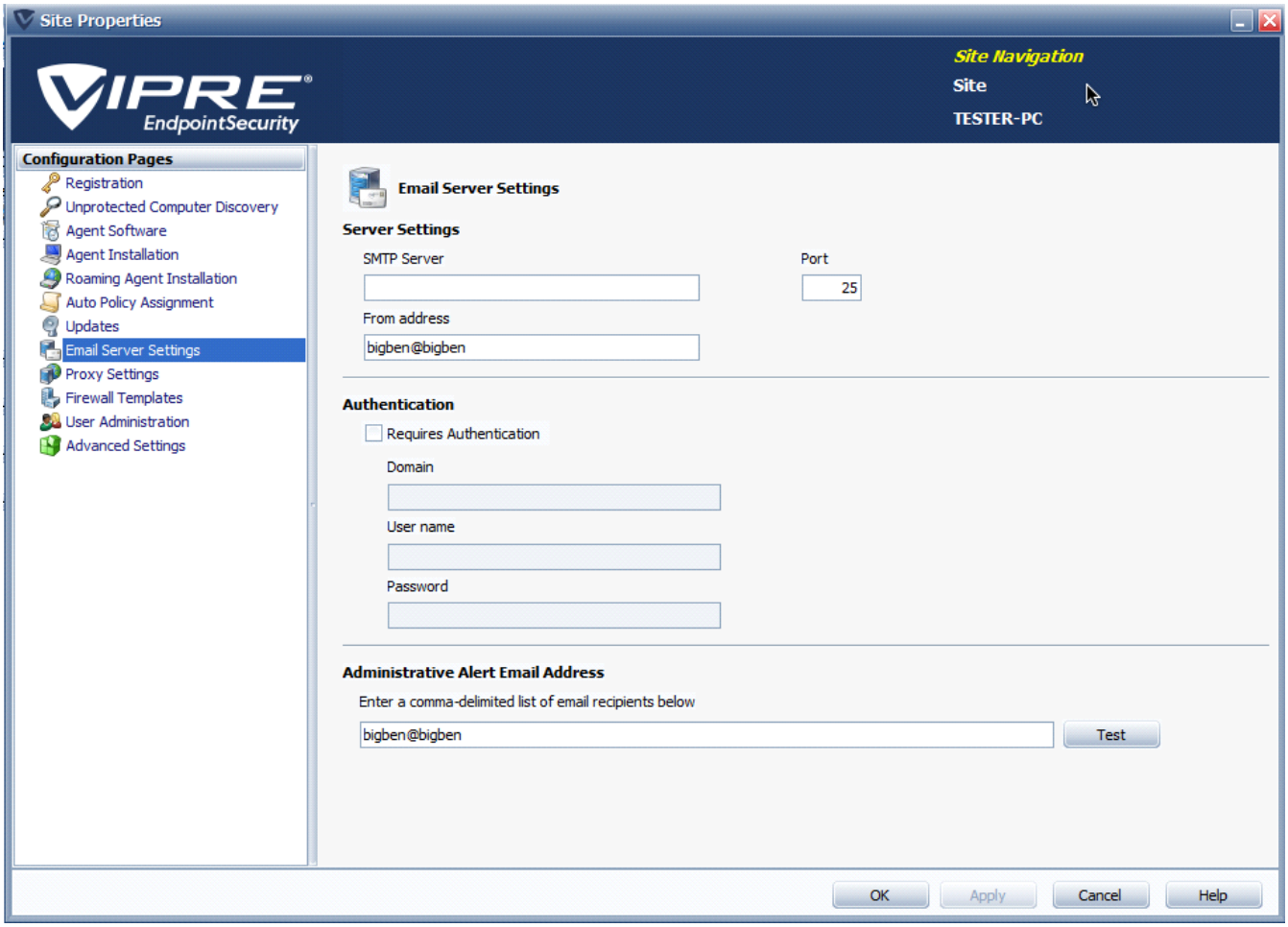
Automatic Agent Installation:

- **Enable scheduled automatic agent installation**: select the checkbox to enable scheduled Agent Installation for all policies under this site that have Automatic Agent Installation enabled at the policy level.
- **Scheduled time**: enter the time for which you wish to schedule the Automatic Agent Installation. The time is configurable for 24 hour time. For example, 23:30 is 11:30 p.m.

> **Note:** Automatic Agent Installation occurs once per day. The time is based on the Time Zone setting of the VIPRE Site Service.

8.4 — Configure Email Server Settings

Configure **Email Server Settings** to set up the email server and authentication for all email alerts under this site. Email messages include administrative alerts from the VIPRE Site Service and agent-related alerts, which are sent at the policy level.



To configure email server settings:

1. From **Site Navigator**, double-click the Site you want to configure.
2. From the left pane of Site Properties screen, click **Email Server Settings**.
3. Configure the following **Server Settings**:
   - **SMTP Server**: key in the **Fully Qualified Domain Name (FQDN)** or **IP Address** of the SMTP server. This is typically an Exchange server or an IIS server residing on the network.

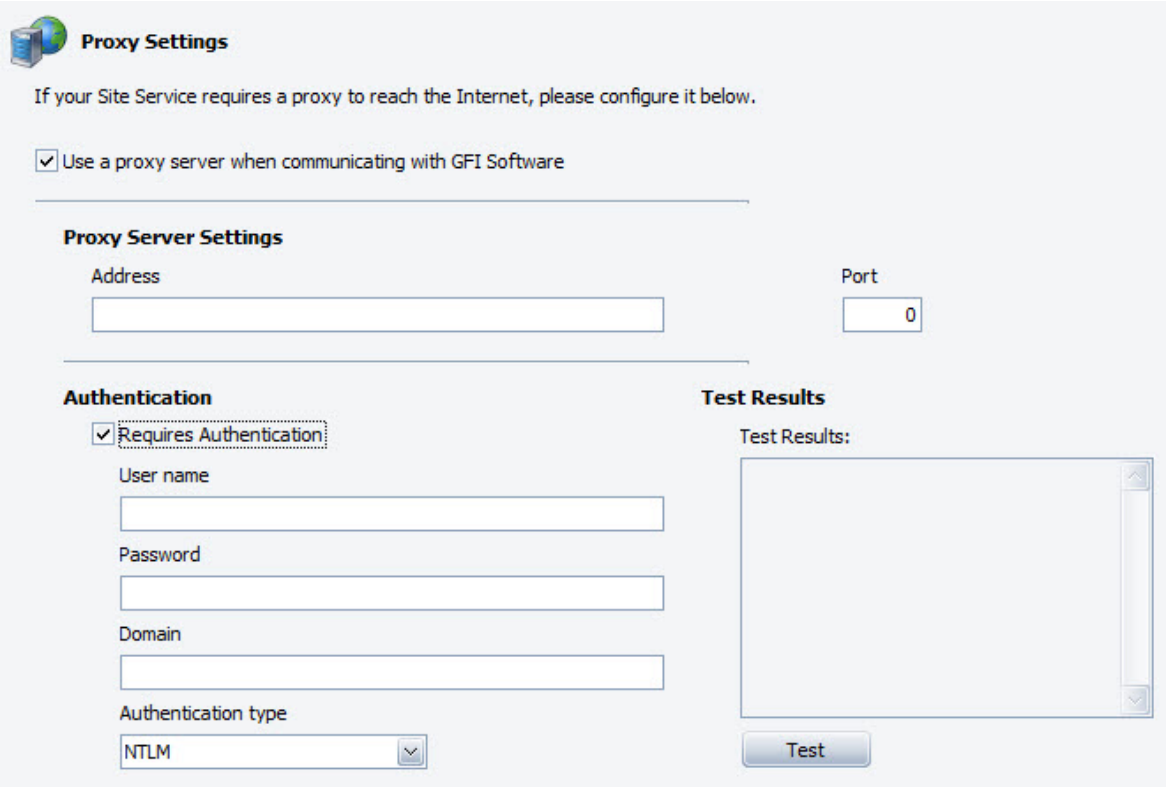
Important: If the site you are managing does not have an SMTP Server, leave the **SMTP Server** field empty. VIPRE will automatically use a free online SMTP service to send your notifications.

   - **Port**: key in the port that is used for email transactions. In most cases the port is **25**.
   - **From address**: enter a "From:" address within your domain to make VIPRE Business email alerts appear as internal email.
4. If required, select the **Requires Authentication** checkbox and enter the Domain, User name, and Password.
5. To receive administrative alerts from the VIPRE Site Service, enter one or more recipients separated by a comma.
6. Click **Test** to test the email server settings you just entered.
7. Click **Apply** to save settings.
8. To receive agent-related alerts, including alerts for Scanning, Active Protection, and Email Protection, configure the Email Alerts in the Policy Properties.

8.5 — Configure Site Proxy Settings

Configure the Site's **Proxy Settings** if your site requires a proxy to reach the Internet.

Note: If you are trying to configure the proxy settings for Agents on a policy see Configure Proxy Settings for Agents.



To configure a Site's proxy settings:

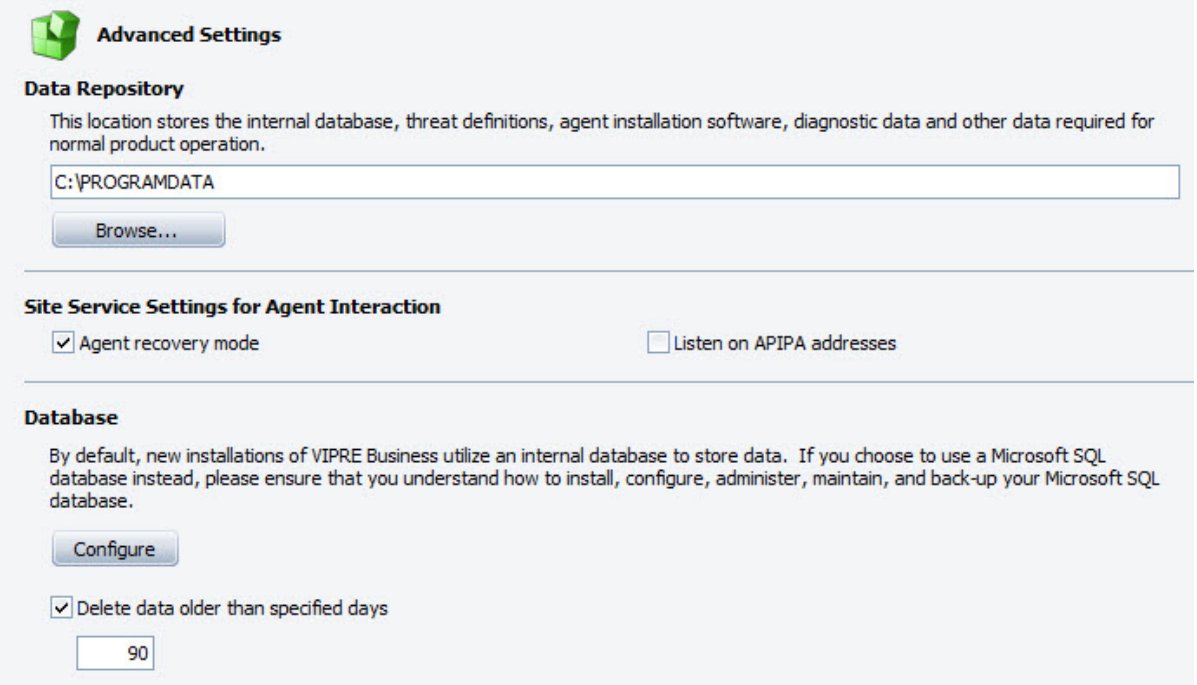
1. Open the site's Proxy Settings screen (**Site Properties>Proxy Settings**).
2. Select **Use a proxy server when communicating with ThreatTrack Security** to enable the Site's proxy settings.
3. In the **Address** box, enter the Fully Qualified Domain Name (FQDN) of the proxy server. The Proxy's IP Address is not recommended.
4. Enter the **Port**, which is typically port 8080.
5. If you are using authentication for the proxy, select the **Requires authentication** checkbox and specify a User name, Password, and Domain, as applicable.
6. Set the **Authentication type** for your proxy by selecting one of the following: NTLM, BASIC, or DIGEST. The common type is NTLM and is used by ISA servers.
7. Click **Test** to test the proxy settings you just entered.
8. Click **Apply** to save changes.

8.6 — Site Properties: Advanced Settings

The **Advanced Settings** screen is used to change the data repository location, set site service for agent interaction, and set database retention. VIPRE Business data include the internal database, threat definitions, agent installation software, diagnostic data, and other data for product operation.

This screen is accessible from the **Site Properties**.

This screen contains the following items:



Data Repository

Optionally, select a location on a local drive to automatically backup VIPRE data. VIPRE Business assigns a default location automatically.

Important: Mapped drives are NOT supported. You MUST save to a local drive only.

Site Service Settings for Agent Interaction

- **Agent recovery mode**: Select to allow the VIPRE Site Service to accept agents without a secure authentication ID. When the agent calls in, it will be told that it needs to re-establish authentication and get added back into the agent catalog. This is useful if you are migrating agents from one VIPRE Site Service to another. If this option is *not* selected *and* the VIPRE Site Service does not have an agent in the catalog, *then* the call will be rejected.
- **Listen on APIPA (Automatic Private IP Addressing) addresses**: The VIPRE Site Service uses Dynamic Host Configuration Protocol (DHCP) to get an IP address; if no DHCP is available, an IP address is randomly selected from a range of addresses. Selecting this option will cause the VIPRE Site Service to answer on APIPA assigned IP addresses.

Database

VIPRE Business uses an internal database to store data. By default, data is automatically purged after 90 days.

- **Configure**: (Experienced SQL Database Administrators ONLY) Click to configure a Microsoft SQL Database, which will override VIPRE Business's default built-in database. For more information, see Advanced Database Configuration.
- **Delete data older than specified days**: Select to automatically delete data that is older than the number of days that you specify. Unselect to allow data to be stored until storage space runs out (not recommended). Values for the selection can be set between 1 and 365 days. This setting is selected by default and is set at 90 days.

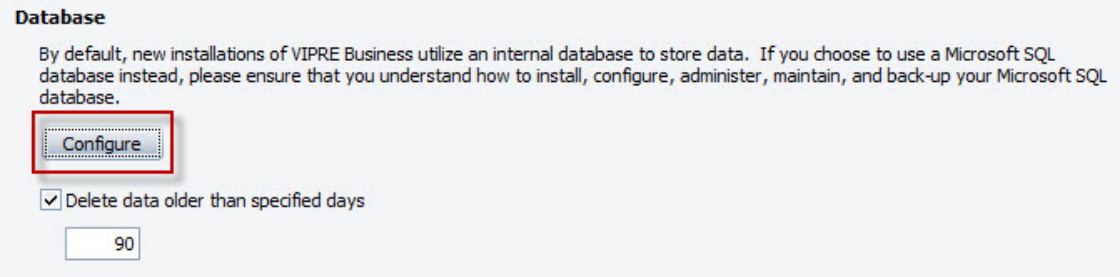
Note: The data deleted does not include quarantined items.

8.6.1 — Advanced Database Configuration

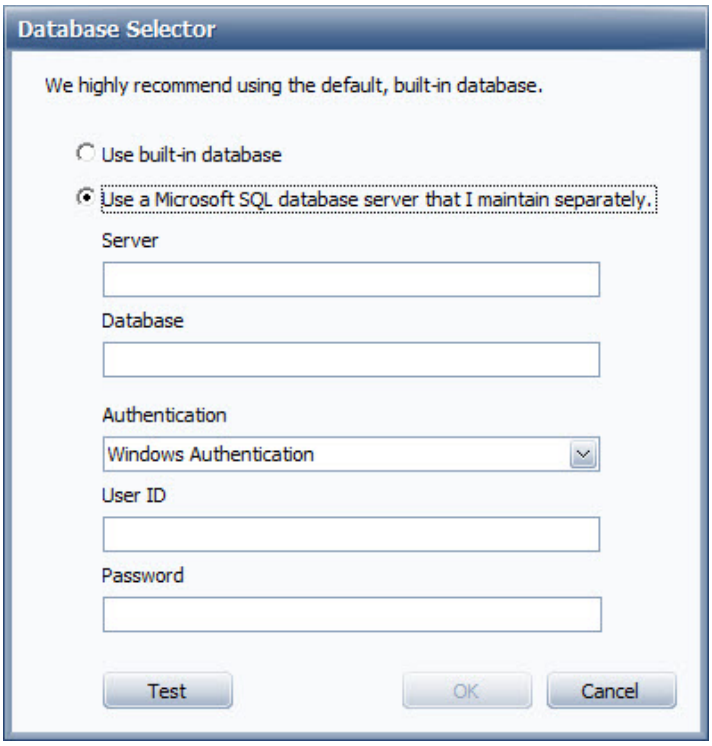
For organizations with over 500 agents, we recommend using Microsoft SQL Express or the full version of SQL.

Important: If you install Agents using VIPRE's built-in database in v. 5.0 and then later switch to a different database, any configurations made to the Site Properties or Policies are NOT transferable. If you have already installed agents, upon switching databases those agents will be automatically added to the Agent Catalog and will be assigned under the Default Policy with the Default settings. You will need to reconfigure policies.

1. In the Admin Console, open **Site Properties>Advanced Settings**.
2. Under the **Database** area, click **Configure**.



The Database Selector dialog box displays.



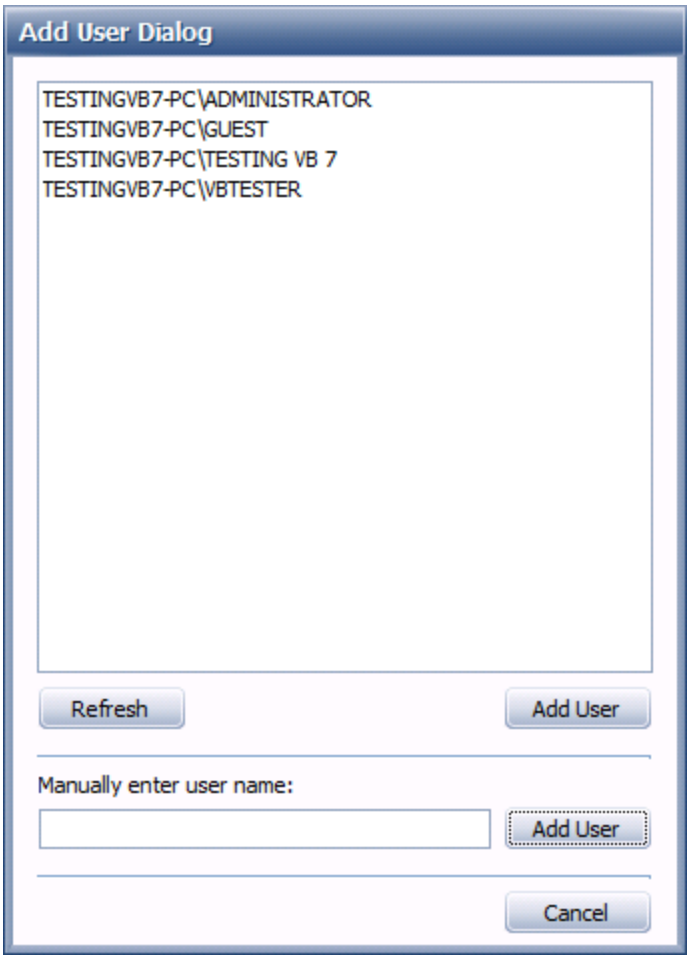
3. Select **Use a Microsoft SQL database server that I maintain separately** and enter the following:
   - Enter the **Server** domain name or IP address of the SQL server.
   - Enter the **Database** or Instance name that will be used as the VIPRE Database.
   - Under **Authentication**, select one of the following:
     - Windows Authentication
     - SQL Server Authentication
     - Enter the **User ID** and **Password** for the database.
4. Click **Test** to verify the data is entered correctly. If the test fails, please recheck entries.
5. Click **OK**. If a new database is being created, it may take several minutes. If you are assigning an existing VIPRE database, all data will be accessible via the Admin Console.

8.7 — Adding Administrators for Console Access

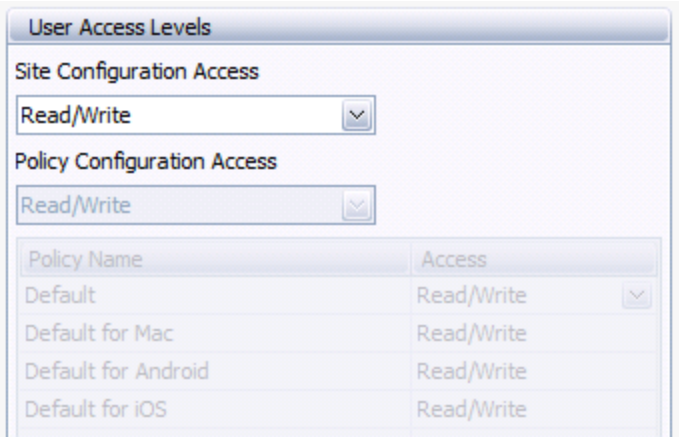
By default, Admin Console security is set to full access for domain and local administrators on the respective site. Optionally, you can add additional users to access the site and control the access they have to it and its policies.

To add an administrator to access the console:

1. From the **Site Properties**, open the **User Administration** screen.
2. Click **Add User** and select a user from the list.



3. Click **OK**. The new user displays in the "Users" area.
4. Under the **User Access Levels** area:



   a. Assign the **Site Configuration Access**.
   b. Assign the **Policy Configuration Access** for each applicable policy.

5. To add additional users, repeat Steps 3-4.
6. Click **Apply** or **OK** to save changes.

9 — Managing Unprotected Computer Discovery

VIPRE Business can automatically detect online computers that are reachable from the machine on which it is installed. These computers are listed under the **Unprotected Computers** tab of the selected security policy. From this tab, you are able to deploy agents on single or multiple computers, as well as assign policies to the new agent(s).

Unprotected Computer Discovery settings for the site are managed from the **Unprotected Computer Discovery** screen in the **Site Properties**.

9.1 — Configure automatic endpoint discovery for the Site:

Set VIPRE Business to automatically perform computer discovery and configure how often VIPRE Site Service should look for new unprotected computers. Additionally, you could specify which domains should be searched.

1. In the **Site Properties**, open the **Unprotected Computer Discovery** screen.
2. Configure the following:
   - **Enable endpoint discovery**: if disabled, VIPRE Site Service won't look for unprotected computers for this site; in this case if there are no any unprotected computers Unprotected Computers tab won't be shown.
     - **How often should we look for new unprotected computers**: select how often search is performed.
     - **Select domain(s) to be searched**: select domain(s), which needs to be searched.
     - **Authenticate with unprotected computers using saved credentials**: This lets you deploy a VIPRE agent with a single click, if using the push installation method. We also use this to display the computer type, OS and the logged in user on the "Unprotected Computers" tab.

IMPORTANT: When saved credentials are used to authenticate with unprotected computers, you could see an increase in LDAP traffic and DCOM errors in your event logs. You should disable this option if your organization restricts this type of network activity.

3. Click **Apply** to accept changes.

10 — Managing Policies

A **Policy** contains all settings and configurations for Agents assigned to it. **You create and configure your policies based on existing policies**, which can be the Default Policy, an Imported Policy, or an Admin-defined Policy.

Tip: Before creating and configuring any policy, it's a good idea to plan out how best to organize (group) machines into policies. From there, you can create any additional admin-defined policy on which to build from.

10.1 — Policies that can be used as a starting point:

Default Policy:

You can start with the Default Policy to create policies that will be used in your production environment or to create your own default policies. The Default Policy is not "connected" to policies that you create from it; so, you can always use the Default Policy as a starting point for additional policies.

IMPORTANT: The Default Policy is initially set with minimum settings that are the least intrusive. This means that the Agent User Interaction, Active Protection, Email AV, Firewall, and Windows Security Center are all disabled. It's intended to be used as a starting point, not "out-of-the-box-ready" to be deployed over your network.

Default Policies:

VIPRE Business includes default policies for specific machine types (Workstation, Server, Laptop, etc.) to get you started. The included default policies provide preset configurations and exclusions based on best-practice recommendations for many common environments. After selecting a default policy, you may need to further customize your settings to meet any additional requirements of your specific environment and organization.

You may also assign any custom policies you create as Default policies for specific categories.

Imported Policies:

A Policy is an xml-based file that can be imported or exported. How?

Admin-defined Policies:

An Admin-defined Policy is a policy created by you or another administrator based on the Default Policy, an Imported Policy, or any other Admin-defined Policy.

10.2 — Special Considerations for Creating Policies

Important: Failure to provide proper exclusions can result in vital aspects of your infrastructure to stop functioning.

When creating new policies, here are some IMPORTANT policies to consider having, depending on your environment:

10.2.1 — Domain Controllers

- Add "Always Allowed Exception" exclusions for the items listed in Microsoft KB Article 822158.

10.2.2 — Email Servers

- Agents installed on email servers are designed to protect the server, not to provide active email scanning.

10.2.3 — Terminal Servers *such as CITRIX or VMware*

- Do not attempt to automatically install Agents on servers of this type using a "push" method.
- Create a separate MSI package and install on the Terminal Server using "add/remove programs." This will cause the Agent to protect any sessions that are running on that server and not just the Terminal Server itself.
- Initially installing Agents to all sessions should be done with the CITRIX terminal server in install mode. For further information on CITRIX installs please see this CITRIX install guide from Methodology in a Box.

10.2.4 — Low bandwidth agents

Create a separate policy for agents with low bandwidth:

- Set Mark agents inactive after no contact in minutes to a value that is at least three times the value of the "Heartbeat Interval" setting.
- Set the Agent status heartbeat in minutes to an interval as much as 1 hour. As long as the console can ping the agents, they will be notified to come and pick up a deferred work item if any is added for them; so, the 1 hour update interval will not hurt agent responsiveness for deferred work.
- Set agents to get definitions updates from the Internet, which is similar to laptop users.
- Create Remote Updates Server in geographic proximity to the agents.

10.2.5 — SQL Database Servers

- Add "Always Allowed Exception" folder exclusions for the SQL Database folder such as: "C:\Program Files\Microsoft SQL Server\MSSQL10.SQLEXPRESS"
- See Microsoft KB Article 309422 for more information on SQL exceptions.

10.2.6 — Microsoft SharePoint Servers

- Add "Always Allowed Exception" folder exclusions for the items listed in Microsoft KB Article 952167.

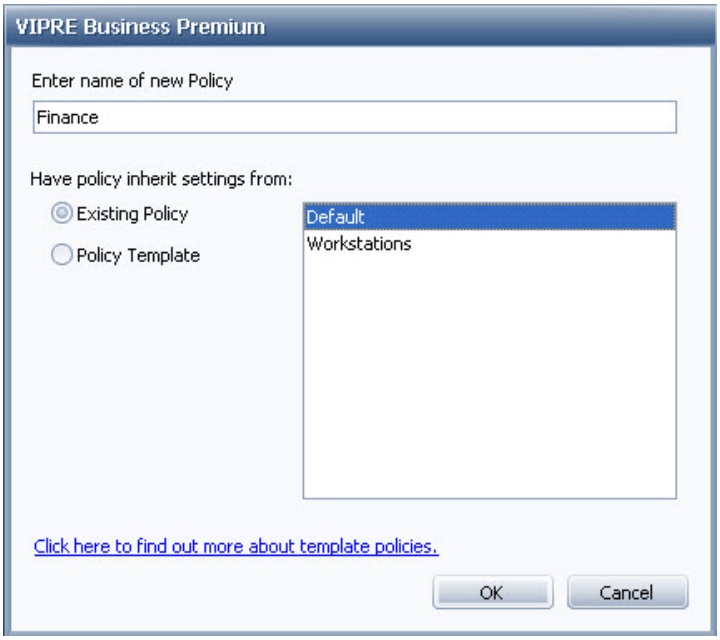
10.3 — Creating Policies

VIPRE Business allows you to add, copy, export, or import a Policy, as well as move Agents from one policy to another.

Note: All newly created policies are based on an existing policy, including either a Default policy, or a pre-existing policy. All policy settings are "copied" over EXCEPT for **Installation Management>Computers**.

To add a policy:

1. Click the **Add Policy** icon .
2. In the New Policy dialog box, enter an alphanumeric name for the new policy.
3. Choose a policy to inherit settings from:



   - **Existing Policy**: the listed options will be the "Default" policy and any policy that exists under the site you are creating a policy from.

4. Click **OK**. Your new policy is created with settings inherent from the selected policy in Step 3 above, and displays in the Site Navigator.

To copy a policy:

1. From the Site Navigator, right-click on a policy and select **Copy Policy**.
2. Enter an alphanumeric name for the new policy. The maximum length for a policy name is 255 characters.
3. Click **OK**. A policy based on the policy you selected is created and is displayed in the Site Navigator.

Now, you can edit/configure this policy and add agents to it for Agent Installation.

To export a policy:

1. From the Site Navigator, right-click on a policy and select **Export Policy**.
2. Choose a location and enter a filename for the xml-based policy file. The maximum length for a policy name is 255 characters.
3. Click **Save**. A copy of the policy you selected is saved to the chosen location.

Now, this policy can be imported from any console.

To import a policy:

1. From the Site Navigator, right-click on a site and select **Import Policy**.
2. **Locate** and **Open** the xml-based policy file from a saved location. The policy is imported to the site and displays in the Site Navigator.
3. You can right-click on the imported policy and rename it.

Now, you can further edit/configure this policy and add agents to it for Agent Installation.

To move Agents from one policy to another:

1. In the policy's Agent catalog, select the Agent(s).
2. Right-click and select **Reassign Agent to Policy**. The Reassigning Agent(s) dialog box displays.
3. Select the policy you want to move the Agents to and click **OK**. They are moved immediately to the new policy.

10.4 — Configure a Policy: Overview

When configuring a policy, some settings should be especially considered. The policy settings discussed below summarize the most frequently used settings, and highlight **Best Practices**.

> **Note**: For complete information on each screen, press F1 from that page.

10.4.1 — Agent screens

The **Agent** screens control the following:

- **User Interaction** refers to how the end user can interact and control specific functionality in the Agent.
- Configure **User Prompts** that end users experience and how **Rebooting** occurs.
- **Actions** apply to the settings for the agent machine's OS and Data Retention for its Quarantine and Scan History.

> **Note**: **Enable NT event logging** should NOT be enabled unless you are using a 3rd party program that will pull events from the log. It consumes resources (such as memory, CPU, and disk.) on the agent to do the logging. This feature is primarily for SDK customers and resellers.

- **Updates** are distributed to machines based on the Agent Updates settings for each Policy. Agent update settings help you manage the impact to network traffic and machine performance when Policies distribute updates to Agents.
- **Throttle updates from local server in milliseconds** to adjust throttling for lower bandwidth connections. A general guide:

  1 MBPS network: 1000 milliseconds.

  10 MBPS network: 200 milliseconds.

  100 MBPS network: 50 milliseconds.

  1 GBPS network: 20 milliseconds

- **Check for definitions updates periodicity in hours**: Best set between 1 and 3 hours. The default start time for updates is when the computer first boots up. For example, if the computer boots up at 7:43 a.m. and checks for updates every 3 hours, it will check at 10:43 a.m., 1:43 p.m., 4:43 p.m., and so forth.
- **Download via the Internet if local updates are unavailable** should only be enabled for laptops or mobile agents that will not be able to contact the update server. Using this internally will cause extra strain on the WAN.
- **Communication**:
  - **Intervals**: change agent heartbeat times to reduce load on the VIPRE Site Service and your network pipeline. Change **Agent status heartbeat in minutes** using the following formula: # agents (the total number of all agents assigned to all policies under a site) / 120 = Agent heartbeat time. Use a minimum of 5 minutes. Increase the minute value to 10 minutes if you are using more than 2500 agents for one site. For laptops or mobile agents, ensure that the **Heartbeat after failure in days** is at the default of 365.
  - If Agents require a **Proxy** to reach the Internet for obtaining definitions updates, set the proxy settings at the policy level, which will apply to all agent machines assigned to the policy.
  - The **Power** settings are used in separate policies to handle laptops in power saver mode. The default settings for laptops running an Agent require that the laptop be powered by AC power (not battery) in order for the Agent to properly receive updates. This feature is incorporated to ensure the agent software can complete the update cycle which could be interrupted due to an unexpected loss of power from a depleted laptop battery.
  - Use the **Laptop Power Save Mode** on a separate policy just for laptops. When initially installing an Agent to a laptop, **unselect** this option. **Select** this mode once the Agent is set up and configured properly on the laptop.

10.4.2 — Scanning screens

The **Scanning** screens allow you to set the following:

- **Settings**: configure basic Agent scan settings including: detections, on demand scanning, scanning USB devices, and scanning on start up.
- **Scan Start-Up—Randomize scheduled scan start times by in minutes**: this setting is best used in conjunction with setting your agents to check for threat definition updates before a scan starts (**Agent>Updates>Pre-scan**). Use of this setting will spread out the load of definition updates when agents require a threat definition update and should take the throttling interval (**Agent>All Updates>Throttle updates...**) into account. The larger you make this value, the less impact upon your network.

  For policies with several hundred agents or more that check for threat definition updates before starting a scan, the randomized start time should be anywhere from one-half to twice the time it

will take for the agent to download a threat definition update. This setting depends on how sensitive your network is to bursts of data.

- **Full, Quick & Custom Scan** screens: allow you to schedule automatic scans, set scan priority, select drive(s) for scanning, and to set options.
- **Agent scan intervals**: Best practices for scheduling scans are:
  - Schedule quick scans to run at least once daily.
  - Schedule a full scan to run each night during non business hours, when possible, and after nightly backups for least possible impact. If an after-hours scan is not possible, set the full scan to run at a low priority during working hours. Regardless, full scans should run daily.

10.4.3 — Active Protection

The **Active Protection** screens allow you to enable and configure the AP (real-time/on-access) settings for agents.

- **On Access**: controls how AP will respond to files when accessed. You can set it based on the needs of your security environment, whether it be more for performance or more for security.
- **User Control**: it is recommended to restrict user access to experienced users.

10.4.4 — Email Protection

The **Email Protection** screen allows you to enable email protection and control whether the end user can turn this feature off.

- **Agents on Email Servers**: Email scanning should be disabled for email server agents. Agents installed on email servers are designed to protect the server, not to provide active email scanning.
- **Email Client Ports**: If the agent computer uses an email client that requires specific port settings, then those port settings MUST be set the same here. The default of POP3 to 110 and SMTP to 25 is applicable to most configurations, especially over a network. This is sometimes changed for Agents installed on laptops or remote users.

10.4.5 — Remediation

The **Remediation** screen allows you to customize the remediation settings down to the sub-category of threat, offering great versatility in its configuration. Remediation applies to scanning, email protection, and Active Protection.

10.4.6 — Exceptions

The **Exceptions** screens allow you to list files that you know to be good or bad, so that those files will be automatically allowed (ignored) or blocked accordingly.

Add an Exclusion (always allowed/ignored) exception for the Exchange Store and Temp folders to prevent Active Protection from scanning them. This will alleviate resource demand on the Email Server.

10.4.7 — Allowed Threats

The **Allowed Threats** screen allows you to quickly search for and remove threats from the Allowed Threats list. The Definitions Database is comprehensive and may detect applications not considered as threats by all end users.

10.4.8 — Firewall

IMPORTANT: By default, the Firewall is **TURNED OFF**. Upon initial installation of VIPRE Business, you must configure the Firewall settings to your organization's needs.

The **Firewall** screens consist of the following:

- **Basic Firewall Protection**: includes all Exceptions settings (Application, Network, and Advanced rules), IDS, and Trusted Zones.
- **Web Filtering**: includes settings for Advertisement Web Sites, Allowed Web Sites, and Bad URL Blocking.
- **Advanced Firewall Protection**: contains process protection settings.
- **Assigned Firewall Templates**: allows you to assign firewall templates to the policy. Firewall templates are created at the site-level from the Site Properties.

10.4.9 — Agent Installation Management

The **Agent Installation Management** screens are configured during Agent installation. See manual or automatic agent installation for more information.

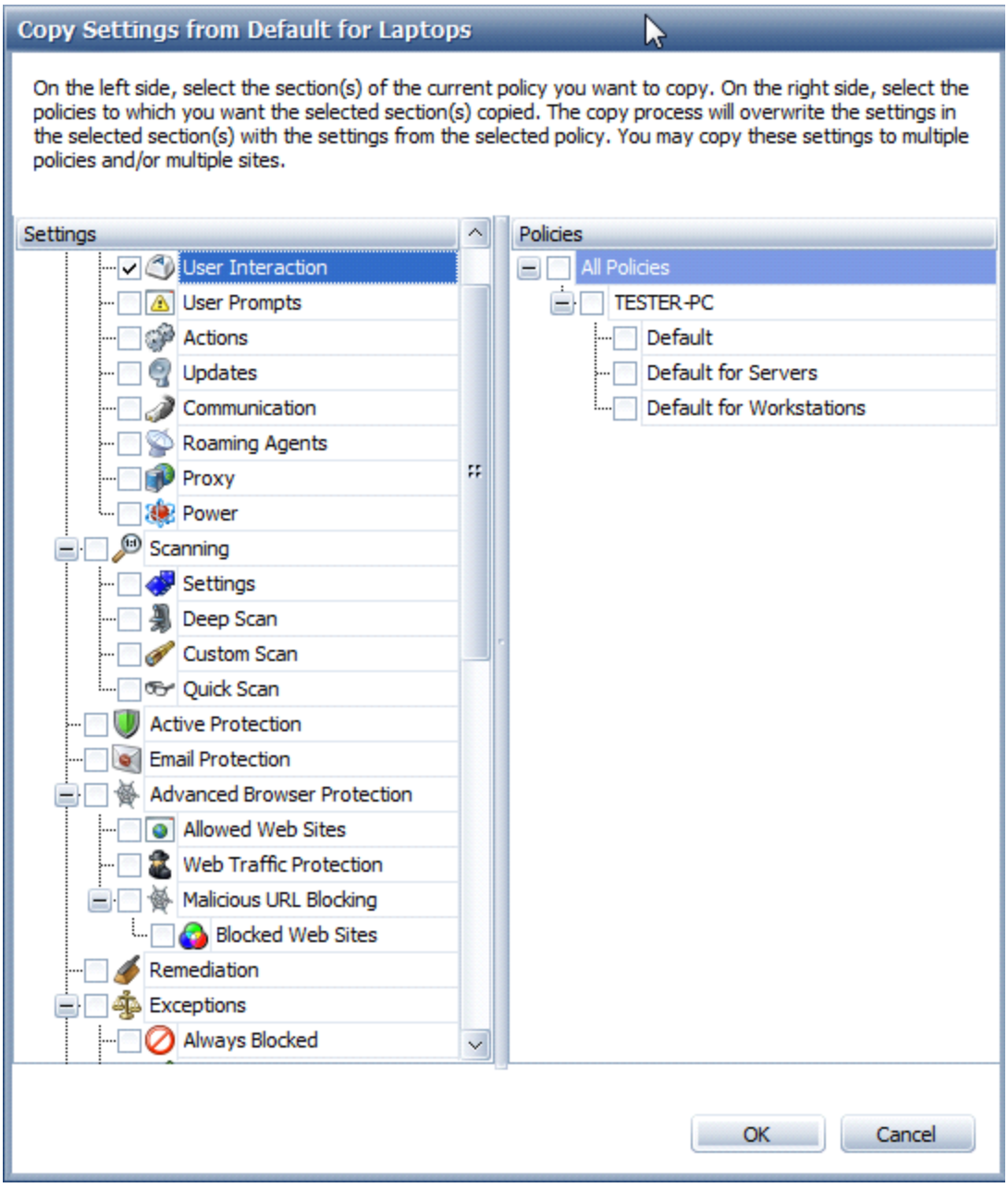
10.5 — Copy Settings from [Policy Name] Dialog Box

The **Copy Settings from [Policy Name]** dialog box is used to copy selected settings to one or more policies at a time. Once you click OK, the selected settings are immediately applied to the policy or policies that you select.

This dialog box is accessible from the **Copy to** button on the **Policy Editor**. When clicking **Copy to**, the related checkboxes will be selected based on the page that you launch this dialog from.

Note: All Policy settings, EXCEPT for the Deployment Scopes, can be copied from one policy to another.

Note: Copying settings from one policy to the other will overwrite the target policy. For example, copying exceptions list from policy "A" to "B" will overwrite "B".



The dialog box contains the following items:

Settings

The **Settings** area displays a tree structure of all policy settings. You can check or uncheck any listed item.

Policies

Select one or more policies from the **Policies** box. Once you click **OK**, the settings in the Policy sections are applied to the selected policies immediately.

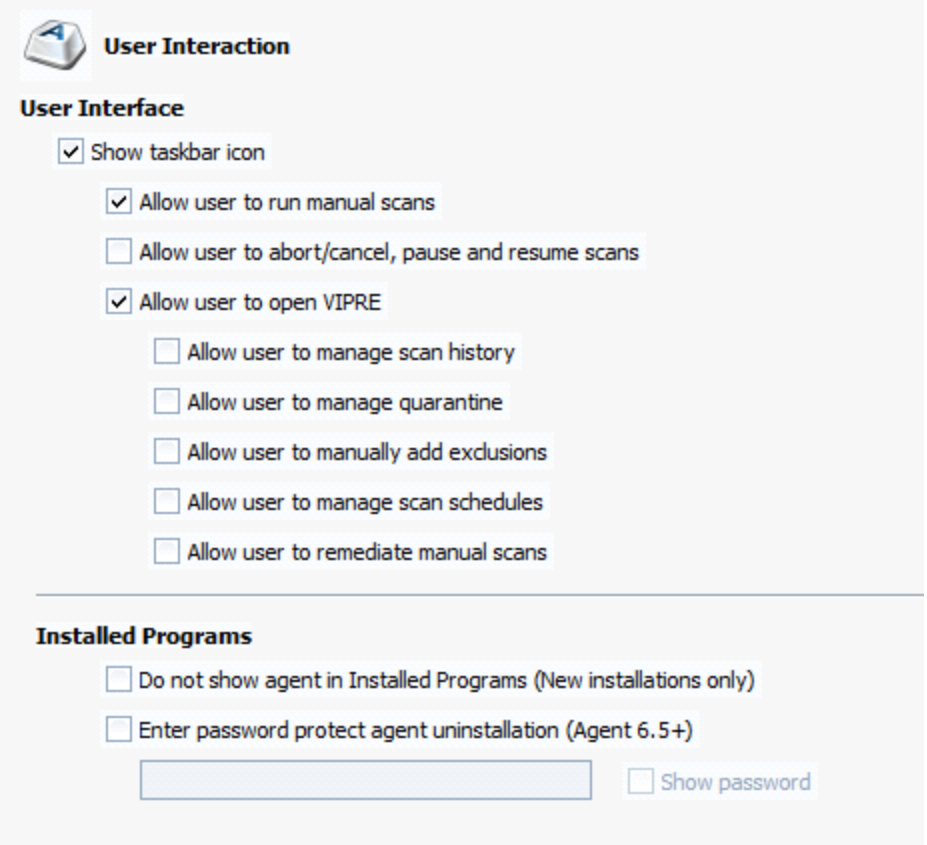
11 — Configuring Windows Policies

This section of the guide covers policies intended for use with Microsoft Windows, and is divided into the following sections:

11.1 — Configuring Agent Settings

11.1.1 — Configure User Control of Agent Interface

User Interaction refers to how the end user can interact and control specific functionality in the Agent.



To configure user control of Agent interface:

1. Open the **User Interaction** screen (**Policy Properties>Agent>User Interaction**).
2. Configure the **User Interface** settings:

   - **Show taskbar icon**: select to place a VIPRE Business icon in the system tray of end user machines. With this option enabled, users are able to open the agent UI as well as perform various tasks that can be enabled/disabled by policy settings, as listed below. With this option unselected, end users will have no access to the agent UI and will be dependant on the settings in the agent's assigned policy.
   - **Allow user to run manual scans**: select to enable end users to manually perform either a quick or a full scan whenever they want. Unselect for agent scans to be dependant on assigned policy.
   - **Allow user to abort/cancel, pause and resume scans**: select to enable end users to abort/cancel, pause, and resume running scans. Unselect to not allow users to have any user-interaction over a scan; as a

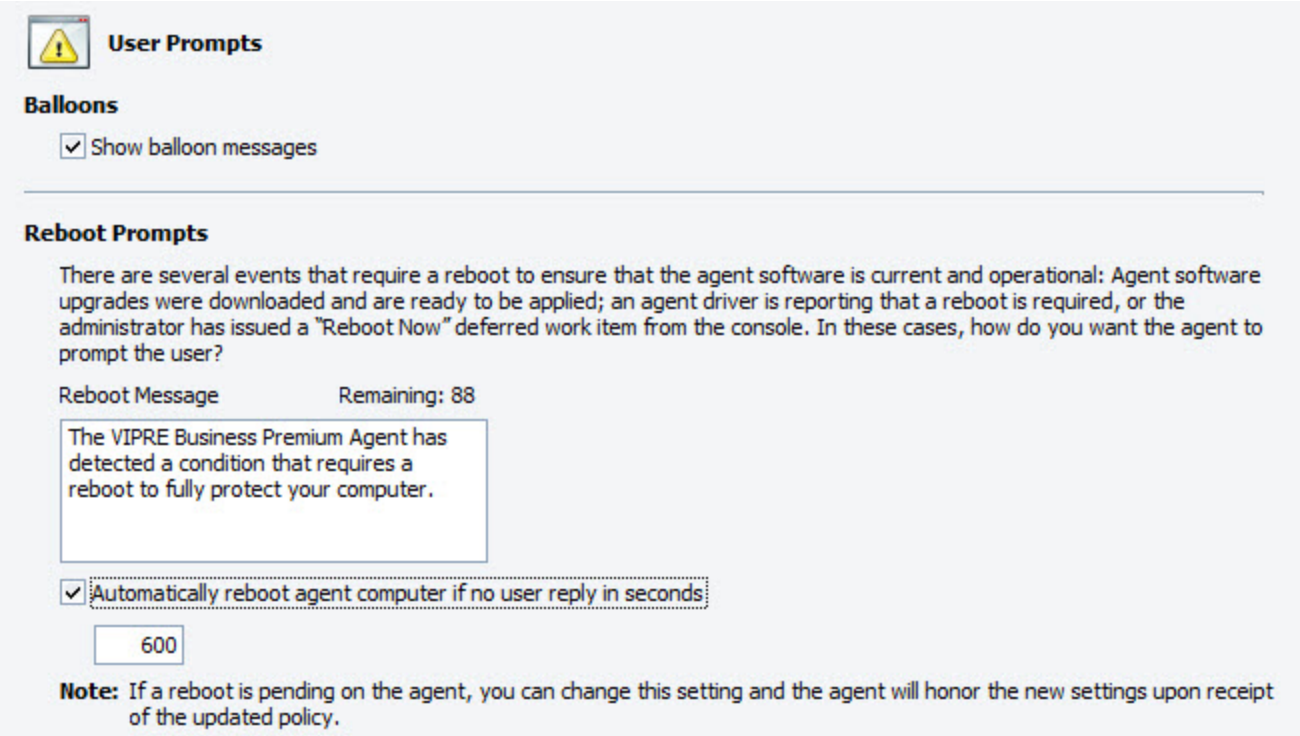
result, scans may only be stopped from the Admin Console (right-click on the agent and select **Scanning>Abort Scan**).

- **Allow user to manage scan history**: select to enable end users to delete scan, AP, and email histories, and clear system history. Unselect to not allow end users to delete/clear any history items made by the agent; instead, histories will be cleared based on the settings in the Agent Actions area listed below.
- **Allow user to manage quarantine**: select to enable end users to restore an item in quarantine and to delete an item from the computer. Unselect to not allow end users to manage any quarantine items on their computer.
- **Allow user to manually add exclusions**: select to allow end users to be able to add exclusions to scans that will always be allowed, as well as manage those items. Unselect for the agents to be dependant on Policy level exclusions.
- **Allow user to manage scan schedules**: select to allow end users to edit their scan schedule. When selected, admin control is locked out of editing this schedule. If the admin turns this on after a user has created their own schedules, then all of those new schedules that the user made will be cleared from the agent. After making this selection and applying the change, "USER MANAGED" will be displayed at the top of the Full Scan, Quick Scan, and Custom Scan screens, as shown below. In addition, the options will be grayed out.
- **Allow user to remediate manual scans**: select to allow end users to decide the action to take on the results of a scan. Unselect for the agents to be dependent on the Remediation settings.

3. Optionally, select **Do not show agent in Installed Programs** for the end user to be unable to uninstall or modify the program in any way. This MUST be done prior to installing the Agent on the workstation. Otherwise, you'll have to uninstall the agent, select and save this setting, and then reinstall the agent.
4. Click **Apply** to save changes.

11.1.2 — Configure User Prompts and Rebooting

Configure **User Prompts** that end users experience and how **Rebooting** occurs.

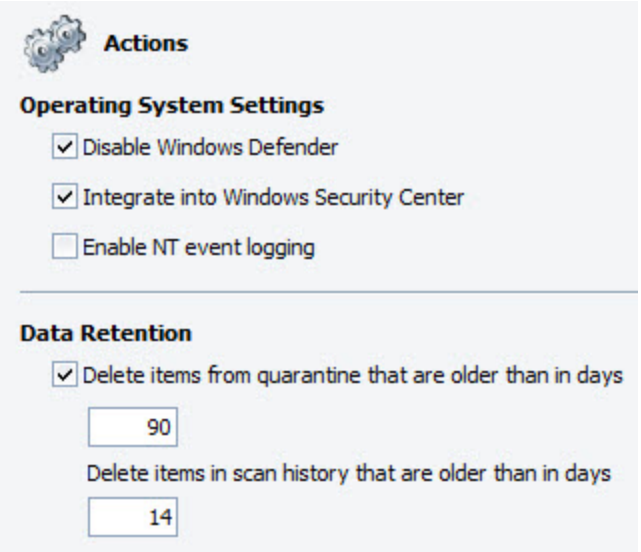


To configure user prompts and rebooting:

1. Open the User Prompts screen (**Policy Properties>Agent>User Prompts**).
2. Configure the following:
   - **Show balloon messages**: select to show the balloon popups for the agents under this policy. Unselect to hide the popups.
   - **Reboot Message**: use existing or modify the message that the user will see when the machine needs to reboot. The field is limited to 200 characters.
   - **Automatically reboot agent computer if no user reply in seconds**: when selected, the machine will reboot automatically after the number of seconds entered if the user.
3. Click **Apply** to save changes.

11.1.3 — Configure Agent Actions

Actions apply to the settings for the agent machine's OS and Data Retention for its Quarantine and Scan History.



To configure agent actions:

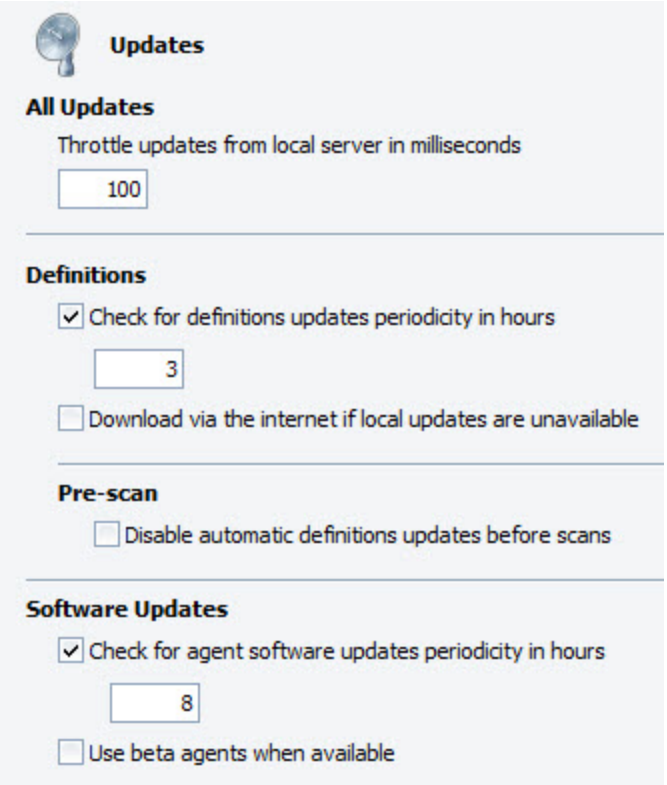
1. Open the Agent Actions screen (**Policy Properties>Agent>Actions**).
2. Configure the **Operating System Settings**:
   - **Disable Windows Defender**: if agent machines have Windows Defender installed, it's best to disable it to avoid conflicts.
   - **Integrate into Windows Security Center**: select to integrate into Windows Security Center.

> **Note: Enable NT event logging** should NOT be enabled unless you are using a 3rd party program that will pull events from the log. It consumes resources (such as memory, CPU, and disk.) on the agent to do the logging. This feature is primarily for SDK customers and resellers.

3. Configure the **Data Retention** settings:
   - **Delete items from quarantine that are older than in days**: select to enable the agent to delete items stored in quarantine after a specified number of days ranging from 1 to 365. The default setting is 90 days. These items are deleted from quarantine on the agent machine.
   - **Delete items in scan history that are older than in days**: enter an interval between 1 and 365 days. The default interval is 14 days.
4. Click **Apply** to save changes.

11.1.4 — Manage Agent Updates for Policies

Updates are distributed to machines based on the Agent Updates settings for each Policy. Agent update settings help you manage the impact to network traffic and machine performance when Policies distribute updates to Agents.



To manage distribution of updates per policy:

1. Open the **Agent>Updates** screen in the **Policy Properties** for each Policy.
2. Set **Throttle updates from local server in milliseconds** to cut down the load on the update server when distributing updates to the machines under the selected policy. The default value for throttling is 100 milliseconds but can be set as high as 60,000 milliseconds (or 1 minute) for networks with extreme bandwidth constraints. The average update chunk size is approximately 67 KB. A general guide:

   1 MBPS network: 1000 milliseconds.

   10 MBPS network: 200 milliseconds.

   100 MBPS network: 50 milliseconds.

   1 GBPS network: 20 milliseconds
3. Configure automatic Definition Updates for Agents under this policy:

   - Select **Check for definitions updates periodicity in hours** to turn on automatic definition updates and then enter a number in hours for the update interval. The default is to automatically check at 1 hour intervals. The interval values are 1-72 hours. Best set between 1 and 3 hours. The default start time for updates is when the computer first boots up. For example, if the computer boots up at 7:43 a.m. and checks for updates every 3 hours, it will check at 10:43 a.m., 1:43 p.m., 4:43 p.m., and so forth.
   - The "Disable automatic definitions updates before scans" setting:
   - **Unselect** (recommended) to ensure that the Agent automatically gets the latest definitions before running any type of scan.

- **Select** if Agent machines are older models and run slower, or if the interval for definitions updates is set frequently (1-3 hours).

Note: This setting should be done in conjunction with the Scan setting "Randomize scheduled scan start times in minutes."

4. To have Agents on laptops (or remote users) connect to ThreatTrack Security over the Internet if the agent fails to contact the VSS or the update server, select **Download via the Internet if local updates are unavailable**. If machines require a Proxy to access the Internet, ensure that you configure Policy proxy settings.

Important: If this is used for agents over your network, this could put a strain on the WAN.

5. Configure Software Updates for Agents under this policy:
   - (recommended) To turn on automatic software updates, select **Check for agent software updates periodicity in hours**, and then enter a number in hours for the update interval. The default setting is on and at 8 hour intervals. The interval values are 1-72 hours.
   - To turn off automatic software updates, unselect **Check for agent software updates periodicity in hours**.
   - To participate in Beta releases, select **Use beta agents when available**. This is best used under policies with a limited number of agents and non-production machines.

Important: **Use this option with care**. If you need to rollback to a previous version, a manual uninstall and reinstall of each agent may be required.

6. Click **OK** to accept your changes. All changes are applied to the Agents assigned to the Policy the next time the Agent communicates to the Site.

11.1.5 — Manage Agent Communication

The Communication screen enables you to control how agents communicate with the VIPRE Site Service (VSS). The default settings are suitable for environments that consist of 100 to 400 agents, including agents running on laptops. Larger environments of around 500+ agents may require adjustments to these defaults.

Note: Modify agent communication intervals only if it becomes necessary.

To manage agent communication intervals with the VSS:

1. From **Site Navigator**, double-click the Windows policy you want to configure.
2. From the left pane of the Policy Properties screen, expand **Agent** and click **Communication**.
3. Configure the following communication **Intervals**:
   - **Agent status heartbeat in minutes** determines how often the agent calls into the VSS, primarily to verify that the agent is working. Particular information passed through the communication includes agent, threat database and Operating System versions, IP address, and agent status.
     The default is 5 minutes and works well for 100 agents or less. Larger organizations can put a greater load on the VSS and may require 15-60 minutes or even more. The heartbeat is adjustable between 1 and 10,080 minutes (1 week).

- **Heartbeat after failure in days**: if the heartbeat fails, the agent will continue attempting communication with the VSS for this number of days. After the number of days, communication attempts will cease, **resulting in the agent not completing any of its scheduled scans, and disabling Active Protection**. If the agent is able to communicate with the server at any time prior to the set period, the Agent will reset its counter. If the agent has gone dormant, every time it's restarted, as during a reboot, it will try to communicate with the server once. If that heartbeat then fails again, the agent will go dormant again. If communication is successful, the agent will reset its counter and continue its scheduled communications.
  The default setting is 365 days. The setting is adjustable from 1 to 365 days.
- **Mark agents inactive after no contact in minutes**: set the length of time an agent is quiet prior to being marked inactive by the VIPRE Site Service.
  The default value is 30 minutes. The length of time can be set between 0 and 10080 minutes. *The recommended length of time is three times the longest heartbeat interval*.
- **Retry authentication in days** only applies if the **Agent Recovery Mode** in the Advanced Site Settings is turned off.
  If an agent can successfully say Hello but fails authentication, the agent will be told to reinitialize itself. The agent will retry to authenticate for the specified period, after which it will go dormant. Every time the agent is restarted, it will try one heartbeat before going dormant again. The default setting is 7 days. This setting is adjustable from 1-7 days.
- **Remove agents that have not communicated with the server in days**: remove agent data from the Management Console if there is no communication between the agent and VIPRE Site Service (VSS) for a specified number of days. The agent remains installed on the host computer and can be reused if the computer is protected again.

4. Configure the following **Server** settings:
   a. In the **Policy Server** field, key in the machine **Name** or **IP address** of the VIPRE server that distributes policy updates to the agents managed by this policy.
   b. In the **Port** field, key in the TCP port that the VIPRE Site Service uses to receive agent requests and security information.
5. Configure **Site Server Settings for Agent Interaction**:

Important: This following option (procedure step a) must not be used unless instructed by a technical support representative.

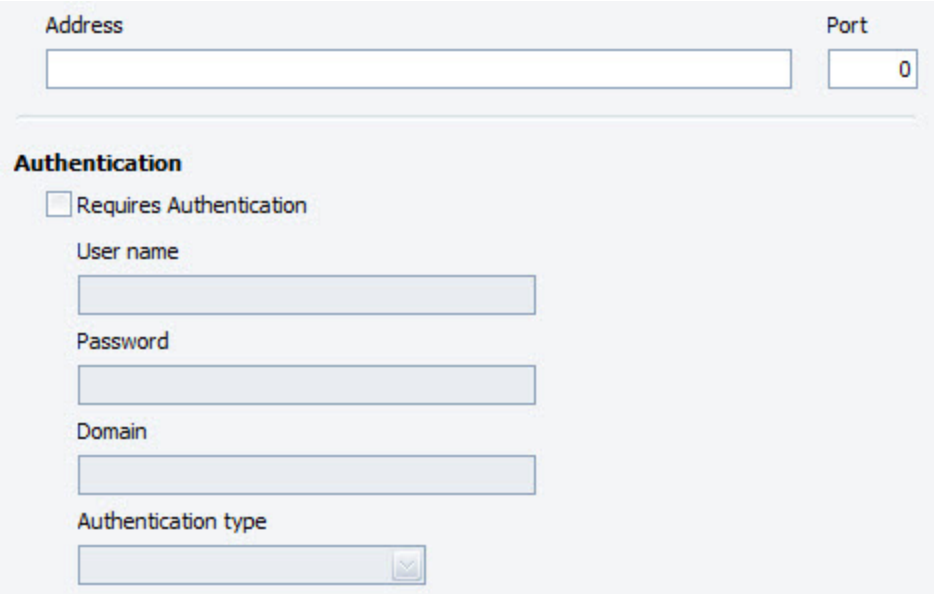
- **Archive agent event files**: (This setting is for **DEBUGGING WITH TECH SUPPORT ONLY**) scanning and Active Protection reports coming from an agent are stored in the "Incoming XML" folder. The information is then stripped out of the XML and stored in a database, and the XML file deleted. Selecting this option moves the XML file into the "ProcessedXML" folder where the file is stored until deleted manually. Storing this file is useful only for debugging and is best when working with Technical Support.
- **Notify agents of pending work**: when you make a change to a policy, the VSS stores the information in a deferred work queue. Agents get that information during their next scheduled communication. Selecting this option causes the VIPRE Site Service to contact the agent and tell them to do a heartbeat and get the information prior to the scheduled time.

6. Click **Apply** and **OK**.

11.1.6 — Configure Proxy Settings for Agents

If Agents require a **Proxy** to reach the Internet for obtaining definitions updates, set the proxy settings at the policy level, which will apply to all agent machines assigned to the policy.

Note: Ensure that the proxy settings are enabled.

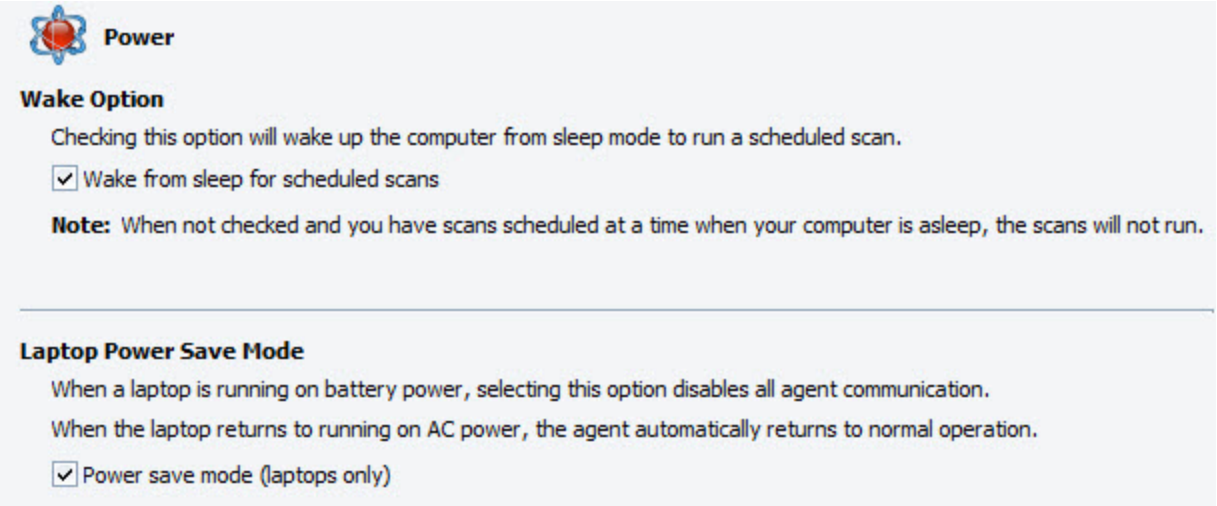


To configure proxy settings for Agents at the Policy level:

1. Open the Policy's Proxy Settings screen (**Policy Properties>Agent>Proxy Settings**).
2. Select **Use a proxy server when communicating with ThreatTrack Security** to enable the Policy's proxy settings.
3. In the **Address** box, enter the Fully Qualified Domain Name (FQDN) of the proxy server. The Proxy's IP Address is not recommended.
4. Enter the **Port**, which is typically port 8080.
5. If you are using authentication for the proxy, select the **Requires authentication** checkbox and specify a User name, Password, and Domain, as applicable.
6. Set the **Authentication type** for your proxy by selecting one of the following: NTLM, BASIC, or DIGEST. The common type is NTLM and is used by ISA servers.
7. Click **Apply** to save changes.

11.1.7 — Configure Agent Power Save Settings

The **Power** settings are used in separate policies to handle laptops in power saver mode. The default settings for laptops running an Agent require that the laptop be powered by AC power (not battery) in order for the Agent to properly receive updates. This feature is incorporated to ensure the agent software can complete the update cycle which could be interrupted due to an unexpected loss of power from a depleted laptop battery.



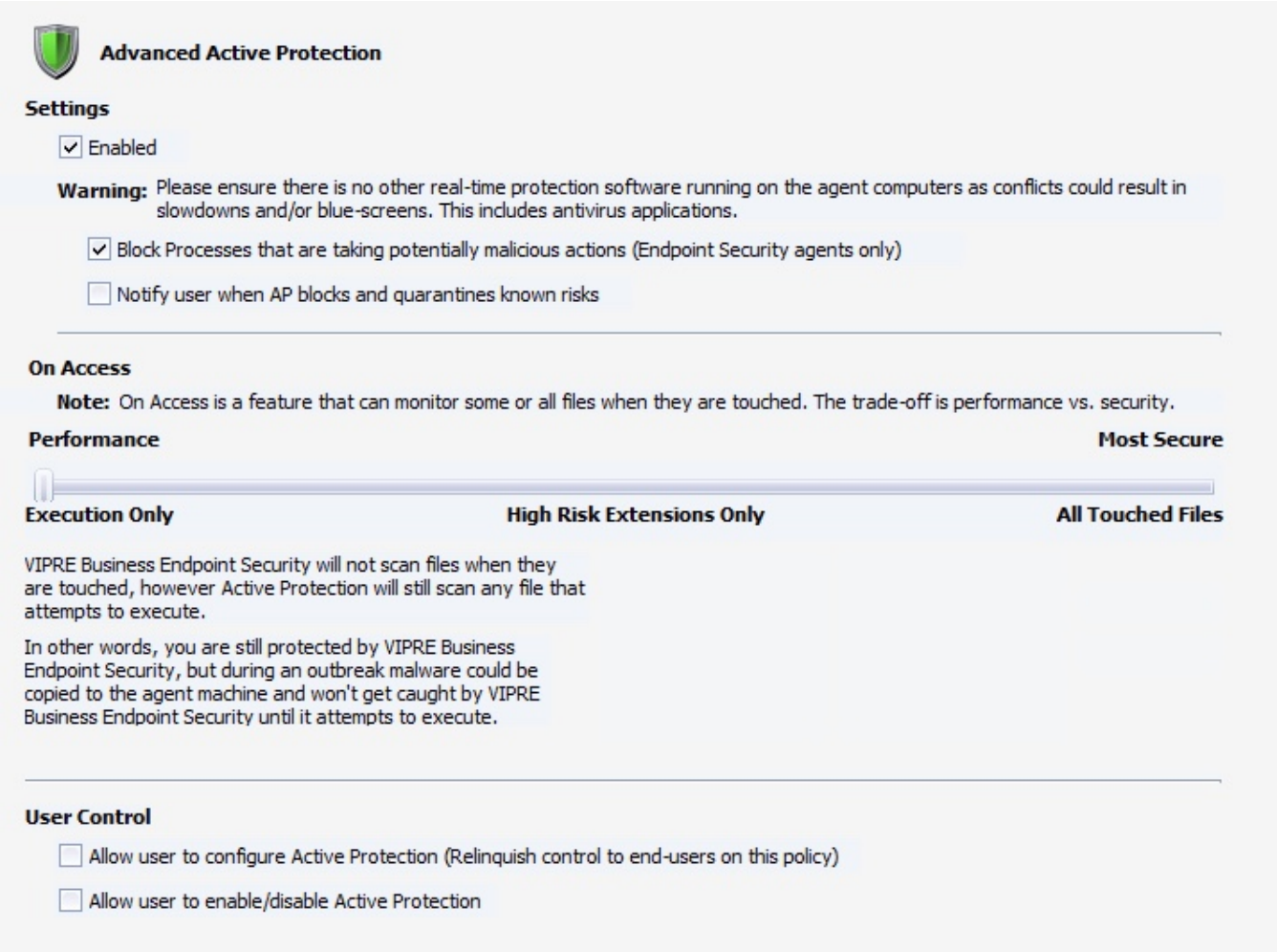
To configure power save settings:

1. In the **Policy Properties**, open **Agent>Communication**.
2. Modify any of the following default settings accordingly:
   - **Wake from sleep for scheduled scans**: selecting this option will wake up the computer from sleep or hibernate modes to run a scheduled scan. Unselecting this option tells the agent to ignore any scheduled scan while in sleep or hibernate modes. When an agent's computer is using Windows sleep mode and this option is unselected, the computer is at risk of missing important system scans, especially during periods of inactivity. To ensure that the computer is protected, run manual scans or schedule a scan at a likely time that it is not asleep.
   - **Power save mode (laptops only)**: when a laptop is running on BATTERY POWER, selecting this option disables the agent from running scheduled scans or checking for updates. However, Active Protection will continue to operate and scans and updates can be run manually. When the laptop returns to running on AC power, the agent automatically returns to normal operation. Unselecting this option will allow an agent to continue checking for updates and running scheduled scans on battery power.
3. Click **Apply** to save changes.

11.2 — Configure Active Protection Settings

Configure the **Active Protection (AP)** settings for on access protection for all Agents installed under the policy.

Important: Active Protection must NOT be enabled with any other on-access scanner. A noticeable decrease in system performance and/or blue-screens could result.



To configure Active Protection settings:

1. In the **Policy Properties**, open **Active Protection**.
2. Select **Enabled** to turn on AP for agents under this policy.
3. Optionally, select **Block Processes that are taking potentially malicious actions** *(VIPRE Endpoint Security only)*. This actively monitors processes to check for potentially malicious behavior. If a malicious process is found, the process is stopped and blocked from starting again. Any malicious files the process may have created are removed.
4. Optionally, select **Notify user when AP blocks and quarantines known risks** to let end users know that something has been quarantined on their computer.
5. Configure **On Access** to control how AP will respond to files when accessed. You can set it based on the needs of security for your environment, whether it be more for performance or more for security:
    - **Execution Only** (Performance): select for AP to scan any file that attempts to execute. This setting is optimal during **normal conditions**.
    - **High Risk Extensions Only**: select for AsP to only scan files with extensions that ThreatTrack Security and you (Admin Known) consider "high risk." So, when a file with one of the listed

extensions is touched, it will be scanned. In addition, any file that attempts to execute will be scanned.

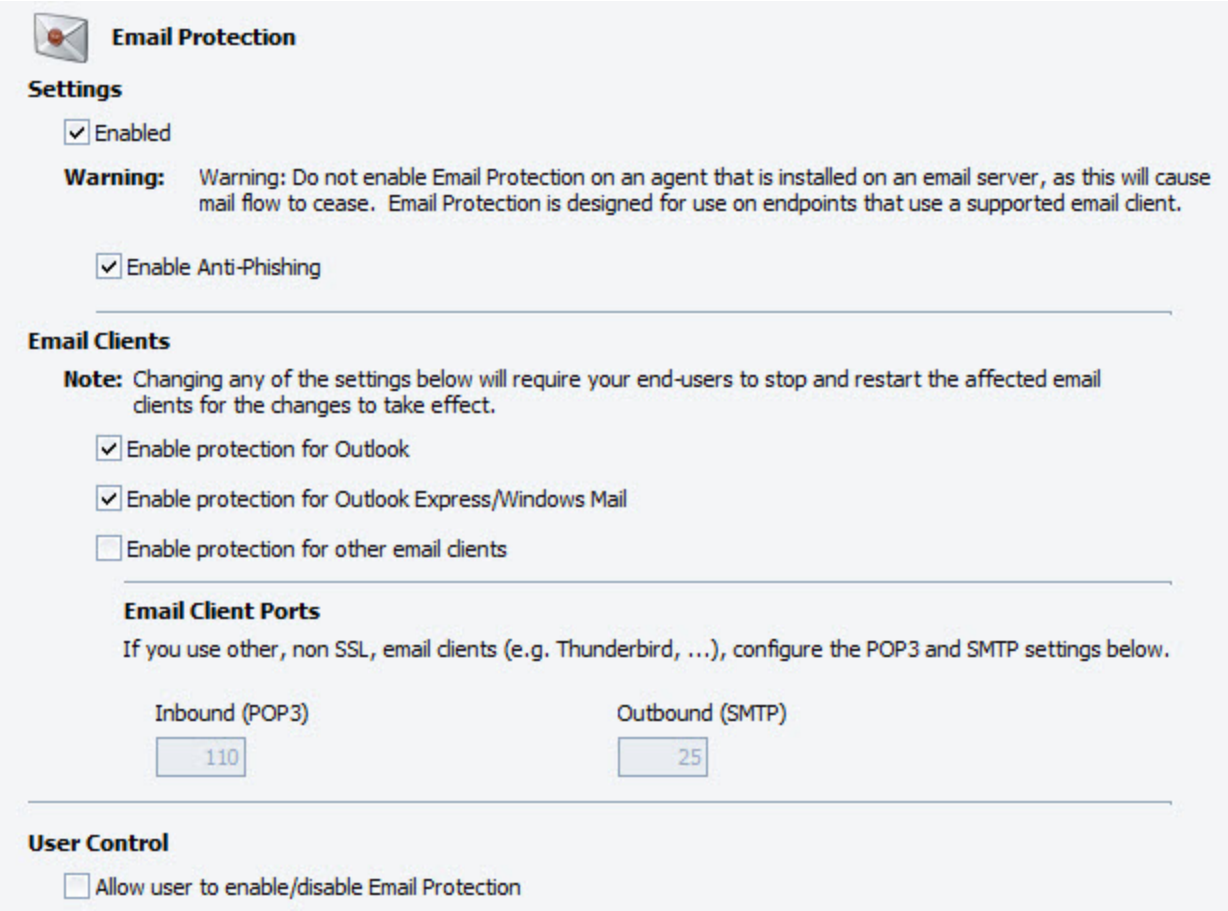
- **VIPRE Known**: lists the file extensions (such as EXE, INI, HLP, and BAT) that have proven to be "high risk." You can unselect any of these extensions that you may want AP to NOT check on access.
- **Admin Known**: lists Admin-defined extensions that will be checked on access. You can add to and remove from this list, and then select the extension that you want to be checked on access.
- **Add**: click to add a new extension to the Admin Known list. Select to enable the new extension.
- **Remove**: highlight (without checking the box) an extension from the Admin Known list and click **Remove**. The extension will be removed immediately from the list without confirmation.
- **All Touched Files** (Security): is for a higher state of protection and should only be enabled in the event that a malware outbreak is suspected or has occurred. When enabled, ALL files are scanned when they are copied or touched.

> Warning: When using "All Touched Files," you MUST watch it frequently and with great care. This setting can result in slower system performance, depending on computer specifications, as well as the number and type of programs running.

6. Configure **User Control**:
   - **Allow user to configure Active Protection**: select to turn over complete control of AP to end users. Unselect for the agents to be dependent on what is set for AP in this console.
   - **Allow user to enable/disable Active Protection**: select to allow users to activate/deactivate AP from their agent.
7. Click **Apply** to save changes.

11.3 — Configure Email Protection Settings

The following email clients are supported: Outlook 2000+, Outlook Express 5.0+, Windows Mail, and SMTP and POP3. Infected email attachment are removed and replaced by a .TXT file indicating that it was infected and thus quarantined.



To configure Email Protection settings:

1. In the **Policy Properties**, open **Email Protection**.
2. Enable **Email Protection Settings**:
   - **Enabled**: select to turn on Email Protection for this policy, which will scan all inbound and outbound email messages, including attachments.
   - **Enable Anti-Phishing**: select to enable anti-phishing. When enabled and when a phishing email is received, the known bad URL link is stripped from the email, protecting the end user from the phishing scam. *(This function applies to VIPRE Premium and VIPRE Endpoint Security).*
3. Enable one or more **Email Clients** (SSL is not supported):

> **Note**: If enabling/disabling an email client with an email client running on an Agent machine, the email client will need to be restarted before the changes can take effect.

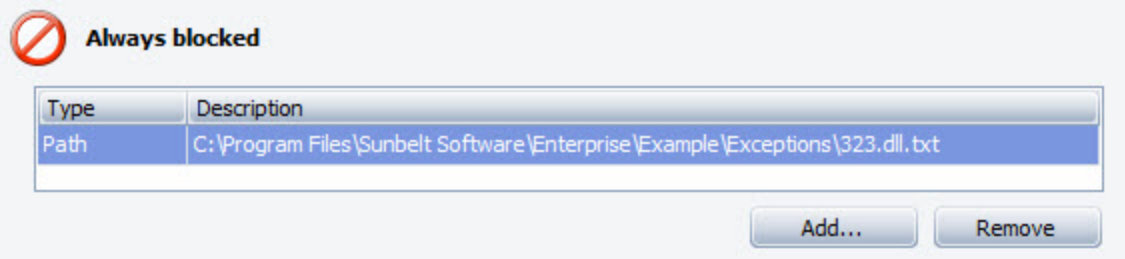
   - **Enable protection for Outlook**
   - **Enable protection for Outlook Express/Windows Mail**
   - **Enable protection for other email clients**
   - If **Email Client Ports** are different than the defaults of 110/25, configure accordingly.

4. Configure **User Control**:
   - **Allow user to enable/disable Email Protection**: when selected, the UI controls for email protection are accessible to the agents under this policy. When unselected, enabling/disabling the email protection is inaccessible to the agents.
5. Click **Apply** to save changes.

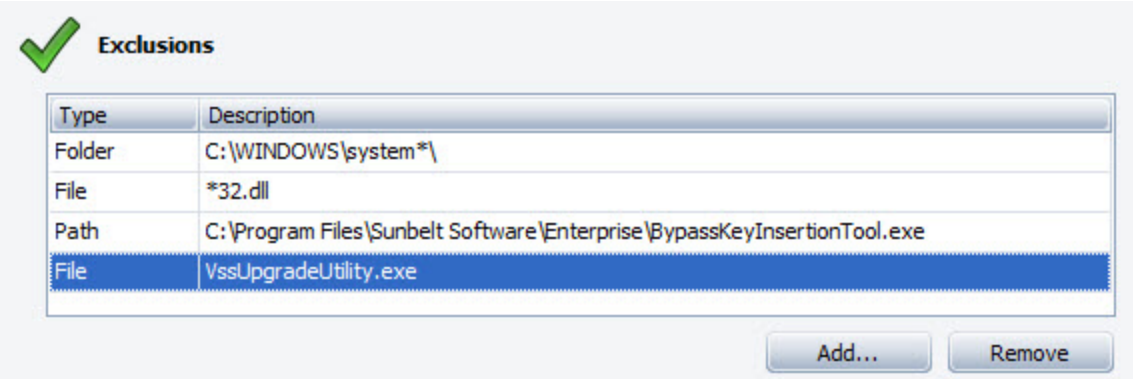
11.4 — Configure Policy Exceptions

The **Exceptions** screens are used to assign files, files with path, and/or folders that you, as the administrator, want allowed or blocked for all Agents assigned to a policy. This applies to all of the methods that VIPRE Business uses to detect threats, including Active Protection, Email Protection, and Scans.

Add **Always Blocked** items to be treated as a known threat. For example, if you were to add ABCX as a bad application, then if ABCX is executed on a machine under this policy, ABCX will be automatically blocked from running.

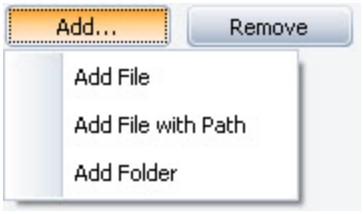


Add **Exclusions** that will always be allowed to run, over-riding the threat definitions.



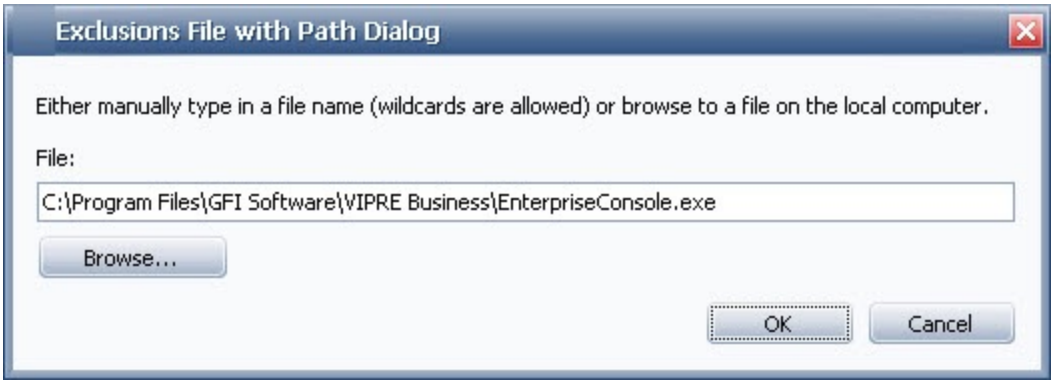
To add an item:

1. In the **Policy Properties**, open the **Exceptions>Always Blocked** or **Exclusions** screen, as applicable.
2. Click **Add** and choose from the following options:



- **Add File**: select a file for VIPRE Business to block/ignore all files named “example.exe” regardless of where the file is located (such as email attachment, network, user's machine, portable drive, and so forth).
- **Add File with Path**: select a file with the path for VIPRE Business to block/ignore all files named “example.exe” with that exact path. If the file is ever moved or another file with this name is somewhere else, VIPRE Business will once again interrogate that file as potential malware.
- **Add Folder**: select a folder for VIPRE Business to block/ignore all contents in it. If a particular folder is ever moved or another folder with this name is somewhere else, VIPRE Business will once again interrogate programs in that folder as potential malware.

3. Enter the name of the File, Path, of Folder.



Note: Wildcards (* and ?) are supported for Exclusions only. For more information, See Using Wildcards in Exclusions.

-or-
Click **Browse** and locate the File, Path, or Folder to add.

4. Click **OK**.
5. Click **Apply** to save changes.

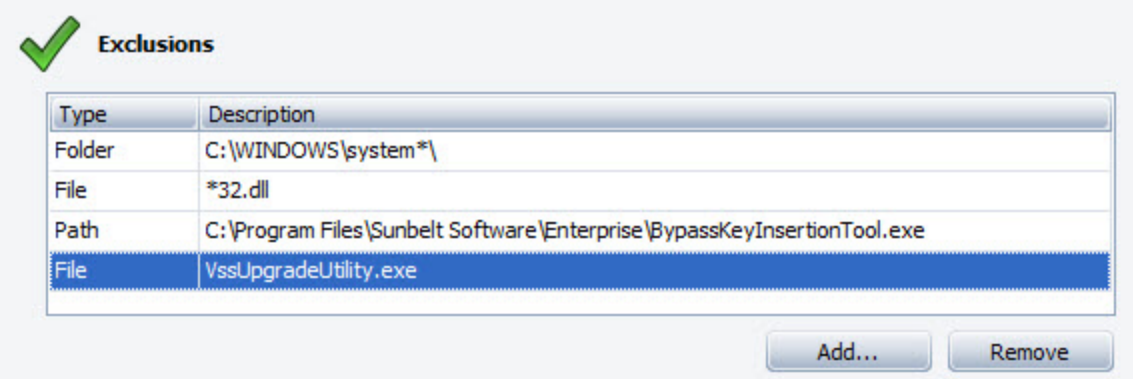
To remove an item

1. Select a row and click **Remove**.
2. Click **Apply** to save changes.

11.4.1 — Using Wildcards in Exclusions

VIPRE Business supports wildcards for Exclusions (always allowed items) only. This does NOT include environment variables. Supported wildcards are:

- '?' - matches exactly ONE character, EXCEPT the directory separator.
- '*' - matches ZERO or MORE characters, EXCEPT the directory separator.



Supported entity types:

Full Path

Fully specified path to a file, wildcards NOT permitted.
Example: "C:\WINDOWS\system32\kernel32.dll"

Full Path Pattern

Fully specified path to a file, wildcards permitted.
Example: "C:\WINDOWS\system32*32.dll"

File Name

Just the name of a file, wildcards NOT permitted.
Example: "kernel32.dll"

File Name Pattern

Just the name of a file, wildcards permitted.
Example: "*32.dll"

Folder

Fully specified path to a folder, wildcards NOT permitted (must be terminated with directory separator).
Example: "C:\WINDOWS\system32\"

> **Note**: Folder patterns are implemented as Full Path Patterns terminated with a directory separator.

Example: "C:\WINDOWS\system*\"

> **Note**: Folder entities are recursive and thus will match the folder itself and any descendant files and folders.

Examples:"C:\WINDOWS\" matches "C:\WINDOWS\", "C:\WINDOWS\SYSTEM32\", "C:\WINDOWS\notepad.exe", "C:\WINDOWS\SYSTEM32\regedit.exe", and so forth

Multiple Path Levels

Wildcards should behave exactly as they do in a Windows Command Prompt, with the added feature of supporting wildcards at multiple path levels including the drive.

Examples:

"*.dll" - matches "kernel32.dll", "advapi32.dll", etc

"C:\WINDOWS\system32*.dll" - matches "C:\WINDOWS\system32\kernel32.dll",

"C:\WINDOWS\system32\advapi32.dll", etc

"?:\WIN*\system**.dll" - matches "C:\WINDOWS\system32\kernel32.dll", "D:\WINNT\system\advapi32.dll", etc

Note: User Known Entities are NOT case-sensitive.

11.5 — Adding Allowed Threats

VIPRE may detect items that you may consider non-threatening in your network, for which you would want to allow to run.

For example, Virtual Network Computing (VNC) and Remote Administrator (Radmin) may both be considered acceptable for use in your organization, but may be considered threats in another organization.

To add an allowed threat:

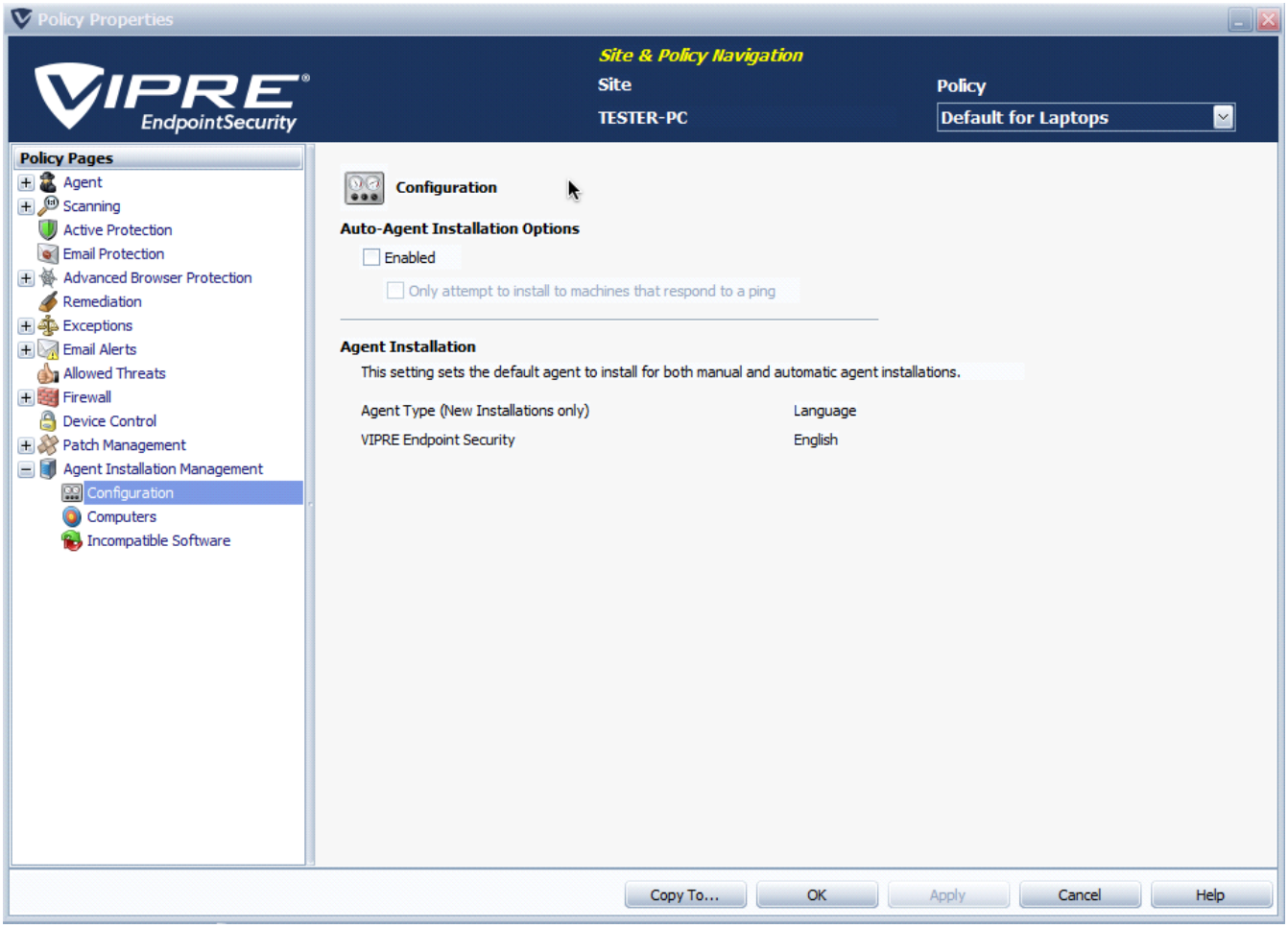
1. Navigate to a **Site>Quarantine tab** or **Policy>Quarantine tab**.

Or:

1. Navigate to **Protected Computers>Agent Details>Scan History tab**.
2. Right-click on a threat, and select **Allow Threat**. The Allow Threat window displays.
3. Select the policies on which this threat should be allowed.
4. Click **OK**.
5. The allowed threat now displays in the Allowed Threats list for the policies you selected (**Policy Properties>Allowed Threats**).

11.6 — Policy: Agent Installation Management - Configuration

The **Configuration** screen allows you to configure Site Service settings for agent interaction and enable/disable Automatic Agent Installations for the policy.



Auto-Agent Installation Options:

- **Enabled**: select to enable Automatic Agent Installation at the policy level. The checkboxes below "Enabled" are grayed out until "Enabled" is selected.

Important: You MUST enable scheduled Agent installation at both the policy and site level for a scheduled Agent installation to occur. To enable scheduled Agent installation at the site level, go to: **Site Properties>**Automatic Agent Installation Settings.

- **Only attempt to install to machines that respond to a ping**: when selected, the VSS tries to ping each machine first, then only installs to those that respond, reducing Agent Installation time considerably.

Note: If you are blocking ICMP (Internet Control Message Protocol) traffic between VIPRE Business and the workstations, do NOT select this option. This will result in the pings failing and creating a large ping timeout value, thus increasing the deployment time considerably.

Agent Installation:

Important: In order for these Agent Installation options to appear, you must first select them at the site level (Agent Software screen) and give them a chance to be downloaded. Once downloaded, the ability to select them will then be available.

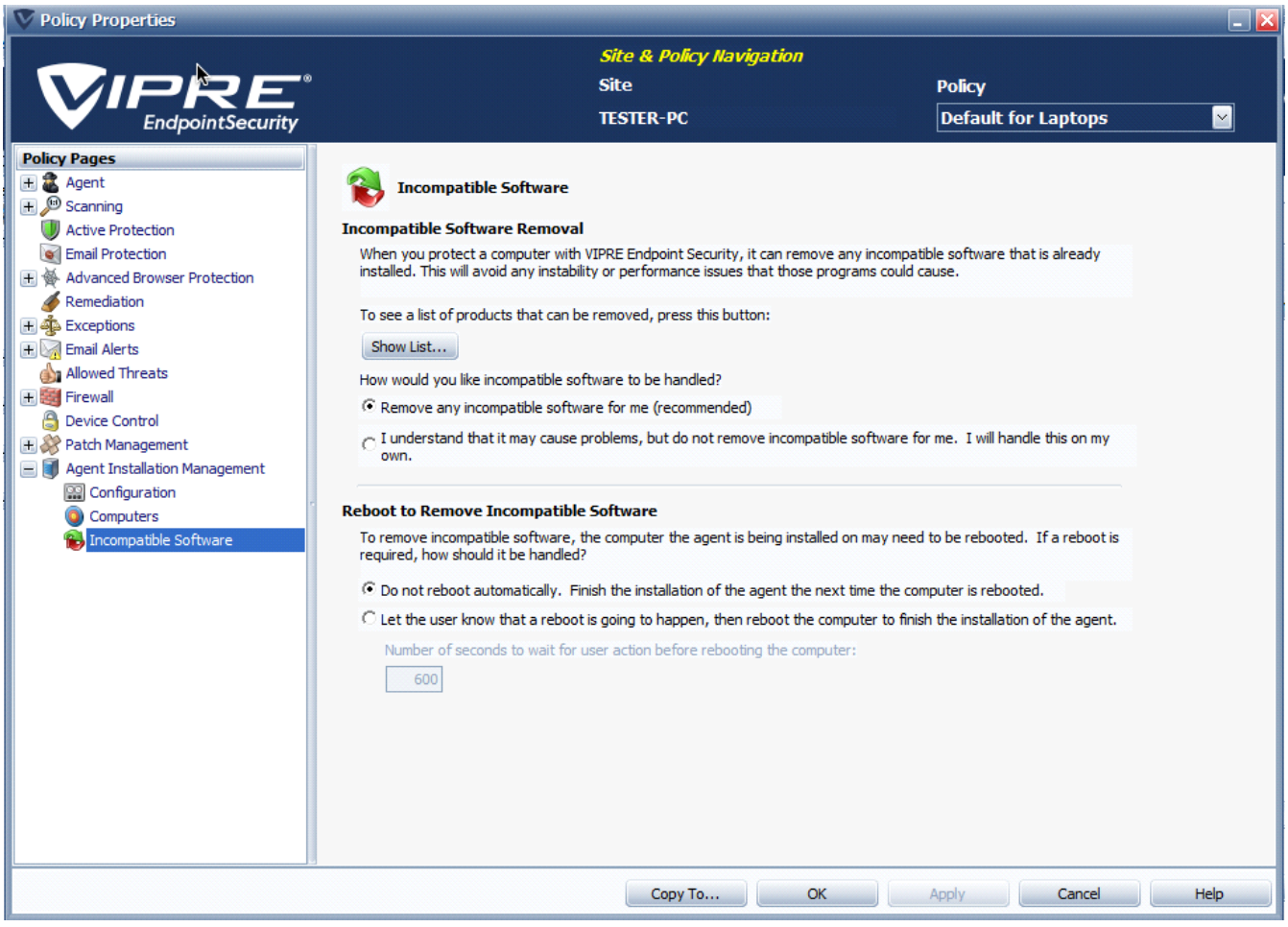
- **Agent Type**: choose an agent from the drop-down box to be used for the selected policy.

Important: If agents are already installed on machines under this policy, you MUST uninstall them first. Then, select a different agent and reinstall them for this policy.

11.7 — Configure Incompatible Software Removal

When an agent is deployed on a computer, it automatically scans the system for incompatible software. Incompatible Software are applications that may interfere with VIPRE's performance if they are running at the same time and on the same machine as a VIPRE agent.

Incompatible Software settings enable you to specify the actions that are performed by VIPRE, when an incompatible application is detected.



To configure the incompatible software removal settings:

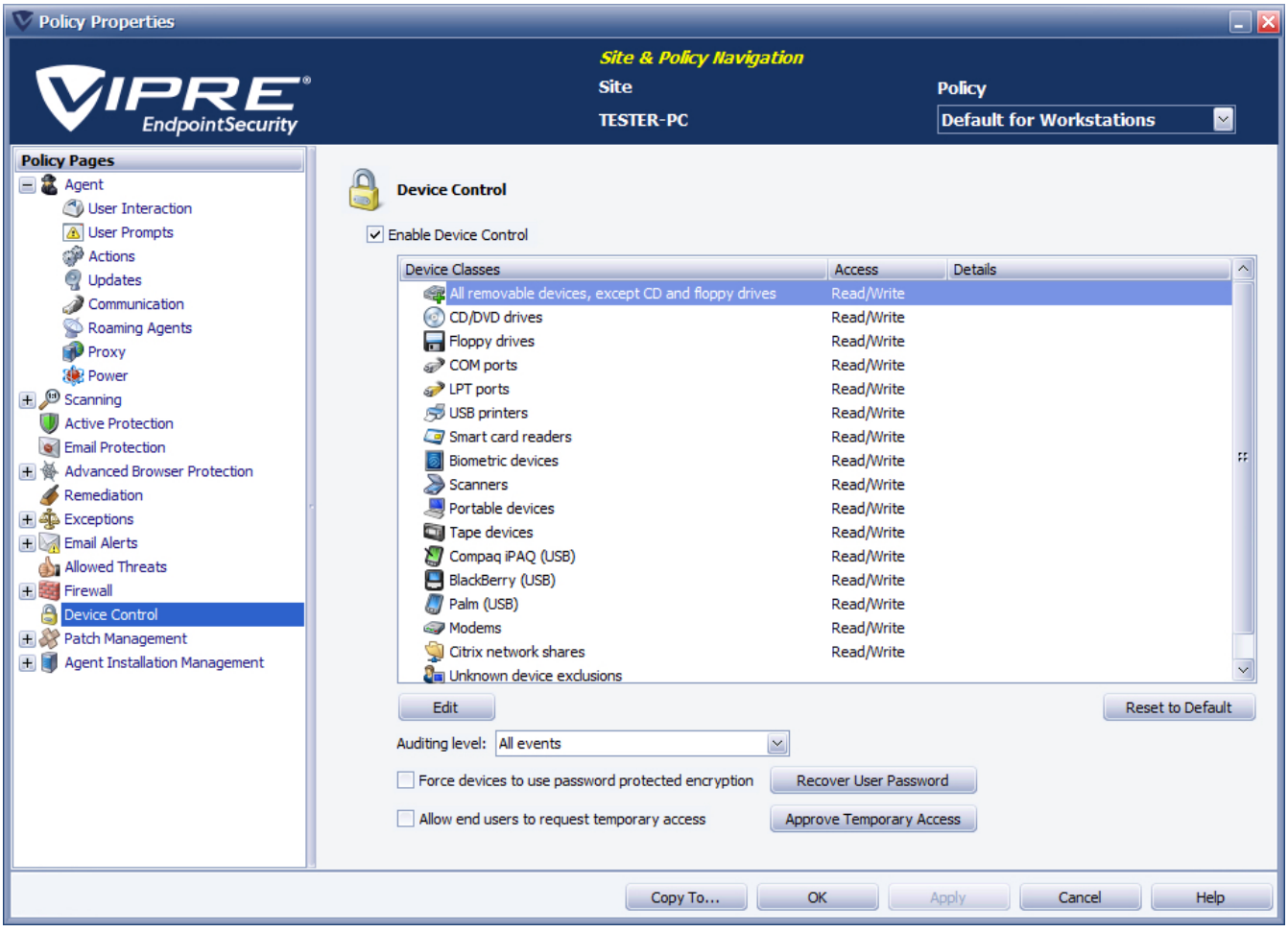
1. From **Site Navigator**, double-click the Windows policy you want to configure.
2. From the left pane of the Policy Properties screen, expand **Agent Installation Management** and click **Incompatible Software**.
3. Click Show List... for a full list of incompatible software.
4. Open **Policy Properties > Installation Management > Incompatible Software**.
5. Enable/disable the removal of incompatible software.
6. Enable/disable auto-reboot of agent machine after removal of the software.
7. Click **Apply** to accept changes.

11.8 — Configure Device Control

This topic applies to VIPRE Endpoint Security only.

(Windows policies only)

Device Control allows for administration of external devices interacting with remote agents. This option is useful for limiting how users may transmit sensitive information to third-party devices, as well as protecting the agent from potential third-party threats.



Screenshot 4: The Device Control screen.

Device Control allows you to manage the following features:

- Force devices to use password protected encryption
- Recover a User Password
- Allow end users to request temporary access
- Approving Temporary Access
- Port Blocking

Note: The *Enable Device Control* check box acts as the "master switch" to enable/disable Device Control for the current policy. Unchecking Enable Device Control turns off all Device Control options for the current policy (though you may still recover user passwords as needed).

11.8.1 — Force devices to use password protected encryption

This topic applies to VIPRE Endpoint Security only.

When a device is connected to the agent, the user is informed that mandatory encryption is required in order to use that device.

If the user agrees to the encryption, the device is encrypted using AES 256 (FIPS 140-2 certified).

Note: Depending on the size of the device, the encryption process may take a significant amount of time to finish.

When an encrypted device is inserted into a machine, the user will be prompted to enter a password in order to access the device. At this point, the user may click the **Recover Password** button to initiate the Recover a User Password process.

11.8.1.1 — Recover a User Password

This topic applies to VIPRE Endpoint Security only.

When an encrypted device is inserted into a machine, the user will be prompted to enter a password in order to access the device. If they do not know their password, they may click the **Recover Password** button to initiate the recovery process.

Note: If the user fails to enter the correct password within 5 attempts, they will be locked out of accessing the device, and presented with instructions to contact their Administrator. Clicking on the device in Windows Explorer at this point will result in an "Access denied" message.

To unlock the device, the user should remove and then reinsert the device. This will also initiate the Recover Password process.

To recover a password for an encrypted device:

1. When a user clicks the **Recover Password** button, they will be presented with an **Encrypted Medium ID** and **Security Code**, which they should send to you.

2. Key in (or copy and paste) the Encrypted Medium ID and Security Code from the user into the appropriate fields; then, click **Generate Passphrase**.
3. Provide the passphrase to your user.

Screenshot 5: The Recover User Password screen

11.8.2 — Allow end users to request temporary access

This topic applies to VIPRE Endpoint Security only.

When enabled, a user may request temporary access for a device that is otherwise universally blocked based on the policies affecting the user. The user will provide you with an access code, which you use to approve and define the limits of the temporary access with.

When granting temporary access, you specify the **device type**, the **read/write capability**, and the **time until the temporary privileges expire**.

11.8.2.1 — Approving Temporary Access

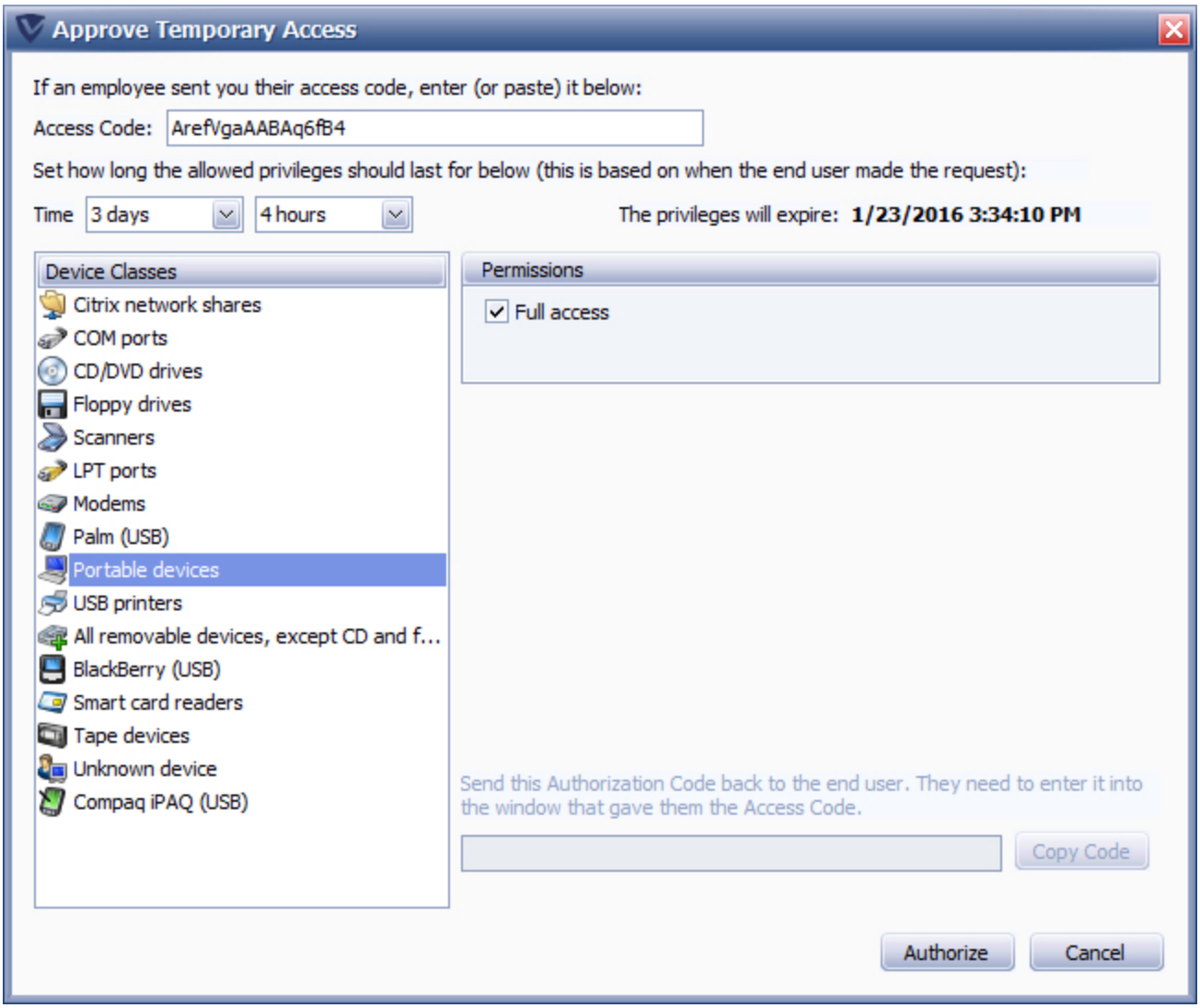
This topic applies to VIPRE Endpoint Security only.

When a user requests temporary access, you must manually approve the request. A separate request is required for each device.

To approve a temporary access request:

1. In the Policy Properties, select **Device Control**. Click the **Approve Temporary Access** button.
2. Enter the **Access Code** that the user has provided.
3. Select the **Device Type** from the drop-down, and click the appropriate **Read/Write** or **Read Only** check boxes.
4. Select the Time until the privileges expire using the **Time** drop-downs.
5. Click **Authorize**. You will receive an authorization code.
6. Provide this authorization code to your user.

Note: The *Time remaining* starts from when the agent generates the access request.



Screenshot 6: Approving temporary user access

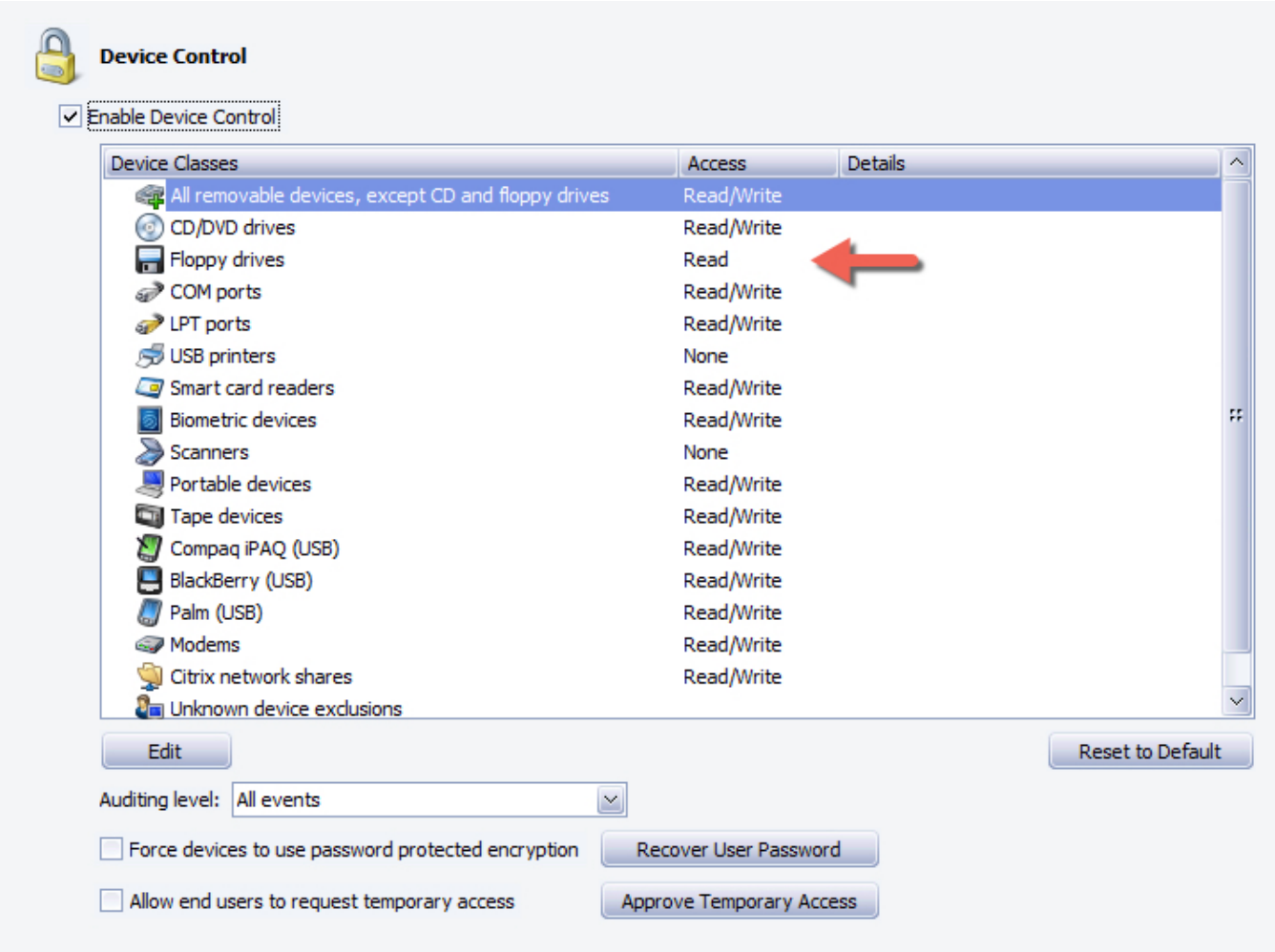
11.8.3 — Port Blocking

This topic applies to VIPRE Endpoint Security only.

You may select Deny Access or Read Only for specific device ports across an entire policy.

To manage device ports:

1. In the **Policy Properties**, select **Device Control**.
2. Double-click on a **Device Class**.
3. Select the appropriate permissions for the device, and click **OK**.
4. Click **OK** or **Apply**.



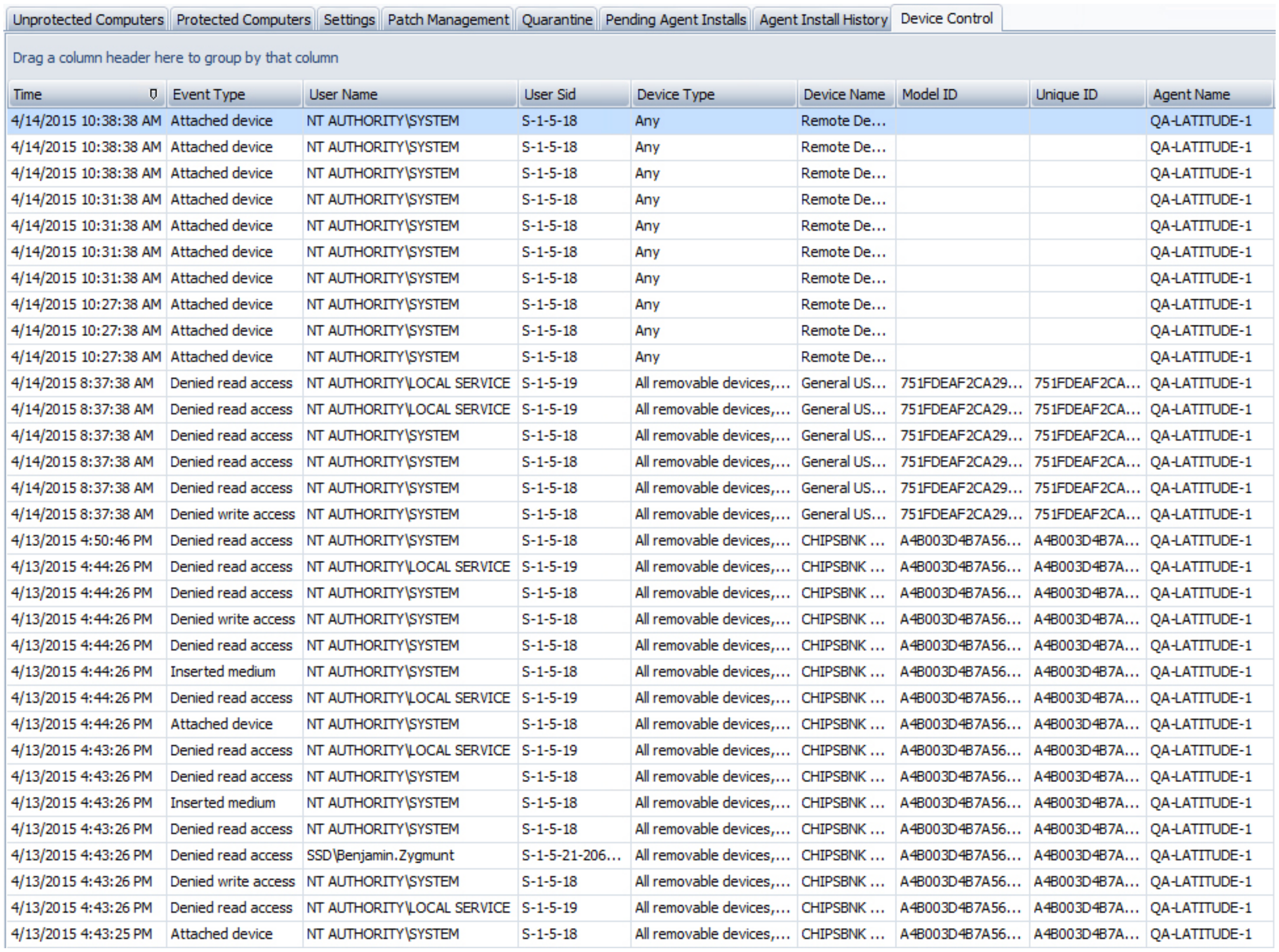
Screenshot 7: Example Read-only Port Blocking settings for Floppy drives

You may also adjust port blocking for specific devices, certain types of devices, and Users or Groups via Device Exclusions (page 117).

11.8.4 — Device Control tab

This topic applies to VIPRE Endpoint Security only.

An additional Device Control tab has been added to the Site Navigator grid for each policy which allows Device Control. This tab displays an overview of Device Control related information.



Time	Event Type	User Name	User Sid	Device Type	Device Name	Model ID	Unique ID	Agent Name
4/14/2015 10:38:38 AM	Attached device	NT AUTHORITY\SYSTEM	S-1-5-18	Any	Remote De...			QA-LATITUDE-1
4/14/2015 10:38:38 AM	Attached device	NT AUTHORITY\SYSTEM	S-1-5-18	Any	Remote De...			QA-LATITUDE-1
4/14/2015 10:38:38 AM	Attached device	NT AUTHORITY\SYSTEM	S-1-5-18	Any	Remote De...			QA-LATITUDE-1
4/14/2015 10:31:38 AM	Attached device	NT AUTHORITY\SYSTEM	S-1-5-18	Any	Remote De...			QA-LATITUDE-1
4/14/2015 10:31:38 AM	Attached device	NT AUTHORITY\SYSTEM	S-1-5-18	Any	Remote De...			QA-LATITUDE-1
4/14/2015 10:31:38 AM	Attached device	NT AUTHORITY\SYSTEM	S-1-5-18	Any	Remote De...			QA-LATITUDE-1
4/14/2015 10:31:38 AM	Attached device	NT AUTHORITY\SYSTEM	S-1-5-18	Any	Remote De...			QA-LATITUDE-1
4/14/2015 10:27:38 AM	Attached device	NT AUTHORITY\SYSTEM	S-1-5-18	Any	Remote De...			QA-LATITUDE-1
4/14/2015 10:27:38 AM	Attached device	NT AUTHORITY\SYSTEM	S-1-5-18	Any	Remote De...			QA-LATITUDE-1
4/14/2015 10:27:38 AM	Attached device	NT AUTHORITY\SYSTEM	S-1-5-18	Any	Remote De...			QA-LATITUDE-1
4/14/2015 8:37:38 AM	Denied read access	NT AUTHORITY\LOCAL SERVICE	S-1-5-19	All removable devices,...	General US...	751FDEAF2CA29...	751FDEAF2CA...	QA-LATITUDE-1
4/14/2015 8:37:38 AM	Denied read access	NT AUTHORITY\LOCAL SERVICE	S-1-5-19	All removable devices,...	General US...	751FDEAF2CA29...	751FDEAF2CA...	QA-LATITUDE-1
4/14/2015 8:37:38 AM	Denied read access	NT AUTHORITY\SYSTEM	S-1-5-18	All removable devices,...	General US...	751FDEAF2CA29...	751FDEAF2CA...	QA-LATITUDE-1
4/14/2015 8:37:38 AM	Denied read access	NT AUTHORITY\SYSTEM	S-1-5-18	All removable devices,...	General US...	751FDEAF2CA29...	751FDEAF2CA...	QA-LATITUDE-1
4/14/2015 8:37:38 AM	Denied read access	NT AUTHORITY\SYSTEM	S-1-5-18	All removable devices,...	General US...	751FDEAF2CA29...	751FDEAF2CA...	QA-LATITUDE-1
4/14/2015 8:37:38 AM	Denied write access	NT AUTHORITY\SYSTEM	S-1-5-18	All removable devices,...	General US...	751FDEAF2CA29...	751FDEAF2CA...	QA-LATITUDE-1
4/13/2015 4:50:46 PM	Denied read access	NT AUTHORITY\SYSTEM	S-1-5-18	All removable devices,...	CHIPSBNK ...	A4B003D4B7A56...	A4B003D4B7A...	QA-LATITUDE-1
4/13/2015 4:44:26 PM	Denied read access	NT AUTHORITY\LOCAL SERVICE	S-1-5-19	All removable devices,...	CHIPSBNK ...	A4B003D4B7A56...	A4B003D4B7A...	QA-LATITUDE-1
4/13/2015 4:44:26 PM	Denied read access	NT AUTHORITY\SYSTEM	S-1-5-18	All removable devices,...	CHIPSBNK ...	A4B003D4B7A56...	A4B003D4B7A...	QA-LATITUDE-1
4/13/2015 4:44:26 PM	Denied write access	NT AUTHORITY\SYSTEM	S-1-5-18	All removable devices,...	CHIPSBNK ...	A4B003D4B7A56...	A4B003D4B7A...	QA-LATITUDE-1
4/13/2015 4:44:26 PM	Denied read access	NT AUTHORITY\SYSTEM	S-1-5-18	All removable devices,...	CHIPSBNK ...	A4B003D4B7A56...	A4B003D4B7A...	QA-LATITUDE-1
4/13/2015 4:44:26 PM	Inserted medium	NT AUTHORITY\SYSTEM	S-1-5-18	All removable devices,...	CHIPSBNK ...	A4B003D4B7A56...	A4B003D4B7A...	QA-LATITUDE-1
4/13/2015 4:44:26 PM	Denied read access	NT AUTHORITY\LOCAL SERVICE	S-1-5-19	All removable devices,...	CHIPSBNK ...	A4B003D4B7A56...	A4B003D4B7A...	QA-LATITUDE-1
4/13/2015 4:44:26 PM	Attached device	NT AUTHORITY\SYSTEM	S-1-5-18	All removable devices,...	CHIPSBNK ...	A4B003D4B7A56...	A4B003D4B7A...	QA-LATITUDE-1
4/13/2015 4:43:26 PM	Denied read access	NT AUTHORITY\LOCAL SERVICE	S-1-5-19	All removable devices,...	CHIPSBNK ...	A4B003D4B7A56...	A4B003D4B7A...	QA-LATITUDE-1
4/13/2015 4:43:26 PM	Denied read access	NT AUTHORITY\SYSTEM	S-1-5-18	All removable devices,...	CHIPSBNK ...	A4B003D4B7A56...	A4B003D4B7A...	QA-LATITUDE-1
4/13/2015 4:43:26 PM	Inserted medium	NT AUTHORITY\SYSTEM	S-1-5-18	All removable devices,...	CHIPSBNK ...	A4B003D4B7A56...	A4B003D4B7A...	QA-LATITUDE-1
4/13/2015 4:43:26 PM	Denied read access	NT AUTHORITY\SYSTEM	S-1-5-18	All removable devices,...	CHIPSBNK ...	A4B003D4B7A56...	A4B003D4B7A...	QA-LATITUDE-1
4/13/2015 4:43:26 PM	Denied read access	SSD\Benjamin.Zygmunt	S-1-5-21-206...	All removable devices,...	CHIPSBNK ...	A4B003D4B7A56...	A4B003D4B7A...	QA-LATITUDE-1
4/13/2015 4:43:26 PM	Denied write access	NT AUTHORITY\SYSTEM	S-1-5-18	All removable devices,...	CHIPSBNK ...	A4B003D4B7A56...	A4B003D4B7A...	QA-LATITUDE-1
4/13/2015 4:43:26 PM	Denied read access	NT AUTHORITY\LOCAL SERVICE	S-1-5-19	All removable devices,...	CHIPSBNK ...	A4B003D4B7A56...	A4B003D4B7A...	QA-LATITUDE-1
4/13/2015 4:43:25 PM	Attached device	NT AUTHORITY\SYSTEM	S-1-5-18	All removable devices,...	CHIPSBNK ...	A4B003D4B7A56...	A4B003D4B7A...	QA-LATITUDE-1

Screenshot 8: The Device Control tab on the Site Navigator grid

The Device Control tab displays audit trail information for all devices affected by the currently selected policy.

Information is presented for Time, Event Type, User Name, User Sid, Device Type, Device Name, Model ID, Unique ID, and Agent Name.

From this tab, you may quickly create a **User Exclusion** or **a Device Exclusion**.

11.8.5 — Device Exclusions

This topic applies to VIPRE Endpoint Security only.

You may exclude devices from the current policy by creating device exclusions. Excluded devices are exempt from policy settings that would otherwise affect them.

Exclusions fall into three categories:

- **Specific devices** – A single device identified by its Windows device ID
- **Device types** – A selection of device types, chosen from the Allowed Privilege list

- **Users** - All devices belonging to an Active Directory user
- **Groups** - All devices belonging to an Active Directory group

Note: Users and Groups are only available if your machine is part of a domain environment.

11.8.5.1 — Creating a Device Exclusion

This topic applies to VIPRE Endpoint Security only.

To exclude devices by type

1. In the **Policy Properties**, select **Device Control**.
2. Double-click on a **Device Class**.
3. Click **Add**.
4. Enter a name for the exclusion.
5. Select the appropriate permissions for the device, and click **OK**.
6. Click **OK**; then, click **OK** or **Apply**.

To exclude a specific device

1. In the **Site Navigator**, select the policy that controls the device; then, click the **Device Control** tab.
2. Right-click the device and select **Create Device Exclusion...**
3. Enter a name for the exclusion.
4. Select the appropriate permissions for the device, and click **OK**.
5. Click **OK**; then, click **OK** or **Apply**.

Or

1. In the **Policy Properties**, select **Device Control**.
2. Double-click on a **Device Class**.
3. Click **Add**.
4. Enter a name for the exclusion.
5. Select the appropriate permissions for the device.
6. Enter the **Model ID** and **Hardware serial number** for the device, and click **OK**.
7. Click **OK**; then, click **OK** or **Apply**.

To exclude devices belonging to a group

1. In the **Policy Properties**, select **Device Control**.
2. Double-click on a **Device Class**.
3. Click **Add**.
4. Enter a name for the exclusion.
5. Select the appropriate permissions for the device.
6. Click **Add**.

7. Select the Group(s) you with to exclude, and click **Add...**, then click **OK**.
8. Click **OK**; then, click **OK** or **Apply**.

To exclude devices belonging to a user

1. In the **Site Navigator**, select the policy that controls the device; then, click the **Device Control** tab.
2. Right-click the user and select **Create Device Exclusion...**
3. Enter a name for the exclusion.
4. Select the appropriate permissions for the device, and click **OK**.
5. Click **OK**; then, click **OK** or **Apply**.

Or

1. In the **Policy Properties**, select **Device Control**.
2. Double-click on a **Device Class**.
3. Click **Add**.
4. Enter a name for the exclusion.
5. Select the appropriate permissions for the device.
6. Click **Add**.
7. Select the User(s) you with to exclude, and click **Add...**, then click **OK**.
8. Click **OK**; then, click **OK** or **Apply**.

11.8.5.2 — Editing or Removing Device Exclusions

This topic applies to VIPRE Endpoint Security only.

To remove a device exclusion

1. In the **Policy Properties**, select **Device Control**.
2. Double-click on a **Device Class**.
3. Select an exclusion and click **Remove**.
4. Click **OK**; then, click **OK** or **Apply**.

To edit a device exclusion

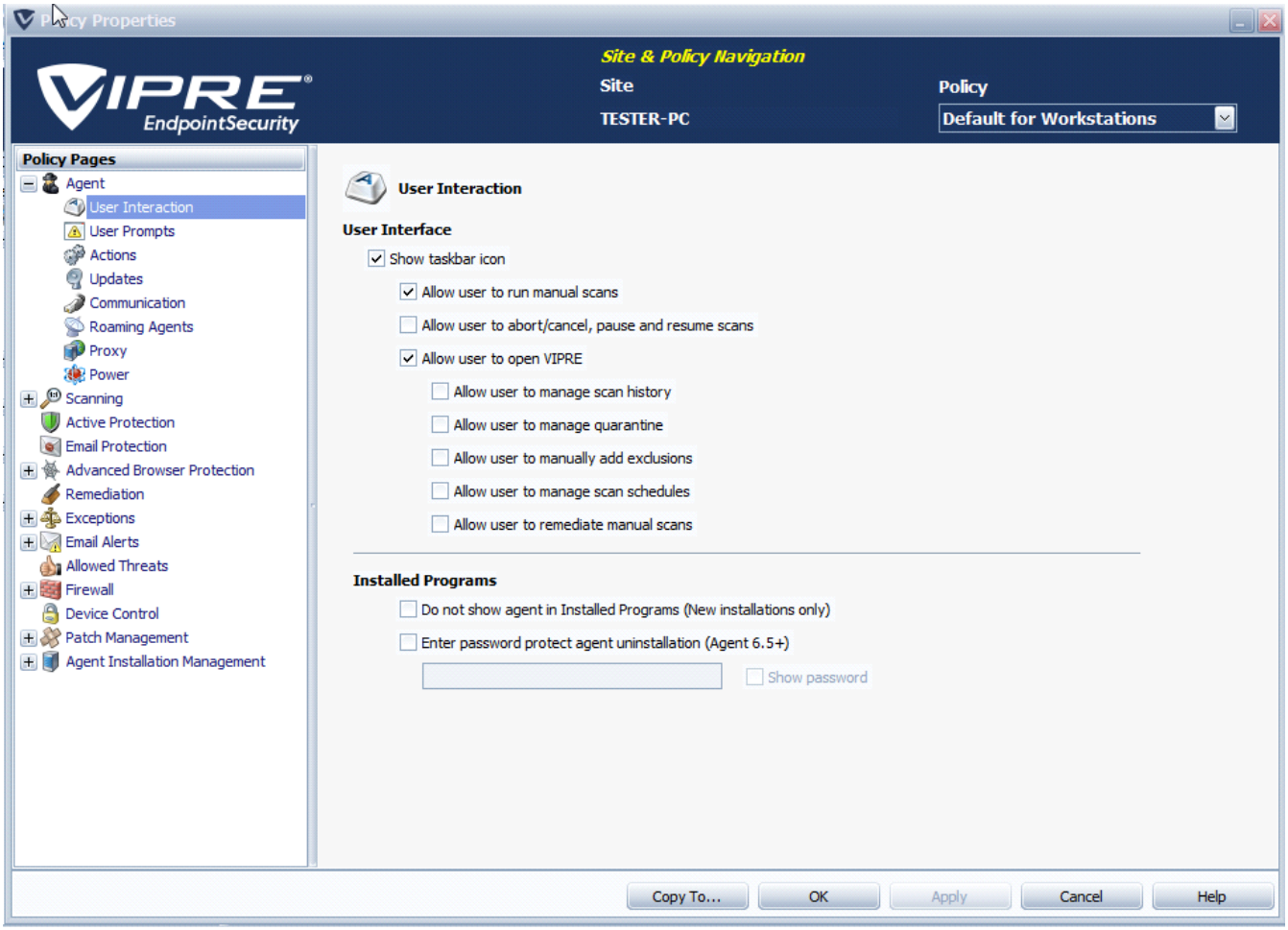
1. In the **Policy Properties**, select **Device Control**.
2. Double-click on a **Device Class**.
3. Select an exclusion and click **Edit**.
4. Make your changes, then click **OK**.
5. Click **OK**; then, click **OK** or **Apply**.

12 — Configuring Mac Policies

12.1 — Configuring Agent Settings

12.1.1 — Configuring User Interaction

The User Interaction screen is used to configure how the end-user interacts with an agent.

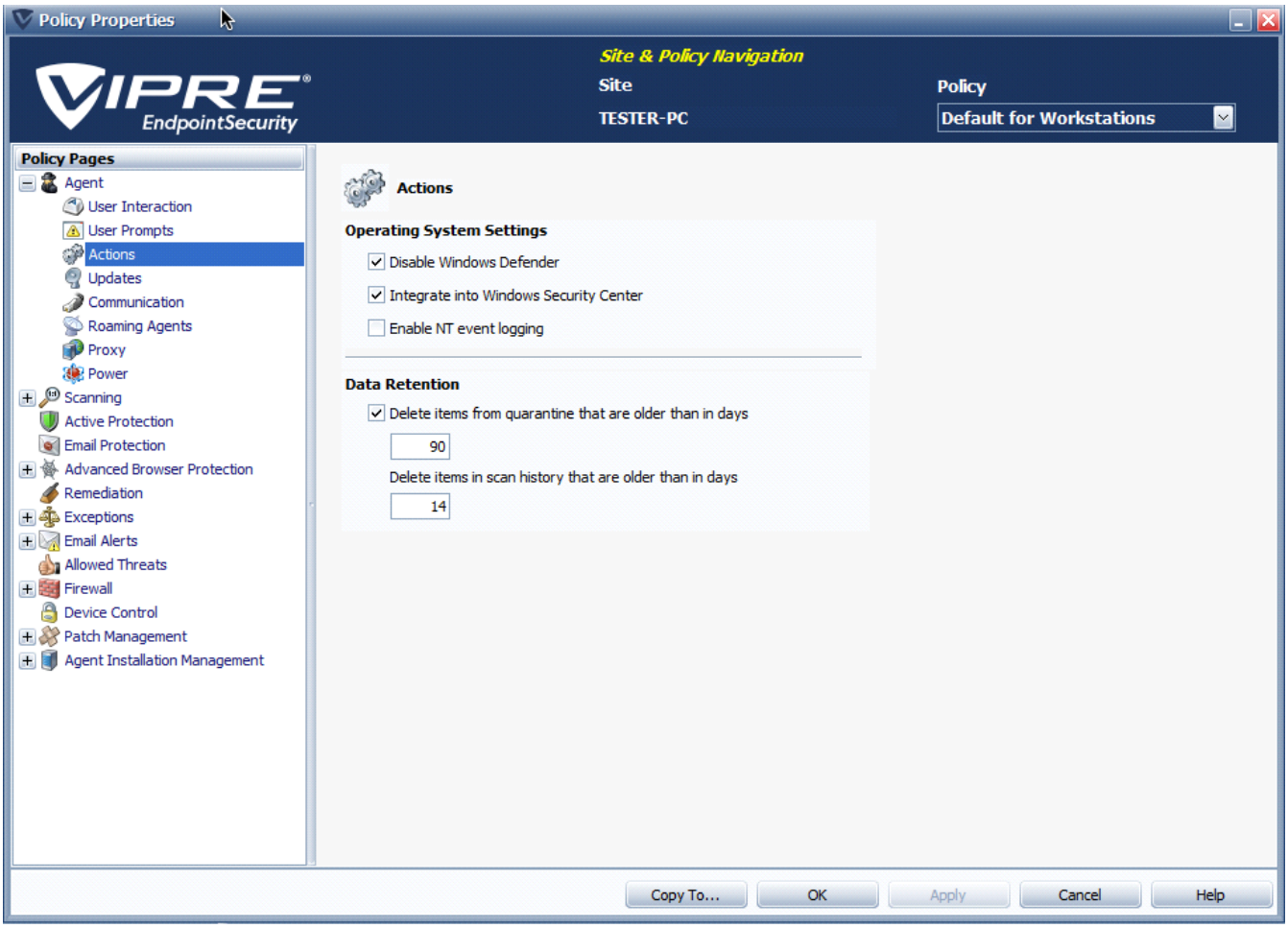


To configure user interaction settings:

1. From **Site Navigator**, double-click the Mac policy you want to configure.
2. From the left pane of the Policy Properties screen, expand **Agent** and click **User Interaction**.
3. From the right pane, select **Show taskbar icon**. This displays the agent icon on the end-users' taskbar, through which the user can run agent commands, if allowed by the controlling policy.
4. Click **Apply** and **OK**.

12.1.2 — Configuring Agent Actions

The Actions screen is used to configure data retention settings for quarantine and scan history data.



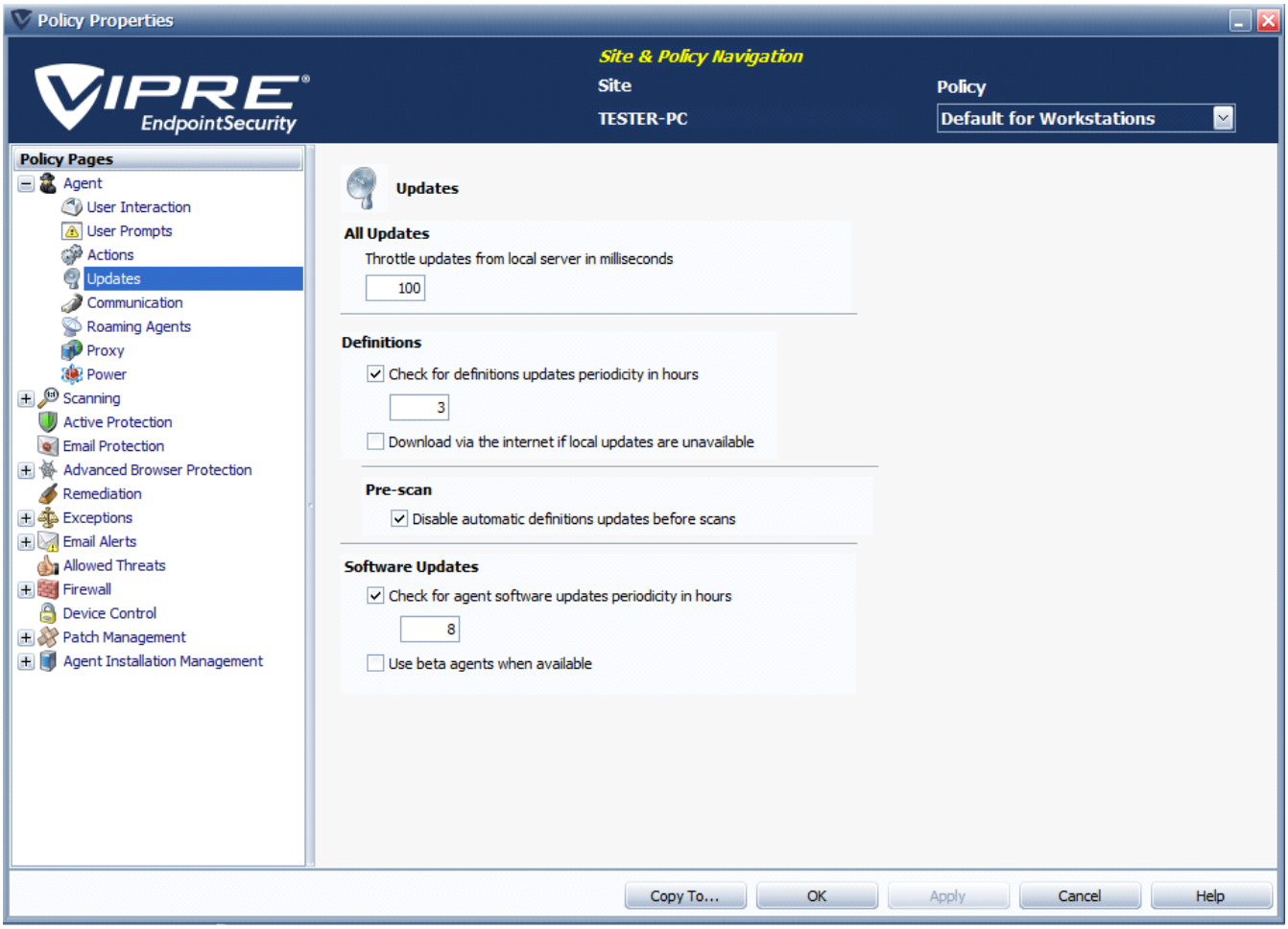
To configure data retention settings:

1. From **Site Navigator**, double-click the Mac policy you want to configure.
2. From the left pane of the Policy Properties screen, expand **Agent** and click **Actions**.
3. To automatically delete quarantine items, based on a schedule, select **Delete items from quarantine that are older than in days**. Key in the number of days that have to pass before quarantine items are deleted.
4. To automatically delete scan history logs, based on a schedule, select **Delete items in scan history that are older than in days**. Key in the number of days that have to pass before scan history logs are deleted.
5. Click **Apply** and **OK**.

12.1.3 — Configuring Agent Updates

The Updates screen enables you to configure the time when agents check for definition updates as well as turn on/off pre-scan update checks. This helps you manage network bandwidth utilization as well as system performance for all the agents in your network. If a significant number of agents attempt to check for and download updates at the same time, network performance depreciates.

Note: It is recommended to use different time intervals for different policies.



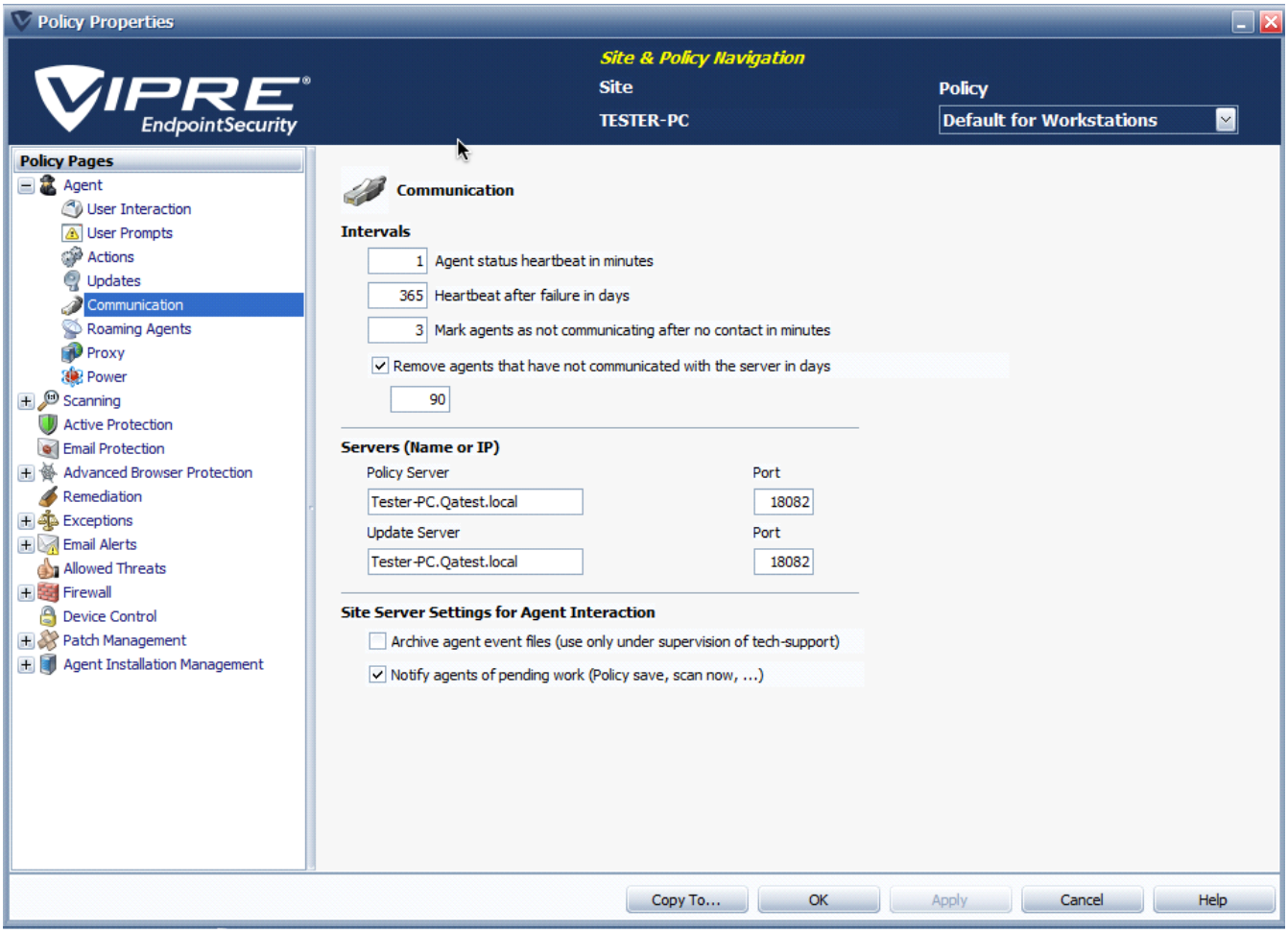
To configure updates settings:

1. From **Site Navigator**, double-click the Mac policy you want to configure.
2. From the left pane of the Policy Properties screen, expand **Agent** and click **Updates**.
3. To enable/disable automatic definition updates, select/unselect **Check for definitions updates periodicity in hours**. Key in the time interval in hours.
4. To disable automatic pre-scan checking for definition updates, select **Disable automatic definitions updates before scans**.
5. Click **Apply** and **OK**.

12.1.4 — Configuring Agent Communication

The Communication screen enables you to control how agents communicate with the VIPRE Site Service (VSS). The default settings are suitable for environments that consist of 100 to 400 agents, including agents running on laptops. Larger environments of around 500+ agents may require adjustments to these defaults.

Note: Modify agent communication intervals only if it becomes necessary.



To configure communication settings:

1. From **Site Navigator**, double click the Mac policy you want to configure.
2. From the left pane of the Policy Properties screen, expand **Agent** and click **Communication**.
3. Configure the following agent **Intervals**:

   - **Agent status heartbeat in minutes**: determines how often the agent calls into the VSS, primarily to verify that the agent is working. Particular information passed through the communication includes agent, threat database and Operating System versions, IP address, and agent status.
     The default is 5 minutes and works well for 100 agents or less. Larger organizations can put a greater load on the VSS and may require 15-60 minutes or even more. The heartbeat is adjustable between 1 and 10,080 minutes (1 week)
   - **Heartbeat after failure in days**: if the heartbeat fails, the agent will continue attempting communication with the VSS for this number of days. After the number of days, communication attempts will cease, **resulting in the agent not completing any of its scheduled scans, and disabling Active Protection**. If the agent is able to communicate with the server at any time prior to the set period, the Agent will reset its counter. If the agent has gone dormant, every time it's restarted, as during a reboot, it will try to

communicate with the server once. If that heartbeat then fails again, the agent will go dormant again. If communication is successful, the agent will reset its counter and continue its scheduled communications The default setting is 365 days. The setting is adjustable from 1 to 365 days.

- **Mark agents inactive after no contact in minutes**: set the length of time an agent is quiet prior to being marked inactive by the VIPRE Site Service.
  The default value is 30 minutes. The length of time can be set between 0 and 10080 minutes. *The recommended length of time is three times the longest heartbeat interval*
- **Retry authentication in days**: only applies if the **Agent Recovery Mode** in the Advanced Site Settings is turned off.
  If an agent can successfully say Hello but fails authentication, the agent will be told to reinitialize itself. The agent will retry to authenticate for the specified period, after which it will go dormant. Every time the agent is restarted, it will try one heartbeat before going dormant again.
  The default setting is 7 days. This setting is adjustable from 1-7 days.

4. (Optional) An agent can be configured to automatically uninstall itself from the host, if there is no communication with the VIPRE Site Service (VSS) for a set number of days. To enable this feature, select **Remove agents that have not communicated with the server in days**, and key in the number of days that have to pass before the agent is automatically uninstalled.
5. Configure the following **Server** settings:
   a. In the **Policy Server** field, key in the machine **Name** or **IP address** of the VIPRE server that distributes policy updates to the agents managed by this policy.
   b. In the **Port** field, key in the TCP port that the VIPRE Site Service uses to receive agent requests and security information.
6. Configure **Site Server Settings for Agent Interaction**:

Important: This following option (procedure step a) must not be used unless instructed by a technical support representative.

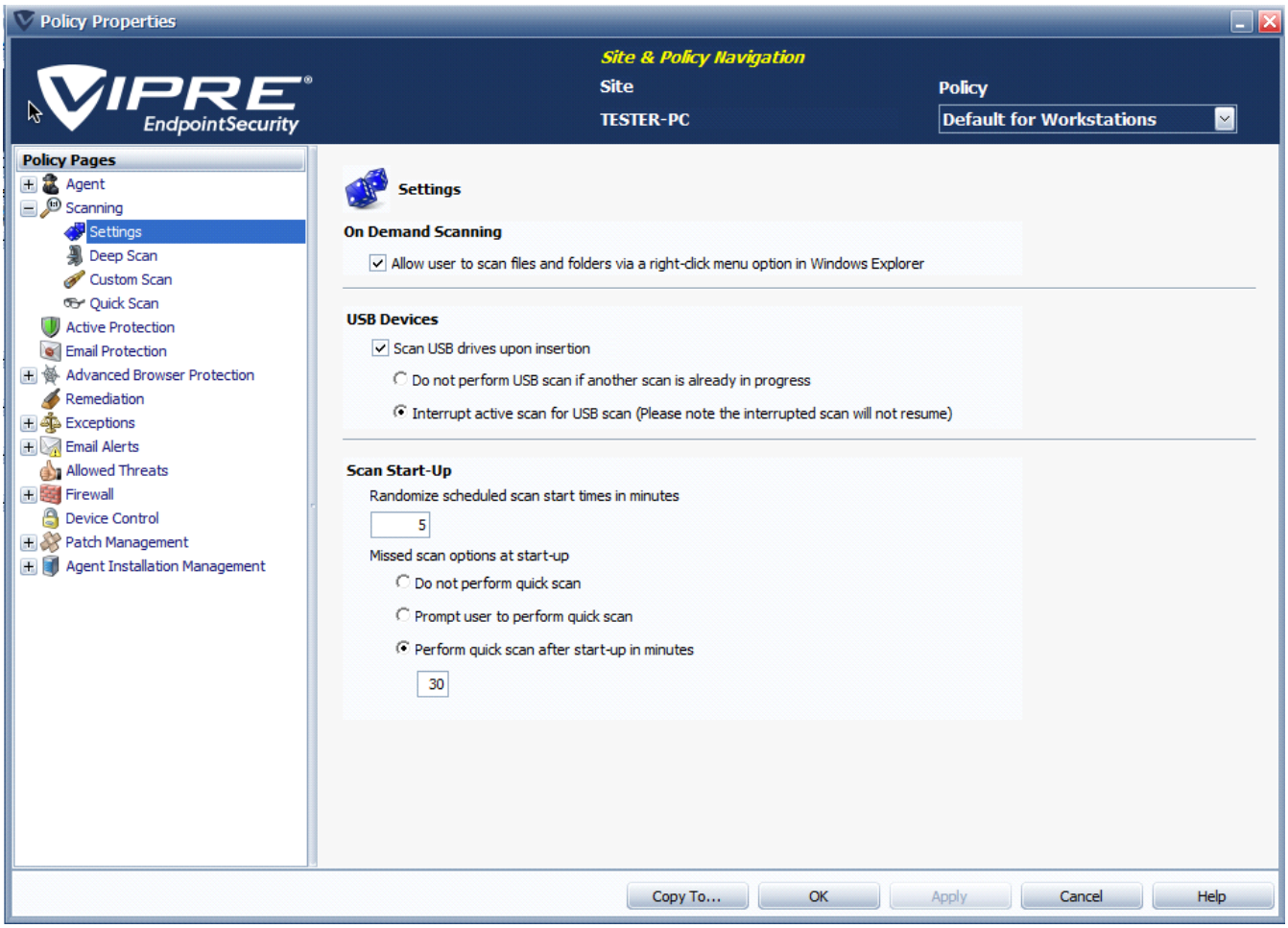
- **Archive agent event files**: (This setting is for **DEBUGGING WITH TECH SUPPORT ONLY**) scanning and Active Protection reports coming from an agent are stored in the "Incoming XML" folder. The information is then stripped out of the XML and stored in a database, and the XML file deleted. Selecting this option moves the XML file into the "ProcessedXML" folder where the file is stored until deleted manually. Storing this file is useful only for debugging and is best when working with Technical Support.
- **Notify agents of pending work**: when you make a change to a policy, the VSS stores the information in a deferred work queue. Agents get that information during their next scheduled communication. Selecting this option causes the VIPRE Site Service to contact the agent and tell them to do a heartbeat and get the information prior to the scheduled time.

7. Click **Apply** and **OK**.

12.2 — Configuring Scan Settings

12.2.1 — Configuring General Scan Settings

The Scan Settings screen enables you to randomize scheduled scans start time. This is used to manage the VIPRE host performance. Since scans start at different times, VIPRE's performance is not effected by polling multiple sources simultaneously.



To configure scan settings:

1. From **Site Navigator**, double-click the Mac policy you want to configure.
2. From the left pane of the Policy Properties screen, expand **Scanning** and click **Settings**.
3. Key in the time interval (example, 60 minutes). This indicates that scheduled scans will start at random intervals of 60 minutes.
4. Click **Apply** and **OK**.

12.2.2 — Configuring Full Scan Settings

Use the Full Scan screen to configure thorough scanning options such as scan priorities, locations and additional scan items.

To configure full scan settings:

1. From **Site Navigator**, double-click the Mac policy you want to configure.
2. From the left pane of the Policy Properties screen, expand **Scanning** and click **Full Scan**.
3. To configure full scan scheduling:

a. Select **Enable** to turn on scan scheduling.
b. In the **Scanning Start Time** field, key in the time you want scans to start.

Note: Scan start times are randomized according to General Scan Settings.

c. In the **Re-scan periodicity in hours** field, key in the time interval (in hours) between scans.
d. In the **Repeat Scans Until** field, key in the latest possible scan start time.

Note: This does not effect scans in progress. Running scans continue until completed.

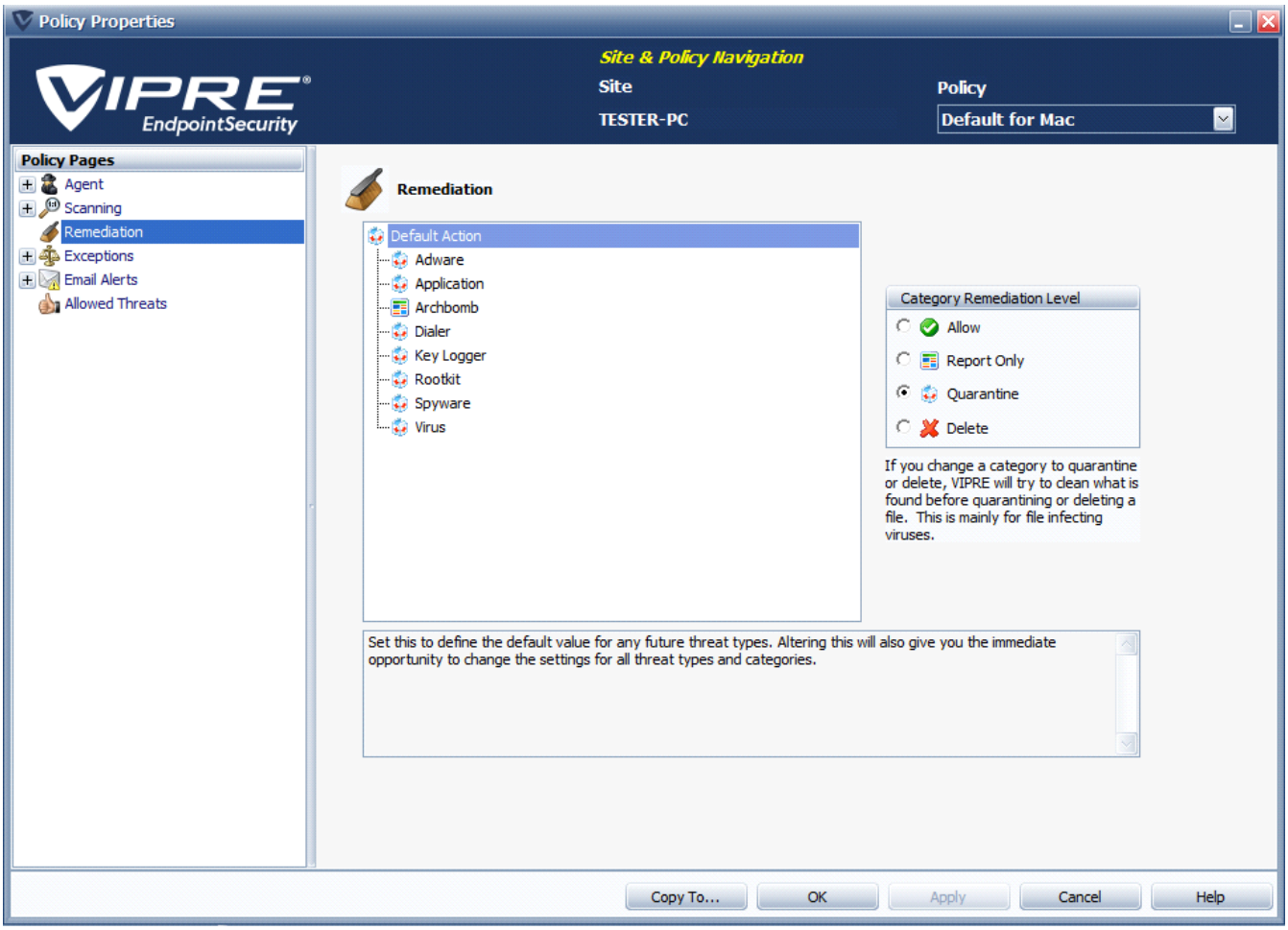
e. Select the days of the week when you want agents to run security scans.

4. From the **Scan priority** drop-down, select one of the following options:
   - **Lowest**: Set the priority to Lowest if you are going to be running the scans in the middle of the day. Windows will run other programs that are requesting to run before the scan. This should reduce the impact of end user performance when a scan runs during working hours
   - **Normal**: Set the priority to Normal when scanning at night or on multi-core machines where scanning at a higher priority won't affect user performance
   - **Highest**: Set the priority to Highest when it is important to have the scan run as quickly as possible, even if the end user is actively using the computer.
5. From the **Locations** section, select the location that VIPRE thoroughly checks for security threats. Select from:
   - **Common threat locations**: select for the scan to include the root of the drive, the program files directory, the system directory, etc
   - **System drive only**: select for the scan to include the main drive (C:) only
   - **Internal drives only**: select for the scan to include internal drives only. This selection excludes USB, FireWire, and other external drives
   - **All local drives**: select for the scan to include all internal drives, partitions, plus any attached USB, FireWire, or other external devices
   - **None**: select for the scan to focus on only the selection(s) in the Options area. When selected, no drive or folder will receive scans.
6. From the **Options** section, select any the following optional scan items:
   - **Processes**: select for the scan to include all running processes (applications)
   - **Archives**: select for the scan to include archive files (such as .RAR or .ZIP). If a .RAR file is found to contain an infected file, the .RAR file will be quarantined. If a .ZIP file is found to contain an infected file, the infected file is quarantined and replaced by a .TXT file with text indicating that it was infected and that it has been quarantined.
7. Click **Apply** and **OK**.

12.3 — Configuring Remediation Settings

Configure how the results of scans are cleaned (remediated). Assign actions according to threat types, such as Adware, Viruses, Worms, and so forth. Actions include allow, report only, quarantine, and delete.

IMPORTANT: For the best results, ensure that you go through the list of threats and assign the appropriate action that best suits the needs of your organization. Select a category to display a detailed explanation below it.



To configure remediation settings:

1. From **Site Navigator**, double-click the Mac policy you want to configure.
2. From the left pane of the Policy Properties screen, click **Remediation**.
3. From the threats list, select a treat type or sub-type.
4. From the **Category Remediation Level** section, assign an action to the selected threat. When the selected treat type or sub-type is detected, one of the following actions is performed:

   Allow: the threat is allowed to run on the machine. Threats with Allow remediation assigned cannot be tracked in reports

   Report Only: the threat is allowed to run and can be tracked in reports

   Quarantine: the threat is placed in quarantine, which resides on the agent machine

   Delete: the threat is completely removed from the agent machine and unrecoverable.

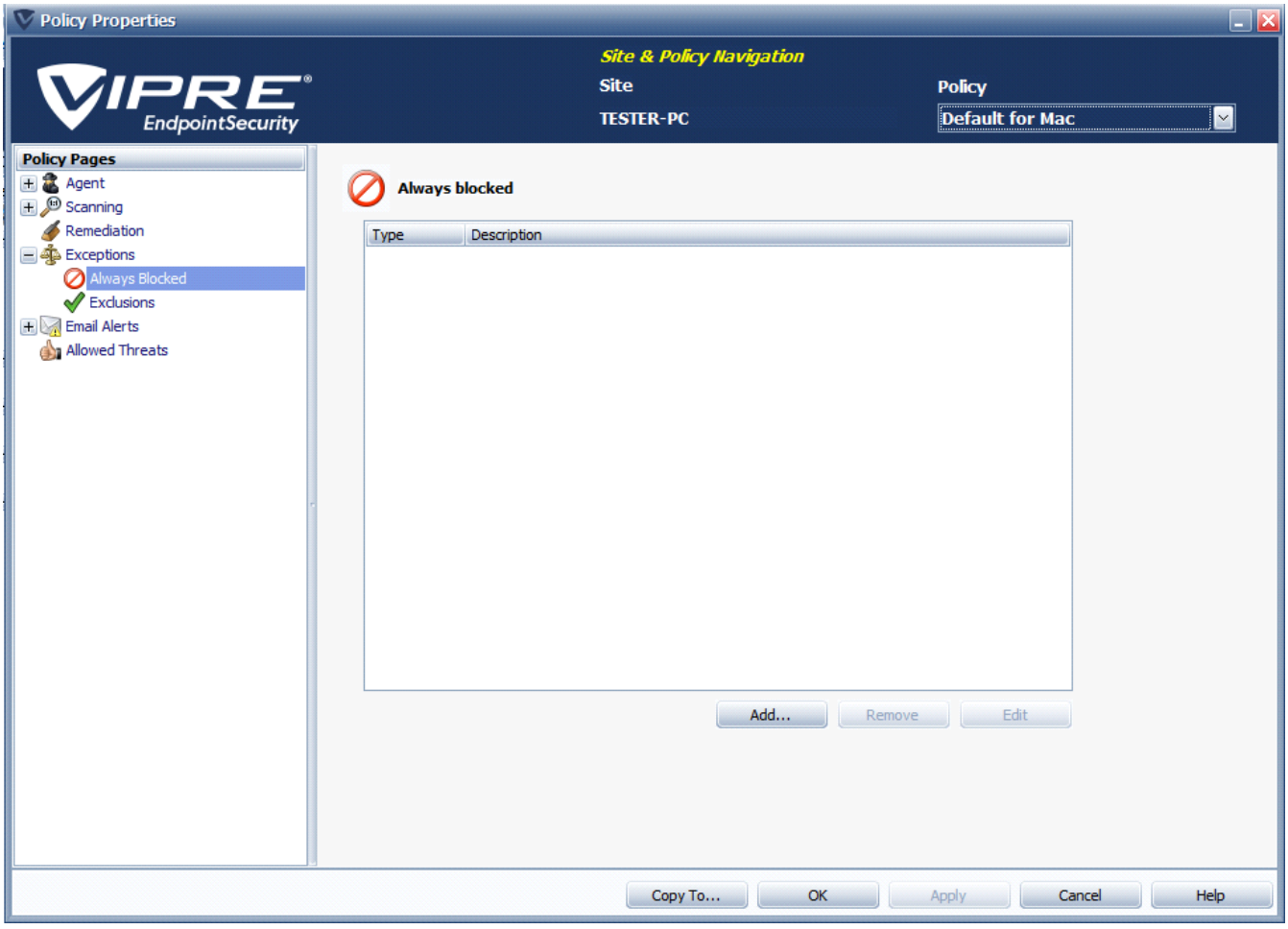
Important: As a safeguard, you may want to select **Quarantine** and not **Delete**. Items in Quarantine can be recovered, deleted items cannot.

5. Click **Apply** and **OK**.

12.4 — Configuring Exceptions Settings

12.4.1 — Adding Blocked Items

The Always Blocked screen is used to add Files, Paths and Folders that you consider as threats to your environment. Blocked items can be any file type you require, example, **File.txt**, **File.exe**, **File.bat**, **File.csv**, and more. When an item from the Always Blocked list is detected, it is treated as a known threat and the pre configured remediation action is performed on it.



To add always blocked items:

1. From **Site Navigator**, double-click the Mac policy you want to configure.
2. From the left pane of the Policy Properties screen, expand **Exceptions** and click **Always Blocked**.

3. To add items to the list, click **Add...** and select one of the following file or folder types you want to add:
   - **Add File**: key in a file name including the file extension. Click **OK** and repeat this step to add more files. This ensures that the file is blocked, even if it is found in multiple locations on the computer
   - **Add File with Path**: key in a path and file name including file extension. Click **OK** and repeat this step to add more files including the path. If multiple files with the same name exist in different locations on your computer, only the one in the specified path is blocked
   - **Add Folder**: key in a folder path including folder name. Click **OK** and repeat this step to add more folders. This ensures that the contents of the specified folder is blocked during security scans.

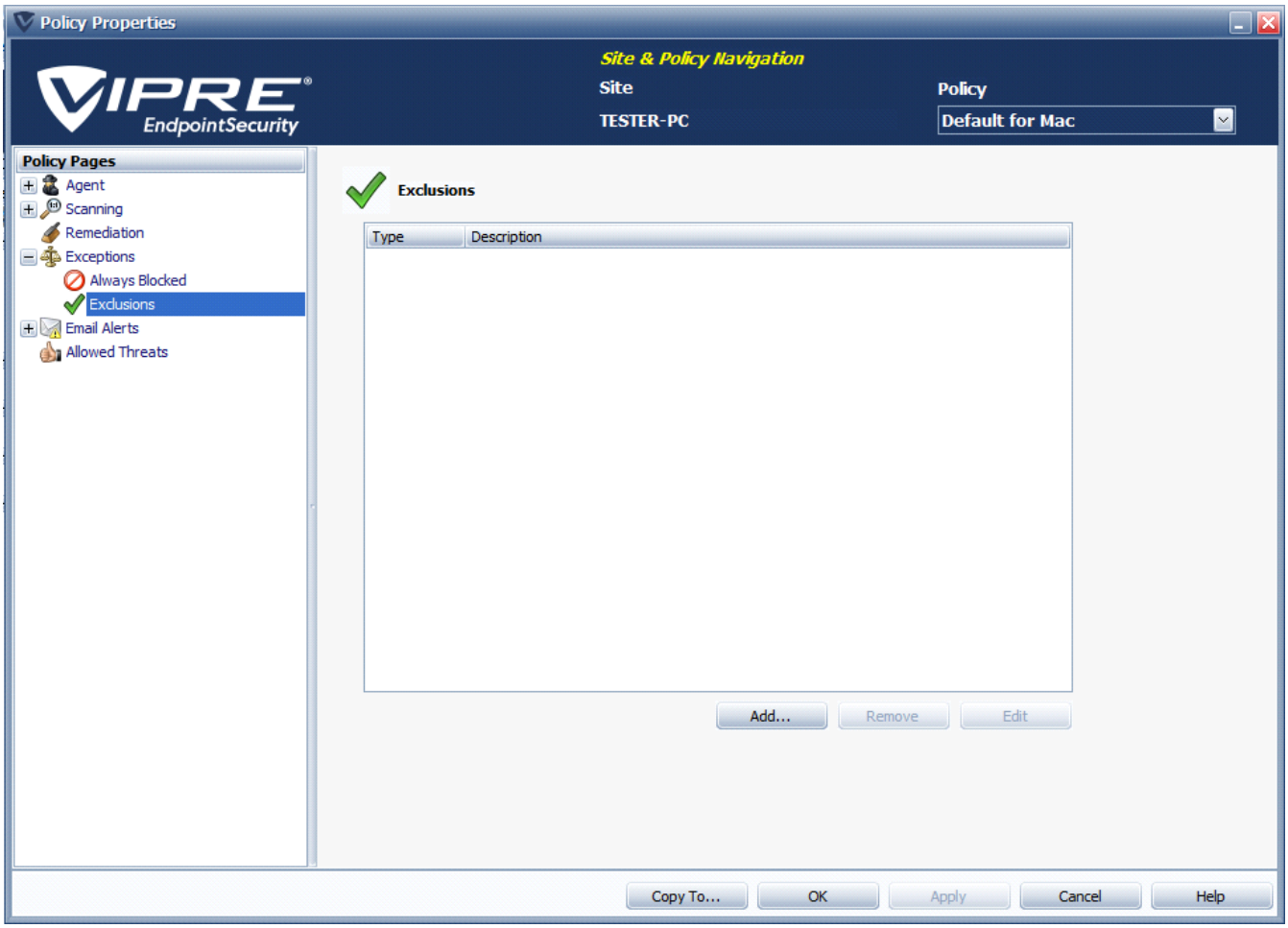
Note: Wildcards (***** and **?**) are supported for **Exclusions** only.

4. To remove files or folders from the list, select one or more item using the Ctrl and Shift keys and click **Remove**.
5. Click **Apply** and **OK**.

12.4.2 — Adding Allowed Items

The Exclusions screen enables you to add Files, Paths and Folders that you want to allow in your environment. Allowed items can be any file type you require, example, **File.txt**, **File.exe**, **File.bat**, **File.csv**, and more. Although threat definitions might consider them as security risks, items in the Always Allowed list are ignored during a scan.

Important: Ensure that files, folder and/or applications you are excluding from security scans are genuine and come from trusted sources.



To add allowed items

1. From **Site Navigator**, double-click the Mac policy you want to configure.
2. From the left pane of the Policy Properties screen, expand **Exceptions** and click **Exclusion**.
3. To add items to the list, click **Add...** and select one of the following file or folder types you want to add:
   - **Add File**: key in a file name including the file extension. Click **OK** and repeat this step to add more files. This ensures that if the specified file exists in multiple locations on the computer, all the files with the same name are allowed
   - **Add File with Path**: key in a path and file name including file extension. Click **OK** and repeat this step to add more files including the path. If multiple files with the same name exist in different locations on your computer, only the one in the specified path is allowed
   - **Add Folder**: key in a folder path including the folder name. Click **OK** and repeat this step to add more folders. This ensures that the contents of the specified folder is allowed during security scans.

Note: Wildcards (***** and **?**) are supported for Exclusions. For more information, See Using Wildcards in Exclusions.

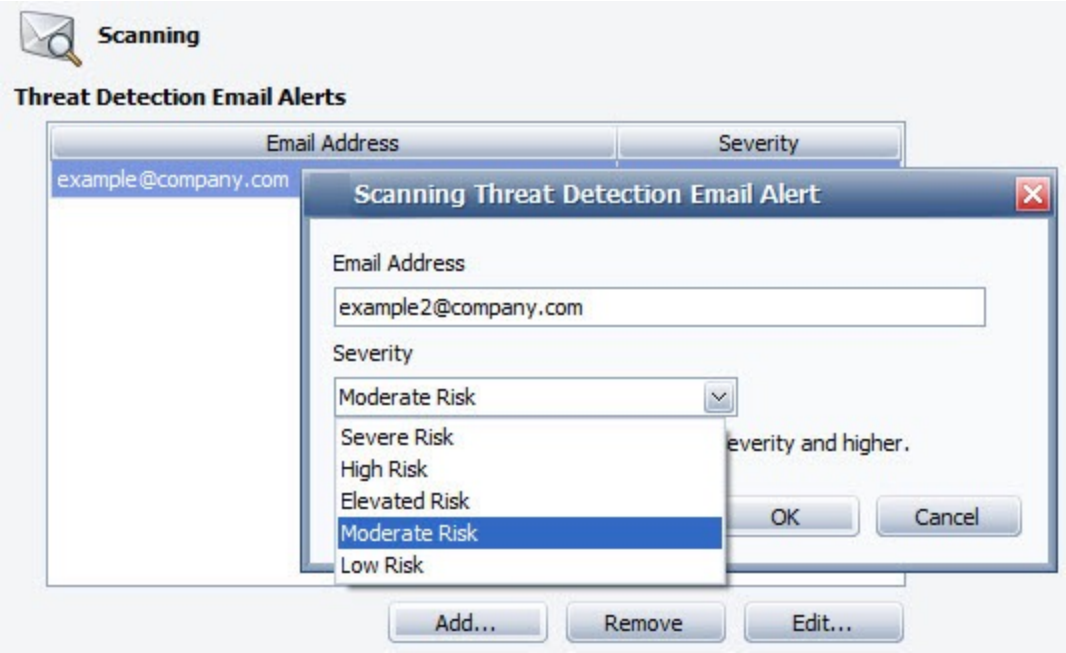
4. To remove files or folders from the list, select one or more item using the Ctrl and Shift keys and click **Remove**.
5. Click **Apply** and **OK**.

12.5 — Configure Email Alerts

Email Alerts are email messages sent by the VIPRE Site Service to recipients that you enter. Configure **Email Alerts** for Agent events, including Scanning, Active Protection, Email Protection, and Patch Management (*VIPRE Premium or Endpoint Security*). Email alerts are configured at the policy level.

To configure email alerts for threat detections by Scanning:

1. Ensure that the Site's Email Server Settings are configured.
2. In the **Policy Properties**, open **Email Alerts>Scanning**.
3. Click **Add**. The Scanning Threat Detection Email Alert dialog box displays.



4. Enter a recipient's email address.
5. From the **Severity** drop-down box, select a risk level. When the severity or higher that you select is detected during a scan, an email is sent with the details to recipients on the list.
6. Click **OK**. The email address displays in the list.
7. To edit an email alert recipient, select an email address and then click **Edit** to make your desired changes.
8. To remove an email alert recipient, select an email address and then click **Remove**.

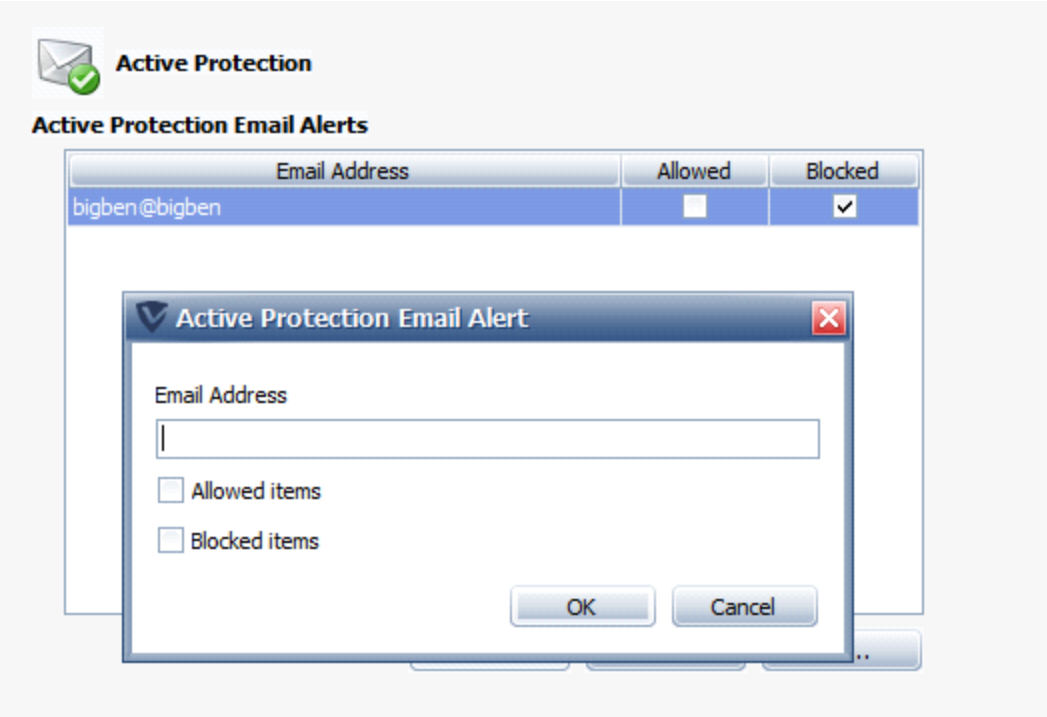
To configure email alerts for Active Protection:

1. Ensure that the Site's Email Server Settings are configured.
2. In the **Policy Properties**, open **Email Alerts>Active Protection**.
3. Click **Add**. The Active Protection Email Alert dialog box displays.

4. Enter a recipient's email address.
5. Select one or both:
   - **Allowed items**: CAUTION, this setting may result in a multitude of emails. An email is sent with the details to the recipient list. "Allowed" items are based on Exclusions.
   - **Blocked items**: emails are triggered whenever AP detects a threat, based on the Active Protection settings. This applies to all agents that are assigned to the policy that you are configuring.
6. Click **OK**. The email address displays in the list.
7. To edit an email alert recipient, select an email address and then click **Edit** to make your desired changes.
8. To remove an email alert recipient, select an email address and then click **Remove**.

To configure email alerts for Email Protection:

1. Ensure that the Site's Email Server Settings are configured.
2. In the **Policy Properties**, open **Email Alerts>Email Protection**.
3. Click **Add**. The Email Protection Email Alert dialog box displays.

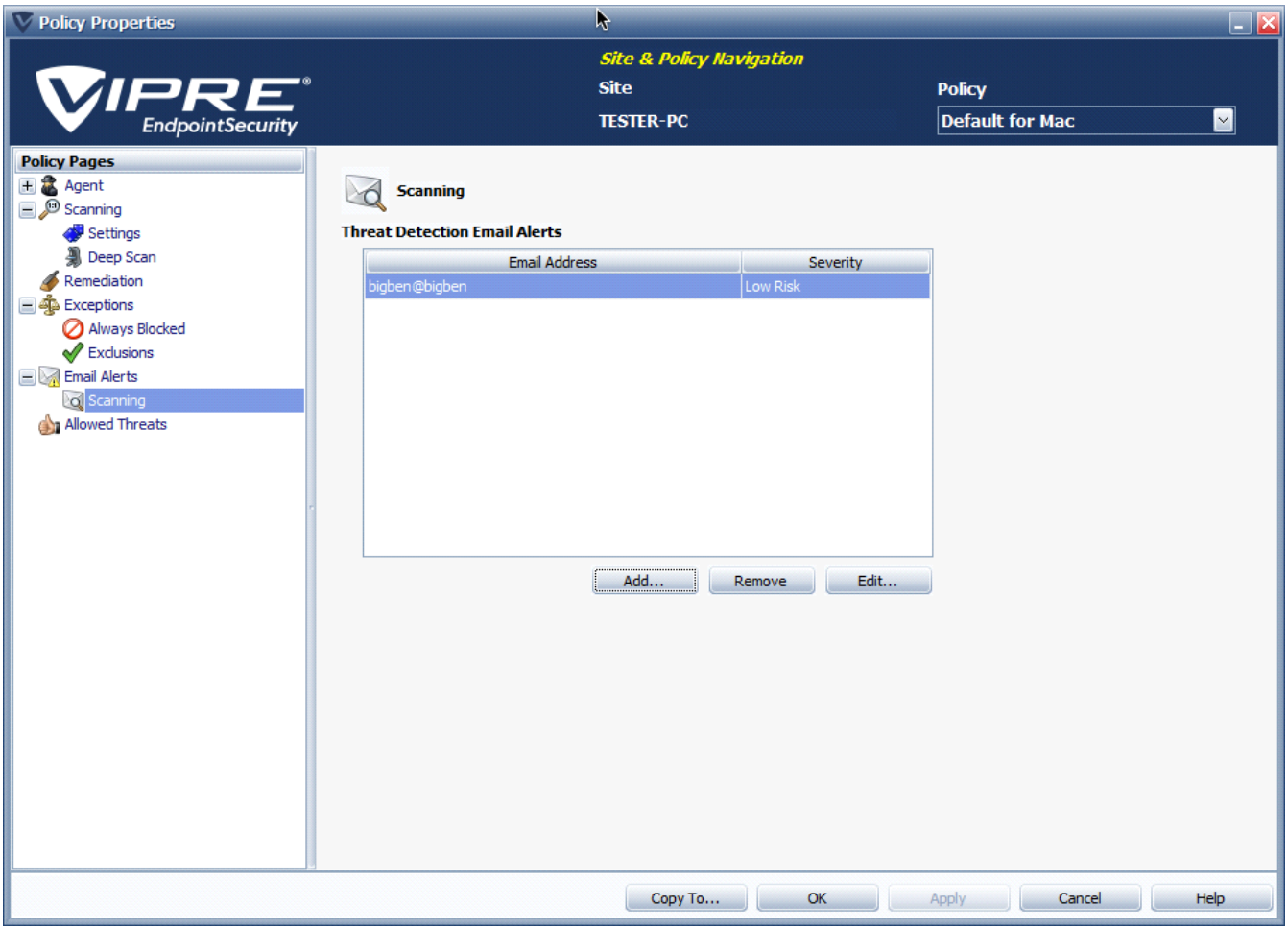


4. Click **OK**. The email address displays in the list. When Email Protection detects malware in an email, recipients on the list will receive an alert with the details.
5. To edit an email alert recipient, select an email address and then click **Edit** to make your desired changes.
6. To remove an email alert recipient, select an email address and then click **Remove**.

Tip: Instead of receiving email alerts in real-time, consider using the Report Viewer to schedule a daily Threat Found Detail report. You can set alerts for the most severe risks after a scan and use reports for the rest.

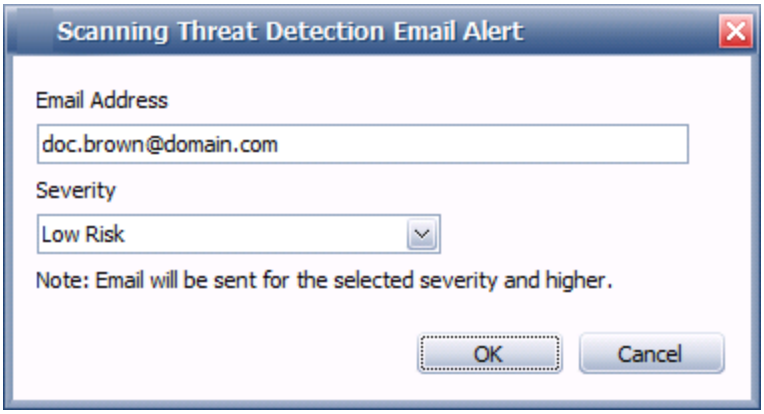
12.5.1 — Configuring Email Alerts Settings

The Email Scanning screen enables you to assign severity ratings to potentially harmful email addresses. When an email is received from a listed address, it is scanned for malicious content and treated according to the severity rating assigned to it.



To configure email scanning options:

1. From **Site Navigator**, double-click the Mac policy you want to configure.
2. From the left pane of the Policy Properties screen, expand **Email Alerts** and click **Scanning**.
3. To add emails to the list:
   a. From the right pane, click **Add...** to launch the Scanning Threat Detection Email Alert dialog.



b. Key in the potentially harmful email address in the **Email Address** filed.
c. From the **Severity** drop-down menu, select one of the following options:
   - Severe Risk
   - High Risk
   - Elevated Risk
   - Moderate Risk
   - Low Risk
d. Click **OK** to close the dialog and return to the Email Scanning screen.

4. To edit ratings and/or email addresses, select an entry from the list and click **Edit...**
5. To delete email addresses, select one or more address using Ctrl or Shift keys and click **Remove**.
6. Click **Apply** and **OK**.

12.6 — Configuring Allowed Threats Settings

VIPRE may detect items that you may consider non-threatening in your network, for which you would want to allow to run.

For example, Virtual Network Computing (VNC) and Remote Administrator (Radmin) may both be considered acceptable for use in your organization, but may be considered threats in another organization.

Allowing a threat enables you to specify these items to be ignored during scans.

To add an allowed threat:

1. Navigate to a **Site>Quarantine tab** or **Policy>Quarantine tab**.

Or:

1. Navigate to **Protected Computers>Agent Details>Scan History tab**.
2. Right-click on a threat, and select **Allow Threat**. The Allow Threat window displays.
3. Select the policies on which this threat should be allowed.
4. Click **OK**.
5. The allowed threat now displays in the Allowed Threats list for the policies you selected (**Policy Properties>Allowed Threats**).

13 — Protecting Android Devices

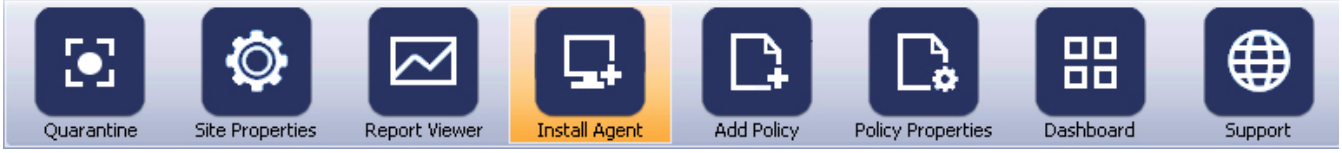
13.1 — Installing Agents on Android Devices

To protect Android devices, you must install **VIPRE Business Mobile Security** on each smart-phone or tablet you want to protect. The application can be downloaded from the Google Play Store, using the smart-phone or tablet device. A Google account is required to access the Google Play Store.

> **Note**: To create a Google account, go to https://accounts.google.com and click **SIGN UP** from the top-right corner of the page.

To install VIPRE Business Mobile Security:

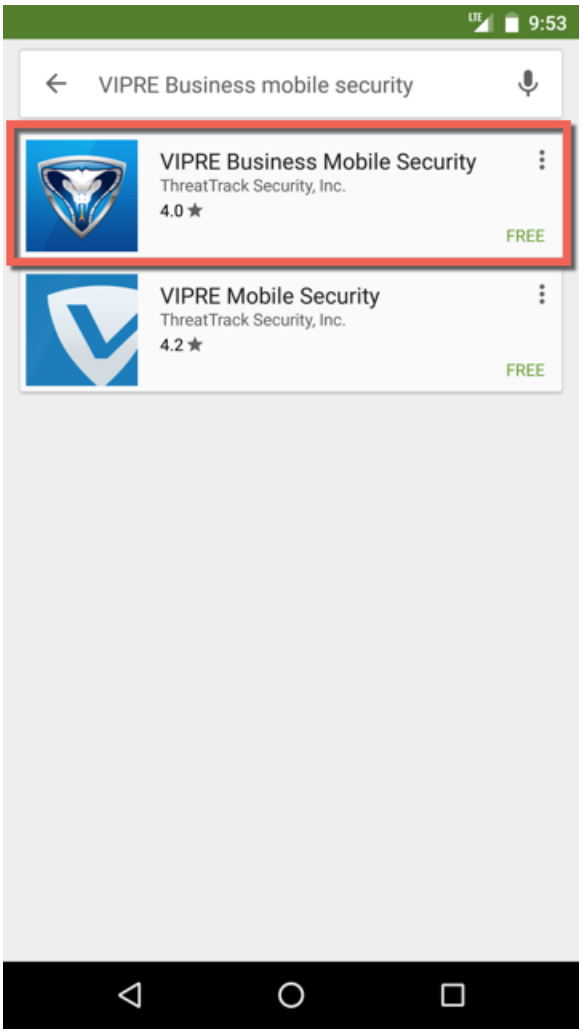
1. From **Site Navigator**, select an Android policy such as **Default for Android**.



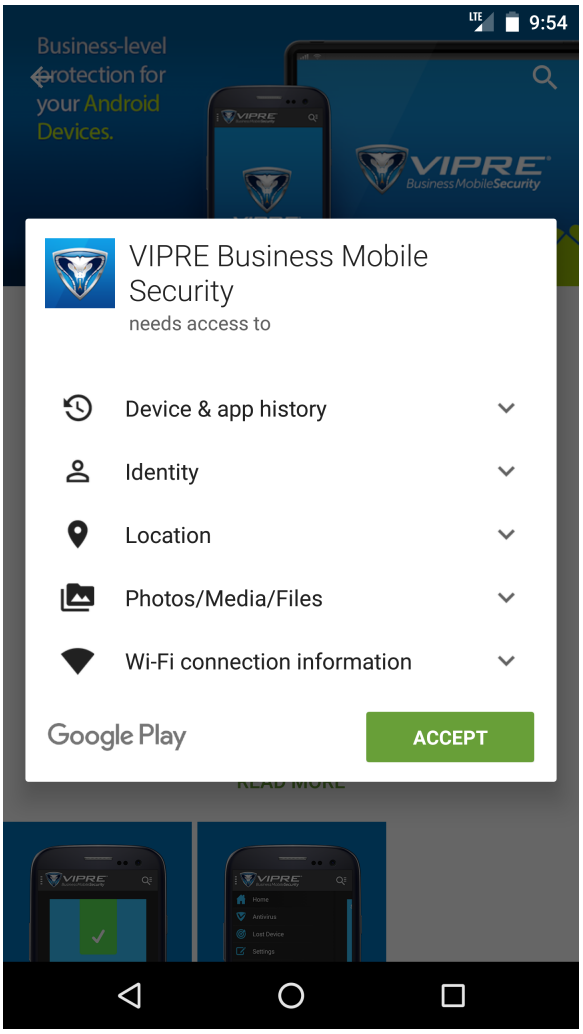
2. From the main menu, click **Install Agent**. This opens the Install Agent Wizard.
3. Choose **Android** from the device type drop-down and click **Continue**.
4. Choose a policy from the policy drop-down and click **Continue**.
5. Select **View installation instructions** and click **Continue**.
6. Take note of the **Access Code** that is provided. This code is used to activate VIPRE Business Mobile Security and also links the device to VIPRE Site Service. This enables you to manage the mobile device from the Management Console.
7. Click **Continue**; then, click **Finish**.

To install VIPRE Business Mobile Security on the Android device:

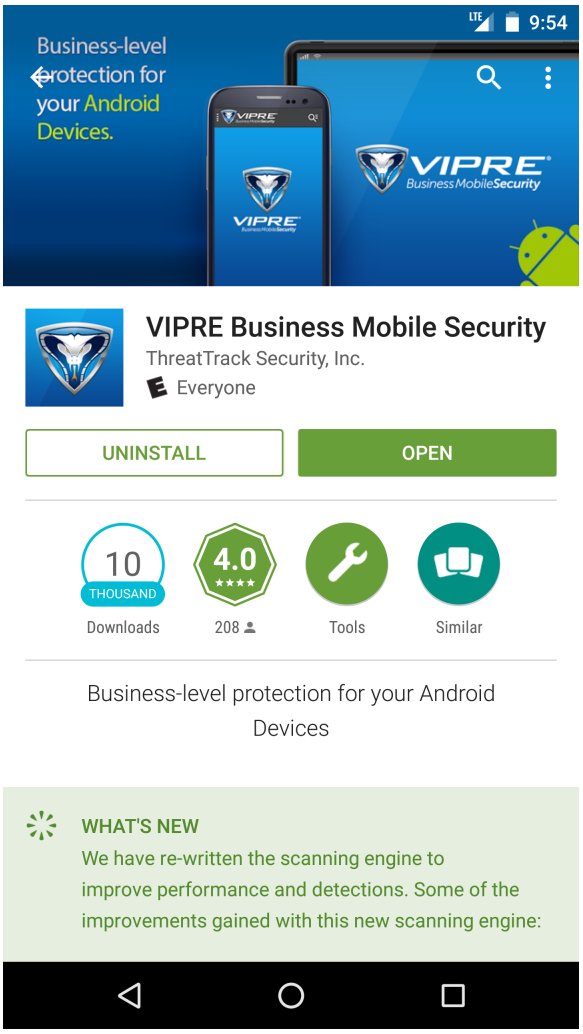
1. From the Android device, launch the Google Play Store and search for **VIPRE Business Mobile Security**.



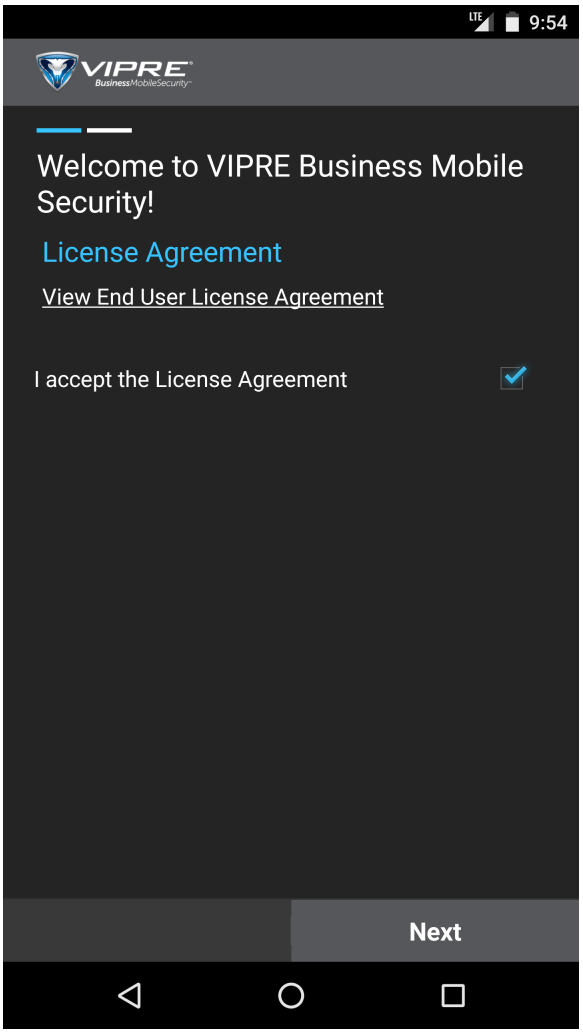
2. Select the highlighted item, then tap **INSTALL** to start downloading and installing the application.



3. To protect a device, VIPRE Business Mobile Security requires some permissions to be enabled. These are enabled automatically during the installation. Review the permissions and tap **ACCEPT** if you agree or tap back to stop the installation.



4. After the installation is complete, tap **OPEN** to launch VIPRE Business Mobile Security.



5. If you accept the terms of the EULA, tap **I accept the License Agreement**; then, tap **Next**.

6. Configure the following post installation settings:

   - **Enter your first and last name**: key in your first and last name.
   - **Enter your access code**: key in the access code that was recorded in Step 6.

Tap **Next**.

7. To manage and protect the device remotely, **Device Administrator** must be activated. This enables you to perform security actions on the device such as wiping it clean from data if it is stolen. If you accept, tap **Activate** or tap **Cancel** to stop the installation.
8. Tap **Finish** to start the application.

Note: After VIPRE Business Mobile Security is activated, the device is displayed under the **Protected Devices** tab of the policy. For information about managing Android devices, refer to Managing Android Agents.

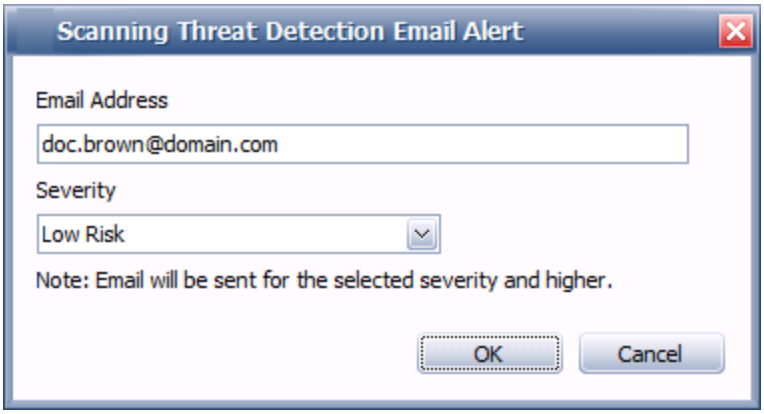
13.2 — Configuring Android Policies

13.2.1 — Configuring Email Alerts Settings

The Email Scanning screen enables you to assign severity ratings to potentially harmful email addresses. When an email is received from a listed address, it is scanned for malicious content and treated according to the severity rating assigned to it.

To configure email scanning options:

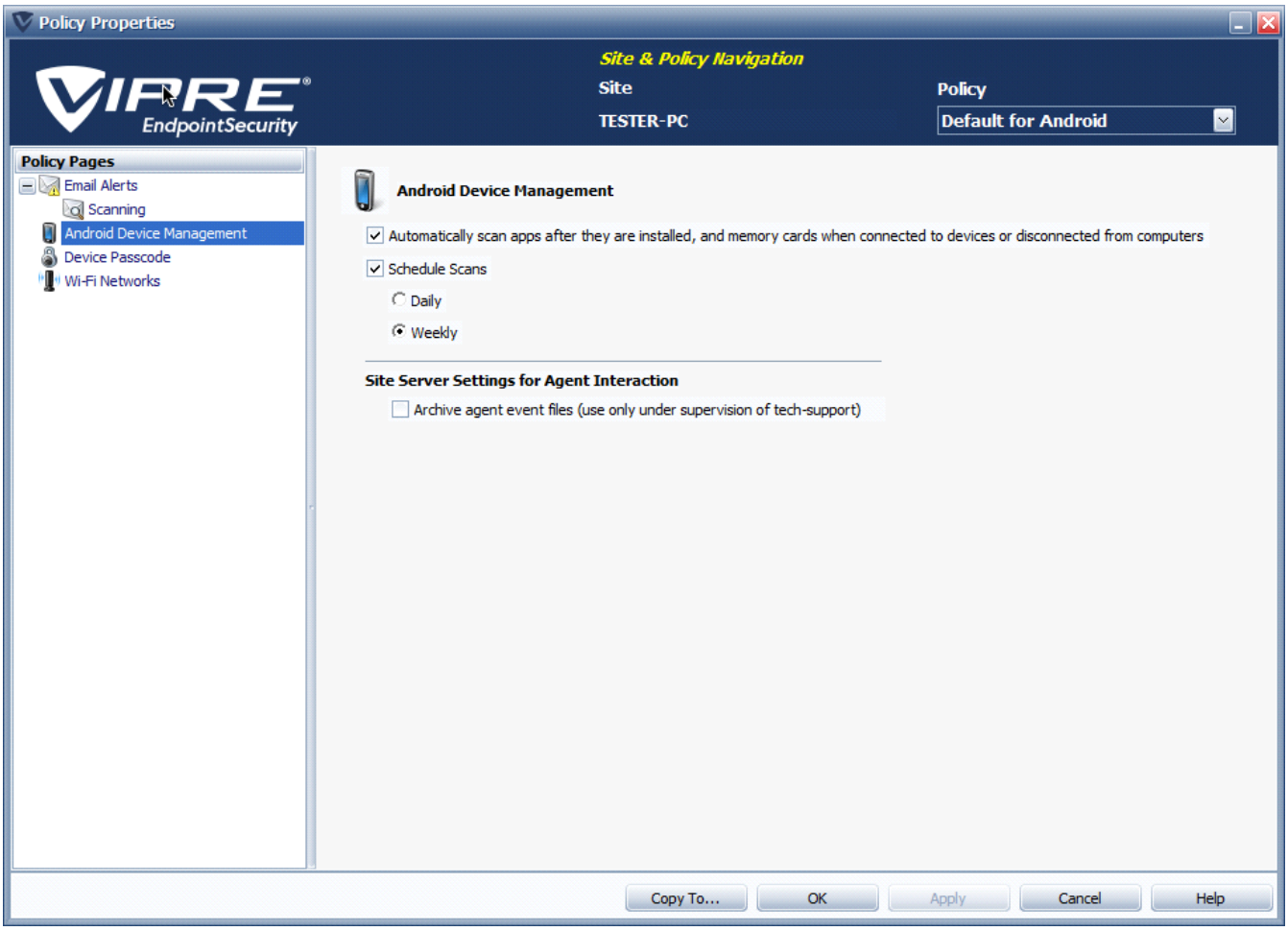
1. From **Site Navigator**, double-click the Android policy you want to configure.
2. From the left pane of the Policy Properties screen, expand **Email Alerts** and click **Scanning**.
3. To add emails to the list:
   a. From the right pane, click **Add...** to launch the Scanning Threat Detection Email Alert dialog.



   b. Key in the potentially harmful email address in the **Email Address** filed.
   c. From the **Severity** drop-down menu, select one of the following options:
      - Severe Risk
      - High Risk
      - Elevated Risk
      - Moderate Risk
      - Low Risk
   d. Click **OK** to close the dialog and return to the Email Scanning screen.
4. To edit ratings and/or email addresses, select an entry from the list and click **Edit...**
5. To delete email addresses, select one or more address using Ctrl or Shift keys and click **Remove**.
6. Click **Apply** and **OK**.

13.2.2 — Configuring Device Management Settings

Device Management settings enable you to protect your Android device by running security scans according to a schedule or when triggered by an event.



To configure device management options:

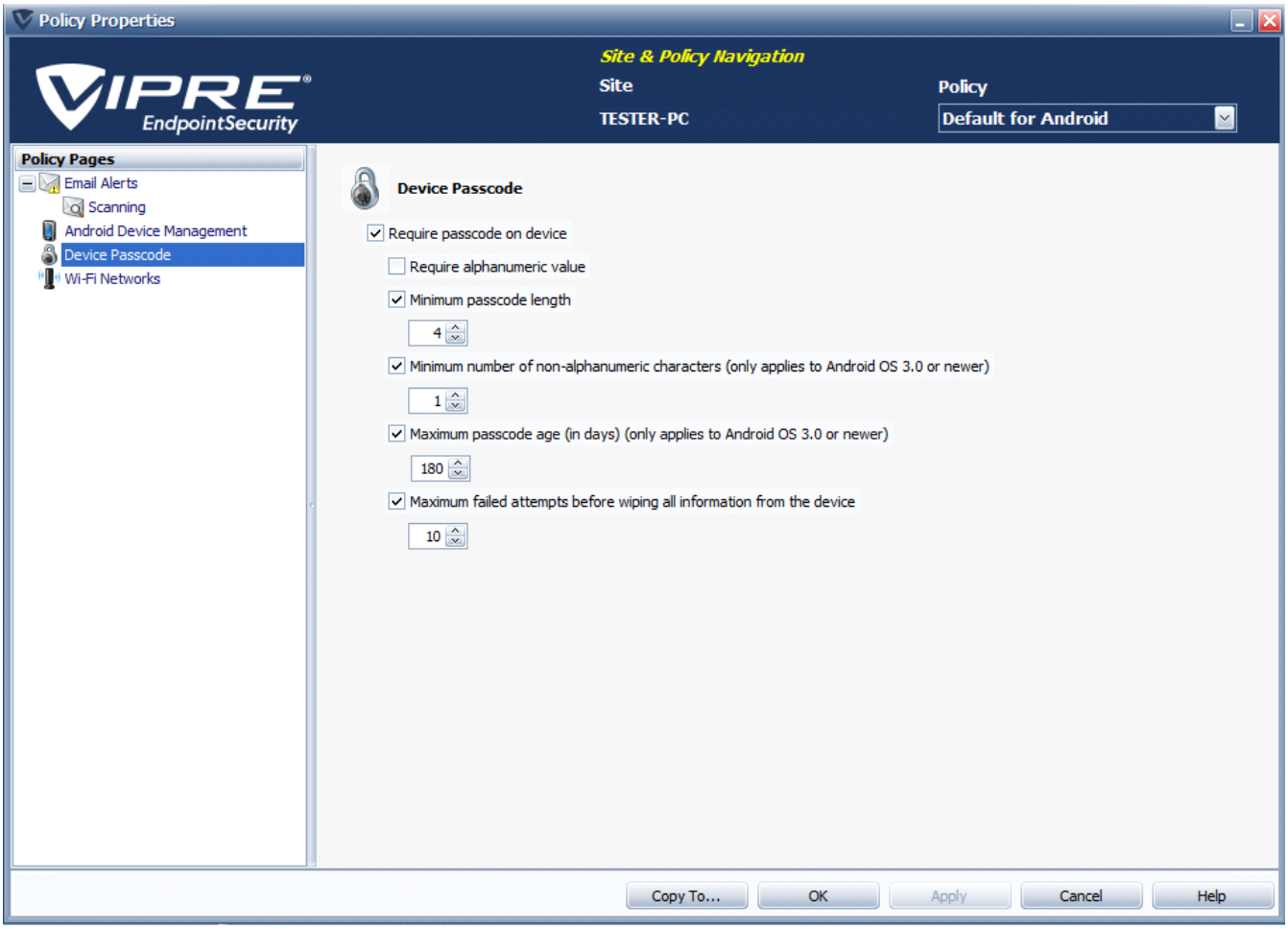
1. From **Site Navigator**, double-click the Android policy you want to configure.
2. From the left pane of the Policy Properties screen, click **Android Device Management**.
3. To scan applications or removable storage devices, select **Automatically scan apps after they are installed, and memory cards when connected to devices or disconnected from computers**.
4. To run scans according to a schedule, select **Schedule Scans** and choose from:
   - **Daily**: run security scans everyday
   - **Weekly**: run security scans on one day of the week.

Important: This following option (Step 5) must not be used unless instructed by a tech-support representative.

5. To troubleshoot problems coming from agents installed on Android devices, VIPRE allows you to gather all the activity logs in one location as a single file. Select **Archive agent event files** to enable log collection. Storing this file is useful for debugging and recommended to be used only when working with Technical Support.
6. Click **Apply** and **OK**.

13.2.3 — Configuring Device Passcode Settings

Device Passcode settings enable you to protect Android devices with an unlock passcode. From the Device Passcode screen, you can configure granular settings related to the passcode strength and complexity as well as other countermeasures that can prevent security breaches.



To configure Android device passcode settings:

1. From **Site Navigator**, double-click the Android policy you want to configure.
2. From the left pane of the Policy Properties screen, click **Device Passcode**.
3. Configure the options described below:

- **Require passcode on device**: enables passcode protection
- **Allow sequential or repeated characters in passcodes**: allows users to input passcodes that contain repeated or sequential characters, such as **3333** and **ABCD**

Note: Using passcodes that contain repeated or sequential characters jeopardizes the security of your device. Such passcodes are easier to hack than complex passcodes, which normally contain a mixture of random alphanumeric and non-alphanumeric characters.

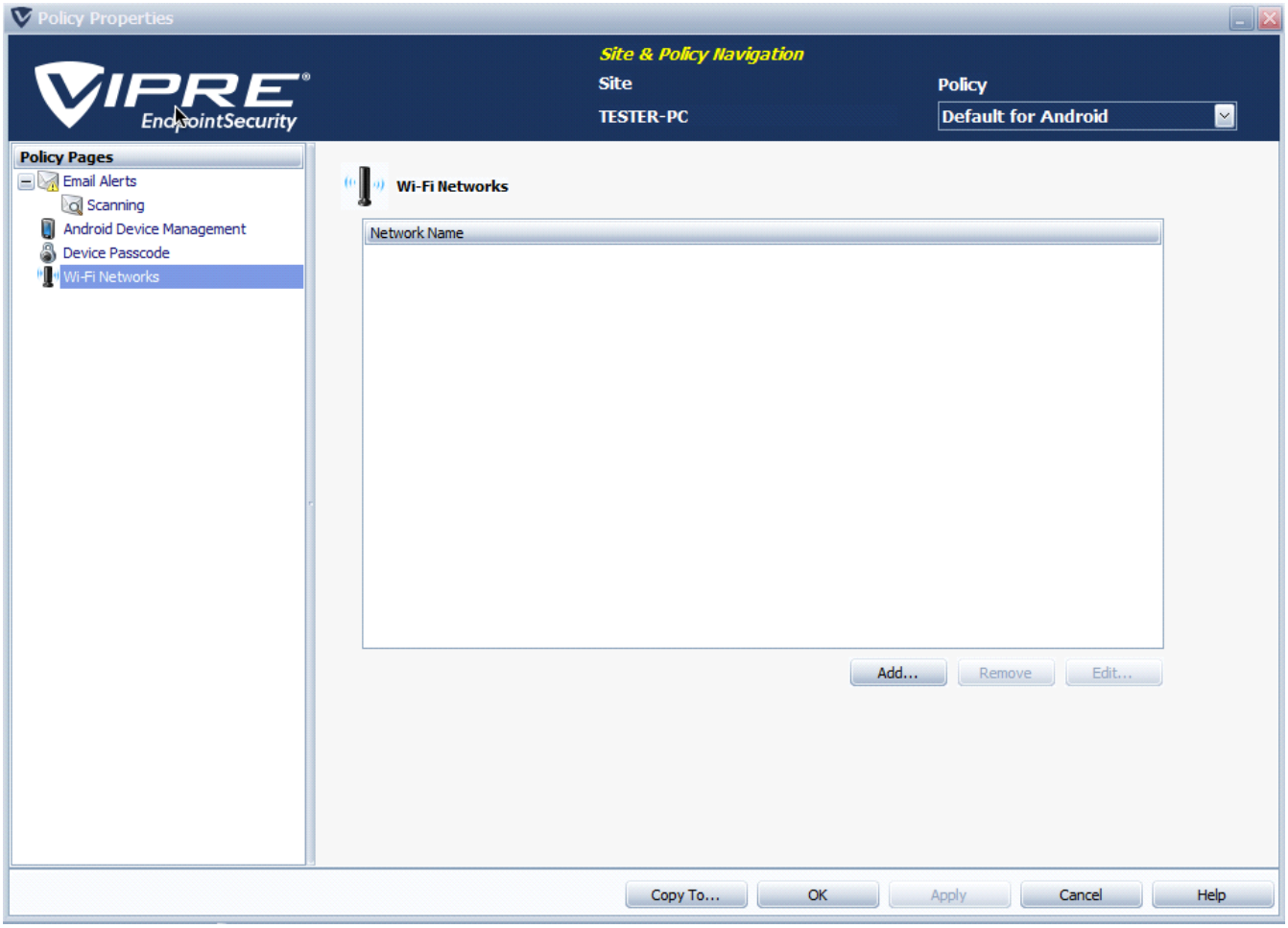
- **Require alphanumeric value**: forces device owners to use passwords that consists of alphabetical and numerical characters
- **Minimum passcode length**: key in the minimum number of characters the passcode must contain
- **Minimum number of non-alphanumeric characters**: key in the number of non-alphanumeric characters the passcode must contain. Non-alphanumeric characters include (but not limited to) **!**, **$**, **%**, **^**, **&**, *****, **(**, **)**, **@**, **#**
- **Maximum passcode age**: specify the number of days that a passcode is valid for. When the password expires, the user is automatically asked to key in a new one
- **Maximum failed attempts before wiping all information from the device**: deletes all the information on the iOS device, when the specified number of failed attempts is reached.

Important: When this option is enabled, ensure that the device owner is aware that the number of attempts to unlock the device is limited.

4. Click **Apply** and **OK**.

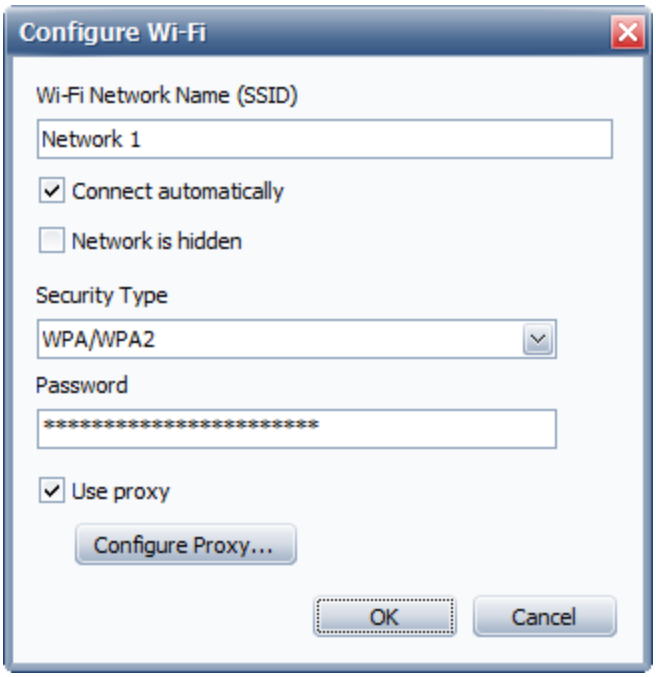
13.2.4 — Configuring Wi-Fi Network Settings

The Wi-Fi Networks screen is used to manage wireless networks accessible by Android devices that are managed by the Android security policy.



To configure Wi-Fi networks settings:

1. From **Site Navigator**, double-click the Android policy you want to configure.
2. From the left pane of the Policy Properties screen, click **Wi-Fi Networks**.
3. Click **Add...** to launch the **Configure Wi-Fi** dialog and add wireless networks to the list.



4. Configure the following options for each wireless network you want to add:
   a. **Wi-Fi Network Name (SSID)**: key in the network name/SSID
   b. **Connect automatically**: automatically connect devices to the network when it is in range
   c. **Network is hidden**: specifies that the Wi-Fi Network Name (SSID) configured is hidden from broadcast
   d. **Security Type**: select the password encryption type of the wireless network you are adding
   e. **Password**: key in the password used to gain access to the wireless network
   f. **Use proxy**: if the wireless network you are adding routes web requests through a proxy server, select this option and click **Configure Proxy...**, to specify the proxy server address, port and optionally, authentication credentials.
   g. Click **OK** to close the dialog and return to the Wi-Fi Networks screen.
5. To edit network settings, select the network and click **Edit...**
6. To delete networks, select one or more network using Ctrl or Shift keys and click **Remove**.
7. Click **Apply** and **OK**.

13.3 — Managing Android Devices

13.3.1 — Android Device Right-Click Menu

The VIPRE Management Console enables you to interact with Android mobile devices, even if they are outside the network (in different geographical areas). This can be done from the **Protected Devices** tab of a selected Android policy. Through the right-click menu, you are able to view and edit device details, as well as perform security actions when device security is breached or even if the device is stolen.

To interact with Android agents:

1. From **Site Navigator**, select the Android policy that has the agents you want to manage.
2. From the **Protected Devices** tab, select one or more agent(s). Use **Ctrl** or **Shift** for multiple

selections.

3. Right-click one of the selected agent(s) and select any of the following options:

- **Refresh**: select to refresh the data on the screen.

- **Print\Email\Export**: select to print, email, or export the entire contents of the grid. Once selected, a preview pane displays how the grid will be printed. From the preview pane, you can modify the background (including the color or watermark), change the print settings, export the grid as a PDF document, and send it via email in any of several formats, including PDF, MHT, RTF, Excel, CSV, TXT, or an image file.

Note: You can select the columns that will display and in what order before printing, emailing, or exporting.

- **Expand All**: select to expand the outline and see more entries.
- **Collapse All**: select to collapse the outline and see fewer entries.

- **Agent Details**: select to display Agent Details.
- **Edit Note**: click to display a text box to enter a note for selected agent. You can only enter a note for one agent at a time.

- **Lost Device...**: opens the Lost Device tab to perform security operations. For more information, refer to Lost Device Tab.
- **Deactivate Device**: deactivates the Android device and removes it from the Management Console. To add the device again, the user must reenter the access code.

- **Add and Install Agent(s)**: select to display the **Installing VIPRE to your Computers** dialog box and add agents to the Agent Catalog and install them on computers.

- **Grid Colors**: select to open the Agent Grid Colors dialog box where you can modify the colors in the grid.

13.3.2 — Android Agent Environment

Through the **Agent Environment** tab you can display Android device information, agent status, agent software and threat definition information.

Note: You can right-click from anywhere on the tab to **Refresh** the displayed data.

To access the Android Agent Environment tab:

1. From **Site Navigator**, select the Android policy that has the agents you want to manage.
2. From the **Protected Devices** tab, select one or more agent(s) using the **Ctrl** or **Shift** keys.
3. Right-click and select **Agent Details...**
4. From the **Agent Environment** tab, you can view the following information:

   Environment

   The Environment section lists specific policy and agent information:

- **Policy**: displays the policy to which the agent is assigned.
- **OS Version**: displays the version number of the Android OD installed on the device.
- **Date Added**: displays the date the agent was added to the device.
- **Device Model**: displays the model of the device running the agent.

Status

The Status section lists the last statuses, communications, scans, and any deferred work for the agent:

- **Last Contact**: displays the date of the last heartbeat from the agent.
- **Last Threat Detection**: displays the date of last threat found, regardless of severity.
- **Last Refreshed**: displays the most recent date and time that the agent communicated with VIPRE Site Service.

Software and Definitions

The Software section lists agent version information:

- **Agent Software Version**: displays the Agent version number.
- **Threat Database Version**: displays the version of the threat database.

Note

The Note box displays the user entered notes for this agent.

To add a note for an agent, right-click on the agent that you want to enter a note for and select **Edit Note**.

5. Click **OK** to close the Agent Details dialog.

13.3.3 — Last Scan Summary Tab

The **Last Scan Summary** tab provides you with a summary of scan information obtained from the last scan performed on the Android device.

> **Note:** You can right-click from anywhere on the tab to **Refresh** the displayed data.

To access the Android Last Scan Summary tab:

1. From **Site Navigator**, select the Android policy that has the agents you want to manage.
2. From the **Protected Devices** tab, select one or more agent(s) using the **Ctrl** or **Shift** keys.
3. Right-click and select **Agent Details...**
4. Click Last Scan Summary tab to display the following information:

Last Severity Level Detection

The Last Severity Level Detection section lists when threats of five varying severity levels were last detected by this agent.

Last Scan Summary

The Last Scan Summary section lists specific information about the last scan completed, including scan duration, threats found, and all processes and files scanned:

- **Last Scan Date**: displays the date and time of the last scan performed.
- **Duration**: displays the duration of the last scan performed.
- **Highest Risk**: displays the most severe threat level found during the last scan.
- **Threats Found**: displays the total number of threats found during the last scan.
- **Severe Found**: displays the number of *Severe* threats found on the agent machine during the last scan.
- **High Found**: displays the number of *High* threats found on the agent machine during the last scan.
- **Elevated Found**: displays the number of *Elevated* threats found on the agent machine during the last scan.
- **Moderate Found**: displays the number of *Moderate* threats found on the agent machine during the last scan.
- **Low Found**: displays the number of *Low* threats found on the agent machine during the last scan.
- **Traces**: The Traces area contains the traces **Scanned** and traces **Found** columns that correspond to specific scanned areas of the agent machine. The numbers in the **Scanned** column simply show the number of items in that area that were scanned during the last scan, while the **Found** column shows the number of threat traces that were found. The Total shows the total number of malware traces that were scanned and found on the agent machine during the last scan.

5. Click **OK** to close the Agent Details dialog.

13.3.4 — Scan History Tab

The **Scan History** tab **Scan History** displays a history of all scans performed, and the results from those scans for that workstation. The length of time items remain in the scan history is admin-defined.

> **Note:** The column headings are dynamic, allowing you to move their order and sort by a category within that column. Click the filter icon  on a column heading to select a filtering option. See Filtering Views for more information on using the available filters.

To access the Scan History tab:

1. From **Site Navigator**, select the Android policy that has the agents you want to manage.
2. From the **Protected Devices** tab, select one or more agent(s) using the **Ctrl** or **Shift** keys.
3. Right-click and select **Agent Details...**
4. Click the **Scan History** tab, to view the following information:

Columns

Scan Date: displays the date and time the scan was performed.

- **Agent**: displays the agent version number.
- **Threat DB**: displays the Threat database version number.
- **Total Found**: displays the total number of spyware and other unwanted applications and artifacts found on the agent machine during the last scan.
- **Report Only**: displays the number of threats in which the only action taken by the system is to report the

threat.

- **Type**: displays the type of scan that was performed.

Expandable Rows

Entries in the **Scan History** tab are also expandable down to two different levels. Clicking the plus sign next to a scan date displays a sub-list detailing threats found.

The columns in the first sub-table displayed include:

- **Name**: displays the name of the particular spyware or other unwanted applications or artifacts found.
- **Category**: displays the type of spyware or other unwanted applications or artifacts.
- **Action**: displays action taken regarding the threat.
- **Severity**: displays the level of severity of the threat found. Severity levels are measured as Low, Moderate, Elevated, High, or Severe.
- **Threat ID**: displays the unique ID number of the threat.
- **Type**: displays the type of threat. For example, Adware.

The second level of expansion is for each particular threat. The columns in the second sub-table displayed include:

- **Type**: displays the specific artifact type found (such as files, registry items, and so forth).
- **Data**: displays specific location information about the artifact.

As with the main Scan History table, all columns are configurable, can be sorted, and can be filtered.

5. Click **OK** to close the Agent Details dialog.

Scan History Right-Click Menu

Right-click anywhere in the tab to display the right-click menu. The following options are available:

- **Refresh**: select to refresh the data on the screen.

- **Print\Email\Export**: select to print, email, or export the entire contents of the grid. Once selected, a preview pane displays how the grid will be printed. From the preview pane, you can modify the background (including the color or watermark), change the print settings, export the grid as a PDF document, and send it via email in any of several formats, including PDF, MHT, RTF, Excel, CSV, TXT, or an image file.

Note: You can select the columns that will display and in what order before printing, emailing, or exporting.

- **Expand All**: select to expand the outline and see more entries.
- **Collapse All**: select to collapse the outline and see fewer entries.

13.3.5 — Lost Device Tab

The **Lost Device** tab enables you to perform security operations on lost or stolen devices. Through this tab you are able to:

- **Sound Alarm**: causes the device to make a loud noise for 2 minutes. This can aid in locating a lost device.

- **Get Location**: opens a browser window to display the last known physical location of the device via Google Maps.
- **Lock Device**: sends a command to the device to force it to lock. This helps prevent unauthorized people from accessing the lost or stolen device.
- **Wipe**: erases all data from the smart-phone or tablet. This yields great security control over stolen devices that contain sensitive information.
- **Clear Passcode**: removes the access passcode from the device, allowing you to gain access.

Note: For these features to work, **Device Administrator** must be activated on the device during the initial setup of VIPRE Business Mobile Security. For more information, refer to Installing Agents on Android Devices.

To access the Lost Device tab:

1. From **Site Navigator**, select the iOS policy that has the agents you want to manage.
2. From the **Protected Devices** tab, select one or more agent(s) using the **Ctrl** or **Shift** keys.
3. Right-click and select **Agent Details...**
4. Click **Lost Device** tab and perform any of the following operations:

Sound Alarm

a. Click **Sound Alarm**.
b. Click **Yes** to confirm.

Note: A command is sent to sound an alarm on the device for a 2 minute period.

Get Location

a. Click **Get Location**. VIPRE will attempt to determine the physical location of the device.
b. Click **View location on map**. A browser window will open to Google Maps, displaying the last known location of the device.

Note: A command is sent to the device to determine its physical location.

Lock Device

a. Click **Lock Device**.
b. Click **Yes** to confirm.

Note: A command is sent to lock the device.

Wipe

a. Click **Wipe**.

Important: This operation cannot be stopped or undone.

b. Click **OK** to confirm.

Note: Information stored on the device is erased and the device is restored to default state.

5. Click **OK** to close the Agent Details dialog.

Clear Passcode

Click **Clear Passcode**. The existing passcode is immediately removed from the device.

Important: This operation cannot be stopped or undone.

14 — Protecting iOS Devices

14.1 — Installing Agents on iOS Devices

iOS device security can be managed by VIPRE Business through **VIPRE Business Mobile Security**. The application must be installed on iOS devices for remote security management. Through VIPRE Business Mobile Security, you can enforce security policies on iOS devices as well as perform security operations, directly from the VIPRE Business Management Console.

To install VIPRE Business Mobile Security:

1. From **Site Navigator**, select an iOS policy such as **Default for iOS**.
2. From the main menu, click **Install Agent**. This opens the iOS Access Code dialog.
3. Take note of the **Access Code** that is displayed on the right hand side of the dialog. This code is used to activate VIPRE Business Mobile Security and also links the device to VIPRE Site Service. This enables you to manage the mobile device from the Management Console.

Note: Follow on-screen instructions to download and complete the installation.

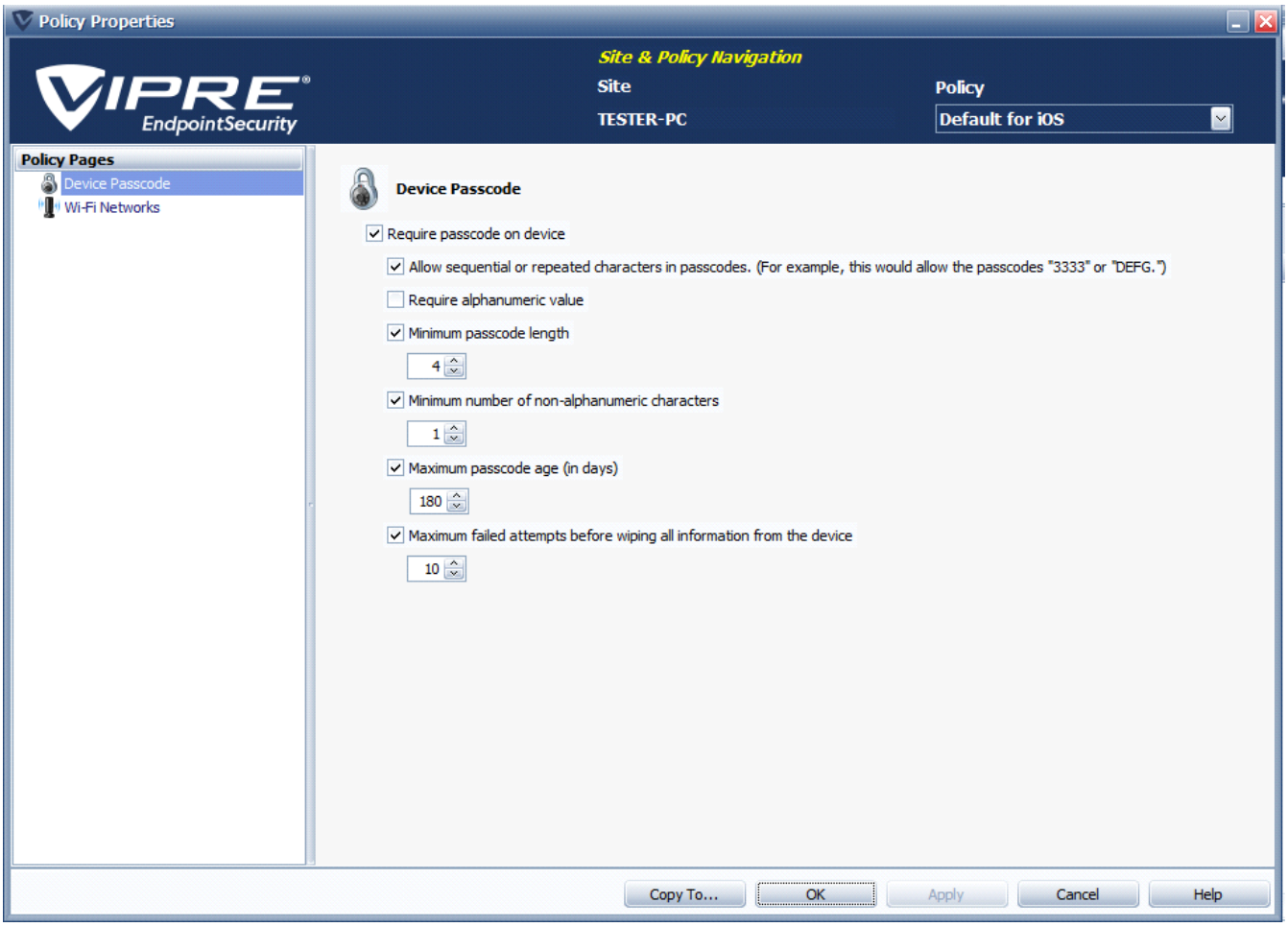
4. Once VIPRE is installed, launch the application and click Sign Up. Configure the following options:
   - **Name**: Key in your full name
   - **Access ID**: key in the access code that was recorded in Step 3.

Note: An Internet connection is required so that VIPRE Business Mobile Security synchronizes with VIPRE Business Management Console and the device can be managed remotely. For information about managing iOS device security, refer to Managing iOS devices.

14.2 — Configuring iOS Policies

14.2.1 — Configuring Device Passcode Settings

Device Passcode settings enable you to protect iOS devices with an unlock passcode. From the Device Passcode screen, you can configure granular settings related to the passcode strength and complexity as well as other countermeasures that can prevent security breaches.



To configure iOS device passcode settings:

1. From **Site Navigator**, double-click the iOS policy you want to configure.
2. From the left pane of the Policy Properties screen, click **Device Passcode**.
3. Configure the options described below:

   - **Require passcode on device**: enables passcode protection
   - **Allow sequential or repeated characters in passcodes**: allows users to input passcodes that contain repeated or sequential characters, such as **3333** and **ABCD**

Note: Using passcodes that contain repeated or sequential characters jeopardizes the security of your device. Such passcodes are easier to hack than complex passcodes, which normally contain a mixture of random alphanumeric and non-alphanumeric characters.

   - **Require alphanumeric value**: forces device owners to use passwords that consists of alphabetical and numerical characters
   - **Minimum passcode length**: key in the minimum number of characters the passcode must contain

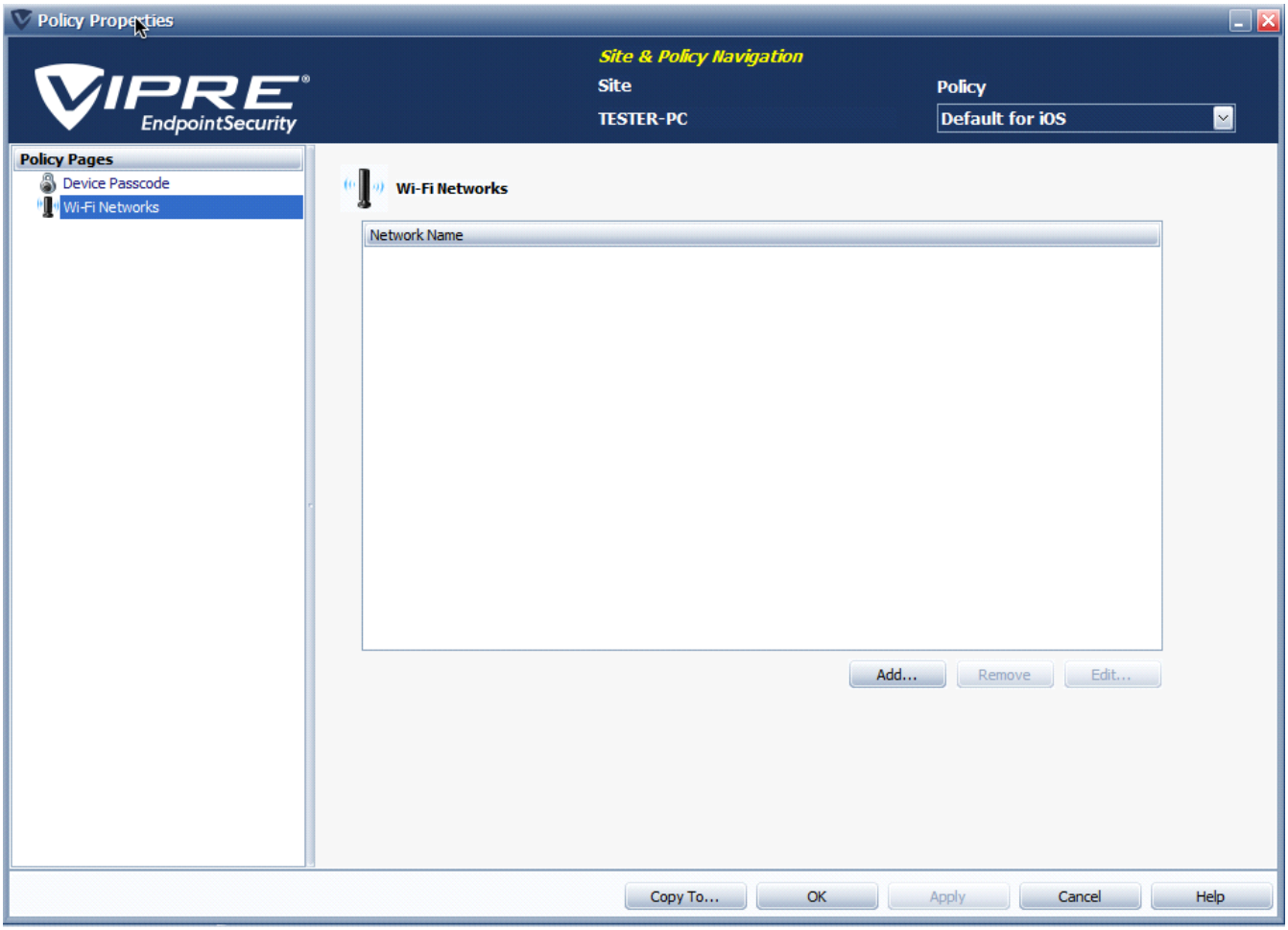
- **Minimum number of non-alphanumeric characters**: key in the number of non-alphanumeric characters the passcode must contain. Non-alphanumeric characters include (but not limited to) **!**, **$**, **%**, **^**, **&**, ***, **(**, **)**, **@**, **#**
- **Maximum passcode age**: specify the number of days that a passcode is valid for. When the password expires, the user is automatically asked to key in a new one
- **Maximum failed attempts before wiping all information from the device**: deletes all the information on the iOS device, when the specified number of failed attempts is reached.

Important: When this option is enabled, ensure that the device owner is aware that the number of attempts to unlock the device is limited.

4. Click **Apply** and **OK**.

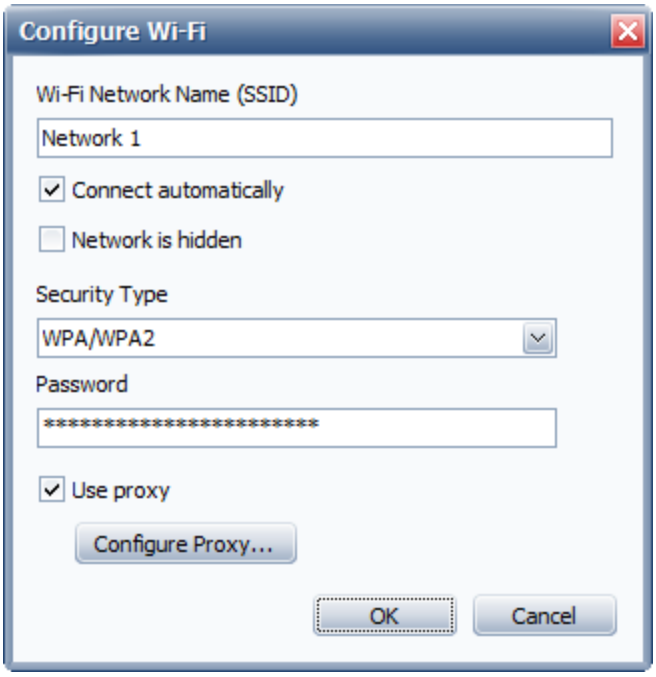
14.2.2 — Configuring Wi-Fi Network Settings

The Wi-Fi Networks screen is used to manage wireless networks accessible by iOS devices that are managed by the iOS security policy.



To configure Wi-Fi networks settings:

1. From **Site Navigator**, double-click the Mac policy you want to configure.
2. From the left pane of the Policy Properties screen, click **Wi-Fi Networks**.
3. Click **Add...** to launch the **Configure Wi-Fi** dialog and add wireless networks to the list.



4. Configure the following options for each wireless network you want to add:
   a. **Wi-Fi Network Name (SSID)**: key in the network name/SSID
   b. **Connect automatically**: automatically connect devices to the network when it is in range
   c. **Network is hidden**: specifies that the Wi-Fi Network Name (SSID) configured is hidden from broadcast
   d. **Security Type**: select the password encryption type of the wireless network you are adding
   e. **Password**: key in the password used to gain access to the wireless network
   f. **Use proxy**: if the wireless network you are adding routes web requests through a proxy server, select this option and click **Configure Proxy...**, to specify the proxy server address, port and optionally, authentication credentials.
   g. Click **OK** to close the dialog and return to the Wi-Fi Networks screen.
5. To edit network settings, select the network and click **Edit...**
6. To delete networks, select one or more network using Ctrl or Shift keys and click **Remove**.
7. Click **Apply** and **OK**.

14.3 — Managing iOS Devices

14.3.1 — iOS Device Right-Click Menu

The VIPRE Management Console enables you to interact with iOS mobile devices, even if they are outside the network (in different geographical areas). This can be done from the **Protected Devices** tab of a

selected iOS policy. Through the right-click menu, you are able to view and edit device details, as well as perform security actions when device security is breached or even if the device is stolen.

To interact with iOS agents:

1. From **Site Navigator**, select the iOS policy that has the agents you want to manage.
2. From the **Protected Devices** tab, select one or more agent(s). Use **Ctrl** or **Shift** for multiple selections.
3. Right-click one of the selected agent(s) and select any of the following options:

- **Refresh**: select to refresh the data on the screen.

- **Print\Email\Export**: select to print, email, or export the entire contents of the grid. Once selected, a pre-view pane displays how the grid will be printed. From the preview pane, you can modify the background (including the color or watermark), change the print settings, export the grid as a PDF document, and send it via email in any of several formats, including PDF, MHT, RTF, Excel, CSV, TXT, or an image file.

Note: You can select the columns that will display and in what order before printing, emailing, or exporting.

- **Expand All**: select to expand the outline and see more entries.
- **Collapse All**: select to collapse the outline and see fewer entries.

- **Agent Details**: select to display Agent Details.
- **Edit Note**: click to display a text box to enter a note for selected agent. You can only enter a note for one agent at a time.

- **Lost Device...**: opens the Lost Device tab to perform security operations. For more information, refer to Lost Device Tab.
- **Deactivate Device**: deactivates the iOS device and removes it from the Management Console. To add the device again, the user must reenter the access code.

- **Add and Install Agent(s)**: select to display the **Installing VIPRE to your Computers** dialog box and add agents to the Agent Catalog and install them on computers.

- **Grid Colors**: select to open the Agent Grid Colors dialog box where you can modify the colors in the grid.

14.3.2 — Lost Device Tab

The **Lost Device** tab enables you to perform security operations on lost or stolen devices. Through this tab you are able to:

- **Lock Device**: sends a command to the device to force it to lock. This helps prevent unauthorized people from accessing the lost or stolen device.
- **Wipe**: erases all data from the smart-phone or tablet. This yields great security control over stolen devices that contain sensitive information.
- **Clear Passcode**: removes the access passcode from the device, allowing you to gain access.

Note: For these features to work, **Device Administrator** must be activated on the device during the initial setup of VIPRE Business Mobile Security. For more information, refer to Installing Agents on iOS Devices.

To access the Lost Device tab:

1. From **Site Navigator**, select the iOS policy that has the agents you want to manage.
2. From the **Protected Devices** tab, select one or more agent(s) using the **Ctrl** or **Shift** keys.
3. Right-click and select **Agent Details...**
4. Click **Lost Device** tab and perform any of the following operations:

Lock Device

a. Click **Lock Device**.
b. Click **Yes** to confirm.

Note: A command is sent to lock the device.

Wipe

a. Click **Wipe**.

Important: This operation cannot be stopped or undone.

b. Click **OK** to confirm.

Note: Information stored on the device is erased and the device is restored to default state.

5. Click **OK** to close the Agent Details dialog.

Clear Passcode

Click **Clear Passcode**. The existing passcode is immediately removed from the device.

Important: This operation cannot be stopped or undone.

15 — Protecting Hyper-V Environments

15.1 — Site Navigator

The **Site Navigator** has a Hyper-V policies section that displays existing Hyper-V policies. These policies are used to apply settings to the Hyper-V agent which protects Hyper-V Virtual Machines.

The right-click menu for the Hyper-V Policies group contains the following items:

- **Host Agent Commands**: Commands that are performed by the Hyper-V agent software, including:
  - **Purge Deferred Work Item(s)**: Purges all work waiting to be sent to the agent from the VSS.
  - **Say Hello**: Forces an agent to say hello. This can be used for agents that didn't get an update to pick up the deferred work.
  - **Check for Policy Update**: Makes the agent check that it has the latest update to its assigned policy.
  - **Issue Remote Restart Command**: Used when an agent is showing via the console that it needs to reboot, and for non-agent related issues. It is not required that an agent exist on the remote computer for the restart command to be issued.
- **Host Updates**: The Hyper-V agent can get updates for itself and its threat definitions via:
  - **Check for Threat Definitions Updates**: Checks for and (if available) retrieves the latest threat definitions for the agent(s) on all policies in the Hyper-V policies group.
  - **Force Full Threat Definitions Update**: Forces all Hyper-V agents to get the full threat database. This takes longer than a definition update.
- **Refresh**: Polls the VSS and refresh the data (hosts and VMs) on the screen.
- **Expand Group**: Expands the Hyper-V Policies group on the Site Navigator.
- **Collapse Group**: Collapses the Hyper-V Policies group on the Site Navigator.
- **Add Policy**: Brings up a dialog that allows the admin to add a new policy to the Hyper-V Policies group.
- **Import Policy**: Allows the admin to import a policy from an exported XML file.

The right-click menu for individual Hyper-V policies contains the following items:

- VM Commands:
  - **Purge Deferred Work Item(s)**: Purges all work waiting to be sent to the VMs under the selected policy from the VSS.
  - **Say Hello**: Forces all VMs under the selected policy to say hello. This can be used for VMs that didn't get an update to pick up the deferred work.
  - **Check for Policy Updates**: Causes VMs under the selected policy to check that they have the latest update to their assigned policy.
  - **Issue Remote Restart Command**: Used when a VM or its host is showing that it needs to Reboot in the console, or for non-agent related issues. This command does not require an agent to exist on the remote computer for the restart command to be issued.
- Host Updates:
  - **Check for Threat Definitions Updates**: Checks for—and retrieves, if available—the latest threat definitions for the agent(s) under the selected Hyper-V policy.
  - **Force Full Threat Definitions Update**: Forces all agents under the selected Hyper-V policy to retrieve the full threat database. This takes longer than a definition update.
- **Copy Policy**: Allows for the selected policy to be cloned, with all of its settings intact.
- **Delete Policy**: Deletes the selected policy (not available on “Default for Hyper-V” policy).
- **Rename Policy**: Renames the selected policy (not available on “Default for Hyper-V” policy).

- **Export Policy**: Exports the policy, with all its settings intact, to an XML document.
- **Properties**: Opens the selected policy's property dialog, where all of its settings can be changed.

15.2 — Creating a Hyper-V MSI Installer Package

Host computers should be protected with a VIPRE Business agent, as the Hyper-V agent only protects guest operating systems and does not scan the host.

15.2.1 — Installing / Uninstalling the Hyper-V agent on the Host to protect VMs

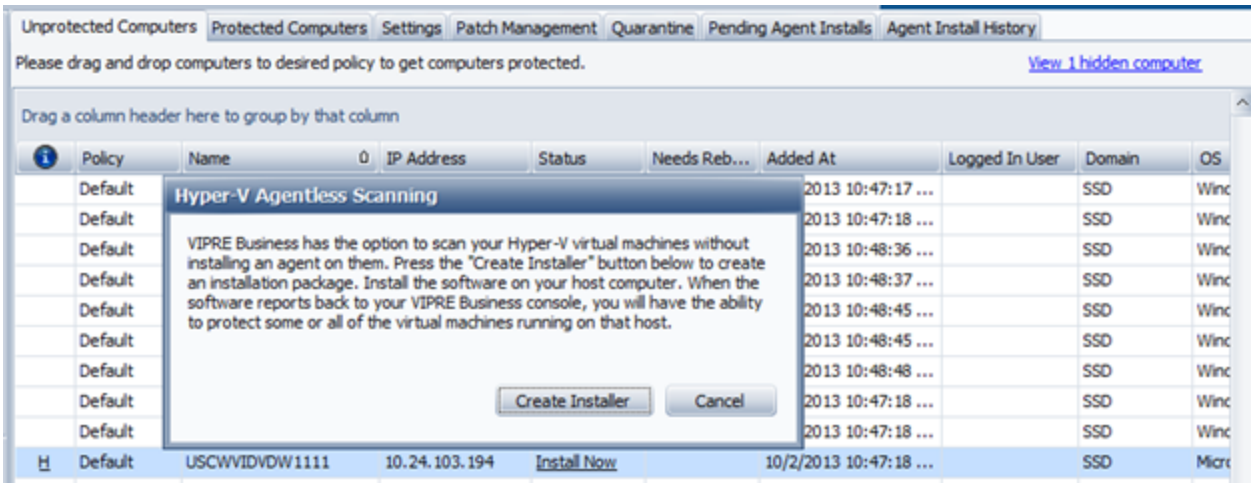
To Install the VIPRE Hyper-V agent on a host computer, follow these steps:

- From the agent grid, click the "H" host indicator in the information column
- Choose the "Agent Installation" menu
- Select "Create Hyper-V MSI Package…"

Or

- Click on "Install Agent" with a Hyper-V policy
- Or the Hyper-V policy group highlighted in the "Site Navigator".

You are presented with the dialog box shown below.



1. Press the **Create Installer** button.
2. You are asked to save the installation file. The default name and location can be accepted.
3. Transfer the saved installation file to the Hyper-V host computer.
4. Double click on the installation file to install the Hyper-V agent onto the host computer. Accept the default value for the computer to which the Hyper-V agent communicates.
5. Once installation is complete, the hosted guest computers shows up in the Unprotected Computers tab for the "Default for Hyper-V" policy in the VIPRE Business console.

Note: To update a Hyper-V agent on a host computer, follow the same steps outlined for installation. This installs the new Hyper-V agent on the host computer without changing the status of your guest computers.

To Uninstall the Hyper-V agent from the host computer:

1. Go to “Control Panel/Programs and Features” on the host computer
2. Select “VIPRE Hyper-V Agent” and press the “Uninstall” button.

This returns any guest computers to an unprotected status and put them back in the “Default” policy in the Windows group.

> **Note:** In evaluation mode, you can have only 1 Hyper-V agent installed.

15.3 — How Host and VM computers are displayed

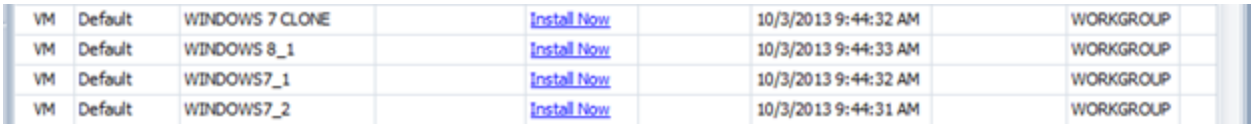
15.3.1 — With no agent installed:

If computer discovery and computer inquiry are turned on and the appropriate credentials have been entered, VIPRE Business can determine

- If a computer hosting guests in Hyper-V is a host, and
- If the guest computers are virtual machines.

These computers are displayed in the Unprotected Computers tab. Host computers are indicated by an “H” in the information column and guest computers are indicated by “VM” in the information column.

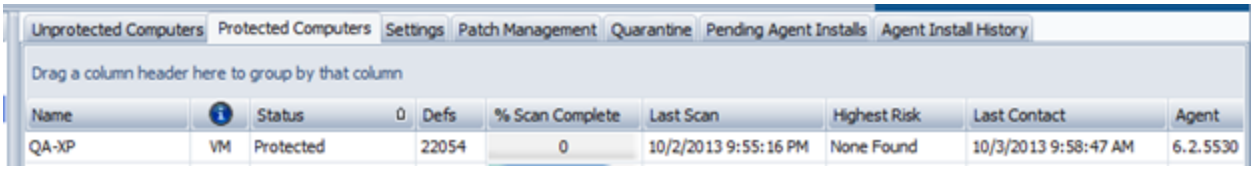
Screenshot 9: Host computer - No agent



Screenshot 10: Guest computers - No agents

15.3.1.1 — With VIPRE Business agent(s) installed:

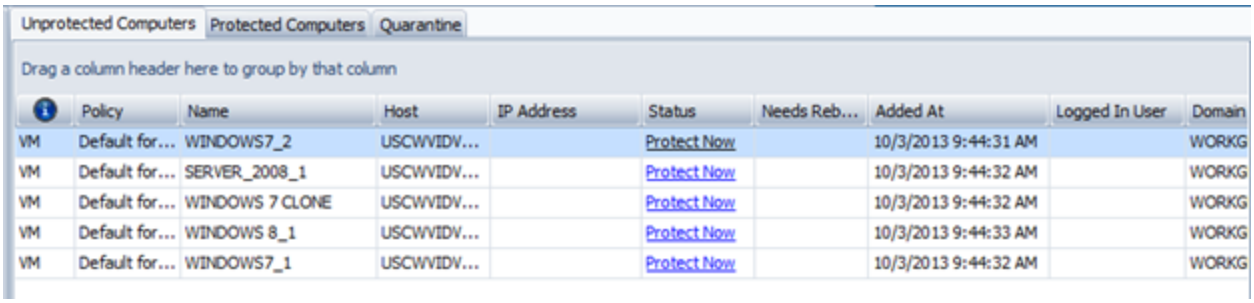
When a VIPRE Business agent is installed on either a host or a guest computer, they are shown in the Protected Computers grid just like any other computer protected by a VIPRE Business agent.



Screenshot 11: Guest Computer - VIPRE Business agent installed

15.3.1.2 — With Hyper-V Agent installed on the Host:

When a VIPRE Hyper-V agent has been installed on a host machine, all guest computers are moved to the Hyper-V Policies group. Initially, guests are placed in the "Default for Hyper-V" policy and all guest computers are unprotected.



Screenshot 12: Unprotected Guest Computers - Hyper-V agent on the host

15.4 — Protecting the Host with VIPRE Business

Host computers should be protected with a VIPRE Business agent, as the Hyper-V agent only protects guest operating systems and does not scan the host.

15.4.1 — Installing / Uninstalling the Hyper-V agent on the Host to protect VMs

To Install the VIPRE Hyper-V agent on a host computer, follow these steps:

1. From the agent grid, click the **H** host indicator in the information column
2. Choose the **Agent Installation** menu
3. Select **Create Hyper-V MSI Package…**

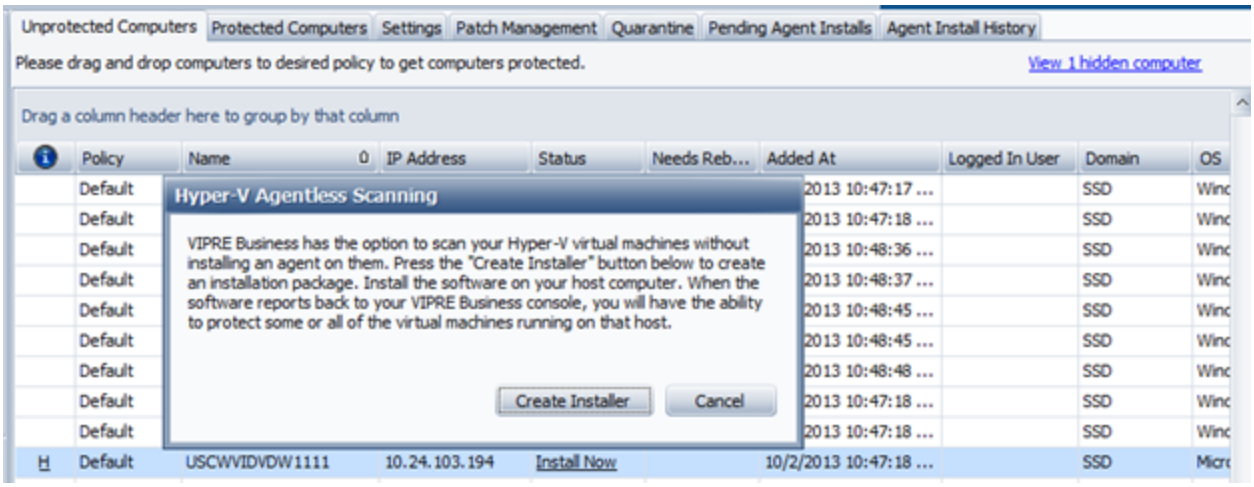
Or

1. Click on "Install Agent" with a Hyper-V policy

Or

1. Click on the **Hyper-V policy group** highlighted in the Site Navigator

You are presented with the dialog box shown below.



1. Click the **Create Installer** button.
2. You are asked to save the installation file. The default name and location can be accepted.
3. Transfer the saved installation file to the Hyper-V host computer.
4. Double click on the installation file to install the Hyper-V agent onto the host computer. Accept the default value for the computer to which the Hyper-V agent communicates.
5. Once installation is complete, the hosted guest computers shows up in the Unprotected Computers tab for the “Default for Hyper-V” policy in the VIPRE Business console.

Note: To update a Hyper-V agent on a host computer, follow the same steps outlined for installation. This installs the new Hyper-V agent on the host computer without changing the status of your guest computers.

To Uninstall the Hyper-V agent from the host computer:

1. Go to “Control Panel/Programs and Features” on the host computer
2. Select “VIPRE Hyper-V Agent” and press the “Uninstall” button.

This returns any guest computers to an unprotected status and put them back in the “Default” policy in the Windows group.

15.5 — Scanning VMs

15.5.1 — Reboot to remove malware

When a threat is detected during VIPRE Hyper-V agent scanning, the guest computer must be rebooted by the Hyper-V agent. The guest computer status on the Protected Computers tab is listed as “Needs Reboot”. Clicking “Needs Reboot” causes the guest computer to be rebooted.

Note: The reboot must be initiated by the VIPRE Hyper-V agent in order to remediate the threat. The threat remains on the guest computer until the reboot happens.

15.6 — Installing / Uninstalling Active Protection on VMs

There is an Active Protection component to the VIPRE Hyper-V agent. In order to provide Active Protection for guest computers, the Hyper-V agent needs to install a small agent to the guest computer to monitor file activity.

When you enable Active Protection on a Hyper-V policy and save that change, all protected guest computers that do not currently have an Active Protection agent installed on them have one installed and configured.

> **Note:** In order to complete Active Protection agent installation, the guest computer must be rebooted. The status for the guest computer is listed as “Needs Reboot”. Clicking “Needs Reboot” triggers the guest computer to reboot.

To disable the Active Protection agent on guest computers, disable it in the Hyper-V policy.

15.7 — Quarantine / Unquarantine

15.7.1 — Reboot to quarantine/unquarantine

In order to quarantine a threat found via a Hyper-V agent scan, the guest computer must be rebooted by the VIPRE Hyper-V agent. When a threat is to be quarantined either automatically or because a user has triggered it, the guest agent status is set to “Needs Reboot”. Clicking on “Needs Reboot” triggers the reboot and the threat is quarantined.

In order to unquarantine a file found during a scan, the guest computer must be rebooted by the Hyper-V agent. When the user selects a file for unquarantine, the guest agent status is set to “Needs Reboot”. Clicking on “Needs Reboot” results in the Hyper-V agent rebooting the guest computer and restoring the file from quarantine.

> **Note:** The reboot must be performed by the Hyper-V agent. Rebooting the guest computer by other means does not result in the threat being unquarantined.

15.8 — Hyper-V Policies

15.8.1 — Manage Agent Communication

The Communication screen enables you to control how agents communicate with the VIPRE Site Service (VSS). The default settings are suitable for environments that consist of 100 to 400 agents, including agents running on laptops. Larger environments of around 500+ agents may require adjustments to these defaults.

> **Note**: Modify agent communication intervals only if it becomes necessary.

To manage agent communication intervals with the VSS:

1. From **Site Navigator**, double-click the Hyper-V policy you want to configure.
2. From the left pane of the Policy Properties screen, expand **Agent** and click **Communication**.
3. Configure the following communication **Intervals**:

- **Mark agents inactive after no contact in minutes**: set the length of time an agent is quiet prior to being marked inactive by the VIPRE Site Service.
  The default value is 30 minutes. The length of time can be set between 0 and 10080 minutes. *The recommended length of time is three times the longest heartbeat interval*.
- **Remove agents that have not communicated with the server in days**: remove agent data from the Management Console if there is no communication between the agent and VIPRE Site Service (VSS) for a specified number of days. The agent remains installed on the host computer and can be reused if the computer is protected again.

4. Configure the following **Server** settings:

In the **Policy Server** field, key in the machine **Name** or **IP address** of the VIPRE server that distributes policy updates to the agents managed by this policy.

5. Configure **Site Server Settings for Agent Interaction**:

> **Important**: This following option (procedure step a) must not be used unless instructed by a technical support representative.

- **Archive agent event files**: (This setting is for DEBUGGING WITH TECH SUPPORT ONLY) scanning and Active Protection reports coming from an agent are stored in the "Incoming XML" folder. The information is then stripped out of the XML and stored in a database, and the XML file deleted. Selecting this option moves the XML file into the "ProcessedXML" folder where the file is stored until deleted manually. Storing this file is useful only for debugging and is best when working with Technical Support.
- **Notify agents of pending work**: when you make a change to a policy, the VSS stores the information in a deferred work queue. Agents get that information during their next scheduled communication. Selecting this option causes the VIPRE Site Service to contact the agent and tell them to do a heartbeat and get the information prior to the scheduled time.

6. Click **Apply** and **OK**.

15.8.2 — Scanning

Settings:

"Remove Hyper-V snapshot after scan" – When Hyper-V guests are hosted on Windows Server 2008 R2, the Hyper-V agent takes a snapshot before it begins to scan the guest. Select this setting to have the snapshot removed after the scan is complete

Full Scan:

A scan of every file on the guest operating system except for files that have been excluded by the user or standard exclusions defined by the VIPRE agent.

Incremental Scan:

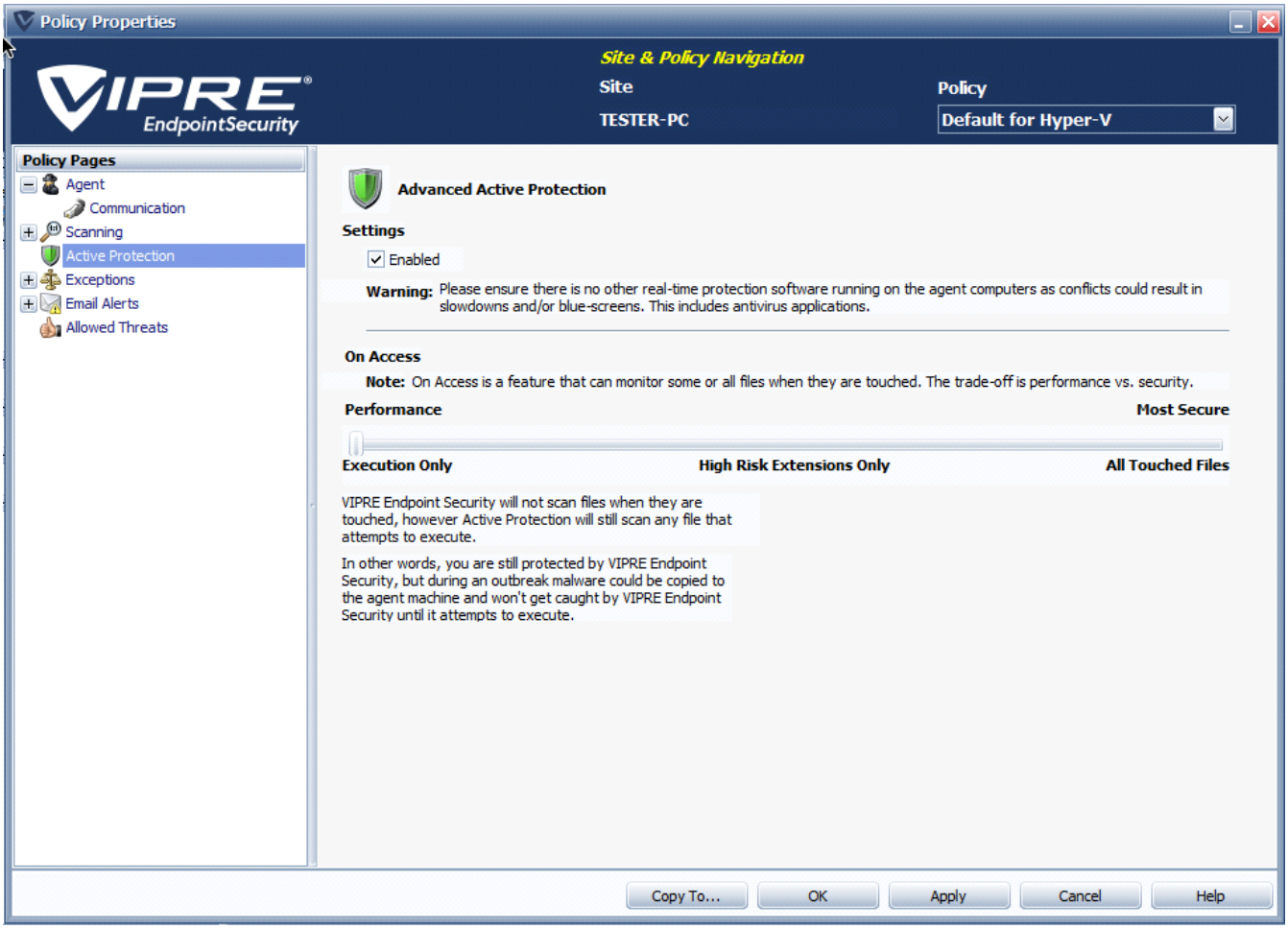
A scan of files that have not been excluded and that have changed since the last scan was performed.

> **Note:** If no scan has been performed, the initial incremental scan processes all files.

15.8.3 — Configure Active Protection Settings

Enabling Active Protection on a policy results in an active protection agent being installed to any guest computer that does not already have an agent on it. Those guest computers need to be rebooted to enable the agent.

Guest computers that already have an active protection agent will have those agents enabled when Active Protection is enabled; those agents are disabled if Active Protection is turned off.



To configure Active Protection settings:

1. In the **Policy Properties**, open **Active Protection**.
2. Select **Enabled** to turn on AP for agents under this policy.
3. Configure **On Access** to control how AP will respond to files when accessed. You can set it based on the needs of security for your environment, whether it be more for performance or more for security:

   - **Execution Only** (Performance): select for AP to scan any file that attempts to execute. This setting is optimal during **normal conditions**.
   - **High Risk Extensions Only**: select for AP to only scan files with extensions that ThreatTrack Security and you (Admin Known) consider "high risk." So, when a file with one of the listed extensions is touched, it will be scanned. In addition, any file that attempts to execute will be scanned.
   - **VIPRE Known**: lists the file extensions (such as EXE, INI, HLP, and BAT) that have proven to be "high risk." You can unselect any of these extensions that you may want AP to NOT check on access.
   - **Admin Known**: lists Admin-defined extensions that will be checked on access. You can add to and remove from this list, and then select the extension that you want to be checked on access.

- **Add**: click to add a new extension to the Admin Known list. Select to enable the new extension.
- **Remove**: highlight (without checking the box) an extension from the Admin Known list and click **Remove**. The extension will be removed immediately from the list without confirmation.
- **All Touched Files** (Security): is for a higher state of protection and should only be enabled in the event that a malware outbreak is suspected or has occurred. When enabled, ALL files are scanned when they are copied or touched.

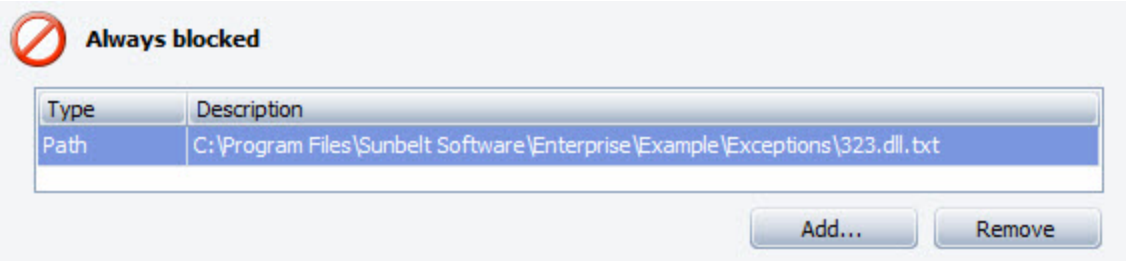
Warning**:** When using "All Touched Files," you MUST watch it frequently and with great care. This setting can result in slower system performance, depending on computer specifications, as well as the number and type of programs running.

4. Click **Apply** to save changes.

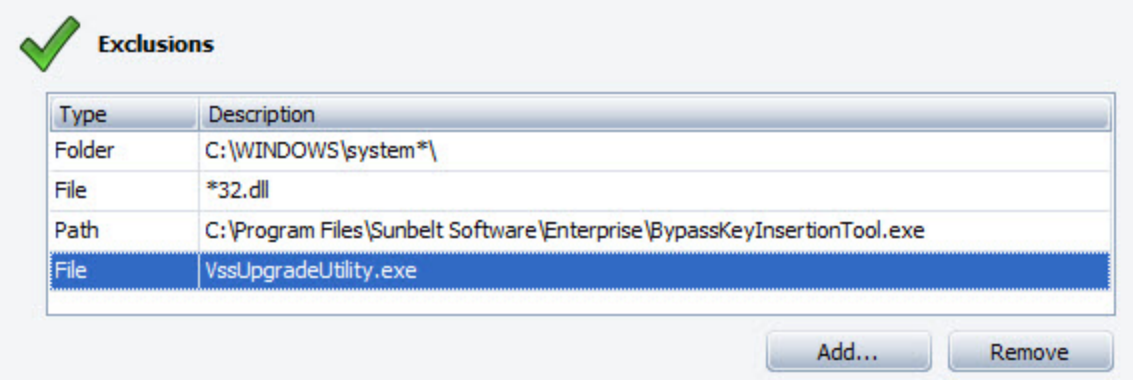
15.8.4 — Configure Policy Exceptions

The **Exceptions** screens are used to assign files, files with path, and/or folders that you, as the administrator, want allowed or blocked for all Agents assigned to a policy. This applies to all of the methods that VIPRE Business uses to detect threats, including Active Protection, Email Protection, and Scans.

Add **Always Blocked** items to be treated as a known threat. For example, if you were to add ABCX as a bad application, then if ABCX is executed on a machine under this policy, ABCX will be automatically blocked from running.

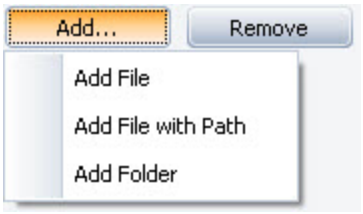


Add **Exclusions** that will always be allowed to run, over-riding the threat definitions.



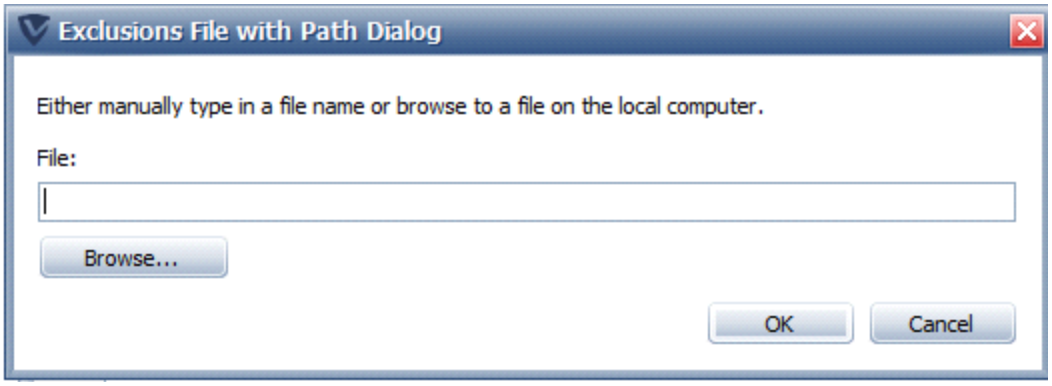
To add an item:

1. In the **Policy Properties**, open the **Exceptions>Always Blocked** or **Exclusions** screen, as applicable.
2. Click **Add** and choose from the following options:



- **Add File**: select a file for VIPRE Business to block/ignore all files named “example.exe” regardless of where the file is located (such as email attachment, network, user's machine, portable drive, and so forth).
- **Add File with Path**: select a file with the path for VIPRE Business to block/ignore all files named “example.exe” with that exact path. If the file is ever moved or another file with this name is somewhere else, VIPRE Business will once again interrogate that file as potential malware.
- **Add Folder**: select a folder for VIPRE Business to block/ignore all contents in it. If a particular folder is ever moved or another folder with this name is somewhere else, VIPRE Business will once again interrogate programs in that folder as potential malware.

3. Enter the name of the File, Path, of Folder.



Note: Wildcards (* and ?) are supported for Exclusions only. For more information, See Using Wildcards in Exclusions.

-or-
Click **Browse** and locate the File, Path, or Folder to add.

4. Click **OK**.
5. Click **Apply** to save changes.

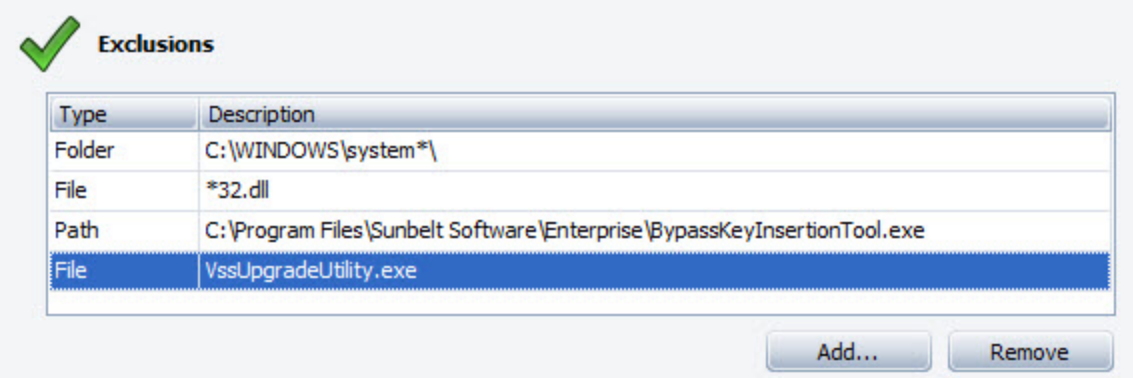
To remove an item

1. Select a row and click **Remove**.
2. Click **Apply** to save changes.

15.8.5 — Using Wildcards in Exclusions

VIPRE Business supports wildcards for Exclusions (always allowed items) only. This does NOT include environment variables. Supported wildcards are:

- '?' - matches exactly ONE character, EXCEPT the directory separator.
- '*' - matches ZERO or MORE characters, EXCEPT the directory separator.



Supported entity types:

Full Path

Fully specified path to a file, wildcards NOT permitted.
Example: "C:\WINDOWS\system32\kernel32.dll"

Full Path Pattern

Fully specified path to a file, wildcards permitted.
Example: "C:\WINDOWS\system32*32.dll"

File Name

Just the name of a file, wildcards NOT permitted.
Example: "kernel32.dll"

File Name Pattern

Just the name of a file, wildcards permitted.
Example: "*32.dll"

Folder

Fully specified path to a folder, wildcards NOT permitted (must be terminated with directory separator).
Example: "C:\WINDOWS\system32\"

Note: Folder patterns are implemented as Full Path Patterns terminated with a directory separator.

Example: "C:\WINDOWS\system*\"

Note: Folder entities are recursive and thus will match the folder itself and any descendant files and folders.

Examples:"C:\WINDOWS\" matches "C:\WINDOWS\", "C:\WINDOWS\SYSTEM32\", "C:\WINDOWS\notepad.exe", "C:\WINDOWS\SYSTEM32\regedit.exe", and so forth

Multiple Path Levels

Wildcards should behave exactly as they do in a Windows Command Prompt, with the added feature of supporting wildcards at multiple path levels including the drive.

Examples:

"*.dll" - matches "kernel32.dll", "advapi32.dll", etc

"C:\WINDOWS\system32*.dll" - matches "C:\WINDOWS\system32\kernel32.dll",

"C:\WINDOWS\system32\advapi32.dll", etc

"?:\WIN*\system**.dll" - matches "C:\WINDOWS\system32\kernel32.dll", "D:\WINNT\system\advapi32.dll", etc

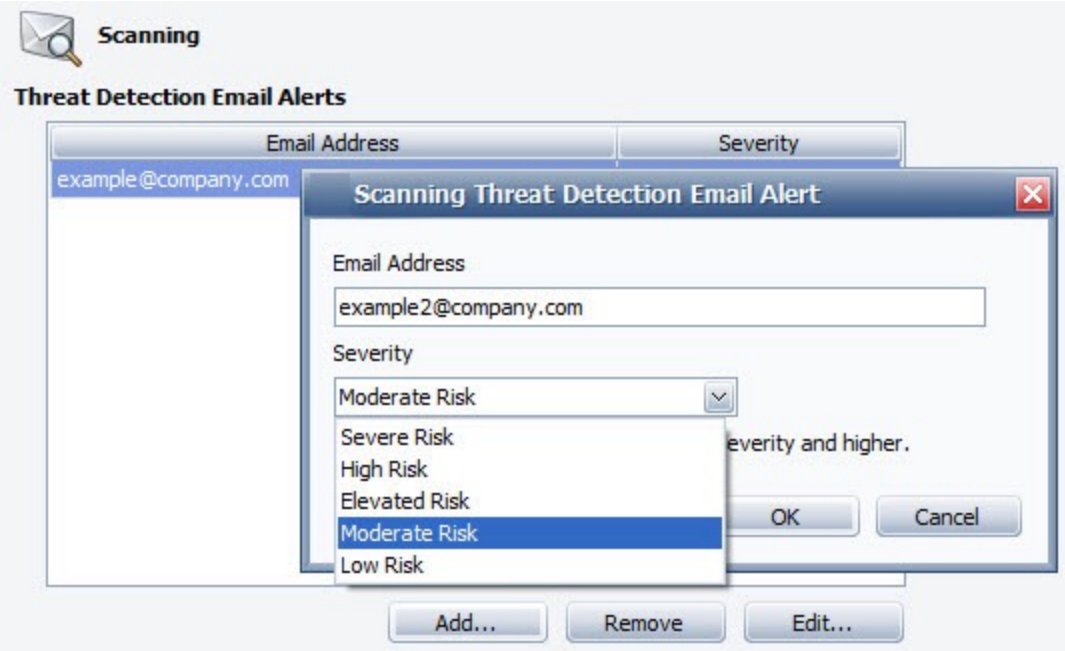
Note: User Known Entities are NOT case-sensitive.

15.8.6 — Configure Email Alerts

Email Alerts are email messages sent by the VIPRE Site Service to recipients that you enter. Configure **Email Alerts** for Agent events, including Scanning, Active Protection, Email Protection, and Patch Management (*VIPRE Premium and Endpoint only*). Email alerts are configured at the policy level.

To configure email alerts for threat detections by Scanning:

1. Ensure that the Site's Email Server Settings are configured.
2. In the **Policy Properties**, open **Email Alerts>Scanning**.
3. Click **Add**. The Scanning Threat Detection Email Alert dialog box displays.



4. Enter a recipient's email address.
5. From the **Severity** drop-down box, select a risk level. When the severity or higher that you select is detected during a scan, an email is sent with the details to recipients on the list.
6. Click **OK**. The email address displays in the list.
7. To edit an email alert recipient, select an email address and then click **Edit** to make your desired changes.
8. To remove an email alert recipient, select an email address and then click **Remove**.

To configure email alerts for Active Protection:

1. Ensure that the Site's Email Server Settings are configured.
2. In the **Policy Properties**, open **Email Alerts>Active Protection**.
3. Click **Add**. The Active Protection Email Alert dialog box displays.

4. Enter a recipient's email address.
5. Select one or both:
   - **Allowed items**: CAUTION, this setting may result in a multitude of emails. An email is sent with the details to the recipient list. "Allowed" items are based on Exclusions.
   - **Blocked items**: emails are triggered whenever AP detects a threat, based on the Active Protection settings. This applies to all agents that are assigned to the policy that you are configuring.
6. Click **OK**. The email address displays in the list.
7. To edit an email alert recipient, select an email address and then click **Edit** to make your desired changes.
8. To remove an email alert recipient, select an email address and then click **Remove**.

To configure email alerts for Email Protection:

1. Ensure that the Site's Email Server Settings are configured.
2. In the **Policy Properties**, open **Email Alerts>Email Protection**.
3. Click **Add**. The Email Protection Email Alert dialog box displays.

15.8.7 — Adding Allowed Threats

VIPRE may detect items that you may consider non-threatening in your network, for which you would want to allow to run.

For example, Virtual Network Computing (VNC) and Remote Administrator (Radmin) may both be considered acceptable for use in your organization, but may be considered threats in another organization.

To add an allowed threat:

1. Navigate to a **Site>Quarantine tab** or **Policy>Quarantine tab**.

Or:

1. Navigate to **Protected Computers>Agent Details>Scan History tab**.
2. Right-click on a threat, and select **Allow Threat**. The Allow Threat window displays.
3. Select the policies on which this threat should be allowed.
4. Click **OK**.
5. The allowed threat now displays in the Allowed Threats list for the policies you selected (**Policy Properties>Allowed Threats**).

15.9 — Report - Hyper-V Related Reports

Hyper-V agents have been added to all reports for which they are relevant. Agents have not been added to Patch Management reports or Firewall reports, as this functionality is not available for these agents. All other reports can include Hyper-V agents.

15.9.1 — Licensing

VIPRE Hyper-V agents are licensed on a per host basis. Each license is associated with a host computer; you may protect as many guest computers as you run on that host.

Installing a VIPRE Hyper-V agent on a host computer does not preclude you from installing VIPRE Business agents on guest computers.

15.9.2 — Ignored installations

If you install a VIPRE Hyper-V agent that is in excess of your number of purchased licenses, that agent is ignored by the VIPRE Business console. You cannot protect guest computers on that host with the VIPRE Hyper-V agent.

The first time that a VIPRE Hyper-V agent installation is ignored, an email is sent to the email address entered in during the console installation process. If you uninstall another VIPRE Hyper-V agent, then the ignored agent begins to be acknowledged.

16 — Managing Updates

There are two different types of updates:

- **Threat definition updates** identify and remediate malware in your environment and are updated several times each day, as often as hourly. The full threat definitions are approximately 70 MB and reside on each machine that contains a VIPRE Agent. The average update chunk size is approximately 67 KB.
- **Software updates** pertain to the Agent software and occur a few times a year. Software Updates are approximately 15 MB. These software updates can include patches, version releases, or Beta releases (Beta releases are only made available by request) for VIPRE Antivirus Business, VIPRE Business Premium, and VIPRE Endpoint Security, as well as different languages besides English.

16.1 — How are updates distributed to Agents?

When an agent is first installed, it immediately gets threat definitions updates. The Agents receive ongoing updates based on the policy they are assigned. Both definitions and software updates are sent from the VIPRE Site Service (VSS) on ports 18082. If you enabled "Download via the Internet if local updates are unavailable," Agents will obtain their definition updates from ThreatTrack Security's update server (Port 80) if they are unable to contact the update server specified in the policy.

> **Note**: Updates are NOT delivered from the VIPRE Business Admin Console or by a request over the Internet from the Agent.

In order for the VSS to get the updates for distribution, it is required that both Simple Object Access Protocol (SOAP) headers and Internet access be allowed from the VSS machine to the external Internet.

Specifically, set SOAP via port 80 outbound and inbound for the following:

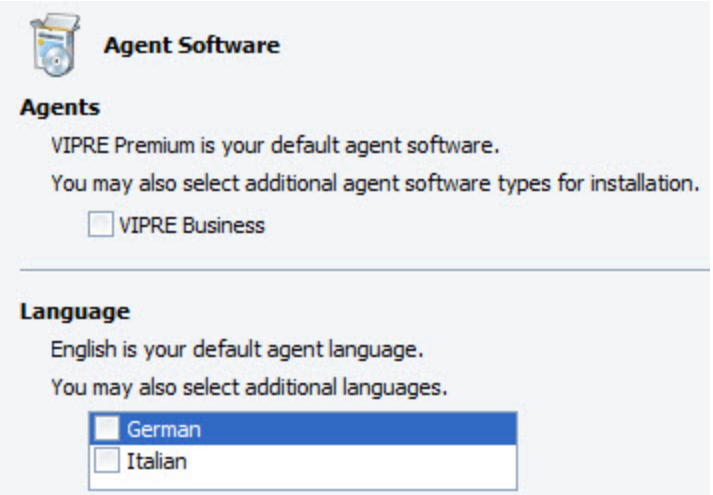
- **updates.sunbeltsoftware.com** checks for software updates and allows software and definition updates to be distributed.
- **ne.edgecastcdn.net** allows software updates and definition updates to be distributed.

16.2 — Configure updates for your environment:

1. Select agent software for the site
2. Manage site updates
3. Manage agent updates for policies
4. If necessary, create a remote update server.

16.3 — Select Agent Software for the Site

Select the agent software that is appropriate for your business. The Agents and Languages selected will be downloaded according your Site Updates settings and then applied according to the Agent Updates policy settings.



To select agent software for the Site:

1. In the **Site Properties**, open the **Agent Software** screen.
2. In the **Agents** area, select the applicable version of Agent.
3. If applicable, in the **Language** area, select the languages.
4. Click **Apply** to accept changes.

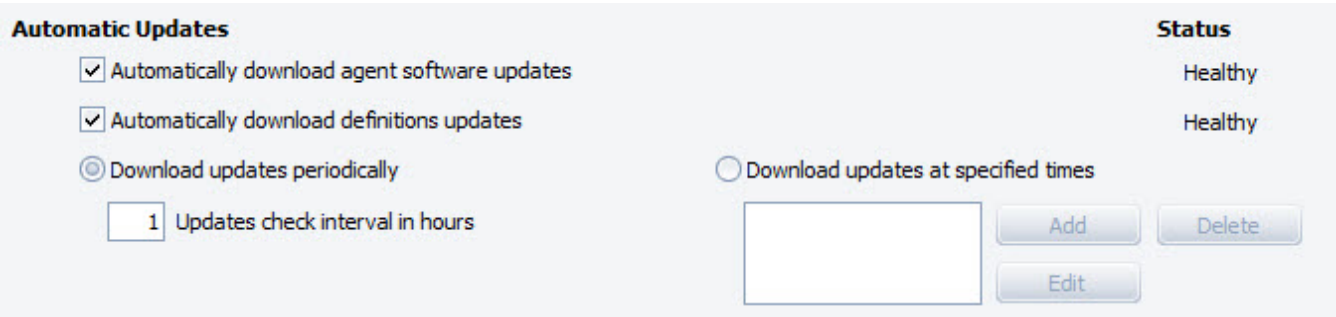
16.4 — Manage Site Updates

Manage updates for Sites from the **Updates** screen in the **Site Properties**. Updates are checked at ThreatTrack Security and require an Internet connection. If your Site requires a proxy to reach the Internet, configure the Site's Proxy Settings.

Configure automatic updates for the Site:

Set VIPRE Business to automatically retrieve updates at either a regular interval or at specified times.

1. In the **Site Properties**, open the **Updates** screen.
2. In the **Automatic Updates** area, configure the following:

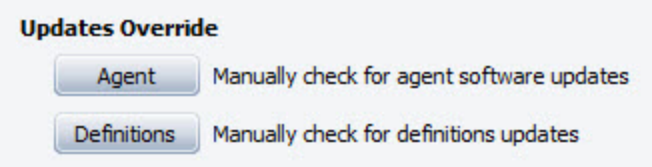


- **Automatically download agent software updates**: if disabled, Agent software updates for this site will NOT be automatically checked; you will have to get agent software updates manually from the "Updates Override" area below.
- **Automatically download definitions updates**: if disabled, threat definition updates for this site will NOT be automatically checked; you will have to get definitions updates manually from the "Updates Override" area below.
- **Download updates periodically**: select to receive updates at regular intervals.
- **Updates check interval in hours**: enter a number between 1 and 72 hours.
- **Download updates at specified times**: select to receive updates at the times that you create.

3. Click **Apply** to accept changes.

Manually update software and definitions for the Site:

1. In the **Site Properties**, open the **Updates** screen.
2. In the **Updates Override** area, configure the following:

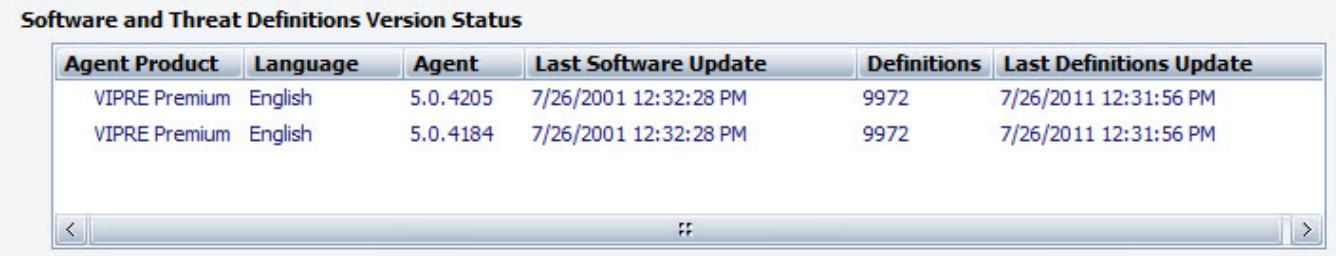


- Click **Agent** to manually check for the associated software or definitions update. This will update the Site.
- Click **Definitions** to manually check for the associated software or definitions update. This will update the VSS.

3. Click **Apply** to accept changes.

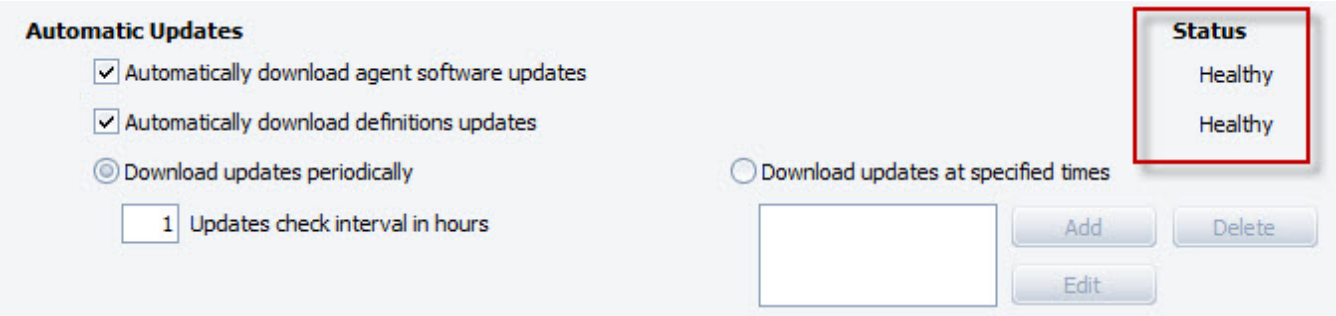
Check version status for software and threat definitions:

The **Software and Threat Definitions Version Status** area displays the following information:



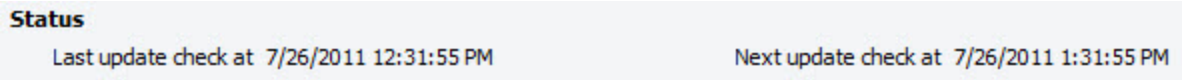
- **Agent Product** displays the product name of the agent.
- **Language** displays the language of the update.
- **Agent** displays the last version number of the agent software that is available.
- **Last Software Update** displays the date and time for this version of the agent software.
- **Definitions** displays the last version number for Definitions that is available.
- **Last Definitions Update** displays the date and time for the version listed in the Definitions column.

The **Status** column under **Automatic Updates** displays the following status types:



- **Healthy** indicates that automatic updates have no errors and that it is operating normally; not actively doing anything.
- **In progress** indicates that updates are being downloaded.
- **Warning** indicates that there is an intermittent error of no Internet connectivity, and will automatically try again. Check the VSS logs for more information.
- **Task pending** indicates that the VSS is waiting to pick up the task.
- **Work in progress** indicates that the VSS is actively performing the task.
- **Error** indicates that an error is in a continuous state. Check the site logs for more information.

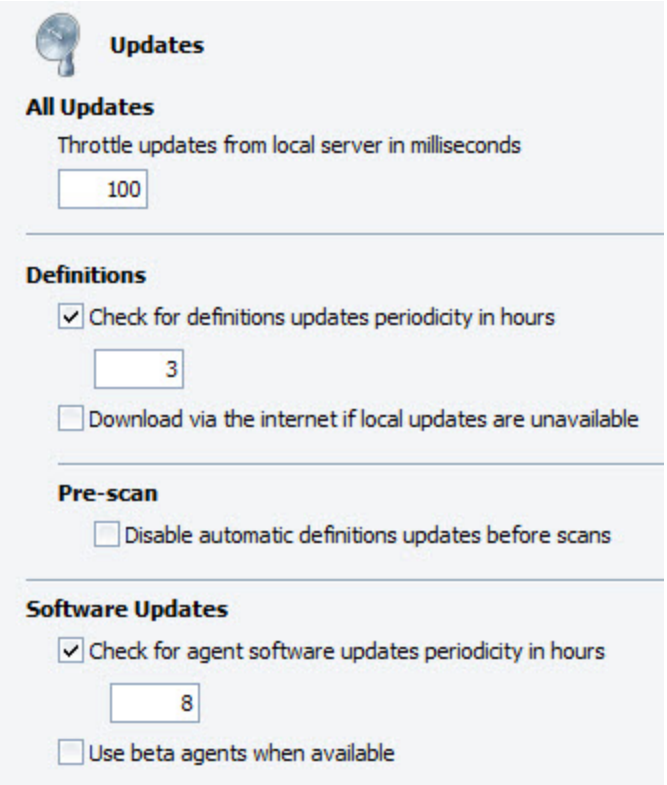
The bottom **Status** area displays the following information:



- **Last update check at** displays the date and time that updates were last checked, whether it was done automatically or manually.
- **Next update check at** displays the date and time that updates are scheduled to be automatically checked.

16.5 — Manage Agent Updates for Policies

Updates are distributed to machines based on the Agent Updates settings for each Policy. Agent update settings help you manage the impact to network traffic and machine performance when Policies distribute updates to Agents.



To manage distribution of updates per policy:

1. Open the **Agent>Updates** screen in the **Policy Properties** for each Policy.
2. Set **Throttle updates from local server in milliseconds** to cut down the load on the update server when distributing updates to the machines under the selected policy. The default value for throttling is 100 milliseconds but can be set as high as 60,000 milliseconds (or 1 minute) for networks with extreme bandwidth constraints. The average update chunk size is approximately 67 KB. A general guide:

   1 MBPS network: 1000 milliseconds.

   10 MBPS network: 200 milliseconds.

   100 MBPS network: 50 milliseconds.

   1 GBPS network: 20 milliseconds
3. Configure automatic Definition Updates for Agents under this policy:

   - Select **Check for definitions updates periodicity in hours** to turn on automatic definition updates and then enter a number in hours for the update interval. The default is to automatically check at 1 hour intervals. The interval values are 1-72 hours. Best set between 1 and 3 hours. The default start time for updates is when the computer first boots up. For example, if the computer boots up at 7:43 a.m. and checks for updates every 3 hours, it will check at 10:43 a.m., 1:43 p.m., 4:43 p.m., and so forth.
   - The "Disable automatic definitions updates before scans" setting:
   - **Unselect** (recommended) to ensure that the Agent automatically gets the latest definitions before running any type of scan.

- **Select** if Agent machines are older models and run slower, or if the interval for definitions updates is set frequently (1-3 hours).

Note: This setting should be done in conjunction with the Scan setting "Randomize scheduled scan start times in minutes."

4. To have Agents on laptops (or remote users) connect to ThreatTrack Security over the Internet if the agent fails to contact the VSS or the update server, select **Download via the Internet if local updates are unavailable**. If machines require a Proxy to access the Internet, ensure that you configure Policy proxy settings.

Important: If this is used for agents over your network, this could put a strain on the WAN.

5. Configure Software Updates for Agents under this policy:
   - (recommended) To turn on automatic software updates, select **Check for agent software updates periodicity in hours**, and then enter a number in hours for the update interval. The default setting is on and at 8 hour intervals. The interval values are 1-72 hours.
   - To turn off automatic software updates, unselect **Check for agent software updates periodicity in hours**.
   - To participate in Beta releases, select **Use beta agents when available**. This is best used under policies with a limited number of agents and non-production machines.

Important: **Use this option with care**. If you need to rollback to a previous version, a manual uninstall and reinstall of each agent may be required.

6. Click **OK** to accept your changes. All changes are applied to the Agents assigned to the Policy the next time the Agent communicates to the Site.

16.6 — Create Remote Update Servers

Additional update servers are beneficial for companies operating at more than one physical location and trying to manage loads on Internet traffic. For example, let's say your primary location is New York and you have a secondary office in San Diego. Having an update server in San Diego would put less burden on bandwidth—the agents in San Diego would not have to connect over the Internet to get updates; instead they can get them locally from the secondary update server.

Basically, run the Full VIPRE Business installation on a secondary machine, which will be used as the "Update Server." Then, download the latest updates and assign policies to the new update server.

IMPORTANT: Use Static IP Addresses only.

To create a remote update server:

Set VIPRE Business to automatically retrieve updates at either a regular interval or at specified times.

1. Download your product installer.
2. Run the installer on the machine that will be the update server, ensuring that "Full Installation" is

selected. Follow all default settings.

3. Configure the following in the **Site Properties**:
   - On the **Registration** screen, use your main license key.

Note: Installing additional update servers does not require a new key or the purchase of additional software licenses. However, entering your existing key is required in order for the update server to receive updates.

   - On the **Updates** screen, ensure that the threat definitions and agent software updates have been downloaded, as indicated in the "Status" column. Please be patient, as this may take a few minutes.

4. From the primary machine where VIPRE Business (this is also known as the "main policy server") is installed, change the update server settings for the desired policies:
5. In the **Policy Properties**, open **Agent>Communication**.
6. Under **Update Server**, enter the IP address and Port number of the machine you just installed on, which will be the update server.

7. Click **Apply**.
   For creating additional update servers, repeat Steps 1-5.
   For assigning additional policies to the update server, repeat Steps 4-5.

Tip: You can copy the update server setting to other policies. For more information See Copy Settings from [Policy Name] Dialog Box.

The remote update server is now configured. Agent polices will still be administered via the main policy server, while updates will be handled via the update server.

17 — Configuring Advanced Browser Protection

17.1 — Adding Allowed Web Sites for Advanced Browser Protection

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

Allowed Web Sites allow a website that is blocked by the Bad URL list, overriding the Configure Malicious URL Blocking Settings (page 182). When you add an allowed website, you can customize control over the content filtering and privacy settings.

> **Note**: Changes made here will override the settings on the Malicious URL Blocking screen.

To add an allowed website:

> **Note**: The grid area is not editable; you need to select a row to display the editable fields below it.

1. Navigate to the **Allowed Web Sites** screen. (**Policy Properties>Advanced Browser Protection>Allowed Web Sites**).
2. Click **Add**.
3. Enter the **domain**.

> **Note**: Do not include http:// or www.

4. Optionally, select any of the Web Page Content Filtering or Privacy Settings, which will override the global web filtering settings for the above domain.

> **Note**: After adding an allowed website, you can delete it or modify its settings.

5. Click **Apply** to accept changes.

17.2 — Web Traffic Protection

Configure the **Web Traffic Protection** settings for all Agents assigned to the Policy.

To enable Web Traffic Protection for VIPRE Business:

1. Navigate to the **Web Traffic Protection** screen. (**Policy Properties>Advanced Browser Protection>Web Traffic Protection**).
2. Check **Allow user to configure Web Traffic Protection** to allow end users to turn the feature on or off.
3. Click **Apply** to accept changes.

To enable Web Traffic Protection in VIPRE Premium or VIPRE Endpoint Security:

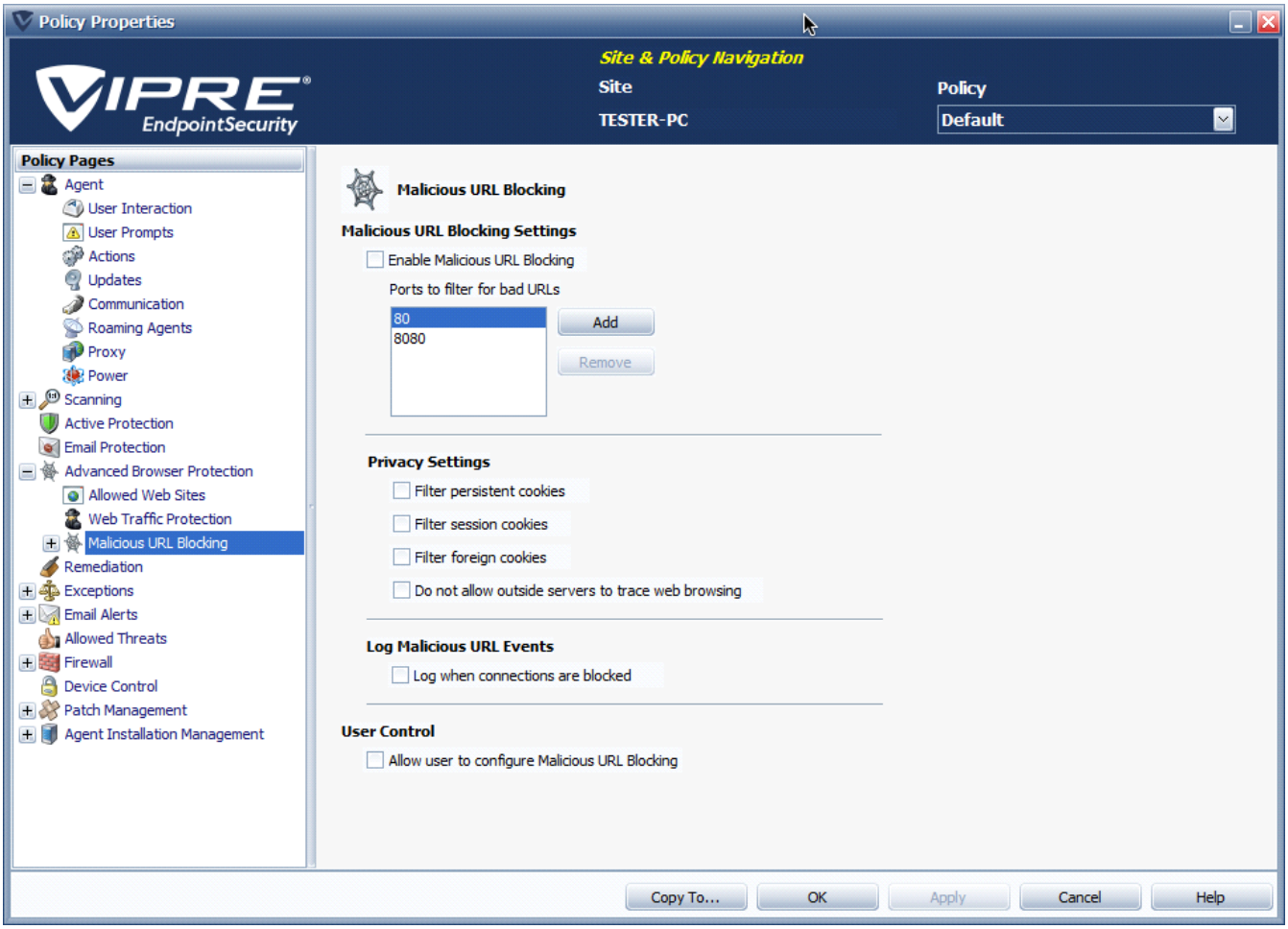
1. Navigate to the **Web Traffic Protection** screen. (**Policy Properties>Advanced Browser Protection>Web Traffic Protection**).
2. Check **Block potential threats in web traffic** (*VIPRE Endpoint Security only*).
3. Optionally, check **Allow user to configure Web Traffic Protection** to allow end users to turn the feature on or off.
4. Click **Apply** to accept changes.

17.3 — Configure Malicious URL Blocking Settings

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

Configure the **Advanced Browser Protection** settings for all Agents assigned to the Policy.

> **Note:** Changes made to the Allowed Web Sites screen will override the Malicious URL Blocking Settings.



To configure the Malicious URL Blocking settings:

1. In the **Policy Properties**, open **Advanced Browser Protection>Malicious URL Blocking**.
2. Enable **Malicious URL Blocking**:
   - **Enable Malicious URL Blocking**: select to enable the global Malicious URL Blocking settings to help prevent end users from accidentally opening known bad Web sites. Unselecting this option disables all Malicious URL Blocking settings including blocked Web site settings.
   - **Ports to filter for bad URLs**: click **Add** and key in the TCP/UDP port that you want to block. This enables you to block web-traffic from specific ports only, from a website listed under the Bad URLs list.

Note: By default, ports **80** and **8080** are added to the filter. Port 80 cannot be removed from the list. This ensures that http requests are filtered for bad URLs.

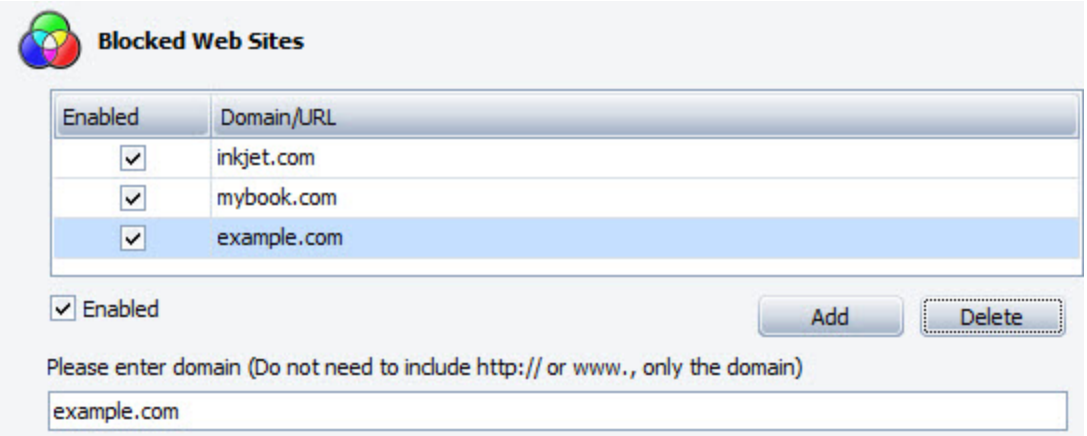
3. Configure **Privacy Settings**, which are based on the Bad URL list maintained by ThreatTrack Security. You can override these global settings for specific Web sites that you want to allow by adding allowed Web sites.
   - **Filter persistent cookies**: a persistent cookie may be required to view certain Web sites. Enabling this option may result in some pages not displaying properly.
   - **Filter session cookies**: a session cookie may be required to view certain Web sites. Enabling this option may result in some pages not displaying properly.
   - **Filter foreign cookies**: a foreign cookie may be required to view certain advertisements or link to 3rd party sites. Enabling this option may result in some content not displaying.
   - **Do not allow outside servers to trace web browsing**: select to keep browsing private when redirected to other Web sites. When selected, the details of a link request are stripped from the referring Web site so that the target Web site cannot identify the page of which the page request originated from. Unselect to allow this referring to occur.
5. Optionally, select **Log when connections are blocked**, to log all attempted connections that are made to a blocked domain/URL on the Agent machine. You can view the log from the **Agent Console (Firewall History > Web History)**.
6. Optionally, select **Allow user to configure Malicious URL Blocking**, to allow users to enable or disable URL blocking on the Agent machine.

17.4 — Manage Blocked Web Sites

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

Add Web sites that you want blocked from end users at the policy level. When an end user attempts to navigate to a blocked Web site, they will be denied access.

Note: The grid area is not editable; you need to select a row to display the editable fields below it.



To add a Domain/URL to the blocked list:

1. Navigate to the **Blocked Web Sites** screen. (**Policy Properties>Advanced Browser Protection>Malicious URL Blocking>Blocked Web Sites**).
2. Click **Add**. A new row is added to the grid area.
3. In the **Domain** text field, enter the domain that you want blocked.
4. By default, the **Enabled** field is automatically selected.
5. Click **Apply** to accept changes.

To manage Domain/URLs:

1. Navigate to the **Blocked Web Sites** screen. (**Policy Properties>Advanced Browser Protection>Malicious URL Blocking>Blocked Web Sites**).
2. In the grid area, select the desired domain/URL. Its editable field(s) display below the grid area.
3. To block this domain/URL, select **Enabled**.
   -or-
   To allow this domain/URL, unselect **Enabled**.
4. Optionally, modify the spelling of the domain listed.
5. Optionally, delete it by clicking **Delete**.
6. Click **Apply** to accept changes.

18 — Configure Patch Management

18.1 — Managing Patches by Product

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

VIPRE agents automatically detect software applications that are installed on the machines on which they reside. These applications are listed under the Manage Patches by Product screen, which enables you to manage patches for individual applications that were detected on the agent machines pertaining to the selected policy.

By default, patches are managed by product. This means that missing and installed patches are grouped under one product name and several patches can be managed at once. For in-depth management of software patches, VIPRE enables you to Manage Patches Individually.

To manage patches by product:

1. From **Site Navigator**, double-click the policy name you want to configure.
2. From the left pane of the Policy Properties screen, click **Patch Management**.
3. From the applications list, select the applications you want to patch.
4. Click **Scan Now** to scan the agents for new missing patches and update the software list.
5. Click **Install Now** to start installing the selected missing patches.

> **Note**: To check patch installation progress, go to the **Protected Computers** tab and ensure that the agent **Status** is **Installing Patches**.

6. (Optional) Select **Turn on automatic Windows Updates**, to allow VIPRE to manage missing Windows Updates.
7. Click **Apply** to accept changes.

18.2 — Managing Patches Individually

By default, patches are Managed by Product. However, the Patch Management screen can be changed so that patches can be managed individually. The Manage Patches Individually view allows you to select individual patches to ensure that only necessary updates are applied to unpatched applications. This view also provides you with the number of computers that have missing, installed and not required patches as well as the computer names for each.

To switch from managing patches by product to managing patches individually:

1. From **Site Navigator**, double-click the policy name you want to configure.
2. From the left pane of the Policy Properties screen, click **Patch Management**.
3. From the bottom of the right pane, click **Manage patches individually instead of by product**.
4. To switch back to Manage by Product view, click **Manage patches by product instead of individually**.

To manage patches individually:

1. Select **Approve all patches that are currently missing**, to automatically approve patches listed in this view.

Important: Only select this option if you are sure that the listed patches belong to trusted applications and come from genuine sources. If enabled, approved patches may install automatically.

2. (Optional) To view patches that were previously approved for installation, select **Show previously approved patches**.
3. Click **Scan Now** to start scanning agents for missing patches.
4. Click **Install Now** to start installing approved patches on agents managed by this policy.

Note: To check patch installation progress, go to the **Protected Computers** tab and ensure that the agent **Status** is **Installing Patches**.

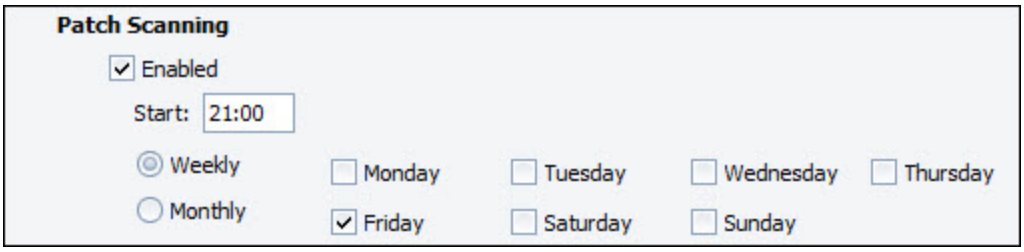
5. (Optional) Select **Turn on automatic Windows Updates**, to allow VIPRE to manage missing Windows Updates.
6. Click **Apply** to accept changes.

18.3 — Scheduling Patch Scanning and Installation

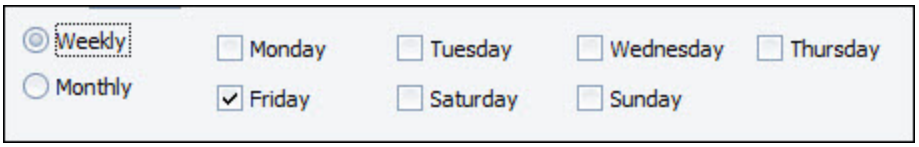
Patch Scheduling enables you to set a specific time when VIPRE scans agent machines for missing patches, as well as when missing patches can be installed.

To schedule patch scanning and installation:

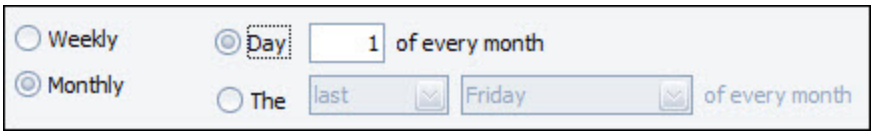
1. From **Site Navigator**, double-click the policy name you want to configure.
2. From the left pane of the Policy Properties screen, expand **Patch Management** and click **Patch Scheduling**.
3. Make your **Patch Scanning** selections:



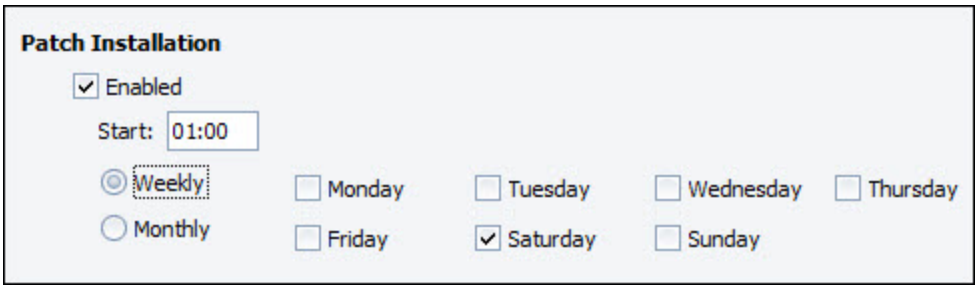
4. Select **Enabled** to turn on patch scanning for this policy.
5. Enter a time for VIPRE to start the patch scanning on the agent machines.
6. Select a scanning interval:
   - **Weekly**: select the days of the week when scanning occurs.



- **Monthly**: select a day of the month when scanning occurs.

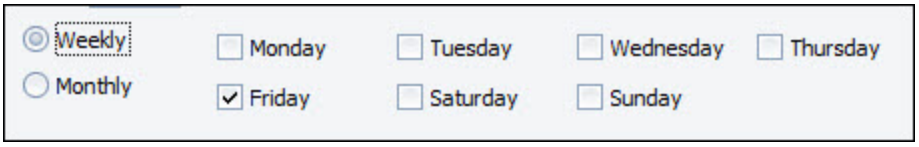


7. Make your Patch Installation selections:

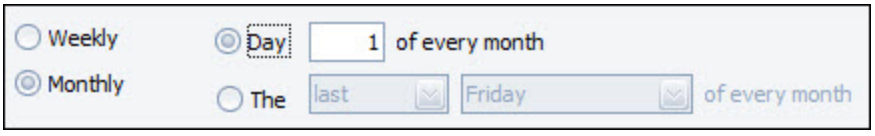


8. Select **Enabled** to turn on patch installation for this policy.
9. Enter a time for VIPRE to start the patch scanning on the agent machines.
10. Select an interval for installation:

- **Weekly**: select the days of the week when patch installation occurs.



- **Monthly**: select a day of the month when patch installation occurs.



11. Click **Apply** to accept changes.

19 — Working with the Firewall

This chapter on Firewall covers all the procedures for managing the VIPRE Firewall (for VIPRE Business Premium and VIPRE Endpoint Security).

19.1 — Configure User Control Settings for Firewall

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

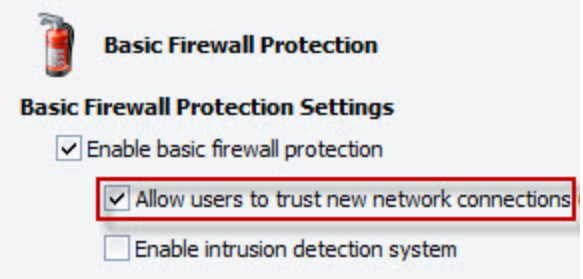
Configure access end users will have to the firewall for all agents under a policy.

To configure the user control settings for the Firewall:

1. For the desired policy, open **Policy Properties>Firewall**.
2. Configure the following:

- **Allow users to configure firewall**: when selected, the firewall functionality will be visible in the Agents, allowing the end users complete control of the firewall settings. When unselected, firewall configuration settings will not be visible in the Agents.
- **Allow users to disable firewall**: when selected, unhides the enable/disable firewall setting in the Agents. When unselected, the ability to disable the firewall by the end users is hidden. Firewall configuration settings are not related to this setting.
- **Allow users to stop/start all traffic**: when selected, unhides the stop/start all traffic firewall setting in the Agents. When unselected, the end users will not be able to stop/start traffic from the Agent.

3. Open **Policy Properties>Firewall>Basic Firewall Protection**.



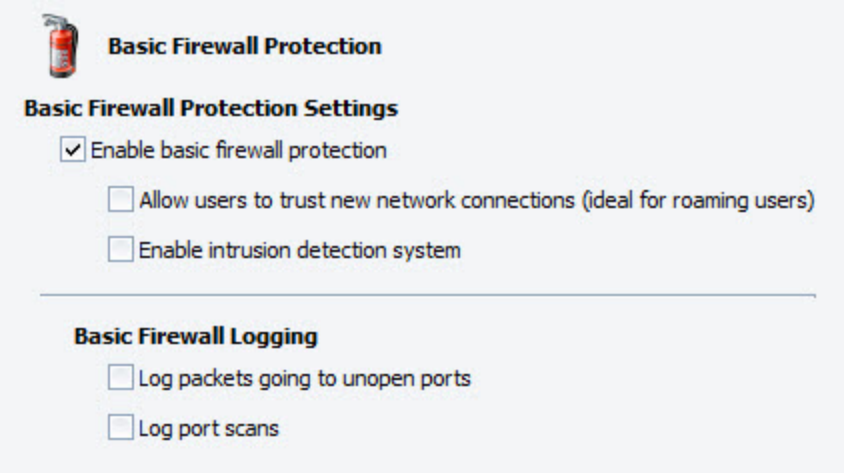
4. Optionally, select **Allow users to trust new network connections**. This setting is ideal for laptop/roaming users.

5. Click **Apply** to save changes.

19.2 — Configure Basic Firewall Protection

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

The **Basic Firewall Protection** screen allows you to turn on/off the basic firewall protection and control firewall logging for all agents under a policy.



Basic Firewall Protection Settings:

- **Enable basic firewall protection**: this is the control switch for all sub controls under "Basic Firewall Protection." This includes all exceptions and trusted zones. This does NOT include IDS.
- **Allow users to trust new network connections**: this sets the agent to automatically trust new network connections, which is an ideal setting for users who travel often with a laptop to avoid frequent prompts asking the user whether to allow a network connection.
- **Enable intrusion detection system**: this is the control switch for all functions on the Intrusion Detection System screen.

Basic Firewall Logging:

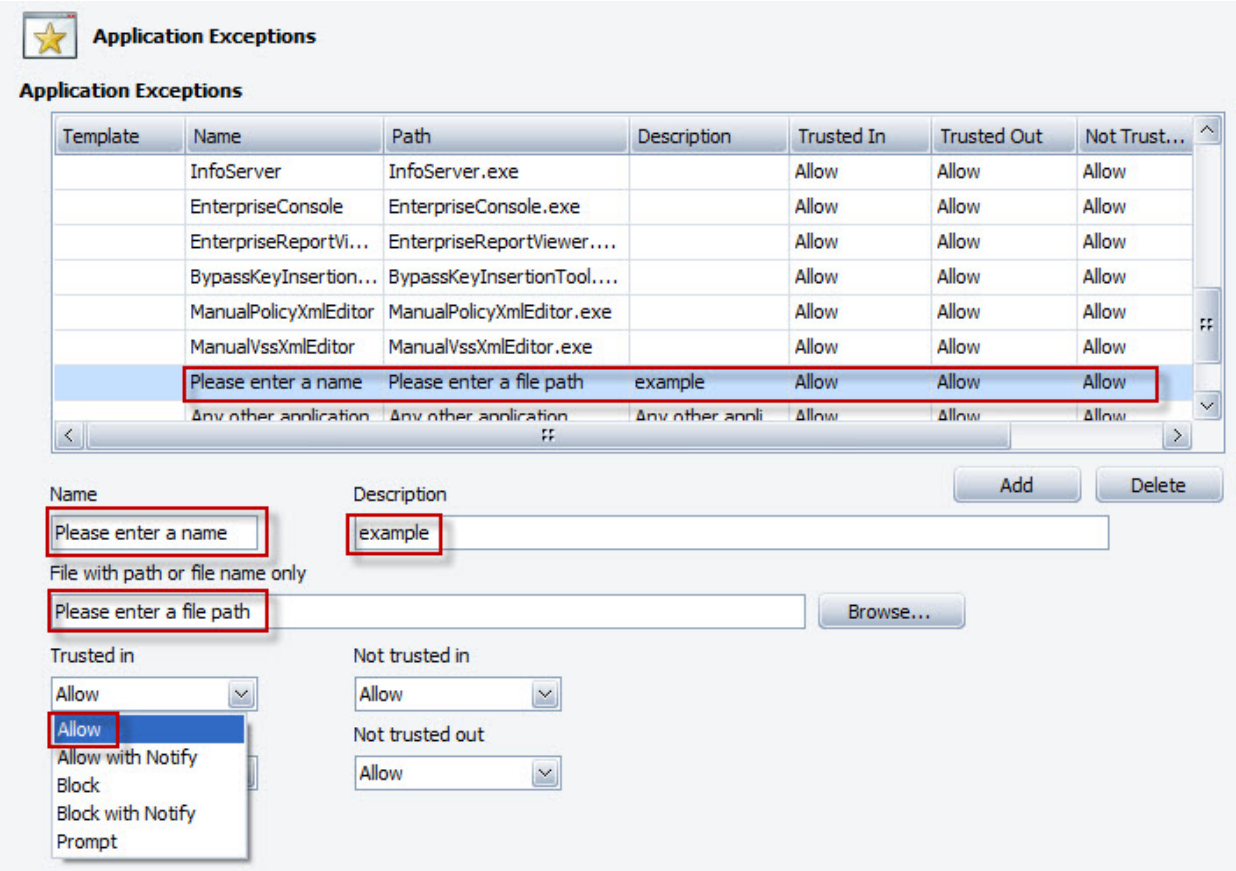
- **Log packets going to unopen ports**: when enabled, logs packets going to unopen ports.
- **Log port scans**: when enabled, logs all attempts at scanning ports over your network.

> **Note**: To view a report of port scans, in the Report Viewer, run the "Firewall Daily Intrusions Blocked" report.

19.2.1 — Configure Firewall Application Exceptions

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

Configure the **Application Exceptions** to control the access an application will have over your network.



To configure firewall application exceptions:

1. Navigate to the **Application Exceptions** screen. **Policy Properties>Firewall>Basic Firewall Protection>Application Exceptions**.
2. To add a new application exception, click **Add**. An exception is added to the table.
   -or-
   To modify an existing application exception, select a row in the Application Exceptions table. Skip to step 5.
   -or-

Note: Default exceptions cannot be deleted and only its firewall action can be modified.

To delete an existing application exception, select a row in the Application Exceptions and click **Delete**, and then click **Apply** to accept changes.

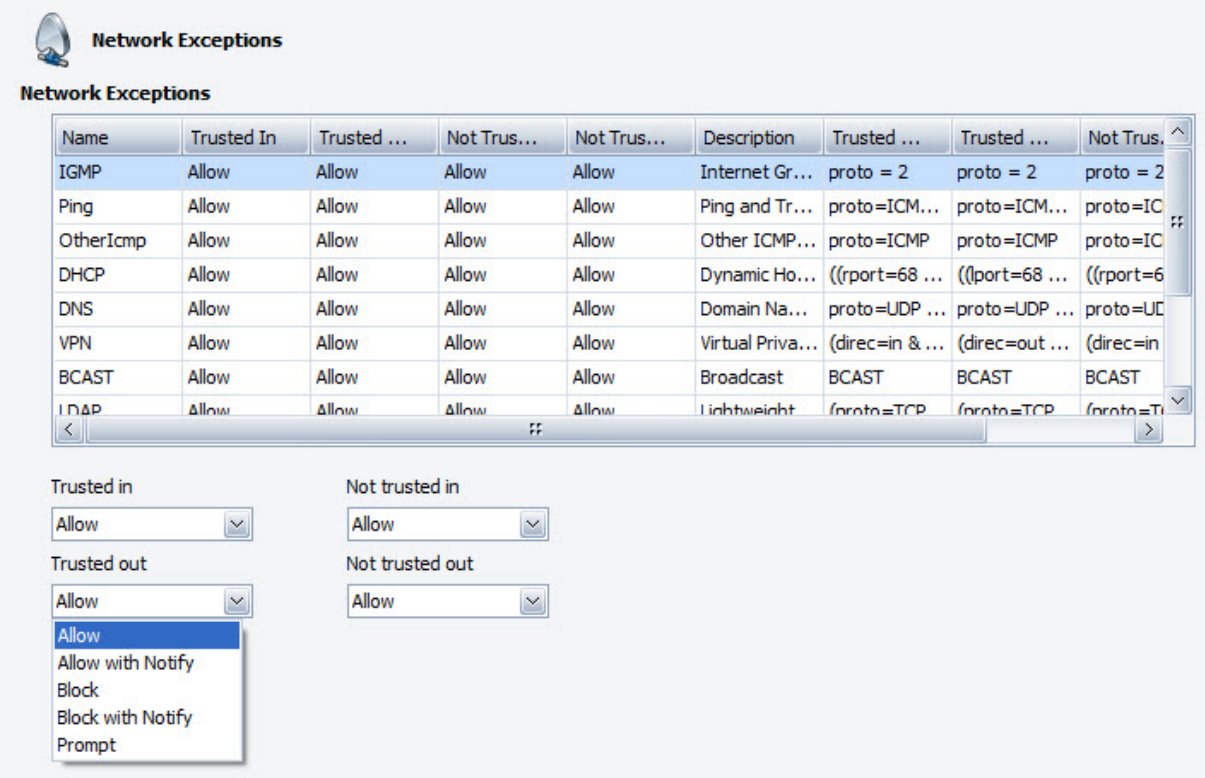
Note: The column headings are dynamic, allowing you to move their order and sort by a category within that column. Click the filter icon on a column heading to select a filtering option. See Filtering Views for more information on using the available filters.

3. Enter a **Name** and **Description** for the exception.
4. Enter a **File Path**, or click **Browse** to locate a file.
5. Select a firewall action (Allow, Allow with Notify, Block, Block with Notify, or Prompt) for the following network conditions:
   - **Trusted in**: applies only to an inbound connection for the Agent's native network(s).
   - **Trusted out**: applies only to an outbound connection for the Agent's native network(s).
   - **Not trusted in**: applies only to an inbound connection for any network that is not native to the Agent.
   - **Not trusted out**: applies only to an outbound connection for any network that is not native to the Agent.
6. Click **Apply** to save changes.

19.2.2 — Configure Network Exceptions

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

Configure the **Network Exceptions** to set how network exceptions are trusted.



To configure a network exception:

1. Navigate to the **Network Exceptions** screen. **Policy Properties>Firewall>Basic Firewall Protection>Network Exceptions**.
2. Select a row from the Network Exceptions table.

Note: The column headings are dynamic, allowing you to move their order and sort by a category within that column. Click the filter icon on a column heading to select a filtering option. See Filtering Views for more information on using the available filters.

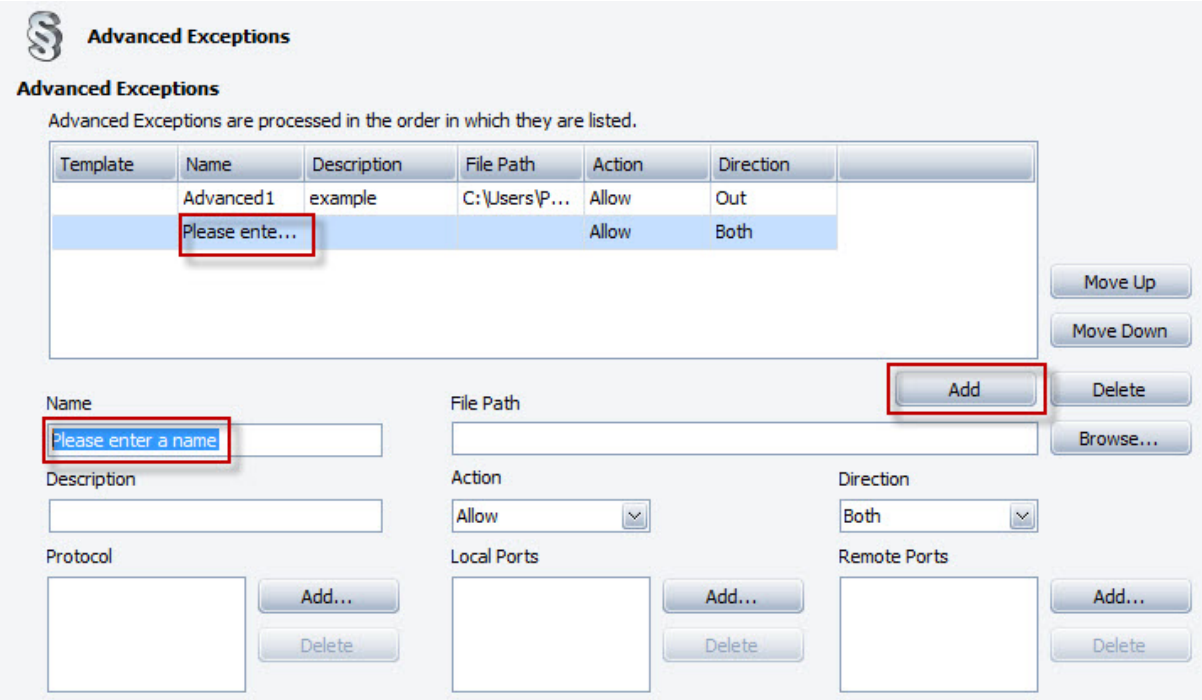
3. Select a firewall action (Allow, Allow with Notify, Block, Block with Notify, or Prompt) for the following network conditions:
   - **Trusted in**: applies only to an inbound connection for the Agent's native network(s).
   - **Trusted out**: applies only to an outbound connection for the Agent's native network(s).
   - **Not trusted in**: applies only to an inbound connection for any network that is not native to the Agent.
   - **Not trusted out**: applies only to an outbound connection for any network that is not native to the Agent.
4. Click **Apply** to save changes.

19.2.3 — Configure Advanced Exceptions

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

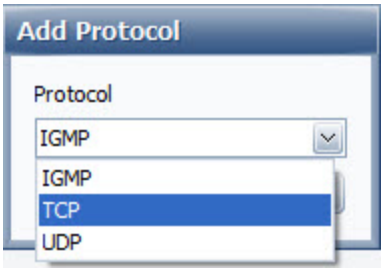
Create and configure an **Advanced Exception** for a more complex rule that can include combinations of protocol, local and remote ports, and direction of traffic, or it can consist of specific port or protocol exceptions that are not application specific.

The advanced exceptions are processed in the order listed and can be rearranged.

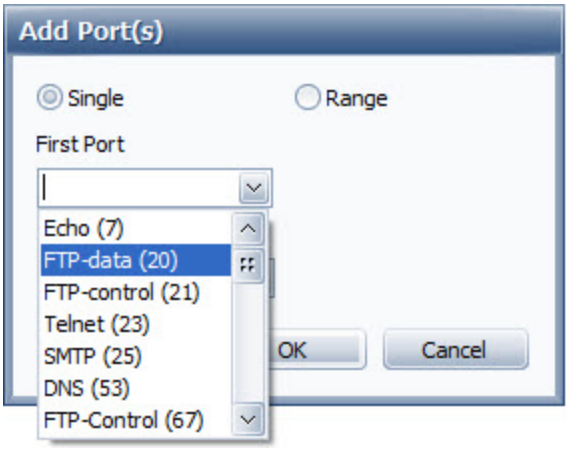


To configure advanced firewall exceptions:

1. Navigate to the **Advanced Exceptions** screen. **Policy Properties>Firewall>Basic Firewall Protection>Advanced Exceptions**.
2. To add a new advanced exception, click **Add**. An exception is added to the table, the UI then allows you to continue populating the fields below the table.
   -or-
   To edit an existing advanced exception, select a row in the Advanced Exceptions table. The fields below the table display for the selected item.
   -or-
   To delete an existing advanced exception, select a row in the Advanced Exceptions table. Click **Delete** and **Apply**. Skip to Step 8.
3. If new, enter a **Name** and **Description** for the exception. You can also modify the name and description of an existing exception.
4. Optionally, enter the **File Path**, or click **Browse** to locate or change a file.
5. Select a firewall **Action** (Allow, Allow with Notify, Block, Block with Notify, or Prompt) for the exception.
6. Select a **Direction** for the exception.
7. Enter one or more of the following:
8. To add a **Protocol**, click **Add** and select a protocol from the popup's drop-down list: ICMP, IGMP, TCP, or UDP.



9. To add a **Local Port**, click **Add** and select Single or Range. Then, enter a port number manually or select from the drop-down list.

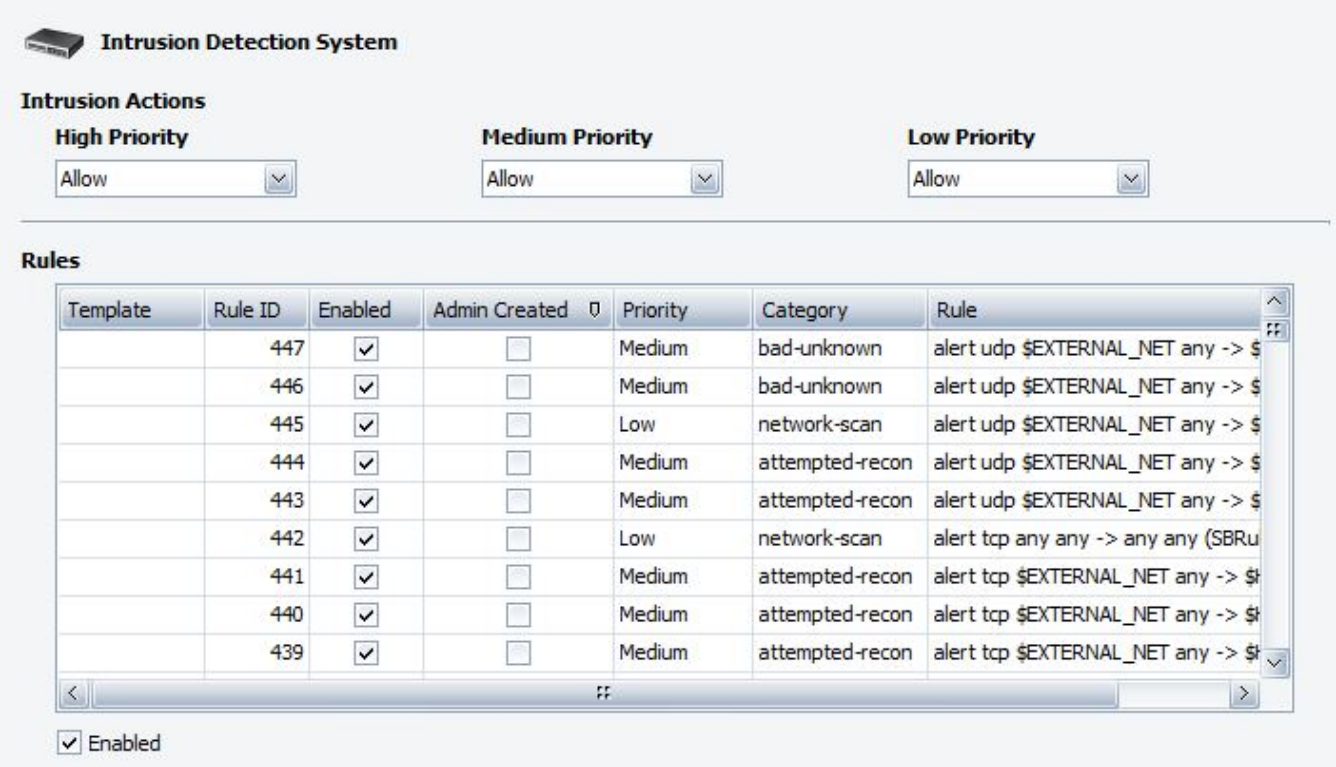


10. To add a **Remote Port**, click **Add** and select Single or Range. Then, enter a port number manually or select from the drop-down list.
11. Click **Apply** to save changes.

19.2.4 — Configure Intrusion Detection System (IDS) Rules

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

The **Intrusion Detection System** manages the IDS Snort® rules. You can enable/disable IDS rules. The agent(s) will block behavior based on the Snort rule(s) defined.



To enable/disable an IDS rule:

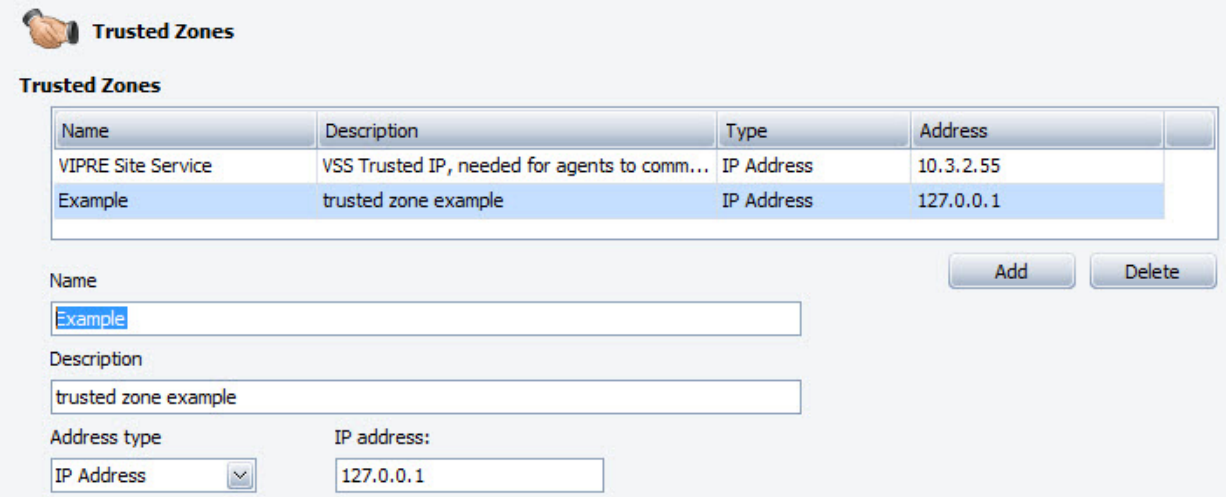
1. Navigate to the **Intrusion Detection System** screen. (**Policy Properties>Firewall>Basic Firewall Protection>Intrusion Detection System**).
2. In the **Rules** table area, select the desired IDS rule to disable.
3. In the **Enabled** check box below the table, unselect to disable the rule, or select to enable it.
4. Click **Apply** or **OK** to accept your changes.
5. Ensure that the "Enable intrusion detection system" check box on the Basic Firewall Protection screen is selected.

Note: To view a report of detected intrusions, in the Report Viewer, run the "Firewall Daily Intrusions Blocked" report.

19.2.5 — Configure Trusted Zones

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

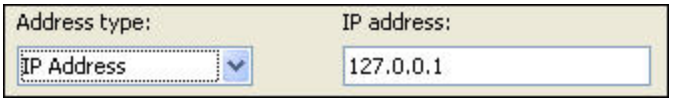
Configure **Trusted Zones** for your firewall.



To configure a trusted zone:

1. Navigate to the **Trusted Zones** screen. **Policy Properties>Firewall>Basic Firewall Protection>Trusted Zones**.
2. To add a new trusted zone, click **Add**. A trusted zone is added to the table.
   -or-
   To edit a trusted zone, select a row in the Trusted Zones table. The fields below become editable.
   -or-
   To delete a trusted zone, select a row in the Trusted Zones table. Click **Delete** and **Apply**. Skip the remaining steps.
3. If new, enter a **Name** and **Description** for the trusted zone. You can also modify the name and description of an existing trusted zone.
4. From the **Address type** drop-down list, select an address type:

   - **IP Address**: enter an IP address. Once selected, the IP address field is populated with an example IP address. Simply select the address and type over it.



   - **Range**: enter a range of IP addresses. When selected, the First and Last IP address boxes display with examples. Simply select the address and type over it.

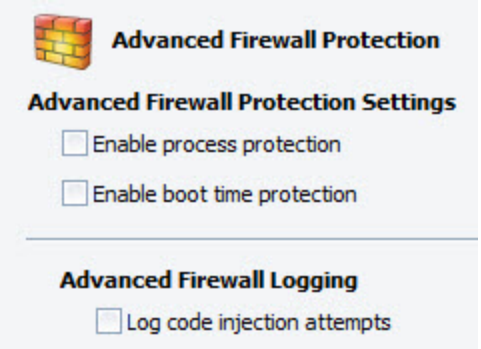
   - **Network**: enter an IP address and a Subnet mask. Simply select the address and mask and type over it.

5. Click **Apply** to save changes.

19.3 — Configure Advanced Firewall Protection Settings

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

Configure the **Advanced Firewall Protection**, which consists of process protection, boot time protection, and code injection logging.



To configure advanced firewall protection settings:

1. Navigate to the **Advanced Firewall Protection** screen. **Policy Properties>Firewall>Advanced Firewall Protection**.
2. Configure the following:
   - **Enable process protection**: the control switch for the **Process Protection** screen.
   - **Enable boot time protection**: when enabled, prevents outside connection attempts during startup.
   - **Log code injection attempts**: the log is accessible from the Agent console (**FIREWALL>Firewall History>HIPS**). Also, you can generate the "Firewall Daily Intrusions Blocked" report and select the "Code Injection Attempts" column.

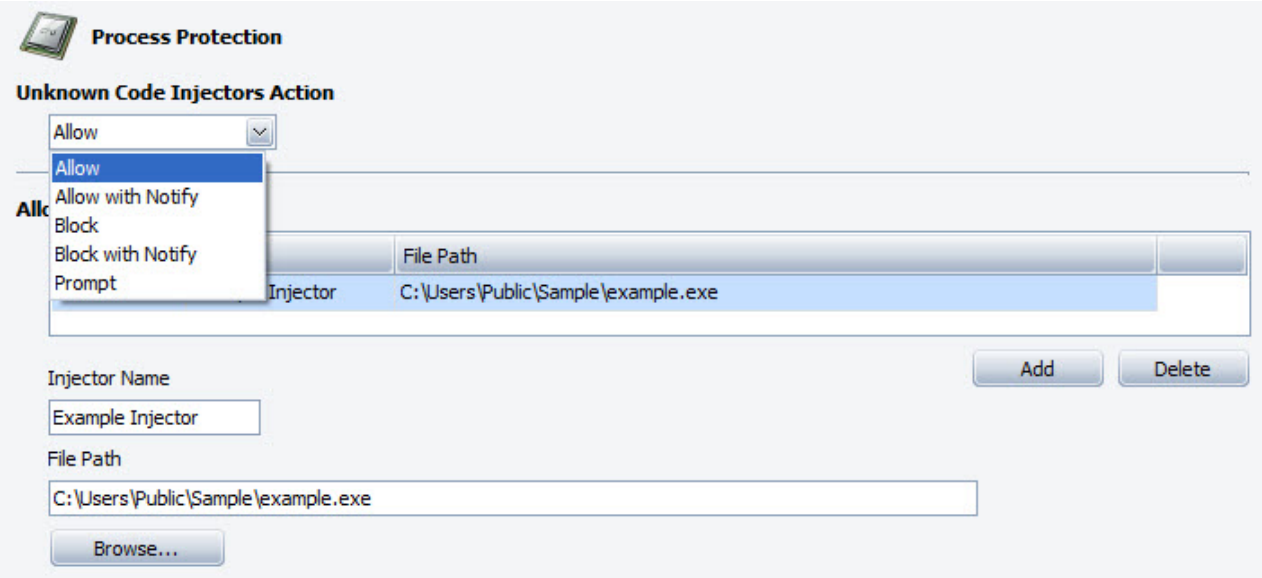
Note: Code injection statistics for the Agent can be accessed from **Agent console>FIREWALL>Statistics**.

3. Click **Apply** to save changes.

19.3.1 — Add Allowed Code Injectors

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

Create and configure **Allowed Code Injectors** by adding a file and assigning an unknown code injector action.



Note: "Enable process protection" must be selected on the Advanced Firewall Protection screen for the code injector settings to take effect.

To add an allowed code injector:

1. Navigate to the **Process Protection** screen. (**Policy Properties>Firewall>Advanced Firewall Protection>Process Protection**).
2. Click **Add**. A new row in the table is created, allowing you to enter the allowed injector.
3. In the **Unknown Code Injectors Action** drop-down, select one of the following: **Allow**, **Allow with Notify**, **Block**, or **Block with Notify**.
4. In the **Injector Name** field, enter a name for the allowed injector.
5. Click **Browse** and locate the application (EXE file only) that you want to allow to inject code.
6. Click **Apply** or **OK** to accept your changes.
7. Ensure that "Enable process protection" on the Advanced Firewall Protection screen is selected.

19.4 — Working with Firewall Templates

19.4.1 — Manage Firewall Templates

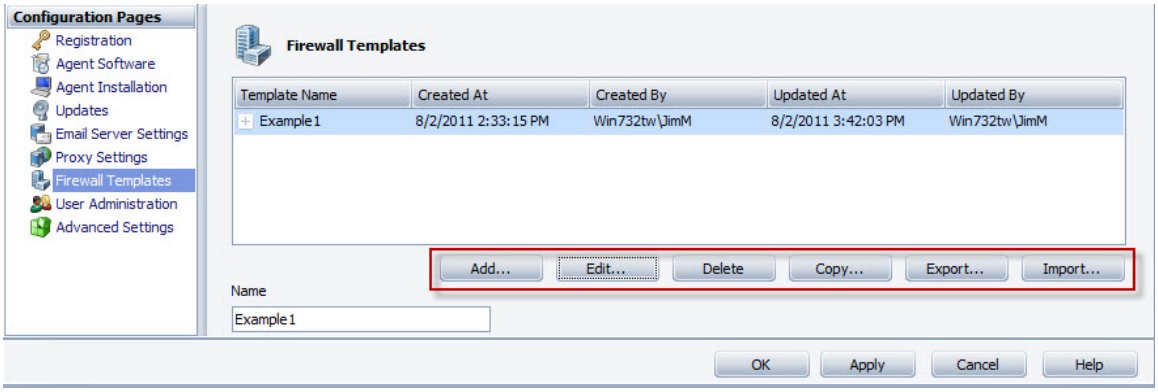
This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

Create **Firewall Templates** that you can assign to policies. You can also import/export them across sites and share them with other Administrators. One or more Firewall Templates can be used for any given policy. For example, you can create separate templates that have specific port exclusions for specific server platform configurations and other templates for specific application exceptions.

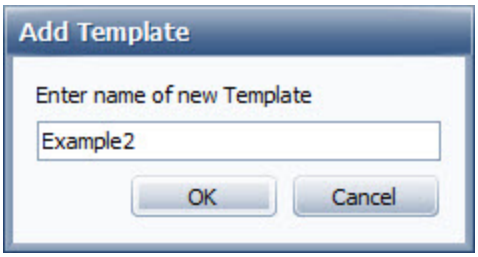
Note: The column headings are dynamic, allowing you to move their order and sort by a category within that column. Click the filter icon on a column heading to select a filtering option. See Filtering Views for more information on using the available filters.

To create and edit firewall templates:

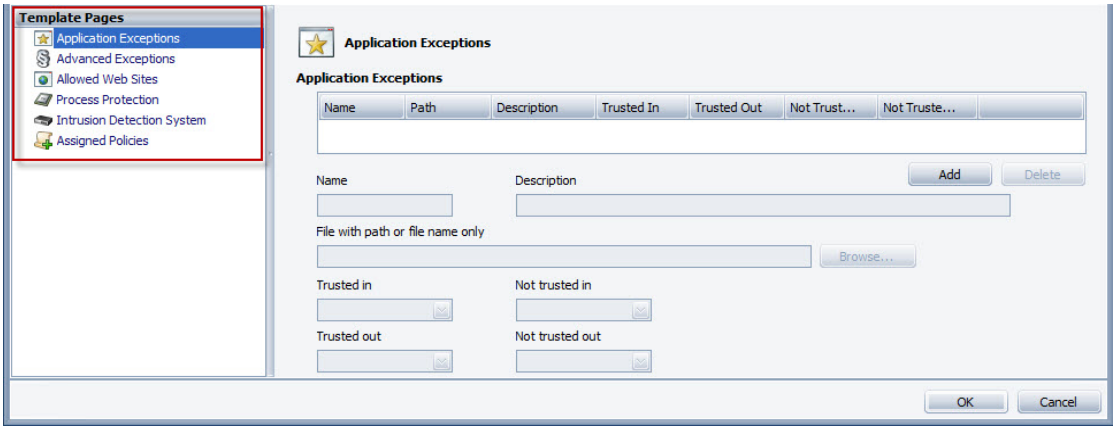
1. In the **Site Properties**, open **Firewall Templates**.



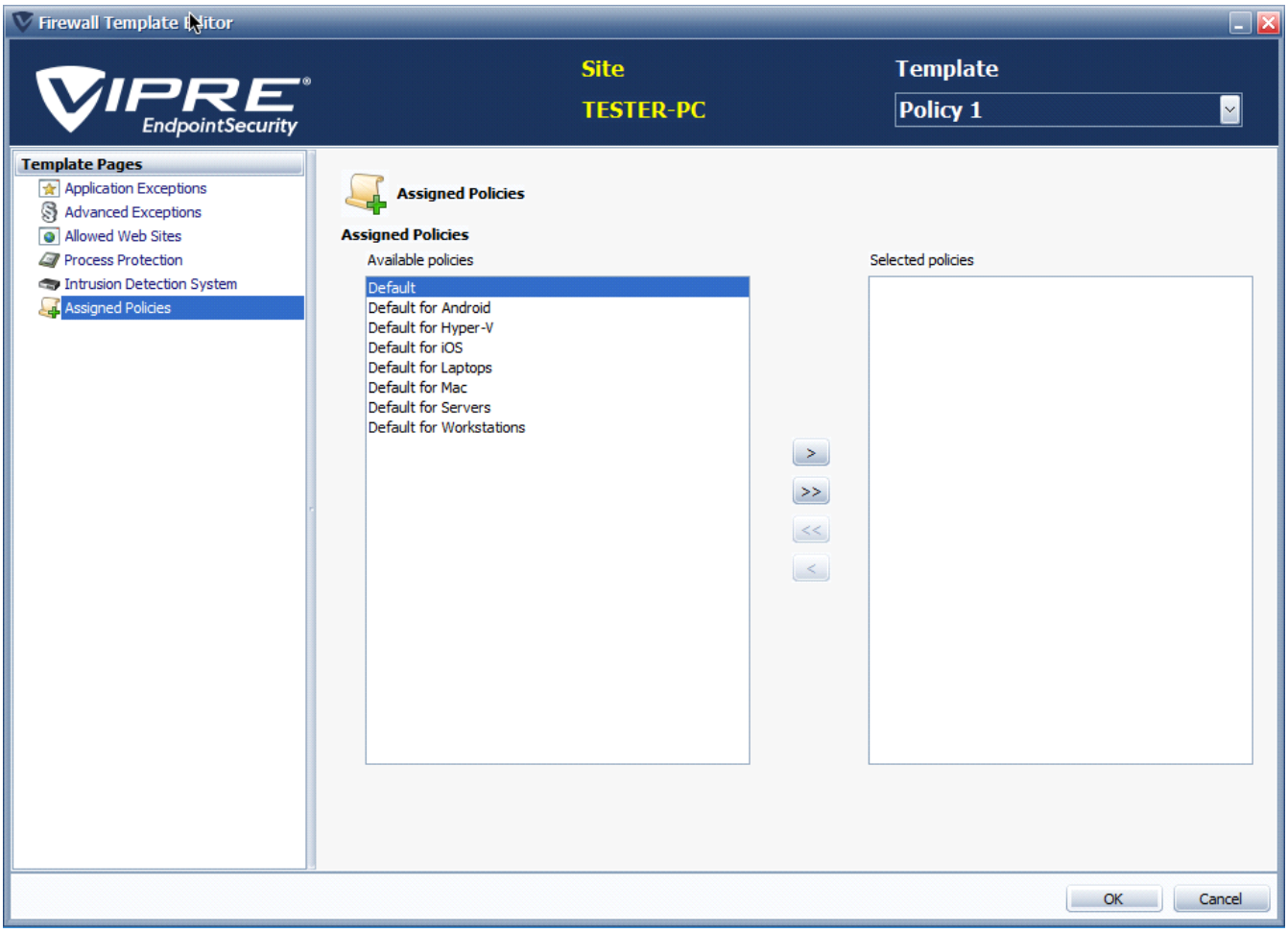
2. Click **Add**. The Add Template dialog box displays.



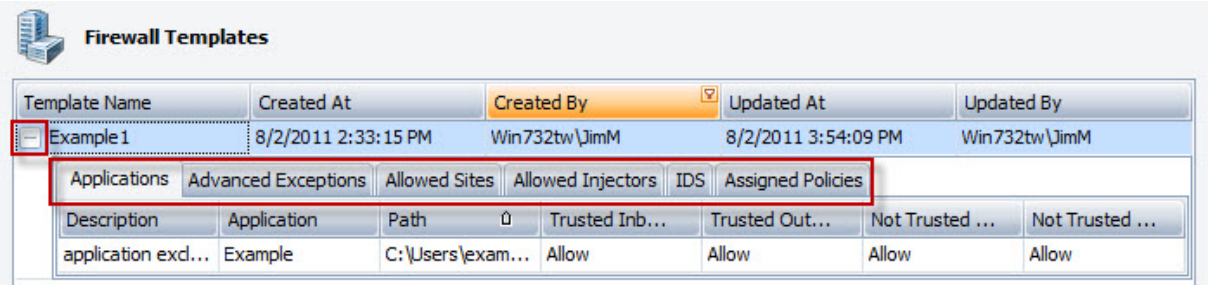
3. Enter a name for the new firewall template and click **OK**.
4. Click **Edit**. The Firewall Template Editor displays allowing you to configure the firewall template.



5. Configure any of the following firewall settings:
   - Application Exceptions
   - Advanced Exceptions
   - Allowed Web Sites
   - Process Protection (Allowed Code Injectors)
   - Intrusion Detection System (IDS)
6. Assign the firewall template to one or more policies:
   a. Click **Assigned Policies**.



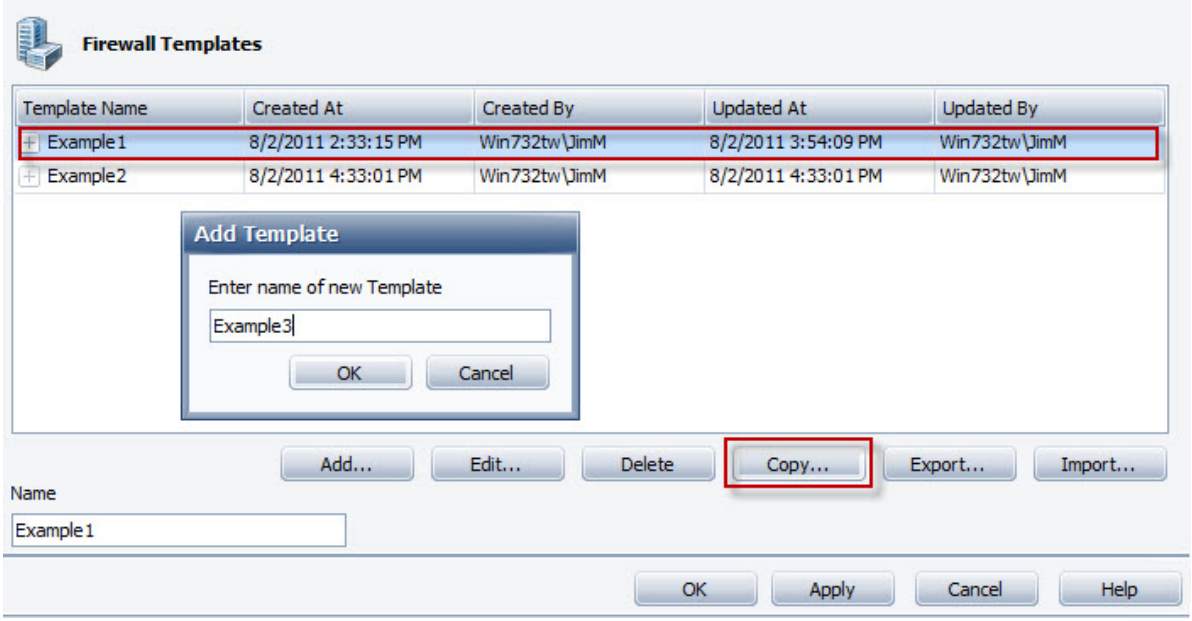
   b. In the **Available policies** area, select the desired policy that you want to assign the firewall template and use the arrows to move the policy to the **Selected policies** area.
   c. Click **OK**. You are returned to the Firewall Templates screen.
7. To view the newly applied settings to the firewall template, click the "+" to expand the properties. From here, you can click on the tabs to view the properties.



8. Click **Apply** to accept changes.

To copy firewall template settings to a new firewall template:

1. In the **Site Properties**, open **Firewall Templates**.
2. Select a template in the grid and click **Copy**. The Add Template dialog box displays.

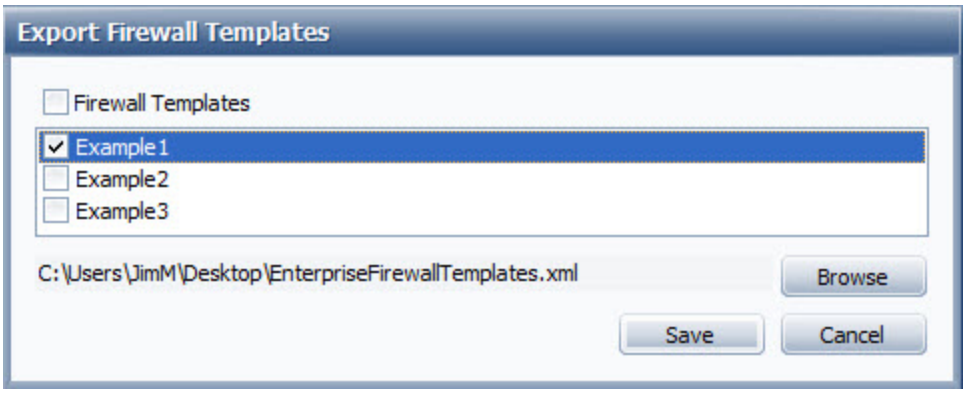


3. Enter the name of the new firewall template and click **OK**.
4. Click **Apply** to accept changes.

To export firewall templates:

Firewall templates are saved as XML files and exported across sites or shared with other VIPRE Business users, such as on the VIPRE Business Forum. The XML file is stored in the Documents and Settings folder. The exact file path is displayed.

1. In the **Site Properties**, open **Firewall Templates**.
2. Select a template in the grid and click **Export**. The Export Firewall Templates dialog box displays.



3. Select the firewall templates that you want to export.
4. Optionally, change the default location where the firewall template file will be saved.
5. Click **Save**.
6. Navigate to the saved XML file and send it to the desired recipient.

To import firewall templates:

1. In the **Site Properties**, open **Firewall Templates**.
2. Click **Import**.
3. Navigate to the firewall template file and open it. The imported template file appears in the Firewall templates list.
4. Click **Apply** to accept changes.

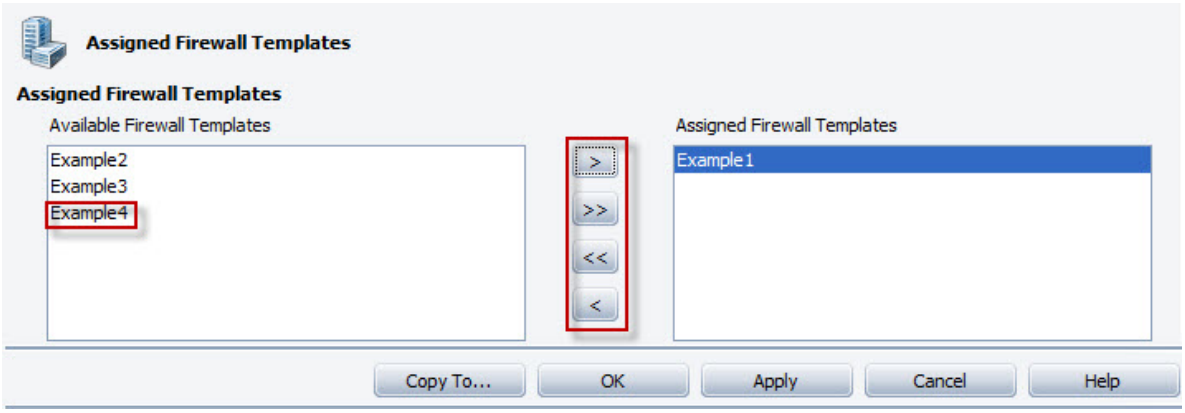
19.4.2 — Assign Firewall Templates to a Policy

This topic applies to VIPRE Premium and VIPRE Endpoint Security only.

Assign one or more firewall templates to a policy. Use the center arrows to move templates from one column to the other.

To assign firewall templates to a policy:

1. If you haven't already, ensure that you have firewall templates in your site. Create firewall templates as needed.
2. Open the **Assigned Firewall Templates** screen. (**Policy Properties>Firewall>Assigned Firewall Templates**).



3. In the **Available Firewall Templates** column, select the desired template and use the arrows to move them to the **Assigned Firewall Templates** column.
4. Click **Apply** to accept changes.

20 — Reporting

You generate reports using the **Report Viewer**, which is a standalone application that is installed and runs along with the Console. It can also be installed by itself on separate machines to be used by administrators and managers who want to run various reports at their convenience. The Report Viewer can be installed on as many machines as required. It supports VIPRE Business, VIPRE Business Premium, and VIPRE Endpoint Security. So, for example, if you have two sites with one running VIPRE Business and the other VIPRE Business Premium, you can use the Report Viewer to generate reporting data for both sites.

To open the Report Viewer:

Select **File>Report Viewer**.
-or-
Select **Start>All Programs>ThreatTrack Security>VIPRE Business>Report Viewer**.
-or-
Click the **Report Viewer** icon in the Admin Console's toolbar.

20.1 — Running Reports

After Agents are installed and scanning, you can generate reports to view various details. VIPRE Business includes several report templates that you can choose from, including:

- Agents scanned by Policy
- Applied Patches Detail
- Applied Patches Summary
- Executive Summary
- Firewall Daily Intrusions Blocked
- Firewall Daily Network Activity
- Firewall Daily Web Filtering
- Infected Machine Detail
- Infected Machine Summary
- Managed Products
- Missing Patches Detail
- Missing Patches Summary
- Patch Management Alerts
- Patch Management Summary
- Threat Count by Machine
- Threat Found Detail
- Threat Severity Detail
- Threat Severity Summary
- Top 25 Infected Machines

To run a report:

1. From the **Admin Console** select **File>Report Viewer**. The Report Viewer displays.
2. Select a report template from the Reports list. The selection fields will change based on the report selected.
3. Select the Start and End Dates of the reporting data.
4. Select the Agents and categories you want in the report.
5. Click **Preview**. The selected report displays.
6. Optionally, you can modify the margins, set a background, and add a header/footer.
7. Optionally, from the **Report Preview toolbar** you can save or email in various formats (such as pdf, mht, rtf, xls, csv, txt, jpg), print, and email.

20.2 — Scheduling Reports

You can schedule reports that include selection criteria, date range of reporting data, report and output type, scheduled frequency, time of report generation, and saving/emailing the output report.

When scheduling a report from the Report Viewer, another selection window displays with a list of **Scheduled Reports** (on the left) and three tabs in the main work area:

- **Selection Criteria**: select reporting data from specific Agents on Sites and Policies. Other criteria options are based on "Selected Report" on the Scheduling Criteria tab.
- **Scheduling Criteria**: set all specifics for scheduled reports.
- **Output Criteria**: set to save to a file and/or email attachment.

Note: Before creating a scheduled report, it's recommended to preview a test report to ensure that you create the report with the data that you are expecting.

To schedule a monthly, weekly, or one-time report:

1. Open the Reporting Scheduler:
   a. From the **Admin Console** select **File>Report Viewer**. The Report Viewer displays.
   b. Click the **Schedule** button in the upper-right corner of the window. The scheduling selection window displays.
   c. Click the **Scheduling Criteria** tab.
2. Under **Criteria**, do the following:
   a. Enter a **Scheduled Report Name**. You can be as descriptive as possible.
   b. Select a report type from the **Selected Report** drop-down. This will change the available options on the Selection Criteria tab.
   c. Select an **Output Format** for the generated report from the drop-down: CSV, EXCL, HTML, MHTML, PDF, PNG, RTF, TXT.
3. Under **Report Frequency**, select how often the scheduled report will run.
4. Under **Criteria**, select a **Date Range**.
5. Enter the **Time of day to run scheduled report**.
6. Choose criteria for the report:
   a. Click the **Selection Criteria** tab.

b. In the **Agents** tree list, select from the site(s), policies, and agents to limit the reporting data that will go into the report.
c. Select the remaining criterion, which varies according to the selected report in Step 2b.

7. Select and enter the output criteria for the scheduled report:
   - **Save to disk**: enter a folder that is visible to the VSS. If the VSS cannot connect to the location entered, the report will be saved to the logs folder.
   - **Email as attachment**: enter one or more email addresses delimited by a comma to receive the scheduled report.
8. Click **Apply** to save the scheduled report. The scheduled report is listed in the Scheduled Reports area and on the Report Viewer screen.

To edit a scheduled report:

1. From the Report Scheduler window, double-click on the scheduled report to open it.
2. Make your changes and click **Apply** to save changes.

To delete a scheduled report:

1. From the Report Scheduler window, right-click on a scheduled report.
2. Select **Delete Scheduled Report**. The scheduled report is removed from the schedule.

To copy a scheduled report:

1. From the Report Scheduler window, right-click on a scheduled report.
2. Select **Copy Scheduled Report**.
3. Enter a name for the copy and click **OK** to save.

21 — Contacting VIPRE Support

USA, CANADA AND CENTRAL AND SOUTH AMERICA

Business and Enterprise Customers

311 Park Place Blvd, Suite 300, Clearwater, FL, 33759, USA

Telephone: +1 (877) 757-4094

https://support.threattracksecurity.com

Contacting VIPRE Sales

311 Park Place Blvd, Suite 300, Clearwater, FL, 33759, USA

Telephone: +1 (855) 885-5566 (+1 727-324-0001)

Email: vipresales@threattrack.com