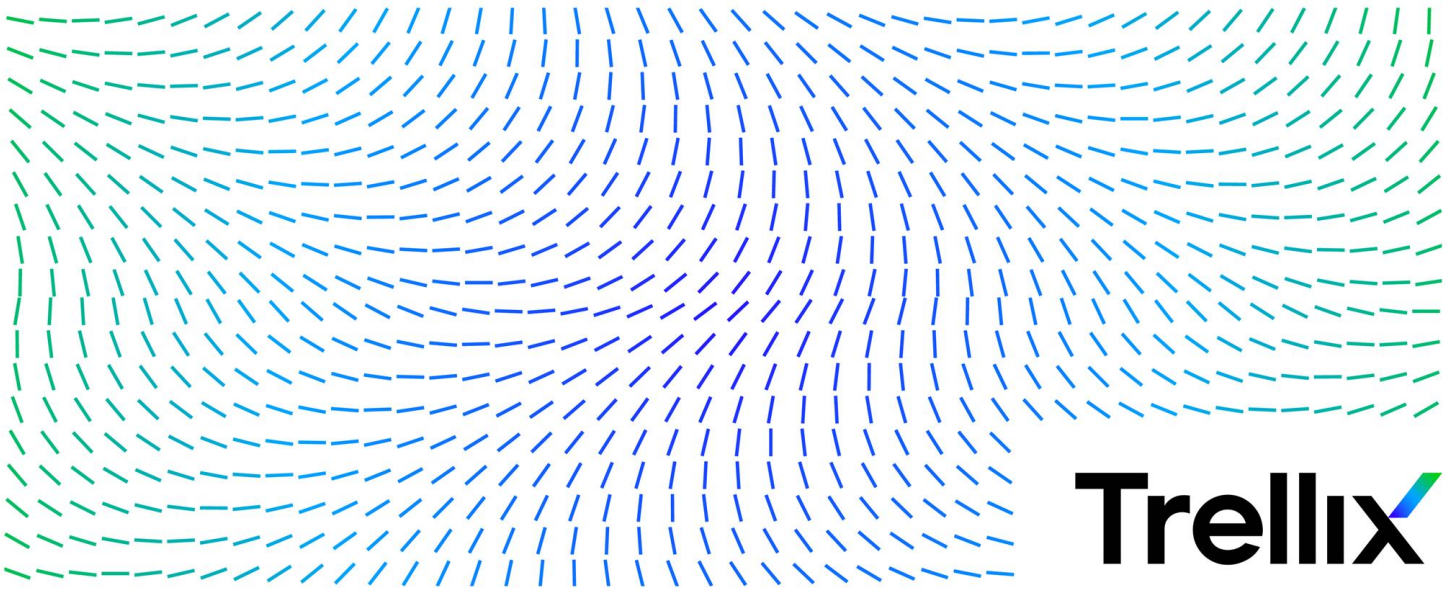
ENDPOINT SECURITY

AGENT DEPLOYMENT GUIDE

RELEASE 35.30.0



Trellix

Endpoint Security Agent Deployment Guide

Software Release 35.30.0

Revision 1

Trellix Contact Information:

Website: www.trellix.com

Technical Support: https://www.trellix.com/en-us/support.html

Phone (US):

1.408.321.6300

1.877.347.3393

Contents

PART I: Overview

CHAPTER 1: System Requirements

This section describes the minimum system requirements for a Endpoint Security version 35.30.0 installation.

Hardware Requirements

For information on hardware requirements, see the *Agent Software Specification Sheet*.

Operating System Requirements

Some Trellix Endpoint Security Agent software features require specific minimum versions of the Endpoint Security Server software. See "About Trellix Endpoint Security Agents" in the *Endpoint Security Agent Administration Guide* for a description of each feature and the minimum Endpoint Security Server version required.

Agents can provision with on-premises, virtual, or cloud Endpoint Security Servers. For more information about these different Endpoint Security form factors, see the appropriate *Endpoint Security Agent Deployment Guide*.

For further information on supported operating systems, see the *Agent Software Specification Sheet*.

PART II: Planning

This section briefly describes the steps to install and deploy Endpoint Security Agent version 35.30.0 to your host endpoints.

IMPORTANT: For complete instructions on installation and deployment, please see Installation and Deployment on page 19.

CHAPTER 2: Preparing for Installation

Before you install Endpoint Security Agent, consider the following:

Task	Instructions
1. Ensure that you have whitelisted Endpoint Security Agent files in your third-party antivirus software packages.	See Before You Install or Upgrade the Agent Software on page 91.
2. Determine whether to install agent software manually on individual host endpoints, or use an enterprise-wide deployment software, such as BigFix or SCCM for Windows, or JAMF for Mac.	See Installing the Agent Installation Package on page 41.
3. Are you deploying agents in a VDI (virtual desktop infrastructure) environment?	See Deploying Agents in a VDI Environment on page 24.
4. Does your enterprise use an HTTPS proxy server to allow endpoints on your network to access the Internet?	See Agent HTTPS Proxy Support on page 25.
5. Will you configure the Removal Protection Password to keep your agents secure and prevent unauthorized removal of the agent software from endpoints in your enterprise?	See Configuring the Agent Removal Protection Password on page 75.
6. Do you plan to turn off Tamper Protection or do you want the local admin to be able to stop the agent?	See Agent Protection on page 27.

CHAPTER 3: Deployment Steps

To deploy Endpoint Security Agent software in your environment:

Task	Instructions
1. Whitelist all Endpoint Security files in your antivirus software packages.	See Before You Install or Upgrade the Agent Software on page 91.
2. Define your server address list.	See Configuring the Server Address List on page 99.
3. Verify that the primary (provisioning) Endpoint Security servers have been identified.	See Deploying Agents in a VDI Environment on page 24.
4. Configure the Removal Protection policy for all of your host endpoints to prevent the unauthorized removal of the Endpoint Security software from your host endpoints.	See Configuring the Agent Removal Protection Password on page 75.
5. Obtain the agent installation images required for your environment.	See Obtaining Agent Installation Software on page 29.
6. Install the agent software on your endpoints.	See Installation and Deployment Steps on page 37.
7. Create malware detection process and folder exclusions for any other antivirus software you have installed on your Windows host endpoints.	See Before You Install or Upgrade the Agent Software on page 91.

PART III: Installation and Deployment

CHAPTER 4: Agent Installation Considerations

Consider the following questions before you install Endpoint Security Agent software on your host endpoints.

- Have you followed Trellix's recommendation that you deploy your Endpoint Security Server software before you deploy your agent software?
- Have you whitelisted Endpoint Security Agent files in your third-party antivirus software packages? See Before You Install or Upgrade the Agent Software on page 91.
- Does your enterprise want to conceal agents or agent installation from host endpoint users? See Setting Up a Disguised Installation on page 68.
- Will you install agent software manually on individual host endpoints, or use an enterprise-wide deployment software, such as BigFix or SCCM for Windows or JAMF for Mac?

  NOTE: Trellix recommends that you manually install the agent software on a few host machines and test the agent software before you deploy the agent software to all your host machines.

- Are you deploying agents on endpoints in a VDI environment? See Deploying Agents in a VDI Environment on page 24.
- Where will the agent software reside on your host endpoints? See Specifying the Agent Installation Location on page 68.
- Does your enterprise use an HTTPS proxy server to allow endpoints on your network to access the Internet? See Agent HTTPS Proxy Support on page 25.
- Will you configure the Removal Protection Password to keep your agents secure and prevent unauthorized removal of the agent software from endpoints in your enterprise? See Configuring the Agent Removal Protection Password on page 75 for more information.

- Do you plan to configure a Tamper Protection policy to prevent the agent software on your Windows endpoints from being stopped or started or protect the agent process from injection and inspection? See "Configuring a Tamper Protection Policy" in the *Endpoint Security Agent Administration Guide* for more information.

Linux Operating System Upgrade Considerations

If you update your Linux-based operating system to a major version, you may be required to uninstall the agent software. The uninstall command required to uninstall the Endpoint Security Agent software version 35.30.0 on your Linux endpoint is determined by the file type you used to install the agent software on your Linux endpoint. See Uninstalling Linux Agent Software on page 85 for more information.

When you are ready to reinstall the agent software on your endpoint, use the `.rpm` or `.deb` file that is compatible with your Linux operating system version. See Installing the Agent Installation Package on page 41 for more information.

IMPORTANT: The `.rpm` or `.deb` file you use to install the agent software on your Linux endpoints must be compatible with your Linux operating system. For example, if your Linux endpoints are currently running RHEL version 6.8, you must use the `xagt-29.x.x-1.el6.x86_64.rpm` file to install the agent software. If your Linux endpoints are running RHEL version 7.3, you must use the `xagt-29.x.x-1.el7.x86_64.rpm` file to install the agent software.

Endpoint Security Agent version 28 deprecated the Linux agent runscript installation package. All new agent software installations on supported RHEL and CentOS versions should use the compatible RPM package provided.

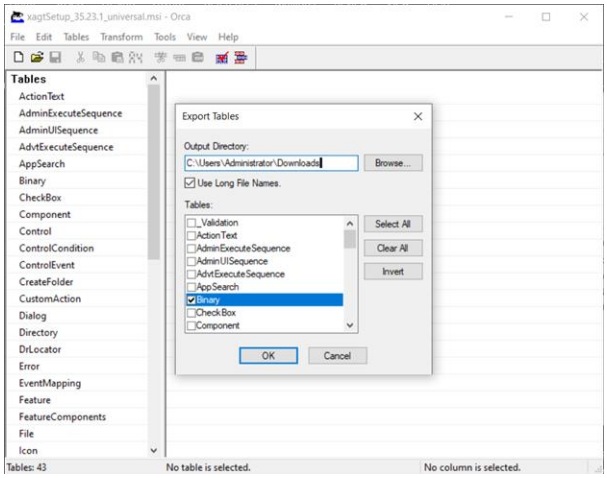
Enabling Device Guard Code Integrity

NOTE: Follow these instructions only when deploying Endpoint Security Agent from Windows-based golden image systems.

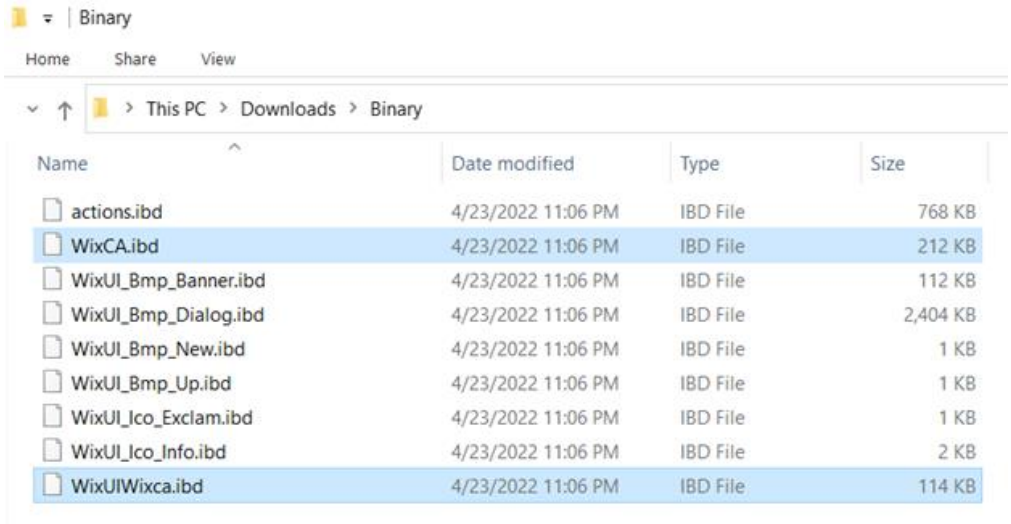
Before you deploy the Endpoint Security Agent software to your host endpoints, the Windows Defender Device Guard Code Integrity feature must be properly configured on your golden image system. This ensures that essential DLL files become part of the Code Integrity policy before you provision this policy across the enterprise.

Follow these steps to extract the relevant DLL files onto the golden image system.

1. Install the agent software on your golden image system.
2. Open the installer MSI package using Orca (included in the Windows SDK).
3. From the File menu, select **Tables** > **Export Tables**.
4. Select the **Binary** box and select OK.



5. From Windows Explorer, navigate to the exported **Binary** folder to find and locate two files: `WixCA.ibd` and `WixUIWixca.ibd`.



6. Change the extension of both files to DLL.
7. Extract both `WixCA.dll` and `WixUIWixca.dll` to the golden system.

When you create the Code Integrity policy, use this policy to enable the "Deploy Windows Defender Application Control" policy.

Deploying Agents in a VDI Environment

IMPORTANT: The `.rpm` or `.deb` file you use to install the agent software on your Linux endpoints must be compatible with your Linux operating system. For example, if your Linux endpoints are currently running RHEL version 6.8, you must use `xagt-27.x.- 1.el6.x86_64.rpm` to install the agent software. If your Linux endpoints are running RHEL version 7.2 or 7.3, you must use `xagt-27.x.x-1.el7.x86_64.rpm` to install the agent software.

A virtual desktop infrastructure (VDI) is virtualization technology that allows you to host a user desktop inside a virtual machine. If you are deploying Trellix Endpoint Security Agent software in a VDI environment, Trellix recommends deploying in a persistent or semi-persistent VDI environment to prevent cloned agents.

IMPORTANT: When deploying the Endpoint Security Agent software in a VDI environment, use the **Specify an alternate Configuration File location** option during installation.

If you need to deploy Endpoint Security Agent software in a non-persistent VDI environment, follow the recommendations in Guidelines for Deploying Agents in a Non-Persistent VDI Environment below to prevent cloned agents and reduce the number of duplicate hosts in your VDI environment.

Cloned agents are Endpoint Security agents that have provisioned with the Endpoint Security server using the same agent ID. Cloned agents may disrupt communication between your Endpoint Security server and host endpoints. See "Managing Cloned Agents" in the *Endpoint Security Agent Administration Guide* for more details.

Duplicate agents are Endpoint Security Agents that have provisioned with the Endpoint Security server using the same hostname.

To learn more about Endpoint Security Agent deployment in a VDI environment, see the community article on this topic.

Guidelines for Deploying Agents in a Non-Persistent VDI Environment

Follow these guidelines to deploy Endpoint Security Agent software in a non-persistent VDI environment.

- Use a Golden or master image to perform the initial installation. See Installing Agents Using a Golden or Master Image on page 71.

To perform any future updates of Endpoint Security Agent in a non-persistent VDI environment, you must uninstall the agent first and then reinstall the agent using an updated golden image.

- From the Endpoint Security server Web UI Aging Settings page, lower your agent aging settings to reduce the number of duplicate hosts. See "Configuring Host Aging Settings" in the *Endpoint Security Agent Administration Guide* for more details.

  When a host endpoint is deleted, all alerts and acquisitions for that host endpoint are also deleted.

VDI Pruning Tool

As a Trellix Endpoint Security administrator, you can remove duplicate hosts in a VDI environment with the VDI pruning tool. For more information about downloading the VDI pruning tool, see the community article on this topic.

IMPORTANT: Data may be lost if you use the VDI pruning tool. To preserve all host attribute data on your Endpoint Security server, perform a manual host merge. See "Merging Hosts Manually" in the Trellix *Endpoint Security Agent Administration Guide* for more information on how to do this.

Agent HTTPS Proxy Support

If your enterprise uses an HTTPS proxy server to allow endpoints on your network to access the Endpoint Security Web UI or the Internet, you must configure your proxy settings before installing the Endpoint Security Agent software on your endpoints. An HTTPS proxy allows the agent to communicate with the Endpoint Security Server and Trellix's DTI cloud to download malware and antivirus content updates and software updates. See HTTPS Proxy Server Overview and Configuration on page 45 for more information about setting up an HTTPS proxy server for your Windows, macOS, and Linux endpoints.

NOTE: Explicit HTTPS proxy support for Internet access is supported in Endpoint Security version 25 or later.

IMPORTANT: An Internet connection is required for the Endpoint Security to download malware definitions and other agent updates.

When to Reboot

The agent upgrade process is completely invisible to endpoint users. The process does not usually require restarting host endpoints and does not prompt end users for action. However, after installing or upgrading Endpoint Security Agent software to version 35.30.0, a reboot may be required for Mac and Windows endpoints to ensure:

- macOS agents receive a new configuration from the Endpoint Security Server.
- Agent notifications start on Windows endpoints.

A reboot may also be required to complete the Windows installation and avoid problems with future installations that check for pending reboots. You can use the `wevtutil qe` application command to query the event log and determine if a reboot is necessary.

To query the event log, open the Windows command line and run the following command at the prompt:

```
wevtutil qe Application /rd:true /f:text /q:"*[System/EventID=1029] and *
[EventData[Data='FireEye Endpoint Agent']]"
```

If a reboot is required, the following event will appear:

```
"FireEye Endpoint Agent. Restart required. The installation or update for the
product required a restart for all changes to take effect. The restart was
deferred for a later time."
```

You can use the following command to identify the name and process ID of the application that locked a Trellix system file open:

```
wevtutil qe Application /rd:true /f:text /q:"*[System/EventID=1025] and *
[EventData[Data='FireEye Endpoint Agent']]"
```

This command returns the name and process ID of the application that locked a file open. In the example below, Firefox has the NamespaceToEvents.dll file open.

```
"FireEye Endpoint Agent. The file C:\Windows\FireEye\NamespaceToEvents.dll is
being used by the following process: Name: firefox , Id 1060."
```

Close the application that caused the reboot. Run the `wevtutil qe Application` command above to verify if a reboot is still required.

An endpoint reboot may also be required in the rare instance when the agent executable cannot be replaced during the upgrade.

See the *Endpoint Security Agent Administration Guide* for more information about upgrading Endpoint Security Agent software on your endpoints.

Agent Notifications

The `xagtnotif.exe` program handles all agent notifications on the endpoint. A copy of the `xagtnotif.exe` program automatically runs with each user login and is required for

Malware Detection and Exploit Guard. This section provides how to instructions for disabling and enabling xagtnotify.exe.

NOTE: You can use an enterprise-wide software delivery program such as SCCM to automate the `reg` commands for disabling and enabling `xagtnotify.exe`.

To disable xagtnotif.exe:

1. Open a Windows command prompt as an administrator.
2. Run the following command:

```
reg delete HKEY_LOCAL_
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v xagtnotif
/reg:32 /f
```

NOTE: `xagtnotif.exe` will continue to run after the service is stopped and disabled.

If your agent configuration has Exploit Guard and malware protection enabled, you **must** follow these steps to enable `xagtnotif.exe`.

To enable xagtnotif.exe:

1. Open a Windows command prompt as an administrator.
2. Run the following command:

```
reg add HKEY_LOCAL_
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v xagtnotif /t
REG_SZ /d "%windir%\FireEye\xagtnotif.exe -n" /reg:32 /f
```

Agent Protection

Endpoint Security Agent software supports tamper protection settings that prevent the unauthorized removal of agent software from your host endpoints, agent process and service terminations, agent process injection and inspection protection, and agent database tampering. See the *Endpoint Security Agent Administration Guide* for more information about configurable and non configurable Endpoint Security Agent tamper protection settings.

NOTE: To improve agent protection on your host endpoints, Endpoint Security Agent version 27 and later disables functionality in the Windows Service panel that allows administrators to manage or terminate agent service on the host endpoint. The `sc stop xagt` and `net stop xagt` commands are also disabled.

Agent Removal Protection

Endpoint Security Agent version 26 or later provides support for configuring a **Removal Protection Password** policy that prevents unauthorized users from removing the agent software from host endpoints in your enterprise.

See Configuring the Agent Removal Protection Password on page 75 for more information.

Agent Tamper Protection

The Agent Tamper Protection policy allows you to protect the Endpoint Security Agent software on your Windows endpoints so that you can have full control over the programs and applications running on your endpoints. This agent policy has two protection components. It prevents agent services from being stopped and restarted on your endpoints and protects the agent process from injection and inspection.

NOTE: Trellix Endpoint Security Agent version 20 or later supports the Tamper Protection policy's injection and inspection protection component for Windows endpoints only.

Trellix Endpoint Security Agent version 29 or later supports the Tamper Protection policy's start and stop functionality for agent services on Windows endpoints only.

IMPORTANT: Trellix does not recommend disabling your Tamper Protection policy because it may allow users with administrative rights, threat actors, and malware to compromise your endpoint protection.

See "Configuring a Tamper Protection Policy" in the *Endpoint Security Agent Administration Guide* for more information.

CHAPTER 5: Obtaining Agent Installation Software

Trellix constantly enhances and updates its agent software. It is important that you keep the software versions on your agents current to ensure they have the most up-to-date protection. This section describes how to obtain agent software and how to maintain the agent versions available on your Endpoint Security server.

New agent installation software images are not automatically included with the Endpoint Security server. After your Endpoint Security server has been installed or upgraded and the server has connected with FireEye's Dynamic Threat Intelligence (DTI) cloud, the newest versions of the agent software images for each platform (Windows, macOS, and Linux) are automatically downloaded to the Endpoint Security server for you. This automatic download may take up to an hour to occur.

After it has connected to the DTI cloud, your Endpoint Security server checks for newer agent software every hour. If newer agent software is available, the Endpoint Security server obtains it, stores it, and makes it available for you to download to your agents.

Previously installed agent software images are retained after you upgrade the Endpoint Security server.

If you do not automatically link your Endpoint Security server to the DTI cloud or if you need an earlier version of the agent software, you must obtain the installation image manually from the DTI cloud or the offline portal and upload it to the Endpoint Security server. See Manually Retrieving Installation Images from the DTI Cloud on page 32 or Obtaining Agent Images Using the Offline Portal on page 34 for more information.

IMPORTANT: Agent installation images obtained manually must be uploaded to the Endpoint Security server before they can be deployed to your host endpoints. This ensures that the correct agent configuration file and agent certificates are included in the agent installation package you deploy to your host endpoints.

If agent software has not yet been downloaded to your Endpoint Security server, the following message appears on the Agent Versions tab:

```
No agent installation software was found. Agent installation software is
automatically downloaded from DTI or can be manually uploaded.
```

This section includes the following topics:

Prerequisites

- Admin or fe_services access

Agent Installation Package Contents

The agent software installation images are `.cms` files for Windows, Mac, and Linux. After uploading an agent installation image to the Endpoint Security server, the server generates an installation package and list the package on the Agent Versions page in the Endpoint Security Web UI. From the Agent Settings page, you can deploy and install an agent installation package on your endpoints.

IMPORTANT: Only Endpoint Security software version 25 or later can run on Linux platforms.

The agent installation package is a `.zip` file (Windows), a `.dmg` file (macOS), or a `.tgz` file (Linux).

- The Windows `.zip` file includes the agent installer file (`.msi`) and the agent configuration file (`agent_config.json`).
- The macOS `.dmg` file includes the agent installer file(`.mpkg`) file and the agent configuration file (`agent_config.json`).
- The Linux `.tgz` file includes the `.rpm`, `.deb`, and `.run` agent software installation files that map to specific Linux operating system versions and the agent configuration file (`agent_config.json`). See Manually Installing Agent Software on Linux Endpoints on page 58 for more information.

The agent configuration file (`agent_config.json`) specifies FireEye Endpoint Security server settings for the agent. Generally, both the agent installer file and the agent configuration file must be in the same folder on any machines on which you want to

install the Endpoint Security agent. However, you can use the CONFJSONDIR installation option to specify an alternate location for the configuration file.

Automatically or Manually Downloading the Agent Installation Image

Agent installation software images are not automatically included when you receive your Endpoint Security server. However, after your Endpoint Security server connects to the DTI cloud, by default, the server checks for newer agent software at hourly intervals. If newer agent software is available, the Endpoint Security server obtains it, stores it, and makes it available for you to download to your agents. You can also manually download agent software from FireEye's DTI cloud or upload it directly from FireEye.

NOTE: Trellix recommends that you retrieve agent installation software from the DTI, rather than directly from Trellix.

IMPORTANT: Agent installation images obtained manually must be uploaded to the Endpoint Security Sserver before they can be deployed to your host endpoints. This ensures that the correct agent configuration file and agent certificates are included in the agent installation package you deploy to your host endpoints.

Disabling Automatic Agent Software DTI Downloads

Using the Endpoint Security Server CLI, you can disable the automatic download of newer agent software from Trellix's DTI cloud to your Endpoint Security Server.

To disable automatic downloads of the agent installation image from the DTI cloud:

1. Enable CLI configuration mode for the Endpoint Security Server:
   ```
   hostname > enable
   hostname # configure terminal
   ```
2. Disable automatic downloads of the agent installation image from DTI cloud:
   ```
   hostname (config) # no fenet hx-agent autoupdate enable
   ```
3. Save your settings:
   ```
   hostname (config) # write mem
   ```


Enabling Automatic Agent Software DTI Downloads

Using the Endpoint Security Server CLI, you can re-enable the automatic download of newer agent software from Trellix's DTI cloud to your HX appliance if this function has previously been disabled.

To enable automatic downloads of agent installation image software from the DTI cloud:

1. Enable CLI configuration mode:
   ```
   hostname > enable
   hostname # configure terminal
   ```
2. Enable automatic downloads of the agent installation image from DTI cloud:
   ```
   hostname (config) # fenet hx-agent autoupdate enable
   ```
3. Save your settings:
   ```
   hostname (config) # write mem
   ```

Manually Retrieving Installation Images from the DTI Cloud

You can manually obtain agent installation images from FireEye's DTI cloud using CLI commands. You can retrieve a specific agent installation image or the latest image. After you have retrieved the image, you must upload it to the Endpoint Security server. See Uploading an Installation Image from FireEye.

To manually obtain an agent installation image from DTI cloud:

1. Enable CLI configuration mode for the Endpoint Security server:
   ```
   hostname > enable
   hostname # configure terminal
   ```
2. Check whether any new agent images are available on the DTI:
   ```
   hostname (config) # fenet hx-agent image check
   ```
   Alternatively, you can use the following command to refresh the agent metadata available on the DTI.
   ```
   hostname (config) # fenet hx-agent metadata refresh
   ```
3. List all agent images available on the DTI, fetched from the DTI, or available on the local server:
   ```
   hostname (config) # show fenet hx-agent image available
   ```
   This command lists supported operating systems, FireEye Endpoint Agent versions, and the content IDs associated with each agent image available.

4. Retrieve an agent image from the DTI:
   `hostname (config) # fenet hx-agent image fetch content-id <content-id>`

   where <content-id> is the content ID associated with the FireEye Endpoint Agent image you want to retrieve.

   You can also simply retrieve the latest agent image from the DTI:

   `hostname (config) # fenet hx-agent image fetch latest`
5. Verify and upload the agent image to the Endpoint Security server :
   `hostname (config) # fenet hx-agent image apply content-id <content-id>`

   where <content-id> is the ID associated with the FireEye Endpoint Agent image you want to upload.

   If you retrieved the latest agent image in Step 4, you can upload it to the Endpoint Security server using the following command:

   `hostname (config) # fenet hx-agent image apply latest`

Uploading an Installation Image from FireEye

You can manually upload a `.cms` (Windows, Mac, or Linux) agent installation image acquired directly from FireEye to the Endpoint Security server.

Agent installation images obtained manually must be uploaded to the Endpoint Security server before they can be deployed to your host endpoints. This ensures that the correct agent configuration file and agent certificates are included in the agent installation package you deploy to your host endpoints.

To upload an installation image from FireEye:

1. Copy the `.cms` agent installation image you acquired from FireEye onto your workstation. Contact your FireEye support representative for help with acquiring an installation image.
2. In the Web UI, select **Agent Settings** on the **Admin** menu and then select the **Agents Versions** tab.
3. On the Agent Versions tab, click **Browse**.
4. In the dialog box, browse to the installation image that you downloaded, select the image, and then click **Open**.

   The file name appears in the Browse box on the Agent Versions tab.
5. Click **Upload**.

After an agent image has been posted to the Agent Versions tab, the software package can be downloaded and installed. See Downloading an Agent Installation Package from the Web UI on page 43 and Installing the Agent Installation Package on page 41.

Obtaining Agent Images Using the Offline Portal

Using the CLI, you can obtain agent installation images for use by the Endpoint Security server using FireEye's Dynamic Threat Intelligence (DTI) offline portal. This section describes the necessary steps.

Agent installation images obtained manually must be uploaded to the Endpoint Security server before they can be deployed to your host endpoints. This ensures that the correct agent configuration file and agent certificates are included in the agent installation package you deploy to your host endpoints.

Prerequisites

- You must have an offline portal account. If you do not already have one, contact your FireEye sales representative.
- Admin access

To obtain agent images from the offline portal and apply them to the Endpoint Security server:

1. Enable CLI configuration mode on the server:

   ```
   host # enable
   host # configure terminal
   ```

2. Enter the following command to put the server in an offline state:

   ```
   <host> (config) # fenet op-mode local
   ```

3. Log into the DTI Offline Update Portal and download the `femeta_HX_AGENT.ensig` metafile from the portal to your machine. Then use scp (secure copy) to copy the file to the `/data/updates` directory on the server. For additional information, see the *DTI Update Portal User Guide*.

4. Enter the following command to refresh the agent metadata:

   ```
   <host> (config) # fenet hx-agent metadata refresh
   ```

5. Download the file `image-hx_agent-<version>.img` (where <version> is the version number of the agent image) from the portal to your machine. Then use scp (secure copy) to copy the file to the `/data/updates` directory on the server. For additional information, see the *DTI Update Portal User Guide*.

6. Enter the following command.

   ```
   <host> (config) # fenet hx-agent image fetch content-id <content-id>
   ```

   where <content-id> is the ID of the agent image.

   To see a list of the IDs available, enter the `show fenet hx-agent metadata image available` command.

7. Enter the following command to apply the agent image on your server.

   ```
   <host> (config) # fenet hx-agent image apply content-id <content-id>
   ```

   where <content-id> is the ID of the agent image you obtained in Step 6.

The agent image is downloaded and applied to your server and appears on the Agent Versions tab. You can then deploy it to your endpoints.

CHAPTER 6: Installation and Deployment Steps

Perform the following steps to deploy Trellix Endpoint Security Agent software in your environment.

IMPORTANT: Trellix recommends that you deploy your Endpoint Security Server software before you deploy your agent software.

NOTE: A single ecosystem, which includes the Endpoint Security Server and any installed DMZ server, can support up to 100,000 agents.

Some of these steps are optional configuration steps that allow you to configure your agent software *before* it is deployed to your endpoints. If you elect to configure your agent software *after* it is deployed to your endpoints, the configuration changes will be applied to the endpoints at the next poll interval.

1. Whitelist Endpoint Security Agent files in your antivirus software packages.

   For example, if you are running Symantec Endpoint Protection (SEP), you should create exclusions in SEP for Trellix Endpoint Security Agent processes and folders. See Before You Install or Upgrade the Agent Software on page 91.

   This will maximize performance and ensure compatibility with other antivirus software.

2. Create malware detection process and folder exclusions for any other antivirus software you have installed on your Windows host endpoints.

   Use the malware detection global policy in the Endpoint Security Web UI to define these exclusions. For example, if you are running Symantec Endpoint Protection (SEP), you should create process and folder exclusions for malware protection in the Agent Default Policy for SEP processes and folders. See "Defining the Malware Detection Exclusion Policy" in the *Endpoint Security Agent Administration Guide*.

   This will maximize performance and ensure compatibility with other antivirus software.

3. Define your server address list. See Configuring the Server Address List on page 99.

4. Optionally, configure your HTTPS proxy server to allow endpoints on your network to access the Internet. This step is only required if your enterprise uses an HTTPS proxy server to allow endpoints to access the Internet. An Internet connection is required for the Endpoint Security to download malware definitions and other agent updates. See HTTPS Proxy Server Overview and Configuration on page 45.

   IMPORTANT: Direct HTTPS proxy support for Internet access is supported in Endpoint Security Agent version 25 or later only.

   You must configure your proxy settings before installing Endpoint Security Agent software version 35.30.0 on your endpoints.

5. Verify that the primary (provisioning) Endpoint Security servers have been identified. See "Designating Provisioning Servers," in the *Endpoint Security Server Deployment Guide*.

   You **must** decide which Endpoint Security Server or DMZ server will be your provisioning server before you download the Trellix Endpoint Security Agent installation software to your host endpoints. When agent installation software is downloaded, the IP addresses or DNS names of the provisioning servers are identified in the agent download package.

6. If you would like to use a Windows file system junction (symbolic link) for the agent data stored in the Windows `ProgramData` folder, set it up before you install the agent software. See Using Symbolic Links for Agent Program Data in Windows Environments on page 103.

7. Obtain the agent installation images required for your environment and upload them to the Web UI. See Obtaining Agent Installation Software on page 29.

   When the agent installation image has been uploaded to the Web UI, the server generates agent installation packages and list the packages on the Agent Versions tab of the Agent Settings page.

8. **For Windows deployments only:** Enable Windows Defender Device Guard Code integrity on the Windows system that you plan to use as a golden image to deploy the Endpoint Security Agent software to multiple host endpoints. See Enabling Device Guard Code Integrity on page 22.

9. Optionally, configure polling settings for endpoints. See Configuring Polling on page 105.

10. Optionally, configure other agent policies and settings. Real-time indicator detection, agent resource use, concurrent host limit, Exploit Guard, and agent logging policies can be configured. In addition, host aging settings can be specified. Defaults are supplied for all these policies and settings. See your *Endpoint Security Agent Administration Guide*.

11. Install the agent software on your endpoints. See Installing the Agent Installation Package on page 41.

    NOTE: Trellix recommends that after installing Endpoint Security Agent version 35.30.0, you restart your host endpoints to ensure agent notifications are started.

12. Configure the Removal Protection policy for all of your host endpoints to prevent the unauthorized removal of the Endpoint Security Agent software from your host endpoints. See Configuring the Agent Removal Protection Password on page 75 for more information.

    Information about uninstalling agent software is also provided. See Uninstalling Endpoint Security Agent Software on page 81.

After Endpoint Security Agents are deployed in your environment, you can upgrade the software on the agents as new versions become available. See "Upgrading Agent Software" in the *Endpoint Security Agent Administration Guide*.

CHAPTER 7: Installing the Agent Installation Package

You can deploy the agent installation package to your host endpoints the same way that your enterprise installs any other software. Trellix clients have successfully used a wide variety of software management utilities, such as BigFix and SCCM (in Windows environments), to deploy the agent software on their endpoints. See Software Management Utility Installation Notes.

Trellix recommends that you deploy your Endpoint Security Server Agent software before you deploy your agent software.

Trellix recommends that you manually install the Endpoint Security Agent on a few host machines and test them according to your enterprise's existing policies before you deploy the agent to all your host machines.

Trellix also recommends that you test the Endpoint Security Agent on host endpoints with other third-party applications to ensure there are no performance or compatibility issues between the agent software and your third-party applications.

Agent Installation Package for Windows and macOS Endpoints

Trellix's universal agent installation package is a `.zip` file (Windows) . The `.zip` file (Windows environments) and `.dmg` file (macOS environments) both contain the agent installation and the agent configuration file. The Windows installation file is a standard `.msi` file. The agent configuration file is an `agent_config.json` file that specifies server settings for the agent. Generally, both files must be in the same folder on any machines on which you want to install the agent. However, you can use the CONFJSONDIR installation option to specify an alternate location for the configuration file.

Agent Installation Package for Linux Endpoints

The `.tgz` file (Linux environment) includes the RPM, Debian, and the agent configuration file (`agent_config.json`).

The following table lists the specific agent installation file required to install the agent software on each supported Linux operating system version and the supported deployment scenario for each installation file.

File Type	Agent Software Installation File	Compatible Linux OS Versions	Deployment
`.rpm`	`xagt-35.30.0-1.el6.x86_64.rpm`	• RHEL 6.10 • CentOS 6.10 • Amazon Linux 2 and AMI 2018.3 • Oracle 6.10, 7.9, 8.0, 8.1 and 8.2	Single or Bulk
	`xagt-35.30.0-1.el7.x86_64.rpm`	• RHEL 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, 8.3, 8.4 and 8.5 • CentOS 6.10, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 8.0 and 8.4 • Amazon Linux 2, AMI2 and AMI 2018.3 • Oracle 6.10, 7.9, 8.0, 8.1 and 8.2	Single or Bulk
	`xagt-35.30.0-1.sle12.x86_64.rpm`	• SUSE (SLES) 12.4, 12.5, and 15 • Open SUSE 15.1, 15.2 and 15.3	Single or Bulk
`.deb`	`xagt-35.30.0-1.ubuntu12_amd64.deb`	• Ubuntu 14.04, 16.04, 18.04, 18.04.3, 19.04, 20.04 and 20.10	Single or Bulk
	`xagt-35.30.0-1.ubuntu16_amd64.deb`	• Ubuntu 14.04, 16.04, 18.04, 18.04.3, 19.04, 20.04, and 20.10	Single or Bulk
`.run`	`xagtSetup_35.30.0.run`	• RHEL 6.10, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, 8.3, 8.4 and 8.5 • CentOS 6.10, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0 and 8.4	Manual install

This section covers the following topics:

Downloading an Agent Installation Package from the Web UI

The agent installation packages available for your agents are listed and maintained on the Agent Versions page, which you can access from the Admin menu in the FireEye Endpoint Security Web UI. See Obtaining Agent Installation Software on page 29.

You **must** designate your provisioning Endpoint Security server or DMZ before downloading the installation software for your agents. When the agent installation software is downloaded, the IP addresses or DNS names of the provisioning servers are identified in the agent download package.

You must download the Endpoint Security software package from your Endpoint Security server to ensure the installation package obtains the agent configuration file and certificates required to provision your Endpoint Security server with the agent.

For a complete overview of what you need to do to deploy agent software to your host endpoints, see Installation and Deployment on page 19.

This section covers the following topics:

Prerequisites

- Admin or Operator access

Downloading a Windows or macOS Agent Installation Package from the Web UI

To use the Web UI to download an agent installation package on your Windows or macOS endpoint:

1. Log in to the Web UI from the Windows or macOS system or virtual machine that you plan to use to deploy the agent software.
2. From the Admin menu, select **Agent Versions**.
3. Locate the Windows or macOS agent installation package version that you want to install on one or more Windows or macOS endpoints.
4. Click the **DOWNLOAD AGENT INSTALLER** link for the Endpoint Security Agent software version that is compatible with your Windows or macOS endpoints and download the agent software package.
    - To download an installer package for the most recent version, click the **Download agent installer** link associated with that version at the top of the agent versions list.
    - To download an installer package for an earlier version, click the **Download agent installer** link associated with that version from the agent versions list.
5. Create a temporary folder on your desktop and name it **FireEye**.
6. Open the **Downloads** folder on your endpoint and copy the Endpoint Security installation software package you downloaded in step 4 into the FireEye folder.

If your enterprise uses an HTTPS proxy server, see HTTPS Proxy Server Overview and Configuration on the facing page before installing the Endpoint Security software on your endpoints. If your enterprise does not use an HTTPS proxy server, see Software Management Utility Installation Notes on page 54 for information about bulk deployment options or Manually Installing Agent Software on page 55 for information about how to manually install the agent software on your endpoints.

Downloading a Linux Agent Installation Package from the Web UI

This section describes how to use the Web UI to download the Linux agent installation package to your Linux endpoint or to any endpoint and transfer it to your Linux endpoint for deployment.

To use the Web UI to download the Linux agent installation package from any endpoint:

1. Log in to the Web UI.
2. From the Admin menu, select **Agent Versions**.
3. Locate the Linux agent installation package version 35.30.0.

4. Click the **Download agent installer** link.
5. Log in to the Linux endpoint that you are using to deploying the agent software.
6. Create a **FireEye** folder on the desktop.
7. Using SCP client, transfer the agent software package to the **Trellix** directory on your Linux endpoint.

   ```
   scp IMAG_HX_AGENT_LINUX_29.x.x.tgz
   username@locahost:/home/<username>/Desktop/FireEye/
   ```

To use the Web UI to download the Linux agent installation package from your Linux endpoint:

1. Log in to the Web UI.
2. From the Admin menu, select **Agent Versions**.
3. Locate the Linux agent installation package version 35.30.0.
4. Click the **Download agent installer** link.
5. Create a **FireEye** folder on the desktop.
6. Use the `mv` command to move the agent software package to the **FireEye** directory.

   ```
   mv IMAG_HX_AGENT_LINUX_29.x.x.tgz /home/<username>/Desktop/FireEye/
   ```

HTTPS Proxy Server Overview and Configuration

A proxy server acts as an intermediary gateway between a local network client or endpoint and another server, such as the Internet. It makes service requests on behalf of a local client and allows the client to make network connections to network services outside its own network.

If your enterprise uses an HTTPS proxy server to allow endpoints on your network to access the Endpoint Security Server or the Internet, you must configure your proxy server to allow communication between the agent and the Endpoint Security Server. Your proxy server will also allow the Trellix DTI cloud to download malware and antivirus content updates and software updates to your agent.

This section describes how to use the Agent Policy Service to configure a proxy policy for host sets in your environment.

NOTE: The Endpoint Security Agent requires an Internet connection to download malware definitions and other agent updates.

Direct HTTPS proxy support for Internet access is supported in Endpoint Security Agent version 25 or later.

NOTE: If an agent tries to communicate with the Endpoint Security server through a proxy where SSL inspection is enabled, then the proxy provides a different SSL certificate than the Endpoint Security server, and the agent cannot communicate with the server. In these circumstances, you receive a 1235, MX_API_SSL_EVERIFY, "SSL verify error" error message in the agent logs. When SSL inspection is enabled on the proxy, agents can still communicate with the server as long as they don't use the proxy to do so. If SSL inspection is not enabled on the proxy, then agents can communicate through the proxy without errors.

Proxy Server Types

The Agent Policy Service allows you to select from three configuration types when setting up an HTTPS proxy server for the agents on your host endpoints: none, system, and manual.

Type Value	Description
`none`	No proxy server. Proxy switch is disabled.
`system`	Configure your local system as a proxy server. See Configuring a Proxy Server Policy. **NOTE:** Web traffic is not blocked for contained Windows endpoints that have a proxy. Host containment works only at the IP protocol layer. If your host endpoints use a proxy server that has been added to the containment whitelist, a contained host will still be able to send and receive Web traffic and other traffic. If you are using an agent proxy and you want to be able to contain compromised hosts, you must set up the proxy server with a separate IP address that can only be used to reach the Endpoint Security server. Use the Endpoint Security Web UI to add the proxy server IP address to the Allowed IP Addresses on the **Containment Settings** page. See the *Endpoint Security User Guide* for more information.

Type Value	Description
`manual`	Manually configure a remote system as your proxy server. See Configuring a Proxy Server Policy. **NOTE:** When the proxy `type` is set to `manual`, the proxy `host` setting is required or your proxy server connection will fail. The proxy `host` setting has no default value.

Using the Web UI or the API, you can set up a direct HTTPS proxy server that allows the agents on your host endpoints to access the Endpoint Security server and the Internet. Set up your proxy server using your Windows, OS X, and Linux operating system proxy settings or manually enter your proxy server settings.

Trellix recommends using your system proxy settings to avoid breaking the provisioning between your Endpoint Security server and agent. Use care when manually supplying proxy settings. If your proxy settings are not correct and your agent and Endpoint Security server are on different networks, you may disrupt or break the communication between your Endpoint Security server and agent.

NOTE: You must configure your HTTPS proxy server through the Web UI before installing or upgrading the Endpoint Security Agents on your host endpoints.

Proxy Server Settings and Default Values

By default, HTTPS proxy support is disabled. The table below defines the proxy settings and default values. Use these settings to configure your proxy server.

Proxy Setting	Description	Default Value
`enabled`	Enable or disable the agent web proxy. Valid values include true (enable) and false (disable).	`false`
`exclude_local_hosts`	Enable or disable local and simple host exclusions from the agent web proxy support.	`false`
`exclude_hosts`	A list of hosts that should be excluded from proxy support.	`["eng.fireeye.com", "host.fireeye.com"]`
`password`	The user password required to authenticate access to the proxy server. The proxy password must have a minimum of six alphanumeric characters.	

Proxy Setting	Description	Default Value
`port`	The HTTPS proxy server port number (optional setting).	80
`failed_ retry_delay`	If the proxy server connection fails, the agent will wait for this specified time period (in seconds) before attempting to reconnect with the proxy server. The default value is 1200 seconds.	1200
`host`	The HTTPS proxy host or IP address. **NOTE:** When the proxy `type` is set to `manual`, the proxy `host` setting is required or your proxy server connection will fail. The proxy `host` setting has no default value.	---
`type`	The type of HTTPS proxy server configuration setting used by your host endpoint. Options include `none`, `system`, and `manual`. See Proxy Server Types on page 46 for more information.	`none`
`username`	The username required to authenticate access to the proxy server.	

Prerequisites

- Admin access to the Endpoint Security server or the endpoints
- Endpoint Security Agent software version 25 or later (Downloaded from the Endpoint Security Server and transferred to the endpoint)

NOTE: You must download the Endpoint Security Agent software package from your Endpoint Security Server to ensure the installation package obtains the agent configuration file and certificates required to provision your server with the agent.

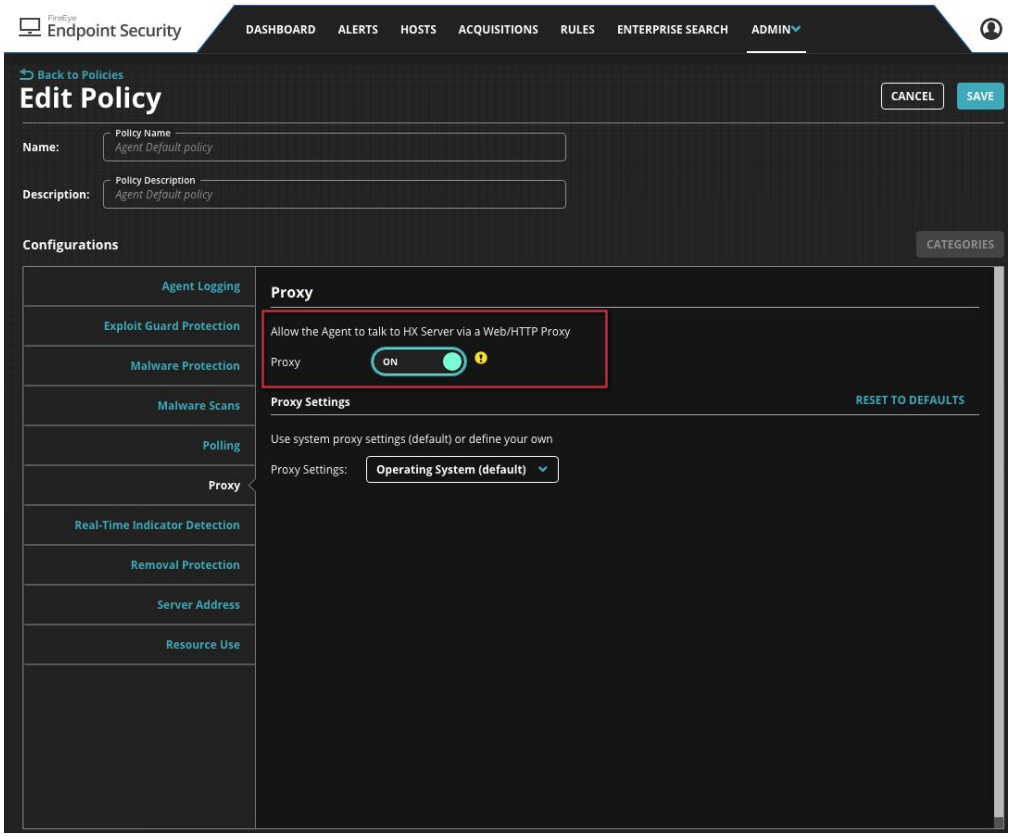
This section covers the following topics:

Configuring an HTTPS Proxy Server for All Host Sets

This section describes how to configure a proxy server in system mode or manual mode for all host sets in your environment by modifying the Agent Default Policy.

To configure a proxy server in system mode for all host sets in your environment:

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. From the Policies table, click the **Agent Default Policy** link to go to the **Edit Policy** page.
4. Select the **Proxy** tab.
5. Toggle the Proxy **ON/OFF** switch to **ON** to enable your HTTPS proxy server.



6. Click the **Proxy Settings** drop-down menu and select **System**.
7. Click **Save** to save the policy settings.

NOTE: If you use the Web UI to configure your proxy server for your agents using the operating system proxy settings on your Windows endpoint, and your endpoint has proxy authentication enabled, you must manually specify the proxy `username` and `password` keys in the agent configuration file. If you do not specify these keys in the agent configuration file, the connection between the agent and the Endpoint Security server will fail.

To configure a proxy server in manual mode for all host sets in your environment:

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. From the Policies table, click the **Agent Default Policy** link to go to the **Edit Policy** page.
4. Select the **Proxy** tab.
5. Toggle the Proxy **ON/OFF** switch to **ON** to enable your HTTPS proxy server.
6. Click the **Proxy Settings** drop-down menu and select **User Defined**.

7. Manually enter the following settings for your proxy server:

Proxy Server Setting	Description
Proxy name:	Enter the HTTPS proxy server hostname or IP address. **CAUTION:** When the proxy `type` is set to `manual`, the proxy `server` setting is required or your proxy server connection will fail. The proxy `server` setting has no default value.
Port:	Enter your HTTPS proxy server port number (optional setting). The default value is 80.
Excluded Hosts:	Enter a list of hosts that should be excluded from proxy support.
Exclude Local/Simple Host Names	Select this box to enable your host list exclusions from proxy support.
Username:	Enter the username required to authenticate access to the proxy server.
Password:	Enter the password required to authenticate access to the proxy server.

Proxy Server Setting	Description
Retry Delay:	Enter the time interval (in seconds) required before the proxy server attempts to reconnect after a connection failure. The default value is 1200 seconds.

8. Click **Save** to save the policy settings.

Manually Applying Proxy Settings to Multiple Endpoints After an Upgrade

After upgrading the Endpoint Security Agent software on your endpoint to 35.30.0, you can use an API custom configuration channel to manually add a proxy policy to the agent configuration file. This will add and apply the settings to your endpoints. Follow the instructions in "Using API Custom Configuration Channels" in the *Endpoint Security Agent Administration Guide* to manually add the following proxy server settings to the agent configuration file for your Windows, macOS, or Linux endpoints:

Proxy Server Settings

```
{
"proxy": {
"type": "manual",
"enabled": true,
"host": "<hostname or IP>",
"port": 80,
"exclude_hosts": ["eng.fireeye.com", "host.fireeye.com"],
"exclude_local_hosts": true,
"username": "<proxy-user>",
"password": "<proxy-user-password>",
"failed_retry_delay": 1200
}
```

IMPORTANT: If the proxy `type` value is set to `manual`, the only proxy setting you are required to change is the `host` setting.

The proxy `host` setting has no default value. When the proxy `type` is set to `manual`, you must provide a `host` value or your proxy server connection will fail.

Using a Proxy Server to Communicate with Contained Hosts

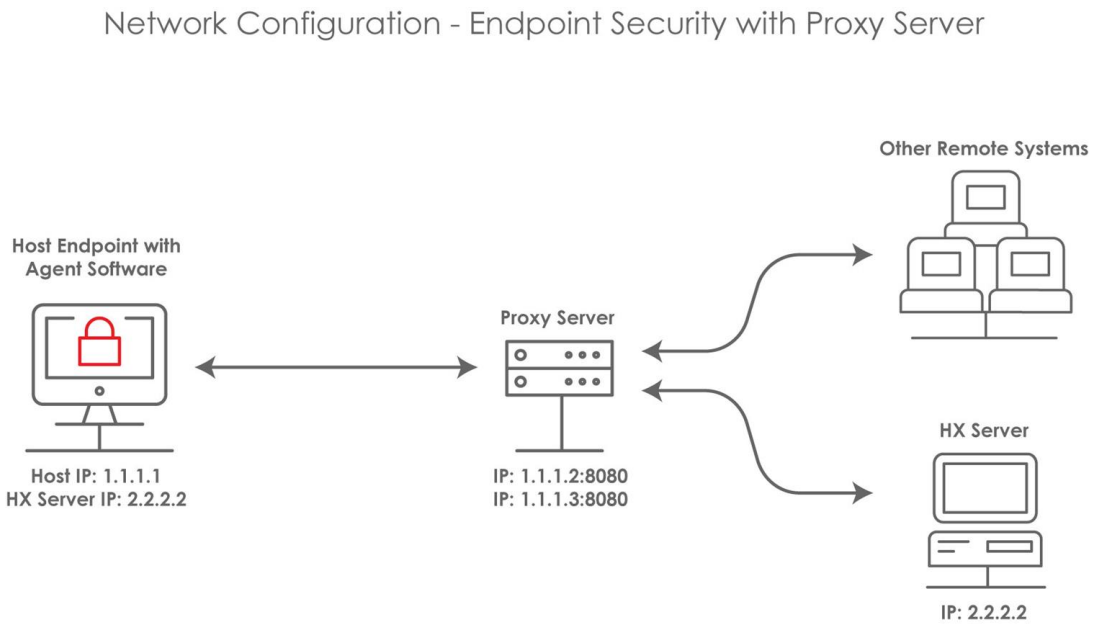
Agent containment allows traffic based on protocol and IP address. Ports are also used to control traffic. When you enable host containment at the lowest layer, traffic is limited to the following:

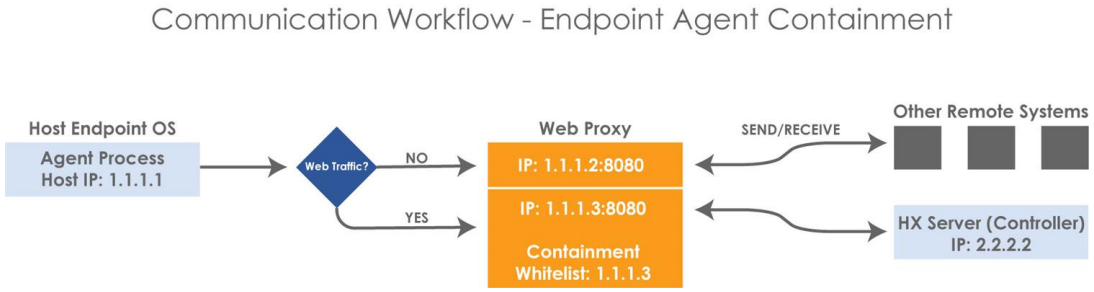
- Ethernet or WirelessWAN (WirelessWan is used by cell providers to allow for access to cell networks for Internet access.)
- UDP port 67 and DHCP port 68 is allowed to ensure that those using DHCP do not lose their IP address reservation while the host is contained.
- TCP traffic over IP addresses defined by the Agent whitelist.
- ICMP type 9 router advertisement and type 10 router solicitation.

NOTE: The Endpoint Security Server IP address is always included in the whitelist.

IMPORTANT: You must whitelist the agent process ID to allow traffic from any contained Windows agent, and any contained macOS agent version 30 and later, as well as any Linux agent version 34 and later, that uses a proxy server to communicate with the Endpoint Security Server version 4.8 and later.

If you are using an agent proxy and you want to be able to contain compromised hosts, you must set up the proxy server with a separate IP address that can only be used to reach the Endpoint Security Server. This separate IP address can be defined in the Endpoint Security Server whitelist. This will allow communication between the host endpoint and the Endpoint Security Server while blocking all other communication flows from the contained endpoint agent. See Before You Install or Upgrade the Agent Software on page 91 for more information.





Use the Endpoint Security Web UI to add the proxy server IP address to the **Allowed IP Addresses** on the **Containment Settings** page. See the *Endpoint Security Server User Guide* for more information.

Software Management Utility Installation Notes

If your site uses software management utilities, such as BigFix or SCCM in Windows environments, to deploy agents, download the `.msi` file for use by the deployment tool as an application, not as a package. Errors may occur if it is downloaded as a package.

Manually Installing Agent Software

After obtaining the Endpoint Security Agent software package, you can manually install agent software on your Windows, macOS, or Linux endpoints. Trellix strongly recommends using a software management utility tool to perform bulk deployments of the agent software to endpoints in your environments. See Software Management Utility Installation Notes on the previous page.

Manually Installing Agent Software on Windows or macOS Endpoints

After you have downloaded or copied the installation package to your host endpoint, follow the instructions provided in this section to manually install the agent software on your Windows or macOS endpoints. See Downloading an Agent Installation Package from the Web UI on page 43.

IMPORTANT: After installing or upgrading to Endpoint Security Agent version 35.30.0, you must restart your Windows endpoints to ensure agent notifications are started.

NOTE: If your endpoints uses a proxy server to connect to an Endpoint Security Server, see HTTPS Proxy Server Overview and Configuration on page 45 before manually installing the agent software on your endpoints.

IMPORTANT: For macOS 10.15 endpoints and above, Trellix and Bitdefender kernel extensions must be authorized to successfully complete installation. See your macOS **System Preferences** > **Security & Privacy** to do this.

To manually install agent software on an individual Windows or macOS endpoint:

1. Unzip the `*.zip` (Windows environments) or `.dmg` (macOS environments) file. The Windows agent installation package consists of these files:
   - `xagtSetup_x.x.x_universal.msi` installation file (Windows environments)
   - `agent_config.json` configuration file

   The macOS agent installation package consists of these files:

- `xagtSetup_x.x.x.mpkg` installation file (macOS environments)
- `agent_config.json` configuration file

2. Double-click the installation file to launch the setup wizard.

   If you want to use installation options in Windows environments, do not double-click on the `.msi` file. Run it as described in Windows Agent Installation and Uninstallation Options on page 67.

3. Accept all suggested settings and the license agreement, and continue through the wizard.
4. When the wizard completes, click **Finish** (Windows environments) or **Close** (macOS environments).

IMPORTANT: After installing or upgrading to Endpoint Security Agent version 35.30.0, you must restart your Windows endpoints to ensure agent notifications are started.

While a reboot is not required for the Windows Endpoint Security to work after it has been installed on a host endpoint, one may be required to complete the Windows installation and avoid problems with future installations that check for pending reboots. One way to determine whether a reboot is necessary is to run the following command at a Windows command prompt:

To query the event log, open the Windows command line and run the following command at the prompt:

```
wevtutil qe Application /rd:true /f:text /q:"*[System/EventID=1029] and *
[EventData[Data='FireEye Endpoint Agent']]"
```

If a reboot is required, the following event will appear:

```
"FireEye Endpoint Agent. Restart required. The installation or update for
the product required a restart for all changes to take effect. The restart
was deferred for a later time."
```

You can use the following command to identify the name and process ID of the application that locked a Trellix system file open:

```
wevtutil qe Application /rd:true /f:text /q:"*[System/EventID=1025] and *
[EventData[Data='FireEye Endpoint Agent']]"
```

This command returns the name and process ID of the application that locked a file open. In the example below, Firefox has the NamespaceToEvents.dll file open.

```
"FireEye Endpoint Agent. The file C:\Windows\FireEye\NamespaceToEvents.dll
is being used by the following process: Name: firefox , Id 1060."
```

Close the application that caused the reboot. Run the `wevtutil qe Application` command above to verify if a reboot is still required.

An endpoint reboot may also be required in the rare instance when the agent executable cannot be replaced during the upgrade.

If you choose to install a Windows agent using the service mode installation option and you specify option 2, you will need to reboot the host endpoints after the installation is complete.

Verifying the Connection Between the Agent and the Endpoint Security

To verify that the agent has provisioned with the Endpoint Security Server, log in to the Web UI on the Endpoint Security Server and navigate to the Hosts page. The host machine

on which the agent is installed is listed on this page.

In macOS environments, open Terminal and enter the following command to review the agent processes that are running:

```
ps aux | grep xagt
```

Depending on when you run this command, one agent process listed in the output may be running in Eventor mode if real-time indicator detection is turned on. The output will include the following text:

```
- -mode EVENTOR
```

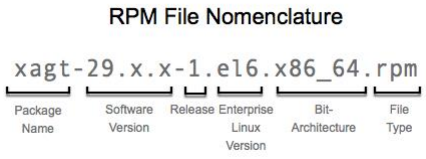
Manually Installing Agent Software on Linux Endpoints

After you download or copy the installation package to your host endpoint, you can manually install the agent software on your Linux endpoints.

This section includes the following topics:

Selecting the Correct Linux Agent Installation File

The Linux agent `.rpm` and `.deb` file nomenclature defines the agent binary, the agent software version, the supported Linux OS version, and the Linux OS-bit architecture. For example, the following agent software installation `.rpm` file installs agent software version 35.30.0 on supported Red Hat Enterprise Linux (RHEL) 6.x versions with a 32 or 64- bit architecture.



You must run the `.rpm` or `.deb` file that is compatible with your Linux environment. For example, if your Linux endpoints are running RHEL version 6.8, run `.rpm` file `xagt-29.x.x-1.el6.x86_64.rpm`. If your Linux endpoints are running RHEL version 7.2, run `.rpm` file `xagt-29.x.x-1.el7.x86_64.rpm`.

The following table shows the specific agent installation file required to install the agent software on each supported Linux operating system version.

File Type	Agent Software Installation File	Compatible Linux OS Versions	Deployment
.rpm	xagt-35.30.0-1.el6.x86_64.rpm	• RHEL 6.10 • CentOS 6.10 • Amazon Linux 2 and AMI 2018.3 • Oracle 6.10, 7.9, 8.0, 8.1 and 8.2	Single or Bulk
	xagt-35.30.0-1.el7.x86_64.rpm	• RHEL 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, 8.3, 8.4 and 8.5 • CentOS 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 8.0 and 8.4 • Amazon Linux 2, AMI2 and AMI 2018.3 • Oracle 6.10, 7.9, 8.0, 8.1 and 8.2	Single or Bulk
	xagt-35.30.0-1.sle12.x86_64.rpm	• SUSE 15	Single or Bulk
.deb	xagt-35.30.0-1.ubuntu12_amd64.deb	• Ubuntu 14.04 (Versions that use "upstart")	Single or Bulk
	xagt-35.30.0-1.ubuntu16_amd64.deb	• Ubuntu 16.04, 18.04, 19.04, 20.04 (Versions that use "systemd")	Single or Bulk
.run	xagtSetup_35.30.0.run	• RHEL 6.10, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, and 8.2 • CentOS 6.10, 7.1, 7.2, 7.3, 7.4, 7.5, and 7.6	Manual install

IMPORTANT: The Linux agent software installation `.run` file supports RHEL and CentOS versions 6.x and 7.x operating systems only.

If you are upgrading your Linux agent to version 35.30.0 and you used the Linux agent runscript to install the agent software for an earlier agent version on your Linux endpoint, use the Linux agent runscript version 35.30.0 to upgrade the agent software on your Linux endpoints.

Using the RPM file to Manually Install Agent Software

Use the compatible `.rpm` file to manually install agent software on your Linux endpoints running supported RHEL, CentOS, Amazon Linux, or SUSE versions.

To manually install the agent software on a single Linux endpoint using the `.rpm` file:

1. Open a Terminal session on the Linux endpoint that has the agent installation `.tgz` package.

   ```
   username@localhost:~$
   ```

2. Use the `cd` command to change to the `FireEye` directory you created in step 6 of Downloading a Linux Agent Installation Package from the Web UI on page 44.

   ```
   username@localhost:~$ cd desktop
   username@localhost:~/Desktop$ cd FireEye
   ```

3. Use the `ls` command to verify that the `IMAGE_HX_AGENT_LINUX_29.x.x.tgz` file is in the `FireEye` directory.

   ```
   username@localhost:~/Desktop/FireEye$ ls
   IMAGE_HX_AGENT_LINUX_29.x.x.tgz
   ```

4. Use the `tar zxf` command to unzip and extract the files from the Linux agent installation image `.tgz` file:

   ```
   username@localhost:~/Desktop/FireEye$ tar zxf IMAGE_HX_AGENT_LINUX_
   29.x.x.tgz.
   ```

   The `.tgz` package (Linux) includes the following files:

   - Agent `.rpm` files
   - Agent `.deb` files
   - Agent `.run` file (`xagtSetup_29.x.x.run`)
   - Agent configuration file (`agent_config.json`).

5. Use the `ls` command to view the files.

   ```
   username@localhost:~/Desktop/FireEye$ ls
   ```

   You will see a list of all the files in the agent installation package. You must have sudo access to perform steps 6-8.

6. Use the `-ihv` command to run the `.rpm` script and install the agent software on your Linux endpoint. **You must have sudo access to perform steps 6-8.**

   ```
   username@localhost:~/Desktop/FireEye$ sudo rpm -ihv xagt-29.x.x-
   1.el6.x86_64.rpm
   ```


CAUTION: If FIPS mode is enabled (run `fips-mode-setup --check` to verify) on Linux endpoints running RHEL 8.x and above, or CentOS 8.x and above, the `--nodigest` flag must be set in the installation command:
`username@localhost:~/Desktop/FireEye$ sudo rpm -ihv --nodigest xagt-29.x.x-1.el6.x86_64.rpm`

IMPORTANT: Run the `.rpm` file that is compatible with your Linux environment. For example, if your Linux endpoints are running RHEL version 6.x, run `xagt-29.x.x-1.el6.x86_64.rpm`, if your Linux endpoints are running SUSE 11.4, run `xagt-29.x.x-1.sle11.x86_64.rpm`, and if your Linux endpoints are running Amazon Linux AMI 2018.3, run `xagt-29.x.x-1.el6.x86_64.rpm`.

The `.rpm` file automatically detects the version of Linux RHEL currently running on the endpoint. If the `.rpm` file is not compatible with the RHEL version running on the endpoint, an error message appears.

7. After the `.rpm` installation script is complete, use the `i` option to import the agent configuration file from the `/opt/fireeye/bin/xagt` binary path:
   `username@localhost:~/Desktop/FireEye$ sudo /opt/fireeye/bin/xagt -i agent_config.json`

NOTE: If the agent installation fails, follow the instructions in Alternate Method for Installing Agent Software on Linux Endpoints on page 65, which describes how to use the `.run` file to manually install the agent software on your Linux endpoints.

8. Start the agent services on your Linux endpoint using the following command:
   `username@localhost:~/Desktop/FireEye$ sudo systemctl start xagt`

NOTE: If you have an older versions of Linux you may require this command:
`username@localhost:~/Desktop/FireEye$ sudo service xagt start`
The "service" command is deprecated in most modern versions of linux.

Using the RPM file to Manually Upgrade Agent Software

Use the compatible `.rpm` file to manually upgrade agent software on your Linux endpoints running supported RHEL, CentOS, Amazon Linux, or SUSE versions.

To manually upgrade the agent software on a single Linux endpoint using the `.rpm` file:

1. Open a Terminal session on the Linux endpoint that has the agent installation `.tgz` package.
   `username@localhost:~$`

2. Use the `cd` command to change to the `FireEye` directory you created in step 6 of Downloading a Linux Agent Installation Package from the Web UI on page 44.

   ```
   username@localhost:~$ cd desktop
   username@localhost:~/Desktop$ cd FireEye
   ```

3. Use the `ls` command to verify that the `IMAGE_HX_AGENT_LINUX_29.x.x.tgz` file is in the `FireEye` directory.

   ```
   username@localhost:~/Desktop/FireEye$ ls
   IMAGE_HX_AGENT_LINUX_29.x.x.tgz
   ```

4. Use the `tar zxf` command to unzip and extract the files from the Linux agent installation image `.tgz` file:

   ```
   username@localhost:~/Desktop/FireEye$ tar zxf IMAGE_HX_AGENT_LINUX_
   29.x.x.tgz.
   ```

   The `.tgz` package (Linux) includes the following files:

   - Agent `.rpm` files
   - Agent `.deb` files
   - Agent `.run` file (`xagtSetup_29.x.x.run`)

5. Use the `ls` command to view the files.

   ```
   username@localhost:~/Desktop/FireEye$ ls
   ```

   You will see a list of all the files in the agent installation package. You must have sudo access to perform steps 6-8.

6. Use the `-uhv` command to run the `.rpm` script and upgrade the agent software on your Linux endpoint. **You must have sudo access to run this command:**

   ```
   username@localhost:~/Desktop/FireEye$ sudo rpm -uhv  xagt-29.x.x-
   1.el6.x86_64.rpm
   ```

   IMPORTANT: Run the `.rpm` file that is compatible with your Linux environment. For example, if your Linux endpoints are running RHEL version 6.x8, run `xagt-29.x.x-1.el6.x86_64.rpm`, if your Linux endpoints are running SUSE 11.4, run `xagt-29.x.x-1.sle11.x86_64.rpm`, and if your Linux endpoints are running Amazon Linux AMI 2018.3, run `xagt-29.x.x-1.el6.x86_64.rpm`.

   The `.rpm` file automatically detects the version of Linux RHEL currently running on the endpoint. If the `.rpm` file is not compatible with the RHEL version running on the endpoint, an error message appears.

Using the Debian file to Manually Install Agent Software

Use the compatible .deb file to manually install agent software on your Linux endpoints running Ubuntu 14.04, 16.04, or 18.04.

To manually install the agent software on a single Linux endpoint using the `.deb` file:

1. Open a Terminal session on the Linux endpoint that has the agent installation `.tgz` package.

   ```
   username@localhost:~$
   ```

2. Use the `cd` command to change to the `FireEye` directory you created in step 6 of Downloading a Linux Agent Installation Package from the Web UI on page 44.

   ```
   username@localhost:~$ cd desktop
   username@localhost:~/Desktop$ cd FireEye
   ```

3. Use the `ls` command to verify that the `IMAGE_HX_AGENT_LINUX_29.x.x.tgz` file is in the `FireEye` directory.

   ```
   username@localhost:~/Desktop/FireEye$ ls
   IMAGE_HX_AGENT_LINUX_297.x.x.tgz
   ```

4. Use the `tar zxf` command to unzip and extract the files from the Linux agent installation package:

   ```
   username@localhost:~/Desktop/FireEye$ tar zxf IMAGE_HX_AGENT_LINUX_
   29.x.x.tgz.
   ```

   The `.tgz` package (Linux) includes the following files:

   - Agent `.rpm` files
   - Agent `.deb` files
   - Agent `.run` file (`xagtSetup_29.x.x.run`)
   - Agent configuration file (`agent_config.json`).

5. Use the `ls` command to view the files.

   ```
   username@localhost:~/Desktop/FireEye$ ls
   ```

   You will see a list of all the files in the agent installation package.

6. Use the `dpkg`, medium-level package manager for Debian and the -i option to run the `.deb` script and install the agent software on your Linux endpoint. **You must have sudo access to perform steps 6-8.**

   ```
   username@localhost:~/Desktop/FireEye$ sudo dpkg -i xagt-29.x.x-
   1.ubuntu12_amd64.deb
   ```

   IMPORTANT: Run the `.deb` file that is compatible with the supported Ubuntu version running on your Linux endpoints. For example, if your Linux endpoints are running Ubuntu 14.04, run `xagt-29.x.x-1.ubuntu12_amd64.deb`. If your Linux endpoints are running Ubuntu 16.04 or later, run `xagt-29.x.x-1.ubuntu16_amd64.deb`.

   The `.deb` file automatically detects the version of Ubuntu currently running on the endpoint. If the `.deb` file is not compatible with the Ubuntu version running on the endpoint, an error message appears.

7. After the `.deb` installation script is complete, use the `i` option to import the agent configuration file from the `/opt/fireeye/bin/xagt` binary path:

   ```
   username@localhost:~/Desktop/FireEye$ sudo /opt/fireeye/bin/xagt -i
   agent_config.json
   ```

   NOTE: If the agent installation fails, follow the instructions in Alternate Method for Installing Agent Software on Linux Endpoints on the facing page, which describes how to use the `.run` file to manually install the agent software on your Linux endpoints.

8. Start the agent services on your Linux endpoint using the following command:

   ```
   username@localhost:~/Desktop/FireEye$ sudo service xagt start
   ```

Using the Debian file to Manually Upgrade Agent Software

Use the compatible .deb file to manually upgrade agent software on your Linux endpoints running Ubuntu 14.04, 16.04, or 18.04.

To manually upgrade the agent software on a single Linux endpoint using the `.deb` file:

1. Open a Terminal session on the Linux endpoint that has the agent installation `.tgz` package.

   ```
   username@localhost:~$
   ```

2. Use the `cd` command to change to the `FireEye` directory you created in step 6 of Downloading a Linux Agent Installation Package from the Web UI on page 44.

   ```
   username@localhost:~$ cd desktop
   username@localhost:~/Desktop$ cd FireEye
   ```

3. Use the `ls` command to verify that the `IMAGE_HX_AGENT_LINUX_29.x.x.tgz` file is in the `FireEye` directory.

   ```
   username@localhost:~/Desktop/FireEye$ ls
   IMAGE_HX_AGENT_LINUX_297.x.x.tgz
   ```

4. Use the `tar zxf` command to unzip and extract the files from the Linux agent installation package:

   ```
   username@localhost:~/Desktop/FireEye$ tar zxf IMAGE_HX_AGENT_LINUX_
   29.x.x.tgz.
   ```

   The `.tgz` package (Linux) includes the following files:

   - Agent `.rpm` files
   - Agent `.deb` files
   - Agent `.run` file (`xagtSetup_29.x.x.run`).

5. Use the `ls` command to view the files.

   ```
   username@localhost:~/Desktop/FireEye$ ls
   ```

   You will see a list of all the files in the agent installation package.

6. Use the `dpkg`, medium-level package manager for Debian and the -i option to run the `.deb` script and upgrade the agent software on your Linux endpoint. **You must have sudo access to run this command:**

   ```
   username@localhost:~/Desktop/FireEye$ sudo dpkg -i xagt-29.x.x-1.ubuntu12_amd64.deb
   ```

   IMPORTANT: Run the `.deb` file that is compatible with the supported Ubuntu version running on your Linux endpoints. For example, if your Linux endpoints are running Ubuntu 14.04, run `xagt-29.x.x-1.ubuntu12_amd64.deb`. If your Linux endpoints are running Ubuntu 16.04 or later, run `xagt-29.x.x-1.ubuntu16_amd64.deb`.

   The `.deb` file automatically detects the version of Ubuntu currently running on the endpoint. If the `.deb` file is not compatible with the Ubuntu version running on the endpoint, an error message appears.

Alternate Method for Installing Agent Software on Linux Endpoints

If the `.rpm` file fails to install the Endpoint Security Agent software on your Linux endpoints running supported RHEL and CentOS versions, follow the steps in this section to use the `.run` file to install the agent software on your Linux endpoints.

To manually install the agent software on a single Linux endpoint using the .run file :

1. Open a Terminal session on the Linux endpoint that has the agent installation package, `.tgz` file.

   ```
   username@localhost:~$
   ```

2. Use the `cd` command to change to the `FireEye` directory you created in step 6 of Downloading a Linux Agent Installation Package from the Web UI on page 44.

   ```
   username@localhost:~$ cd desktop
   username@localhost:~/Desktop$ cd FireEye
   ```

3. Use the `ls` command to verify that the `IMAGE_HX_AGENT_LINUX_29.x.x.tgz` file is in the `FireEye` directory.

   ```
   username@localhost:~/Desktop/FireEye$ ls
   IMAGE_HX_AGENT_LINUX_29.x.x.tgz
   ```


4. Use the `tar zxf` command to unzip and extract the files from the Linux agent installation package:

   ```
   username@localhost:~/Desktop/FireEye$ tar zxf IMAGE_HX_AGENT_LINUX_
   29.x.x.tgz.
   ```

   The `.tgz` package (Linux) includes the following files:

   - Agent `.rpm` files
   - Agent `.deb` files
   - Agent `.run` file (`xagtSetup_29.x.x.run`)
   - Agent configuration file (`agent_config.json`).

5. Use the `ls` command to view the files.

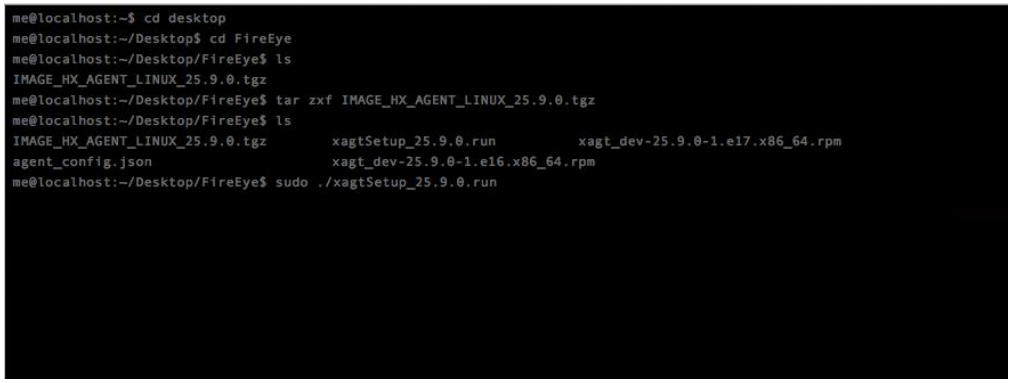
   ```
   username@localhost:~/Desktop/FireEye$ ls
   ```

   You will see a list of all the files in the agent installation package.

6. Use the `./` command to run the `xagtSetup_29.x.x.run` script and install the agent software on your Linux endpoint. **You must have sudo access to perform steps 6-8.**

   ```
   username@localhost:~/Desktop/FireEye$ sudo ./xagtSetup_29.x.x.run
   ```

   After the script completes, you will see the following screen indicating the next installation steps:

   Waiting for updated image.

   Step 1: Import the agent configuration file.

   Step 2. Start the agent services.

   > You must import the agent configuration file before starting the agent services on your Linux endpoint.

7. After the installation script is complete, use the `i` option to import the agent configuration file from the `/opt/fireeye/bin/xagt` binary path:

   ```
   username@localhost:~/Desktop/FireEye$ sudo /opt/fireeye/bin/xagt -i
   agent_config.json
   ```

8. Start the agent services on your Linux endpoint using one of the commands below:

For endpoints running Linux version RHEL 6.x or CentOS 6.x:

```
username@localhost:~/Desktop/FireEye$ sudo service xagt start
```

or

For endpoints running Linux version RHEL 7.x or CentOS 7.x:

```
username@localhost:~/Desktop/FireEye$ sudo systemctl start xagt
```

After starting the agent services, you can check the status of the agent services with the `sudo systemctl status xagt` command.

Windows Agent Installation and Uninstallation Options

Many options are available when you install and uninstall Windows agent software on your host machines.

If you are deploying the Endpoint Security software in a VDI environment, Trellix recommends deploying in a persistent or semi persistent VDI environment. See Agent Installation Considerations on page 21.

Some options are provided by the Windows `msiexec` executable; others are provided by FireEye extensions of `msiexec`.

Specify these options when you initiate the installation. A standard installation setup wizard will perform the installation, using the options you specify.

Standard `msiexec` options you might find useful are listed in the following table. For complete information about all standard `msiexec` options, see your Microsoft documentation or enter `msiexec /h` at a command prompt.

Option	Description
`/i`	Install or configure the software. Specify the name of the installation `*.msi` executable file.
`/x`	Uninstall the software installed by the named installation `*.msi` executable file. If the Removal Protection Password is enabled, you must enter this password to authorize the Endpoint Security uninstall process by appending the `/x` command with `UNINSTALL_PASSWORD=<password>`. Only authorized users can uninstall the agent software. See Configuring the Agent Removal Protection Password on page 75 for more information.

Option	Description
/qn /qb /qr /qf	Set the user interface level for the install or uninstall process: • /qn: no user interface • /qb: basic user interface • /qr: reduced user interface • /qf: full user interface
/quiet	Install the product in quiet mode.
/l*v	Enable agent logging for the install or uninstall process.
/norestart	Do not restart the system after the installation is complete.

This section explains how to use the FireEye extensions to the `msiexec` executable for FireEye Endpoint Security Agent installations.

- Specifying the Agent Installation Location
- Setting Up a Disguised Installation
- Specifying an Alternate Configuration File Location
- Installing the Agent in Service Mode

Specifying the Agent Installation Location

To change the installation location of the agent software, use the TARGETDIR option. Always use quotes around the path name specified with this option.

For example, the following command installs the agent software in `C:\MyInstallationDirectory`:

```
msiexec /i xagtSetup_x.x.x_universal.msi
TARGETDIR="C:\MyInstallationDirectory"
```

The default directory name for installations is `%ProgramFiles%\FireEye\xagt`.

If you are migrating your older agents (agents earlier than version 20) to a newer version of the agent software and you installed your older agents in a customized installation location, see Upgrading Older Agents with Customized Installation Locations on page 70.

Setting Up a Disguised Installation

You can use the disguise installation mode to hide the agent from the Windows Control Panel programs list and conceal the service name and description. To disguise the installation of the agent, you will need to run the installation with the DISGUISE=1 option, change the agent display name, and the agent service description.

IMPORTANT: An upgrade job sent from Endpoint Security will not preserve the disguised settings. FireEye recommends uninstalling the existing agent software and then reinstalling the latest agent software version with the proper disguise parameters.

When you disguise the agent, the following changes occur:

- The Add/Remove program registry keys are not installed, so the disguised agent software does not appear in Windows Programs and Features. This means that it cannot be uninstalled from there. To uninstall a disguised agent, run the installation `.msi` file from the command line, but be sure you use the `.msi` file for the same agent version that is installed on the host endpoint.
- The agent service description is empty. In an undisguised installation, it is `FireEye Agent`.
- The agent display name changes from Trellix Endpoint Agent to the value you input.
- The agent service description changes from Trellix Endpoint Agent to the value you input.

The following example disguises the agent installation, changes the Display Name to My Service, and changes the Service Description to My Service Description:

```
msiexec.exe /i xagtSetup_x.x.x_universal.msi DISGUISE=1 DISPLAYNAME="My
Service" SVCDESCRIPTION="My Service Description"
```

Specifying an Alternate Configuration File Location

You can install the agent when the `agent_conf.json` file is not in the same directory as the `.msi` file downloaded from the Endpoint Security server. Use the CONFJSONDIR option when you run the installation.

The following example runs the installation software using the `agent_conf.json` file in directory `c:\temp`:

```
msiexec.exe /i xagtSetup_x.x.x_universal.msi CONFJSONDIR=c:\temp
```

Installing the Agent in Service Mode

Support for this functionality is provided in FireEye Endpoint Security Agent version 20.40.1 and later.

Use the INSTALLSERVICE option to install the agent software in service mode.

Valid values for the INSTALLSERVICE option are the numbers 1 or 2:

- Specify `1` to install the agent in service mode and start the service. This is the default. Service mode allows you to run the agent as a service.
- Specify `2` to install the agent in service mode without starting the service. Use this option if you intend to use a master or golden image that will be deployed to multiple physical or virtual endpoints. If you do not use this option, all of the endpoints deployed using the golden or master image will report to the Endpoint Security server using the same agent ID. Use option 2 to delay the attempt to obtain an agent ID until the next reboot of the endpoint on which the image is installed. See Installing Agents Using a Golden or Master Image.

The following example installs the agent as a service without starting the service:

```
msiexec /i xagtSetup_x.x.x_universal.msi /norestart INSTALLSERVICE=2
```

If you are deploying the Endpoint Security software in a VDI environment, Trellix recommends deploying in a persistent or semi persistent VDI environment. See Agent Installation Considerations on page 21.

Upgrading Older Agents with Customized Installation Locations

If you used a customized installation location when you installed your older agents (agents earlier than version 20), any upgrade jobs you create using the Web UI will automatically install newer agent software in the same location. For example, if you installed your version 11 agents in a customized directory called `C:\temp\trythis`, the agent upgrade job will install the newer agent software there too.

If you do not use an agent upgrade job to upgrade your older agents, you can install the newer agent software on your hosts by running the regular installation wizard, running the `.msi` installation file from a Windows command prompt, or using a software management utility (such as BigFix or SCCM). In this case, the newer agent software will, by default, be installed into `C:\Program Files\FireEye\xagt`. If you want to install the newer agent software into the same customized installation directory used by your older agents, follow these guidelines:

- Upgrade your Endpoint Security server software before you upgrade your agent software.
- If you use the installation wizard to upgrade, enter the customized location on the appropriate installation wizard screen when prompted.
- If you use command-line prompts or a software management utility to upgrade, specify the TARGETDIR command-line option when you run the installation executable. For more information, see Specifying the Agent Installation Location on page 68.

Installing Agents Using a Golden or Master Image

You can use a master or golden image to deploy the Endpoint Security software to multiple physical or virtual host endpoints in your enterprise. When you install the Endpoint Security software on an endpoint, the agent creates a private key, using information from the endpoint, to encrypt and decrypt all agent data. After installation, agent services will not start unless the private key is decrypted and matches the information on the endpoint where the agent was installed.

A unique agent ID must also be created for each endpoint on which the golden or master image is deployed. Otherwise, all of the endpoints deployed using that image will provision with the Endpoint Security Server using the same agent ID, causing a cloned agent problem in your Endpoint Security environment.

IMPORTANT: For the Endpoint Security Server and Endpoint Security Agent software to communicate properly, each host endpoint must be assigned a unique agent ID. If the Endpoint Security Server reports the presence of cloned agents in your Endpoint Security environment, read "Resolving Cloned Agents" in the *Endpoint Security Server User Guide*.

This section describes how to use a golden or master image to install the Windows or Linux agent software to multiple physical or virtual host endpoints and ensure a private key and a unique agent ID are created for each agent.

NOTE: Windows agent support for master or golden images is provided in Trellix Endpoint Security Agent version 20 or later versions.

Linux agent support for master or golden images is provided in Trellix Endpoint Security Agent version 25 or later.

Installing Windows Agents Using a Golden or Master Image

Follow the steps in this section on the Windows system that you are preparing to use as a golden image that can deploy the Endpoint Security Agent software to multiple physical or virtual host endpoints.

These instructions are only required if you are using Sysprep, or something similar, for your golden image. If you are not using Sysprep, then you can just use `INSTALLSERVICE=2` to install the agent.

IMPORTANT: Before you deploy the Endpoint Security Agent software to your host endpoints, Windows Defender Device Guard Code Integrity must be configured on your golden image system. See Enabling Device Guard Code Integrity on page 22 for more information.

To use a master or golden image to install the agent software on your Windows endpoint:

1. Extract the msi file and agent_config.json file to a directory.

   TIP: Save a copy of the agent configuration file (agent_config.json) in the main agent installation directory—**%ProgramFiles%\FireEye\xagt**—so that the agent reports to the server in the main agent installation directory by default.

2. Install the agent with the `INSTALLSERVICE=2` option.

   ```
   msiexec /i <msi installer> INSTALLSERVICE=2
   ```

   By selecting option 2, you are installing the agent in service mode and preventing the agent from automatically starting the agent service after installation. If you do not use option 2, all of the endpoints deployed using the golden or master image will report to the Endpoint Security server using the same agent ID.

3. In the directory where you extracted the msi file and the agent_config.json file, create a file called setupSchTasks.cmd and add the following text to that file:

   NOTE: Remove the line break at the end of the first line and the tenth line before you paste the script into your file. You can also copy and paste directly from the HTML version of this deployment guide.

   ```
   schtasks /create /ru SYSTEM /sc ONSTART /TN "config_xagt" /tr "cmd.exe
   /c sc config xagt start= demand"
   schtasks /run /TN "config_xagt"
   schtasks /delete /TN "config_xagt" /f
   echo "Delete the agent cryptographic keys"
   rd /s /q C:\ProgramData\FireEye\xagt\xacs
   del C:\ProgramData\FireEye\xagt\main.db
   copy <full path to agent_config.json> c:\ProgramData\FireEye\
   copy <full path to ProvisionxAgt.cmd> C:\ProgramData\FireEye\
   schtasks /create /ru SYSTEM /sc ONSTART /TN "prov_xagt" /tr
   "c:\ProgramData\FireEye\ProvisionxAgt.cmd"
   ```


4. In the same directory, create a file called ProvisionxAgt.cmd, add the following text to the file, and save it with ASCII encoding:

   NOTE: Remove the line break at the end of the third line and the sixth line before you paste the script into your file. You can also copy and paste directly from the HTML version of this deployment guide.

```
@echo off
IF ".%PROCESSOR_ARCHITECTURE%"==".AMD64" (
"C:\Program Files (x86)\FireEye\xagt\xagt.exe" -i
"C:\ProgramData\FireEye\agent_config.json"
) ELSE (
"C:\Program Files\FireEye\xagt\xagt.exe" -i
"C:\ProgramData\FireEye\agent_config.json"
)
sc config xagt start=auto
sc start xagt
schtasks /delete /TN "prov_xagt" /f
del "C:\ProgramData\FireEye\agent_config.json"
del "C:\ProgramData\FireEye\ProvisionxAgt.cmd"
```

5. At the command prompt, change to the agent installation directory and run the setupSchTasks.cmd file as an administrator.

You can now use this system as a golden image. When the system boots for the first time, the scheduled task ProvisionxAgt.cmd runs. This task starts the provisioning process and will provision all systems deployed for the golden image.

If you reboot your golden image to update it, then you must uninstall the agent and use the above steps to reinstall it.

Installing Linux Agents Using a Golden Image

Follow the steps in this section to install the agent software on your Linux endpoint using a master or golden image.

To create a master or golden image to install the agent software on your Linux endpoint:

1. Open a Terminal session on the Linux endpoint that you used to download the Linux agent installation package in Downloading an Agent Installation Package from the Web UI on page 43.

```
username@localhost:~$
```

2. Use the `cd` command to change to the `FireEye` directory you created in step 5 of Downloading an Agent Installation Package from the Web UI on page 43.

```
username@localhost:~$ cd desktop
username@localhost:~/Desktop$ cd FireEye
```

3. Use the `tar zxf` command to unzip the Linux agent installation image `.tgz` file:


```
username@localhost:~/Desktop/FireEye$ tar zxf IMAGE_HX_AGENT_LINUX_
31.x.x.tgz.
```

The `.zip` file (Linux) includes the agent `.rpm` files (`xagt-31.x.x-1.el6.x86_64.rpm` and `xagt-31.x.x-1.el7.x86_64.rpm`), and the agent configuration file (`agent_config.json`).

4. Run the `rpm` file that corresponds to your Linux OS.

   ```
   username@localhost:~/Desktop/FireEye$ sudo rpm -ihv xagt_dev-31.x.x-
   1.el6.x86_64.rpm
   ```

5. Import the Agent configuration file on a master or golden image.

   ```
   username@localhost:~/Desktop/FireEye$ sudo /opt/fireeye/bin/xagt -i
   ./agent_config.json
   ```

   When the golden or master image is created using this installation method, the agent service remains stopped. The agent service will only start if you manually start it or if you restart your system. This allows unique agent IDs to be created for each endpoint on which the golden or master image is deployed.

Since the agent service starts on the next system boot, you should install the FireEye Agent as the last step before preparing the final image.

You can use the master or golden image to deploy the agent to your Linux endpoints. If you reboot your golden image to update it, then you must uninstall the agent and use the above steps to reinstall it.

CHAPTER 8: Configuring the Agent Removal Protection Password

After installing the Endpoint Security Agent software on your host endpoints, you can use a Removal Protection password policy to keep your agents secure. The Removal Protection password prevents unauthorized removal of the agent software from endpoints in your enterprise by requiring users to enter a password before uninstalling the agent software.

The **Removal Protection Password** is supported for Windows agents version 27 or later.

You can configure the Removal Protection password policy for the agent default policy or any custom policy using the Web UI or the API only. You can also create a custom exclusion policy that excludes selected host sets from the agent uninstall password protection list using the Web UI only.

If you run the uninstall audit on a host set that has the Removal Protection policy enabled, the uninstall audit will fail. To successfully run the uninstall audit, disable the Removal Protection policy before running the uninstall audit. See Disabling the Removal Protection Policy on the next page for more information.

This section covers the following topics:

Prerequisites

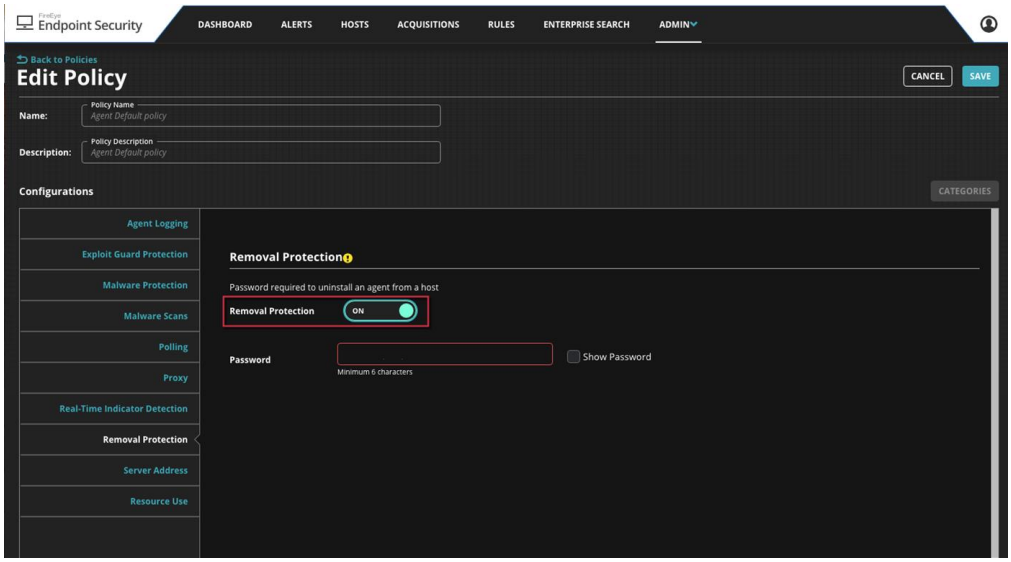
- Admin access when using the Web UI
- The Removal Protection feature requires Endpoint Security Agent version 27 or later.

Enabling the Removal Protection Policy

You can enable the Removal Protection feature for any policy using the Web UI.

To enable the Removal Protection feature for a policy using the Web UI:

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the Policies page.
3. From the Policies table, select the custom policy you want to modify by enabling the Removal Protection feature.
4. Click the policy link to access the Edit Policy page.
5. Select the **Removal Protection** tab.



6. Toggle the Removal Protection **ON/OFF** switch to **ON** to enable the agent uninstall password.
7. Enter your uninstall password in the Password field.

   Your Removal Protection password must have a minimum of 6 alphanumeric characters.

8. Click **Save** to save the policy settings.

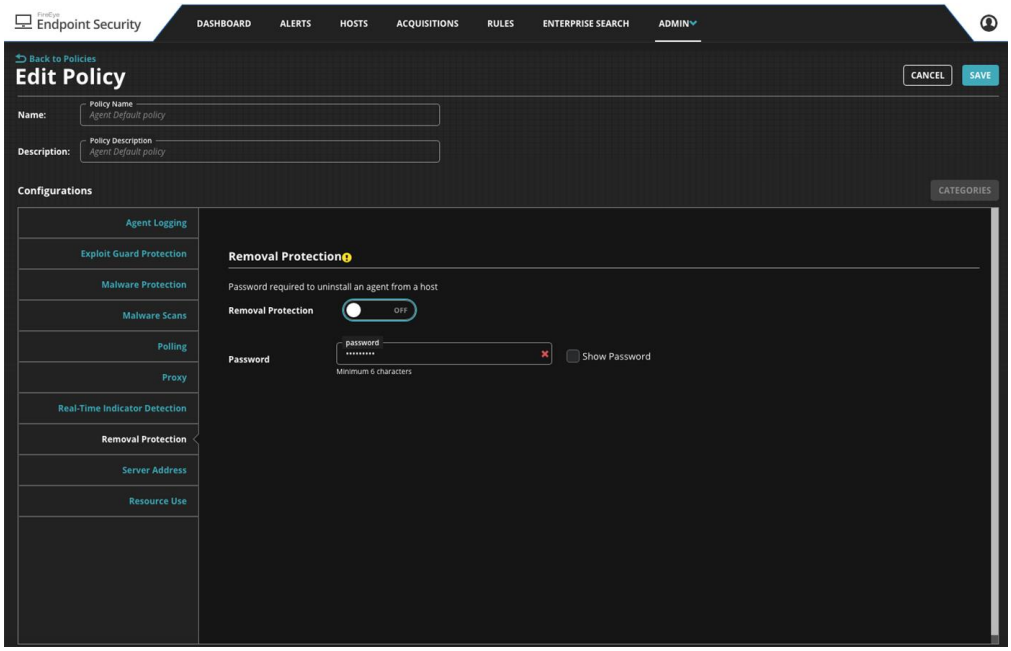
Disabling the Removal Protection Policy

You can disable the Removal Protection feature for any policy using the Web UI.

If you run the uninstall audit on a host set that has the Removal Protection policy enabled, the uninstall audit will fail. To successfully run the uninstall audit, disable the Removal Protection policy before running the uninstall audit.

To disable the Removal Protection feature for a policy using the Web UI:

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the Policies page.
3. From the Policies table, select the custom policy you want to modify by disabling the Removal Protection feature.
4. Click the policy link to access the Edit Policy page.
5. Select the **Removal Protection** tab.
6. Toggle the Removal Protection **ON/OFF** switch to **OFF** to disable the agent uninstall password.



7. If there is a password in the Password field, click the **x** icon in the Password field to delete it.

   To disable the Removal Protection feature, you must delete the password from the Password field before clicking the **Save** button. If you do not delete the password, you will receive an error message when you click save.

8. Click **Save** to save the policy settings.

Excluding Host Sets from the Removal Protection Policy

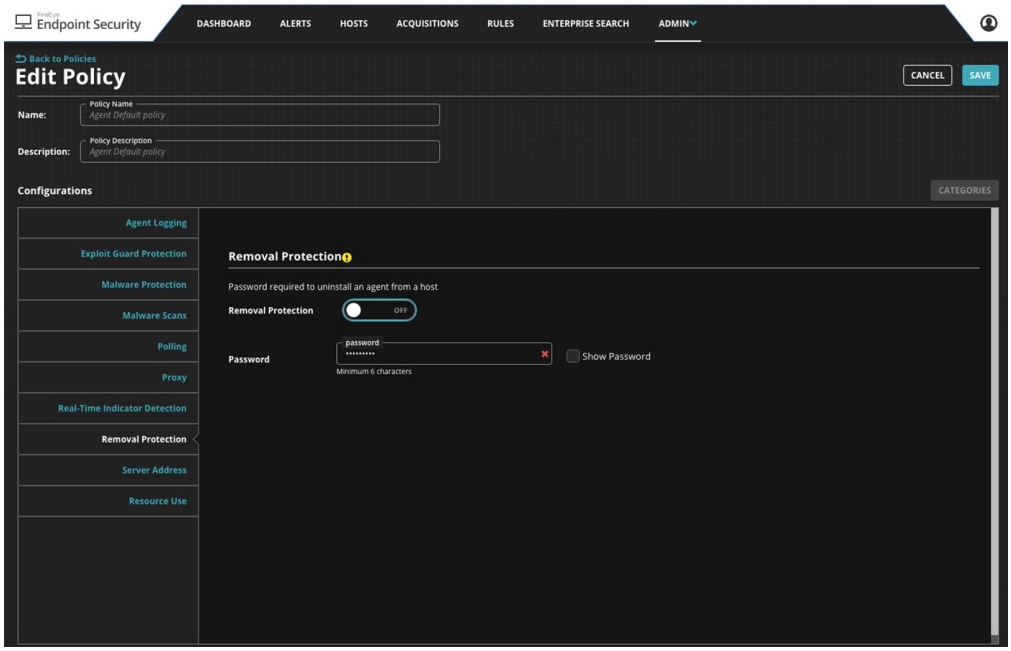
Using the Web UI, you can modify the Agent Default Policy to globally exclude the Removal Protection feature from all host sets in your environment. A global exclusion policy that lists specific host sets that should be excluded from the agent removal protection password policy.

NOTE: Defining a Removal Protection exclusion policy for host sets in your enterprise is not recommended because it allows the Endpoint Security Agent software to be removed from your host endpoints.

A Removal Protection exception policy is ignored for any Windows hosts using Endpoint Security Agent version 25 or earlier.

To exclude all host endpoints from the Removal Protection policy:

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. From the Policies table, select the **Agent Default Policy** and click the policy link to access the Edit Policy page.
4. Select the **Removal Protection** tab.
5. Toggle the Removal Protection **ON/OFF** switch to **OFF** to disable the agent uninstall password.



6. If there is a password in the Password field, click the **x** icon in the Password field to delete it.

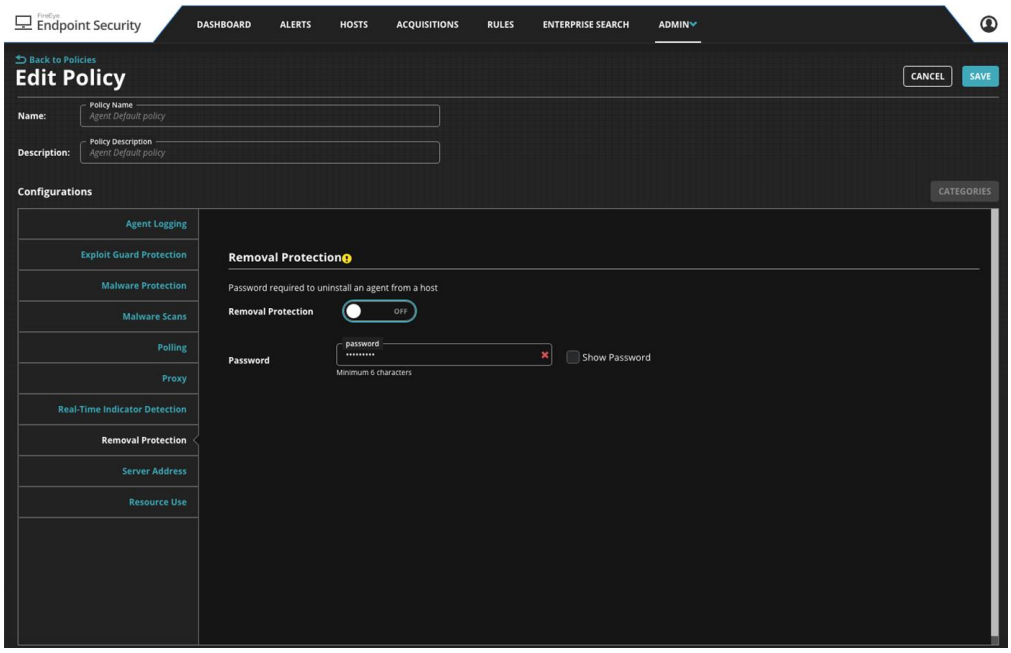
   IMPORTANT: To disable the Removal Protection feature, you must delete the password from the Password field before clicking the **Save** button. If you do not delete the password, you will receive an error message when you click save.

7. Click **Save** to save the policy settings.

To exclude selected host sets from the Removal Protection policy:

NOTE: See "Creating a Custom Policy" in the *Endpoint Security Agent Administration Guide* for more information about using the Web UI to create a custom policy.

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. From the Policies table, select the link for the custom policy you want modify.
4. Select the **Removal Protection** tab.
5. Toggle the Removal Protection **ON/OFF** switch to **OFF** to disable the agent uninstall password.



6. If there is a password in the Password field, click the **x** icon in the Password field to

delete it.

> To disable the Removal Protection feature, you must delete the password from the Password field before clicking the **Save** button. If you do not delete the password, you will receive an error message when you click save.

7. Click **Save** to save the policy settings.

Now you can assign host sets to the custom policy and set the policy priority level. See "Assigning Host Sets to Agent Policies" and "Configuring Policy Priority Using the Web UI" in the *Endpoint Security Agent Administration Guide* for more information.

CHAPTER 9: Uninstalling Endpoint Security Agent Software

You can uninstall Endpoint Security Agent software individually on your endpoint hosts or using software management utilities, such as BigFix and SCCM (in Windows environments) or JAMF (in macOS environments). Refer to the documentation provided for the utility.

If you enable a Removal Protection password policy for host sets in your environment, you must enter the removal password to authorize the agent uninstall process. See "Configuring the Agent Removal Protection Password" in the *Endpoint Security Agent Administration Guide* for more information on setting up an agent uninstall password.

IMPORTANT: If you run the uninstall audit on a host set that has the Removal Protection policy enabled, the uninstall audit will fail. To successfully run the uninstall audit, disable the Removal Protection policy before running the uninstall audit.

This section describes how to uninstall the agent software on a single endpoint host and covers the following topics:

Uninstalling Password-Protected Agent Software

If you need to uninstall a password protected Endpoint Security Agent running on your Windows endpoints, you can use the Endpoint Security Agent Windows Program Manager

or the Windows Installer. Only authorized users can uninstall the agent software.

NOTE: Endpoint Security Agent versions 26 or later support the Removal Protection Password for Windows endpoints only.

IMPORTANT: Endpoint Security Agent removal protection is disabled if Trend Micro AV is running.

Using the Windows Program Manager

This section describes how to uninstall a password-protected agent from your Windows endpoint using the Windows Program Manager.

Artifacts that remain in the `C:\Windows\FireEye` folder after the agent software has been uninstalled will be deleted the next time the endpoint host is rebooted.

If a Windows agent uninstall attempt fails because the binary is missing or corrupt or because the `ProgramData/FireEye` or `Program Files/FireEye` directories are missing or corrupt, reinstall the agent using command-line commands (`msiexec /i <agent software installation msi file> /qb`) and then uninstall it.

1. In the Windows Control Panel, select **Programs and Features**. Depending on your version of Windows, you might have to select **Programs** before you can select **Programs and Features**.
2. Locate **FireEye Endpoint Agent** in the program list and right-click and select **Uninstall**.
3. Select **Yes** when prompted to confirm that you want to uninstall the agent software and to similar confirmation prompts.
4. When prompted, enter the uninstall password and click **OK**. If you are not authorized to remove the agent software from the Windows host or if you enter an incorrect password, the uninstall process will fail.

Using Command-Line to Uninstall a Password-Protected Agent

This section describes how to uninstall password-protection Endpoint Security Agent software from your Windows endpoint using the command line.

1. Open a command line prompt on your Windows host.
2. Use the `msiexec /x` command to uninstall the password-protected agent software by specifying the name of the agent installation `.msi` executable file on the host endpoint and appending `the /x` command with `UNINSTALL_PASSWORD=<password>`.

```
msiexec.exe /x <agent software installation msi file>|<product
identifier #> UNINSTALL_PASSWORD=<password>
```

3. When prompted to confirm that you want to uninstall the agent software, select **Yes**.

Uninstalling the Agent Software in Silent mode

You can also use the command line to uninstall the agent software silently (without any user prompting) by inputting the password as a property to `msiexec`. If this property is missing or if the agent uninstall password is incorrect, the uninstall process will fail.

```
msiexec /x <agent software installation msi file> /qn UNINSTALL_
PASSWORD=password
```

1. Open a command line prompt on your Windows host.
2. Use the `msiexec /x` and /qn commands to uninstall the password-protected agent software in silent mode. Specify the name of the agent installation `.msi` executable file on the host endpoint and appending `the /x` command with `UNINSTALL_PASSWORD=<password>`.

   ```
   msiexec /x <agent software installation msi file>|<product identifier
   #>/qn UNINSTALL_PASSWORD=<password>
   ```

Uninstalling Disguised Windows Agent Software

To uninstall disguised Windows agent software:

1. Locate the `.msi` installation file for the agent software. This must be for the same agent version that is installed on the host endpoint.
2. Run the `.msi` file, selecting the **Remove** option when prompted.
3. Confirm the software removal by responding **Yes** or clicking **Remove** as necessary.

A reboot is necessary after uninstalling FireEye Endpoint Agent 24.9 and before installing the 25.12 agent.

Artifacts that remain in the `C:\Windows\FireEye` folder after the agent software has been uninstalled will be deleted the next time the endpoint host is rebooted.

If a Windows agent uninstall attempt fails because the binary is missing or corrupt or because the `ProgramData/FireEye` or `Program Files/FireEye` directories are missing or corrupt, reinstall the agent using command-line commands (`msiexec /i xagt.msi /qn`) and then uninstall it.

Uninstalling Undisguised Windows Agent Software

To uninstall undisguised Windows agent software:

1. In the Windows Control Panel, select **Programs and Features**. (Depending on your version of Windows, you might have to select **Programs** before you can select **Programs and Features**.)
2. Right-click on the **FireEye Endpoint Agent** you want to uninstall and select **Uninstall**.
3. Select **Yes** when prompted to confirm that you want to uninstall the agent software and to similar confirmation prompts.

A reboot is necessary after uninstalling FireEye Endpoint Agent 24.9 and before installing the 25.12 agent.

IMPORTANT: If Group Policy is used to deploy the Endpoint Security Agent, it can only be uninstalled/upgraded via Group Policy, and not manually uninstalled via **Apps & features**, or upgraded with Endpoint Security Server Server.

Artifacts that remain in the `C:\Windows\FireEye` folder after the agent software has been uninstalled will be deleted the next time the endpoint host is rebooted.

If a Windows agent uninstall attempt fails because the binary is missing or corrupt or because the `ProgramData/FireEye` or `Program Files/FireEye` directories are missing or corrupt, reinstall the agent using command-line commands (`msiexec /i xagt.msi /qn`) and then uninstall it.

Uninstalling macOS Agent Software

To uninstall macOS agent software:

1. Launch the Terminal and enter the following command to run the uninstall script.
   ```
   sudo /Library/FireEye/xagt/uninstall.tool
   ```
   Enter the administrator password when prompted.

2. Enter the following command to verify that no xagt processes are running.
   ```
   ps aux | grep xagt
   ```
   If xagt processes are running on the endpoint, perform one of the following steps:

   - If all the agent artifacts still remain on the endpoint, run the uninstall script again.
   - If all the agent artifacts have been removed from the endpoint, manually terminate the xagt processes.

To completely uninstall macOS agent software and system extensions:

1. Launch the Terminal and enter the following command to run the uninstall script.
   ```
   sudo /Library/FireEye/xagt/uninstall.tool --remove-helper
   ```
   Enter the administrator password when prompted.
2. Enter the following command to verify that no xagt processes are running.
   ```
   ps aux | grep xagt
   ```
   If xagt processes are running on the endpoint, perform one of the following steps:

   - If all the agent artifacts still remain on the endpoint, run the uninstall script again.
   - If all the agent artifacts have been removed from the endpoint, manually terminate the xagt processes.

Uninstalling Linux Agent Software

To uninstall Endpoint Security Agent software version 35.30.0 on your Linux endpoint, you must first determine which uninstall option to use based on the file type you used to install the agent software on your Linux endpoint.

The following table shows the specific uninstall command that corresponds to each supported agent software installation file type.

File Type	Uninstall Command	Compatible Linux Systems
.rpm	`rpm -e <installation_filename.rpm>`	RHEL, CentOS, Amazon Linux AMI, and SUSE
.deb	`dpkg --purge xagt <installation_filename.deb>`	Ubuntu

IMPORTANT: The Endpoint Security software installation `.rpm` and **.deb** files do not include an uninstall script.

This section includes the following topics:

Uninstalling the Linux Agent on RHEL-Based Systems

Follow the steps in this section if you need to uninstall the agent software from your Linux endpoint running a support RHEL-based operating system, including

- RHEL versions 6.8, 6.9, 6.10, 7.2, 7.3, 7.4,7.5, 7.6, 7.7, 8 (64-bit)
- CentOS versions 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 (64-bit)
- Amazon Linux AMI version 2018.3, AMI2 (64-bit)

To uninstall Linux agent software on your RHEL-based system:

1. Open a Terminal session on your Linux endpoint running Endpoint Security Agent software version 35.30.0.
2. Type the following command to identify the `.rpm` or `.run` that was used to install the Endpoint Security Agent software version 35.30.0 on your Linux endpoint.

   ```
   username@localhost:~$ yum list | grep xagt
   ```

   The example below identifies the `xagt-31.28.0-1.el7.x86_64.rpm` file as the file that was used to install the agent software on the Linux endpoint. You can see the Linux OS bit-architecture, the agent software version, and the software status.

   ```
   xagt.x86_64              31.28.0-1.el7                installed
   ```

3. Run the correct uninstall command for the file type you identified in Step 2 to remove the Endpoint Security Agent software version 35.30.0 from your Linux endpoint.
   - If the `.rpm` file was used to install the Endpoint Security Agent software version 35.30.0 on your Linux endpoint, use the `rpm -e` command to uninstall the agent software from your Linux endpoint.

     ```
     username@localhost:~$ sudo rpm -e <installation_filename.rpm>
     ```

   - If the `.run` file was used to install the Endpoint Security Agent software version 35.30.0 on your Linux endpoint, use the binary path and uninstall script to remove the agent software from your Linux endpoint.

     ```
     username@localhost:~$ sudo /opt/fireeye/bin/uninstall.sh
     ```

Uninstalling the Linux Agent on SUSE System

Follow the steps in this section if you need to uninstall the agent software from your Linux endpoint running SUSE Enterprise Linux version 11.4, 12.2, 12.3, or 15.

To uninstall Linux agent software on your Linux endpoint running a supported SUSE version:

1. Open a Terminal session on your Linux endpoint running Endpoint Security Agent software version 35.30.0.
2. Type the following command to identify the `.rpm` that was used to install the Endpoint Security Agent software version 35.30.0 on your Linux endpoint.
3. `username@localhost:~$ rpm -qa | grep xagt`

   The example below identifies the `xagt-29.0.1-1.sle11.x86_64.rpm` file as the file that was used to install the agent software on the Linux endpoint. You can see the Linux OS bit-architecture, the agent software version, and the software status.

   ```
   xagt.x86_64            29.0.1-1.sle11                installed
   ```

4. Run the `rpm -e` command to remove the Endpoint Security Agent software version 35.30.0 from your Linux endpoint.

   ```
   username@localhost:~$ sudo rpm -e <installation_filename.rpm>
   ```

Uninstalling the Linux Agent on an Ubuntu System

Follow the steps in this section if you need to uninstall the agent software from your Linux endpoint running Ubuntu version 14.04, 16.04, or 18.04.

To uninstall Linux agent software on your Linux endpoint running a support Ubuntu version:

1. Open a Terminal session on your Linux endpoint running Endpoint Security Agent software version 35.30.0.
2. Type the following command to identify the `.deb` that was used to install the Endpoint Security Agent software version 35.30.0 on your Linux endpoint.

   ```
   username@localhost:~$ dpkg -l | grep xagt
   ```

   The example below identifies the `xagt-29.0.1-1.ubuntu12_amd64.deb` file as the file that was used to install the agent software on the Linux endpoint. You can see the Linux OS bit-architecture, the agent software version, and the software status.

   ```
   xagt.amd64          29.0.1-1.ubuntu12             installed
   ```

3. Run the `dpkg --purge xagt` command to remove the Endpoint Security Agent software version 35.30.0 from your Linux endpoint.


```
username@localhost: ~$ sudo dpkg --purge xagt <installation_
filename.deb>
```

PART IV: Setup and Configuration

CHAPTER 10: Before You Install or Upgrade the Agent Software

This section describes critical steps you must perform before installing or upgrading the Endpoint Security Agent software on your host endpoints.

If your third-party antivirus software does not allow you to whitelist or exclude agent files or processes until they are present on your host endpoint, perform these steps immediately after installing or upgrading the agent software on your host endpoint.

Excluding Agent Files in Your Antivirus Software

Third-party antivirus software packages use advanced heuristics engines to evaluate and protect your host endpoints. To ensure that Endpoint Security processes are not subject to these heuristics, verify that the agent executable files (`*.exe` files) meet the following requirements for the following antivirus software vendors (if applicable in your environment):

- List agent executable files as low-risk processes in McAfee.
- Exclude agent executable files from behavior monitoring in Trend Micro Office Scan.
- Apply application exclusion to agent executable files in Symantec Endpoint Protection.

For more information, refer to the documentation provided with your antivirus software.

Rarely, third-party security software identifies installed Endpoint Security files and activity as malicious. It is a good idea to whitelist or exclude agent files from real-time scanning and behavioral analysis (sometimes known as HIPS) in your third-party security software. Endpoint Security Agent software version 27 or later supports whitelisting by the original filename. This ensures that whitelisted files remain on the excluded list even if a user changes the filename.

NOTE: Be sure to exclude the `xagt.exe` file as a process in addition to excluding it as a file.

In addition, FireEye **strongly recommends** that you create malware protection process, file and folder exclusions for any third-party antivirus software. For example, if you are running McAfee antivirus software on your host endpoints, you should use the Malware Protection tab to create exclusions for McAfee processes, files, and folders.

Be sure to create malware protection process, file, and folder exclusions for the following third-party antivirus software running on your host endpoints:

- McAfee
- Symantec Endpoint Protection (SEP)
- Trend Micro Office Scan
- Windows Antivirus software

IMPORTANT: See Microsoft Anti-Virus Exclusion List and Running Windows Antivirus Software on Exchange 2016 Servers for more information on the folders, processes, and file name extensions you should exclude from Endpoint Security Agent malware protection processing.

This will maximize performance, ensure compatibility with other antivirus software, and reduce the number of duplicate alerts you receive from the Endpoint Security malware protection feature and your third-party antivirus software. Use the malware protection global policy to define these exclusions. See Defining the Malware Protection Exclusion Policy in the Endpoint Security Agent Administration Guide for more information.

Excluding Agent Files for Your Windows Environment

In your Windows environment, whitelist the directories and file paths listed in this section to exclude specific Endpoint Security program files, plug-in files, driver files, and log files from real-time scanning and behavioral analysis by your third-party antivirus software. The default directory paths (wildcard) and file paths, including the supported Windows version, are shown for each directory and file.

If the TARGETDIR option was used with the Windows MSI to change the installation location of the agent software, then the exclusion path must change. For example, if `TARGETDIR = C:\MyInstallationDirectory` then `C:\MyInstallationDirectory\*.*` should be excluded instead of `%ProgramFiles (x86)%\FireEye\xagt\*.*` or `%ProgramFiles%\FireEye\xagt\*.*`.

NOTE: If the Endpoint Security is installed in an environment where Sophos Antivirus and the Microsoft Enhanced Mitigation Experience Toolkit (EMET) are installed, you might experience Microsoft Internet Explorer crashes. To resolve this problem, start up the EMET GUI and turn off the ROP Caller Check setting for the iexplore.exe application. Refer to the EMET documentation for more information.

Program Files Excluded	Default File Path	Windows Version
audits.dll, mindexer.sys, and xagt.exe	%ProgramFiles%\FireEye\xagt*.*	32-bit
	%ProgramFiles(x86)%\FireEye\xagt*.*	64-bit
32-bit = 32-bit versions of Windows 64-bit = 64-bit versions of Windows		

Driver Files	Default File Path	Windows Version
FeKern.sys	%SystemRoot%\System32\drivers\FeKern.sys	All
FeElam.sys	%SystemRoot%\System32\drivers\FeElam.sys	All
fe_avk.sys	%ProgramData%\FireEye\xagt\exts\MalwareProtection\sandbox\fe_avk.sys	64-bit
64-bit = 64-bit versions of Windows All = See "Operating System Requirements" for a list of all of the supported Windows operating system versions.		

All Data Files	Default File Path	Windows Version
Everything in the `ProgramData\FireEye\xagt` directory	%ALLUSERSPROFILE%\ApplicationData\FireEye\xagt*.*	NT 5.x
	%ProgramData%\FireEye\xagt*.*	NT 6+
NT 5.x = Windows XP SP3 and Windows Server 2003 SP2+R2 NT 6+ = All other supported Windows versions		

Plug-In File	Default File Path	Windows Version
xagtnotif.exe	%SystemRoot%\FireEye\xagtnotif.exe	All

Plug-In File	Default File Path	Windows Version
Any extensions in %ALLUSERSPROFILE%\ApplicationData\FireEye\xagt\exts directories or subdirectories should be whitelisted in your antivirus software.		All
All = All supported versions of Windows		

Excluding Agent Files for Your macOS Environment

In your macOS environment, whitelist the program files, plug-in files, driver files, and log files listed in the tables below. The default file path and the supported macOS version are shown for each file.

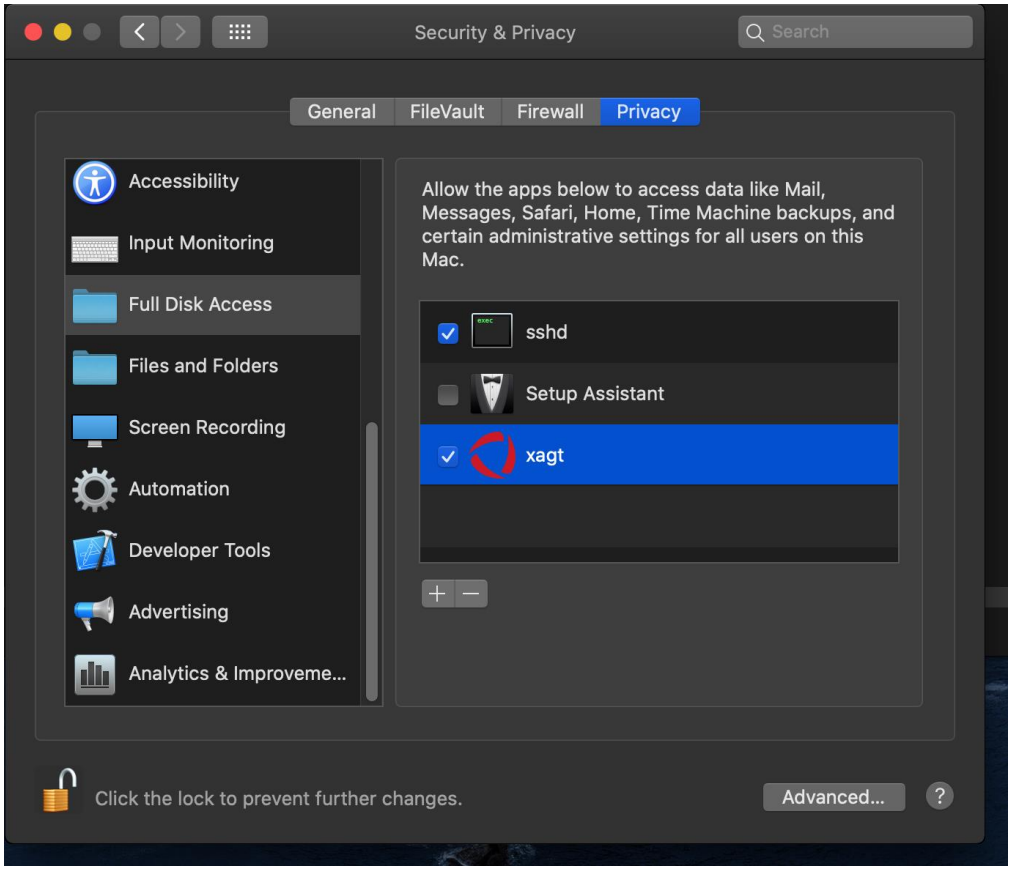
Program Files	Default File Path	macOS Version
xagt/*	/Library/FireEye/xagt/*	All
Support/FireEye/*	/Library/Application Support/FireEye/*	All
FireEye.kext/*	/Library/Extensions/FireEye.kext/*	All
com.fireeye.xagt.plist	/Library/LaunchDaemons/com.fireeye.xagt.plist	All
com.fireeye.xagtnotif.plist	/Library/LaunchAgents/com.fireeye.xagtnotif.plist	All
IOKitBDAv.kext	/Library/Extensions/IOKitBDAv.kext	All
All = Supported macOS versions: 10.9 (Mavericks), 10.10 (Yosemite), 10.12 (Sierra), and 10.15 (Catalina), and 11 (Big Sur).		

Enabling Full Disk Access on macOS

To add the `xagt` app to the "Full Disk Access" list:

1. Open **System Preferences**.
2. Select the **Security & Privacy** tab.
3. In the list of services on the left, choose **Full Disk Access**.
4. Click the **Lock icon** in the bottom left corner to unlock the setting.
5. Enter Administrator credentials.
6. Click the + icon.

7. Navigate to the `/Library/FireEye/xagt/` folder.
8. Select `xagt.app`.
9. Click the **Open** button.
10. Ensure that the `xagt` app checkbox is selected.



11. Quit **Security & Privacy**.

Excluding Agent Files for Your Linux Environment

In your Linux environment, whitelist the program files and directories listed in the table below. The default file path and the supported Linux version are shown for each file.

Program Files	Default File Path	Linux Version
xagt	/etc/rc.d/init.d/xagt	RHEL 6.x
Everything in the `/var/lib/fireeye/` directory	/var/lib/fireeye/*	All

Program Files	Default File Path	Linux Version
Everything in the `/opt/FireEye/` directory	/opt/fireeye/*	All
xagt.service	/usr/lib/systemd/system/xagt.service	RHEL 7.x
All = Supported Linux versions: RHEL 6.8 and RHEL 7.x)		

Excluding Exploit Guard Files in Your Windows Environment

In addition, if you intend to enable Exploit Guard in your Windows environment, whitelist the driver files and log files in the tables below. The default file path and the supported Windows version are shown for each file.

NOTE: The Exploit Guard plug-in files you need to whitelist are included in the %ALLUSERSPROFILE%\Application Data\FireEye\ xagt*.* and %ProgramData%\FireEye\xagt*.* directory exclusions you whitelisted in Excluding Agent Files for Your Windows Environment on page 92.

NOTE: At first installation, the following files will not have the underscore (_) and *xx* number appended to them. Files without the underscore (_) should also be excluded.

Driver Files	Default File Path	Windows Version
AppMonitorDll32_*xx*.dll	%SystemRoot%\FireEye\AppMonitorDll32_*xx*.dll (where *xx* is a series of incrementing numbers, for example: %SystemRoot%\FireEye\AppMonitorDll32_00.dll %SystemRoot%\FireEye\AppMonitorDll32_01.dll %SystemRoot%\FireEye\AppMonitorDll32_02.dll %SystemRoot%\FireEye\AppMonitorDll32_03.dll)	64-bit

Driver Files	Default File Path	Windows Version
JavaAgentDll32_*xx*.dll	%SystemRoot%\FireEye\JavaAgentDll32_*xx*.dll (where *xx* is a series of incrementing numbers, for example: %SystemRoot%\FireEye\JavaAgentDll32_00.dll %SystemRoot%\FireEye\JavaAgentDll32_01.dll %SystemRoot%\FireEye\JavaAgentDll32_02.dll %SystemRoot%\FireEye\JavaAgentDll32_03.dll)	64-bit
AppUIMonitor_*xx*.exe	%SystemRoot%\FireEye\AppUIMonitor_*xx*.exe (where *xx* is a series of incrementing numbers, for example: %SystemRoot%\FireEye\AppUIMonitor_00.exe %SystemRoot%\FireEye\AppUIMonitor_01.exe %SystemRoot%\FireEye\AppUIMonitor_02.exe %SystemRoot%\FireEye\AppUIMonitor_03.exe)	All
AppMonitorDll_*xx*.dll	%SystemRoot%\FireEye\AppMonitorDll_*xx*.dll (where *xx* is a series of incrementing numbers, for example: %SystemRoot%\FireEye\AppMonitorDll_00.dll %SystemRoot%\FireEye\AppMonitorDll_01.dll %SystemRoot%\FireEye\AppMonitorDll_02.dll %SystemRoot%\FireEye\AppMonitorDll_03.dll)	All

Driver Files	Default File Path	Windows Version
JavaAgentDll_*xx*.dll	%SystemRoot%\FireEye\JavaAgentDll_*xx*.dll (where *xx* is a series of incrementing numbers, for example: %SystemRoot%\FireEye\JavaAgentDll_00.dll %SystemRoot%\FireEye\JavaAgentDll_01.dll %SystemRoot%\FireEye\JavaAgentDll_02.dll %SystemRoot%\FireEye\JavaAgentDll_03.dll)	All
64-bit = 64-bit versions of Windows All = All supported versions of Windows		

Certificate-Based Whitelisting

Endpoint Security supports certificate-based whitelisting for malware alerts only. This means that you can specify a family of binaries with a single rule. Certificate-based whitelisting can be provided through the Dynamic Threat Intelligence (DTI) Portal, or you can mark an alert as false positive, selecting the Digital Signature condition. This will identify all alerts with this certificate as false positive.

NOTE: Trellix Endpoint Security Agent version 27 or later supports certificate-based whitelisting for malware alerts only.

CHAPTER 11: Configuring the Server Address List

The server address list is a list of Endpoint Security and DMZ servers installed in your enterprise. If your enterprise deploys both Endpoint Security and DMZ servers on the network, you need to consider the deployment topology when you configure agent communication. For example, if a host endpoint will be used outside the enterprise network and its agent is expected to communicate with a DMZ server, the DMZ server's address needs to be included in the server address list. FireEye recommends that the first server in the server address list be the most accessible to the largest number of hosts.

- **Appliance Address Order**

  Agents attempt to connect to the first Endpoint Security server listed in the server address list. If the first server is unavailable, the agent then attempts to reach the second server, and so on.

  The address order is set by the order in which you add the servers to the server address list. The first server added is the first one in the list. The second server added is the second in the list.

- **Provisioning Appliance**

  Endpoint Security version 3.0 and later support the use of multiple provisioning servers for endpoints running Agent software version 20 or later and a single provisioning server for endpoints running FireEye Endpoint Security Agent software version 11 or earlier. Agents use provisioning servers to connect and complete their installation by establishing their cryptographic agent identity. Any Endpoint Security server, including a DMZ server, can be enabled to do provisioning. Endpoint Security provisioning servers must be accessible by agents within your company's network. DMZ provisioning servers must be accessible inside and outside your company's network.

- **Primary Appliance**

  If the endpoints in your environment have agent software versions earlier than version 20 installed, a single Endpoint Security server needs to be designated as the *primary* server. This server must be accessible within the network by all agents when they are initially installed on hosts. The primary server manages the initial provisioning of the agents. You can use either your internal Endpoint Security server or a DMZ server as your primary server.

The server address policy is available in the Agent Default Policy only. To update the settings for this policy you must access the default policy. You cannot access the Server Address policy category through any other policy.

Endpoint Security server administrators and operators can add or remove servers on the server address list.

- Adding a Server to the Server Address List
- Removing a Server from the Server Address List

Prerequisites

- Admin or Operator access when using the Web UI
- The Endpoint Security server is physically installed on the network for agent access

Adding an Appliance to the Server Address List

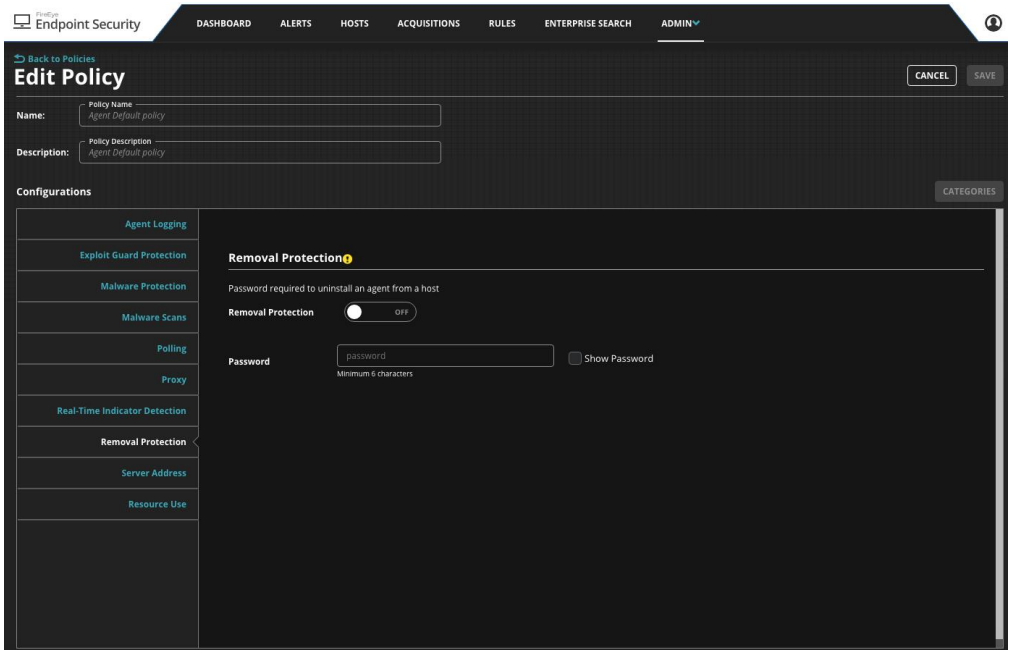
You can add an Endpoint Security server to the server address list using the Web UI or the API

- Adding a Server to the Server Address List

Adding a Server to the Server Address List

To add a server to the server address list:

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. From the Policies table, select the **Agent Default Policy** to access the **Edit Policy** page.
4. Select the **Server Addresses** tab.



5. In the **Enter server address of server(s)**field, enter the hostname or the IP address of the Endpoint Security or DMZ server and click **Add**.

   (Optional) If the endpoints in your environment have agent software version 20 or later installed, select **Enable Provisioning** if the added server will be doing provisioning. At least one server must be designated as a provisioning server.

   (Optional) If the endpoints in your environment have agent software versions earlier than version 20 installed, select **Set as primary** if the added sever will be doing provisioning. This specifies the server as the primary server for your network. Primary server are used to provision agents older than version 20. Only a single server can be designated as a primary server.

6. Click **Save**.

Removing an Appliance From the Server Address List

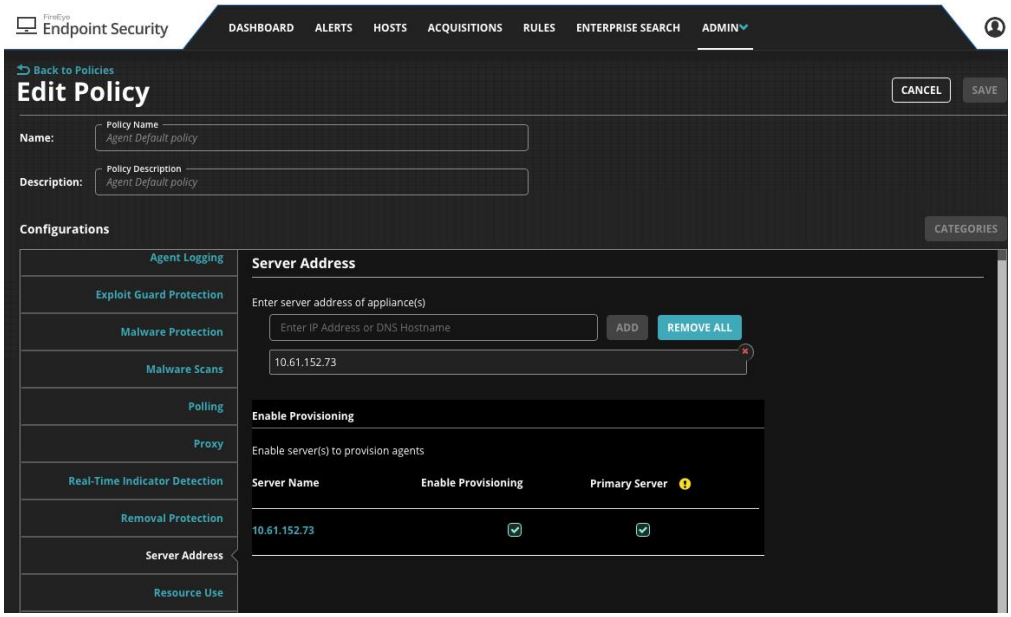
You can remove an Endpoint Security server from the server address list using the Web UI or the API.

- Removing a Server from the Server Address List

Removing a Server from the Server Address List

To delete an appliance from the server address list using the Web UI:

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. From the Policies table, select the **Agent Default Policy** to access the **Edit Policy** page.
4. Select the **Server Addresses** tab.



5. Select the remove icon  next to the IP address or host you want to delete.
6. Click **Save**.

CHAPTER 12: Using Symbolic Links for Agent Program Data in Windows Environments

You can use a Windows file system junction, or symbolic link, for the agent data stored in the Windows `ProgramData` folder (`C:\%ProgramData%\FireEye`).

If you choose to use a symbolic link, consider the following caveats:

- Symbolic links are supported for Endpoint Security version 20 or later. This functionality has not been tested with earlier versions.
- This functionality is supported by the agent only for Windows 7 64-bit systems.
- Agents cannot share symbolic link locations, which means no network shares can be used. Each host endpoint must have its own symbolic link.
- Set up the symbolic link *before* installing the agent software.

For information about setting up symbolic links in Windows environments, refer to your Microsoft Windows system internals documentation (https://technet.microsoft.com/en-us/sysinternals/bb896768.aspx).

CHAPTER 13: Configuring Polling

The following polls occur between the Endpoint Security server and the Endpoint Security Agents installed on your host endpoints. You can configure how frequently each poll occurs using the Web UI and the API. See the *Endpoint Security Agent Administration Guide* for more information on configuring agent policies and settings.

Poll Type	Description
Full	A full poll is used to transfer information and task requests from the Endpoint Security server to the agents installed on the host endpoints. To establish a full poll session, the agent establishes a secure connection with the Endpoint Security server, exchanges information, queries the Endpoint Security server for any tasks to be run, and downloads the instructions for these tasks. See Configuring the Full Poll Interval on the next page.
Fastpoll	A fastpoll is used to determine quickly if a full poll is required. The agent sends a non-encrypted (non-secure) poll request to the Endpoint Security server to determine if any tasks are waiting or if any information is waiting to be shared with the agent. If information is waiting, the agent establishes a standard encrypted full poll session. If no information is waiting, the agent closes the connection. Fastpolls ensure that information sharing occurs promptly without degrading network performance. See Configuring the Agent Fastpoll Interval on page 110.
Indicator	An indicator poll is used to transfer the latest Trellix indicators from the Endpoint Security server to the agents. The agent establishes a secure connection with the server and downloads the latest indicators. Indicator update packages are signed and encrypted files containing versioned sets of indicators and conditions. See "Configuring the FireEye Indicator Update Frequency" in the *Endpoint Security Agent Administration Guide*.

Poll Type	Description
Agent Configuration File	A configuration file poll is used to transfer the latest agent configuration from the Endpoint Security server to the agents. The agent establishes a secure connection with the server and downloads the latest configuration. See Configuring the Agent Configuration File Update Frequency on page 113.
Malware Definition Updates	A malware protection indicator updates poll is used to transfer the latest malware protection indicators to the agent. The agent establishes a secure connection with the Endpoint Security server and downloads the latest malware protection indicators. See "Configuring the Update Interval for Malware Protection Indicators" in the *Endpoint Security Agent Administration Guide*.

Collecting Agent Host System Information

You can also use the Web UI to configure how often agent host system information is collected and updated malware protection indicators are downloaded to the agent. A *system information (sysinfo) task* is scheduled at regular intervals to transfer information from the agents to the Endpoint Security server. The Endpoint Security server requests host system information whenever it sends information to an agent. The sysinfo interval is the longest period of time the server will allow before sending the agent a sysinfo task to collect host system information. See Configuring the System Information Request on page 115and System Information Frequency Setting on page 127.

See the *Endpoint Security Agent Administration Guide* and the *Endpoint Security REST API Guide* for more information on configuring agent policies and settings.

Configuring the Full Poll Interval

A full poll is used to transfer information and task requests from the Endpoint Security Server to the agents installed on the host endpoints. To establish a full poll session, the agent establishes a secure connection with the Endpoint Security Server, exchanges information, queries the Endpoint Security Server for any tasks to be run, and downloads the instructions for these tasks.

You can use the Web UI or the API to configure how often the full agent poll occurs for all host sets in your environment or select host sets in your environment. Valid values for the

full poll range from 60 to 86400 seconds. The full poll interval distributed with the Endpoint Security Agent software is 600 seconds (10 minutes). For guidelines on setting this value, see "Agent Full Poll Interval Setting" in the *Endpoint Security Agent Administration Guide*.

NOTE: In an Endpoint Security environment that includes an Endpoint Security DMZ server, agents attempt full polls and fastpolls a few times to an Endpoint Security server before switching to the DMZ server. If the Endpoint Security Server restore time exceeds your full poll and fastpoll setting times, your agents may revert to polling only your DMZ server. When the Endpoint Security Server becomes available after the restore, the agents will not automatically switch polling from the DMZ Server back to the Endpoint Security Server.

This section covers how to use the Web UI to configure the full poll interval. See the *Endpoint Security REST API Guide* for information on using the API to configure the full poll interval.

- Configuring the Full Poll Interval for All Endpoints below
- Configuring the Full Poll Interval for Selected Host Sets on page 109

Prerequisites

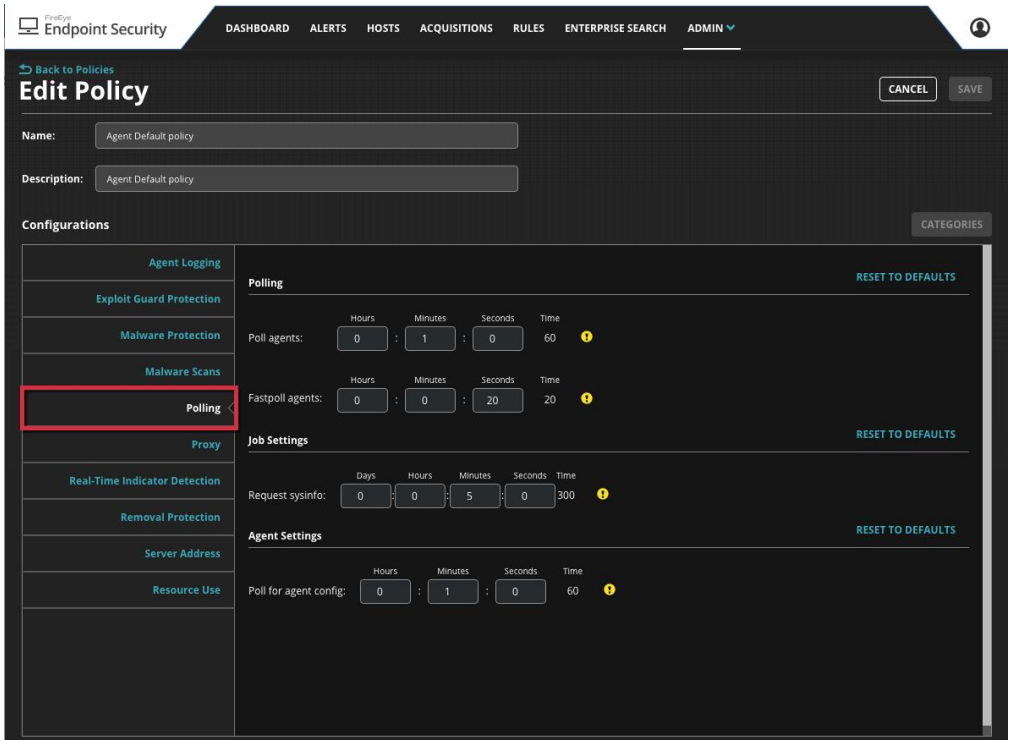
- Admin access to the Web UI

Configuring the Full Poll Interval for All Endpoints

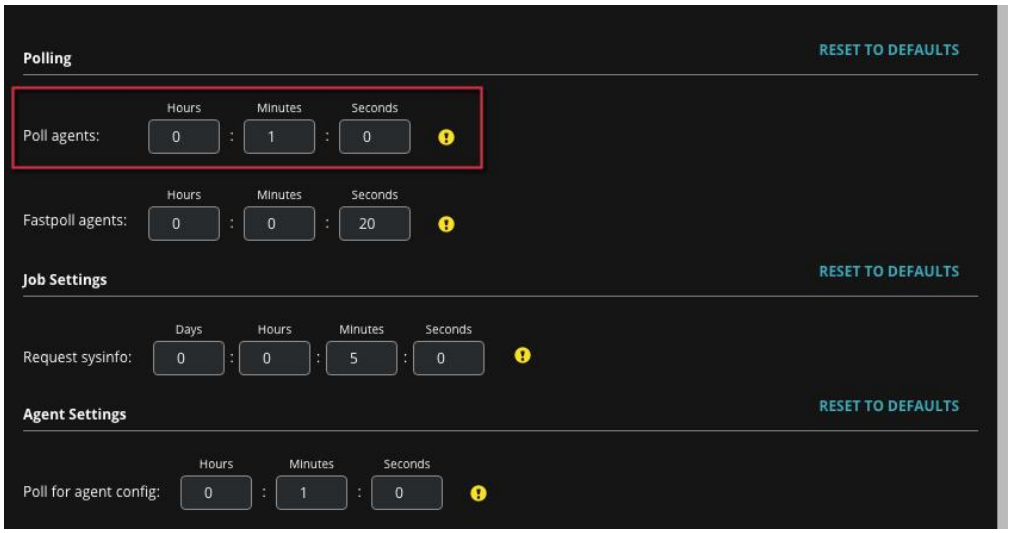
To configure the full poll interval for all host endpoints:

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. From the Policies table, click the **Agent Default Policy** link to go to the **Edit Policy** page.

4. Select the **Polling** tab.



5. Enter the full poll interval **(hours, minutes, and seconds)** in the **Poll agents** fields.



6. Click **Save**.

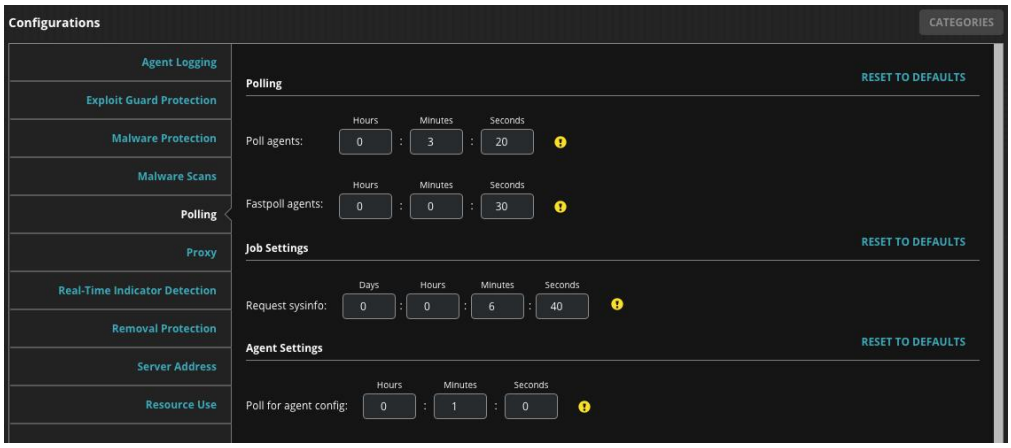
Click **Reset to defaults** to revert the full poll interval to the default setting.

Configuring the Full Poll Interval for Selected Host Sets

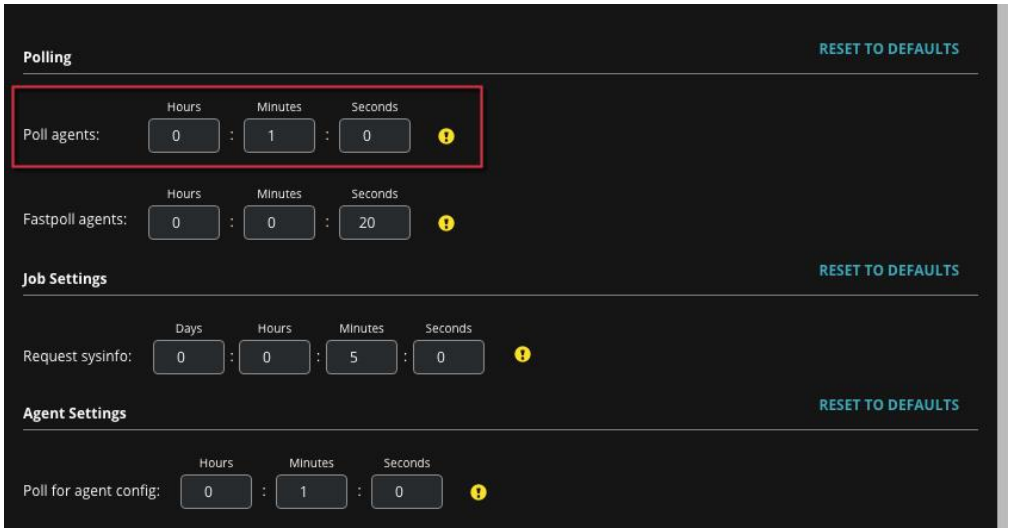
To configure the full poll interval for selected host sets:

NOTE: See "Creating a Custom Policy" in the *Endpoint Security Agent Administration Guide* for more information about using the Web UI to create a custom policy.

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. From the Policies table, click the **Agent Default Policy** link to go to the **Edit Policy** page.
4. Select the **Polling** tab.



5. Enter the full poll interval **(hours, minutes, and seconds)** in the **Poll agents** fields.



6. Click **Save**.

NOTE: Click **Reset to defaults** to revert the full poll interval to the default setting.

Now you can assign host sets to the custom policy and set the policy priority level. See "Assigning Host Sets to Agent Policies" and "Configuring Policy Priority Using the Web UI" in the *Endpoint Security Agent Administration Guide* for more information.

Configuring the Agent Fastpoll Interval

A fastpoll is used to determine quickly if a full poll session is required. The agent sends a non-encrypted (non-secure) poll request to the server to determine if any tasks or information are waiting to be shared with the agent. If information is waiting, the agent establishes a standard encrypted poll session. If no information is waiting, the agent closes the connection.

The fastpoll ensures that information sharing occurs promptly without degrading network performance. The fastpoll interval can be set using the Web UI or the API. Valid values for the fastpoll setting range from 20 to 86400 seconds. The fastpoll interval setting distributed with the Endpoint Security software is 60 seconds.

To disable the fastpoll feature, set the fastpoll interval larger than the full poll interval.

This section covers how to use the Web UI to configure the fastpoll interval. See the Endpoint Security REST API Guide for information on using the API to configure the fastpoll interval.

- Configuring the Fastpoll Interval for All Endpoints
- Configuring the Fastpoll Interval for Selected Host Sets

Prerequisites

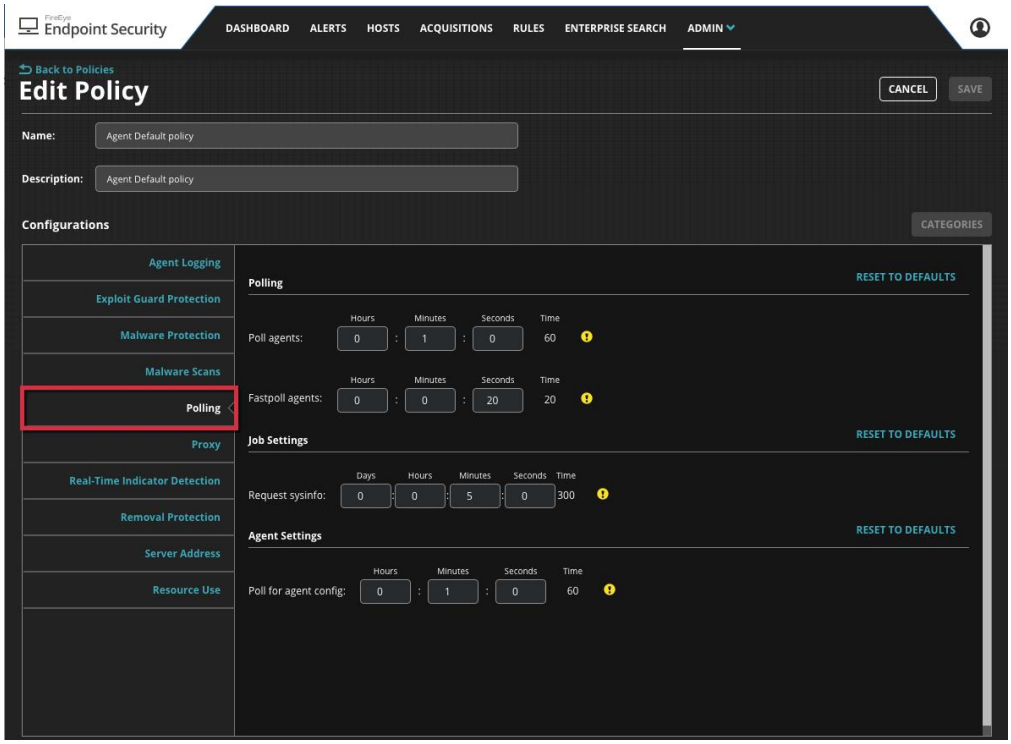
- Admin access to the Web UI

Configuring the Fastpoll Interval for All Endpoints

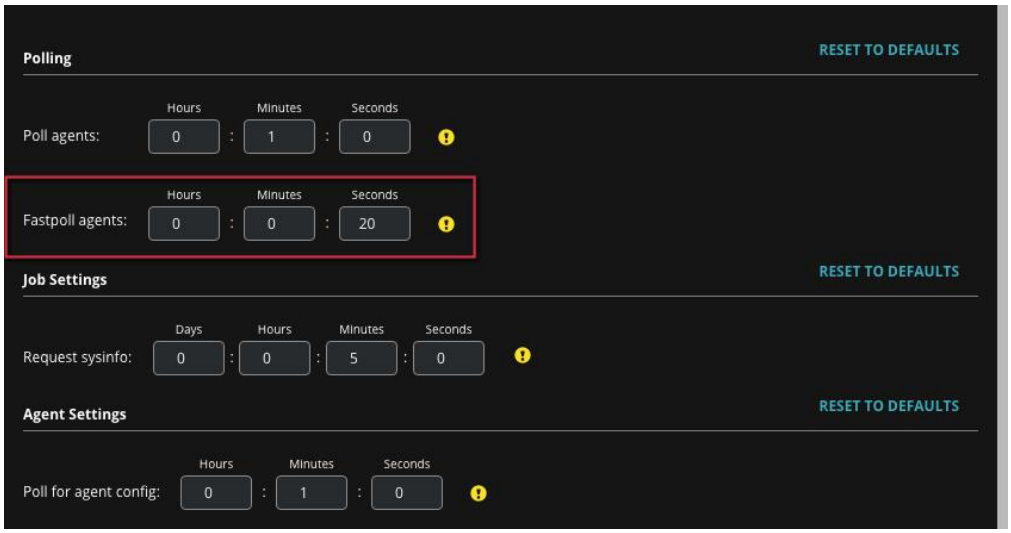
To configure the agent fastpoll interval for all host endpoints:

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. From the Policies table, click the **Agent Default Policy** link to go to the **Edit Policy** page.

4. Select the **Polling** tab.



5. Enter the fastpoll interval **(hours, minutes, and seconds)** in the **Fastpoll agents** fields. Valid values for the fastpoll setting range from 20 to 86400 seconds. The default value is 60 seconds.



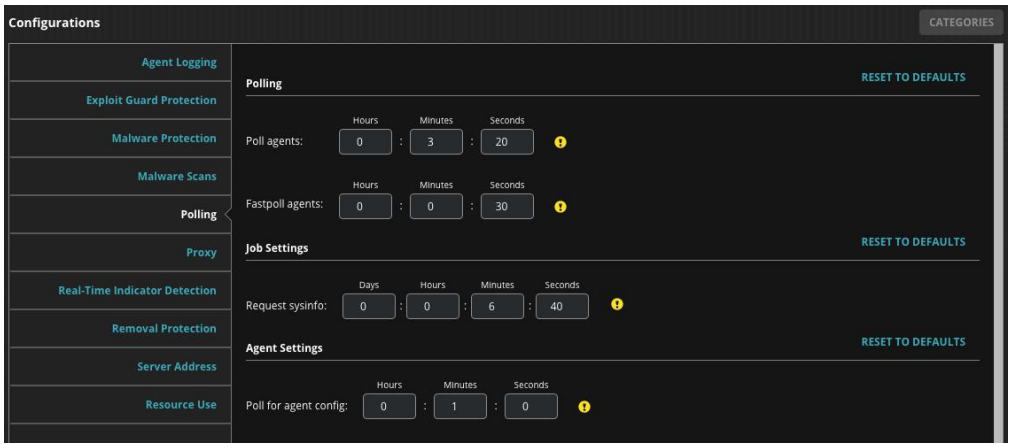
6. Click **Save**.

Click **Reset to defaults** to revert the fastpoll interval to the default setting.

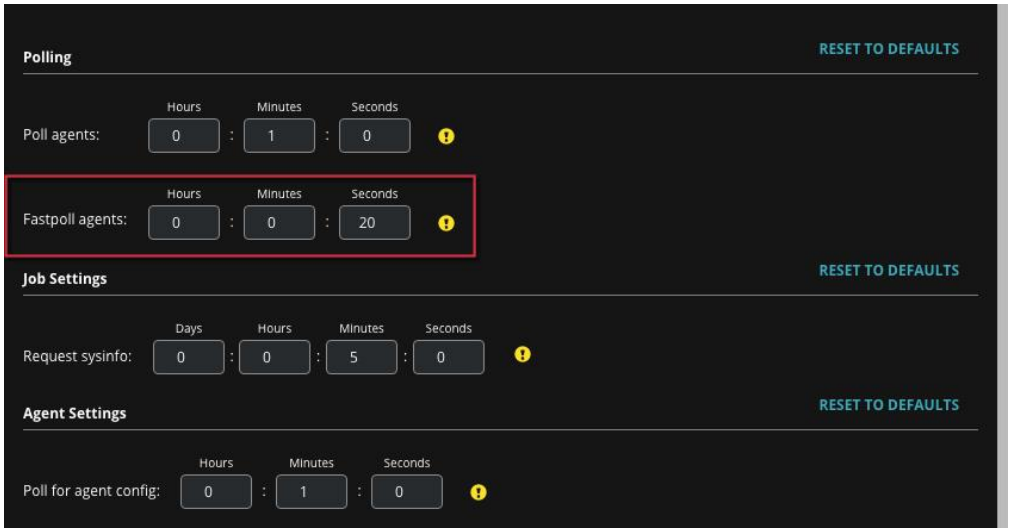
Configuring the Fastpoll Interval for Selected Host Sets

To configure the agent fastpoll interval for selected host sets:

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. In the Policies table, click the link for the custom policy you want to modify.
4. Select the **Polling** tab.



5. Enter the fastpoll interval **(hours, minutes, and seconds)** in the **Fastpoll agents** fields. Valid values for the fastpoll setting range from 20 to 86400 seconds. The default value is 60 seconds.



6. Click **Save**.

> **NOTE:** Click **Reset to defaults** to revert the fastpoll interval to the default setting.

Now you can assign host sets to the custom policy and set the policy priority level. See "Assigning Host Sets to Agent Policies" and "Configuring Policy Priority Using the Web UI" in the *Endpoint Security Agent Administration Guide* for more information.

Configuring the Agent Configuration File Update Frequency

At a specified interval, the agent establishes a secure connection with the server and downloads the latest configuration. See "Understanding When Policies Are Updated" in the *Endpoint Security Agent Administration Guide* for information about how this polling frequency interacts with the system information polling frequency. The agent configuration file update frequency can be set the Web UI and the API.

Valid values for the configuration update frequency range from 60 to 86400 seconds (one minute to one day). The agent configuration file update frequency distributed with the Endpoint Security software is 900 seconds (15 minutes).

This section covers how to use the Web UI to configure the agent configuration file update frequency. See the Endpoint Security REST API Guide for information on using the API to configure the agent configuration file update frequency.

- Configuring the Agent Configuration File Update Frequency for All Endpoints
- Configuring the Agent Configuration File Update Frequency for Selected Host Sets on page 115

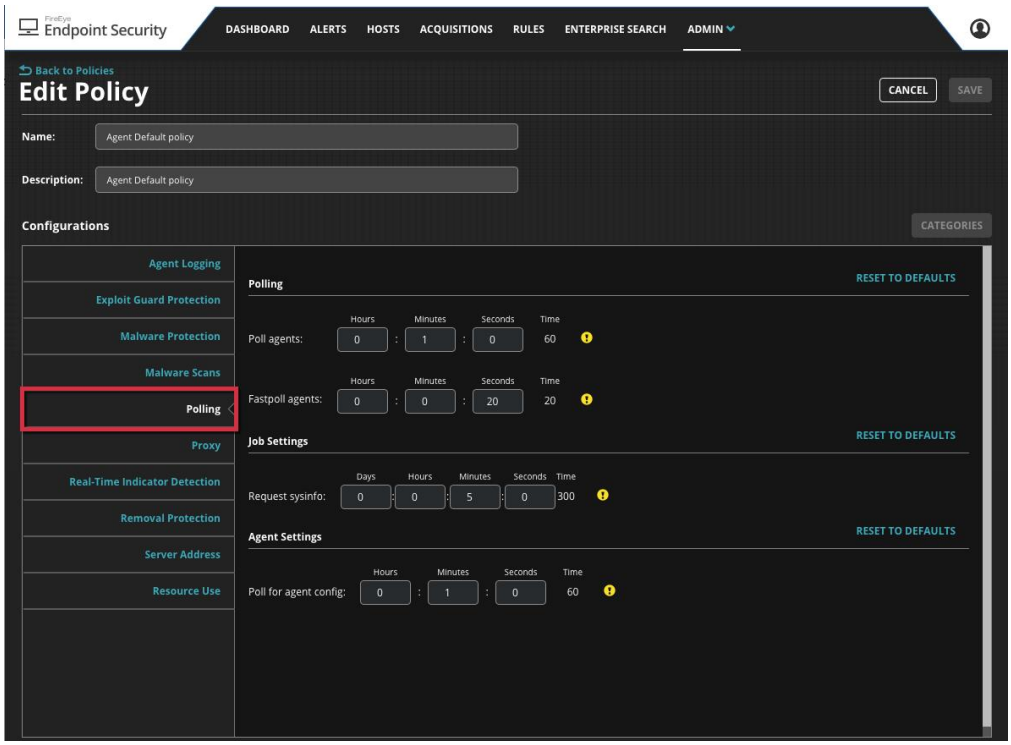
Prerequisites

- Admin access to the Web UI

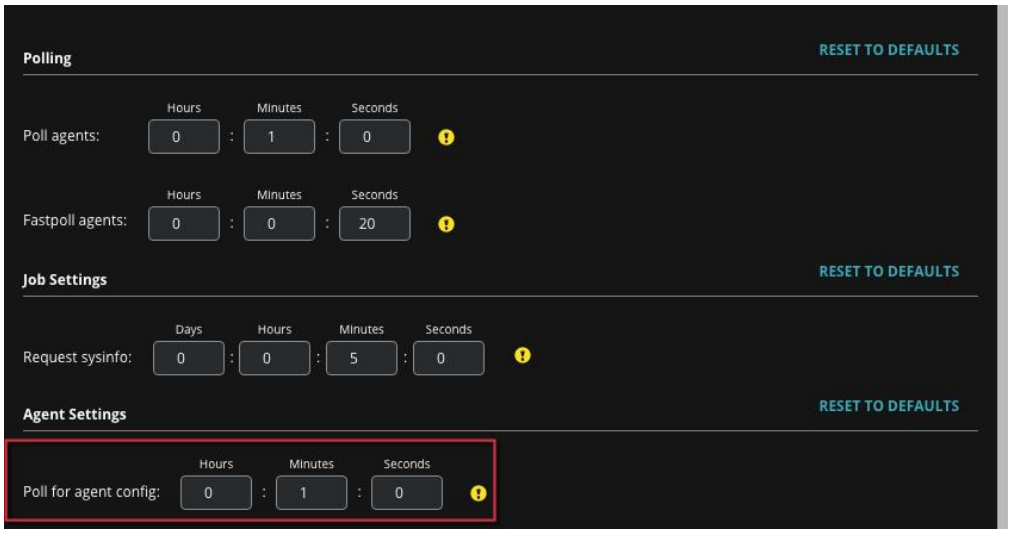
Configuring the Agent Configuration File Update Frequency for All Endpoints

To configure the agent configuration file update frequency for all host endpoints:

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. From the Policies table, click the **Agent Default Policy** link to go to the **Edit Policy** page.
4. Select the **Polling** tab.



5. In the **Poll for agent config:** fields, enter the agent configuration file request frequency **(hours, minutes, and seconds)**. Valid values range from 300 to 604800 seconds (five minutes to seven days). The default is 900 seconds (15 minutes).



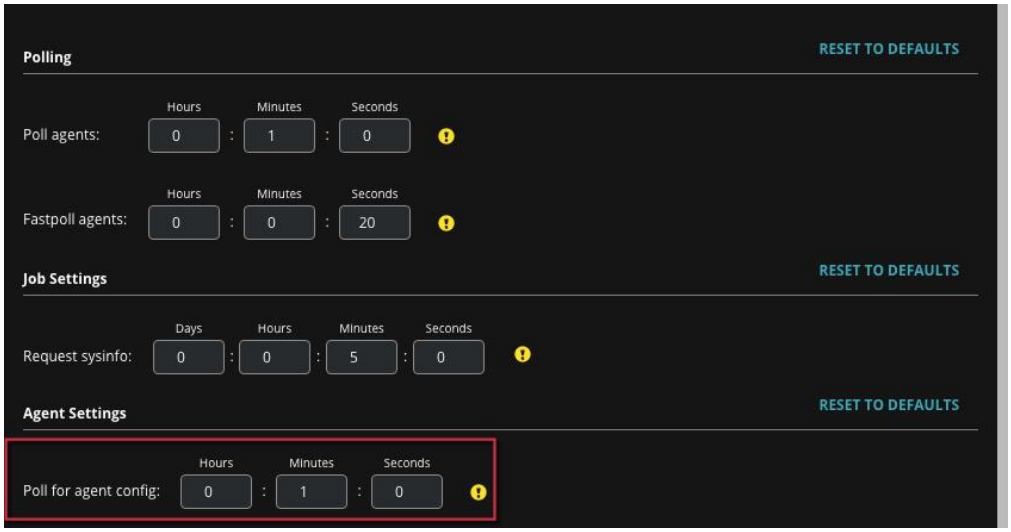
6. Click **Save**.

Click **Reset to defaults** to revert the poll interval to the default setting.

Configuring the Agent Configuration File Update Frequency for Selected Host Sets

To configure the agent configuration file update frequency for selected host sets:

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. In the Policies table, click the link for the custom policy you want to modify.
4. Select the **Polling** tab.
5. In the **Poll for agent config:** fields, enter the agent configuration file request frequency **(hours, minutes, and seconds)**. Valid values range from 300 to 604800 seconds (five minutes to seven days). The default is 900 seconds (15 minutes).



6. Click **Save**.

> **NOTE**: Click **Reset to defaults** to revert the poll interval to the default setting.

Now you can assign host sets to the custom policy and set the policy priority level. See "Assigning Host Sets to Agent Policies" and "Configuring Policy Priority Using the Web UI" in the *Endpoint Security Agent Administration Guide* for more information.

Configuring the System Information Request

The Endpoint Security server requests host system information (sysinfo) whenever it sends information to an agent. The **Request sysinfo every** value sets the maximum time before

the server requests host information from the agent. When this maximum time is reached, the server adds a job request that the agent receives during the next standard poll session. The sysinfo value can affect your system performance. For guidelines on setting this value, see System Information Frequency Setting on page 127.

Valid values for this frequency range from 300 seconds (5 minutes) to 604800 seconds (7 days). The sysinfo frequency distributed with the Endpoint Security software is 14400 seconds (4 hours).

Processing for a system information request stops after a configurable timeout period. You can configure the system information request timeout period using the CLI only. Valid values range from 0 to 31536000 seconds (1 year). The default timeout period is 43200 seconds (12 hours).

This section covers how to use the Web UI to configure the system information request settings. See the *Endpoint Security REST API Guide* for information on using the API to configure the system information request settings.

- Configuring the System Information Request Frequency for All Endpoints
- Configuring the System Information Request Frequency for a Custom Policy on the facing page
- Configuring the System Information Task-Timeout Period on page 118

Prerequisites

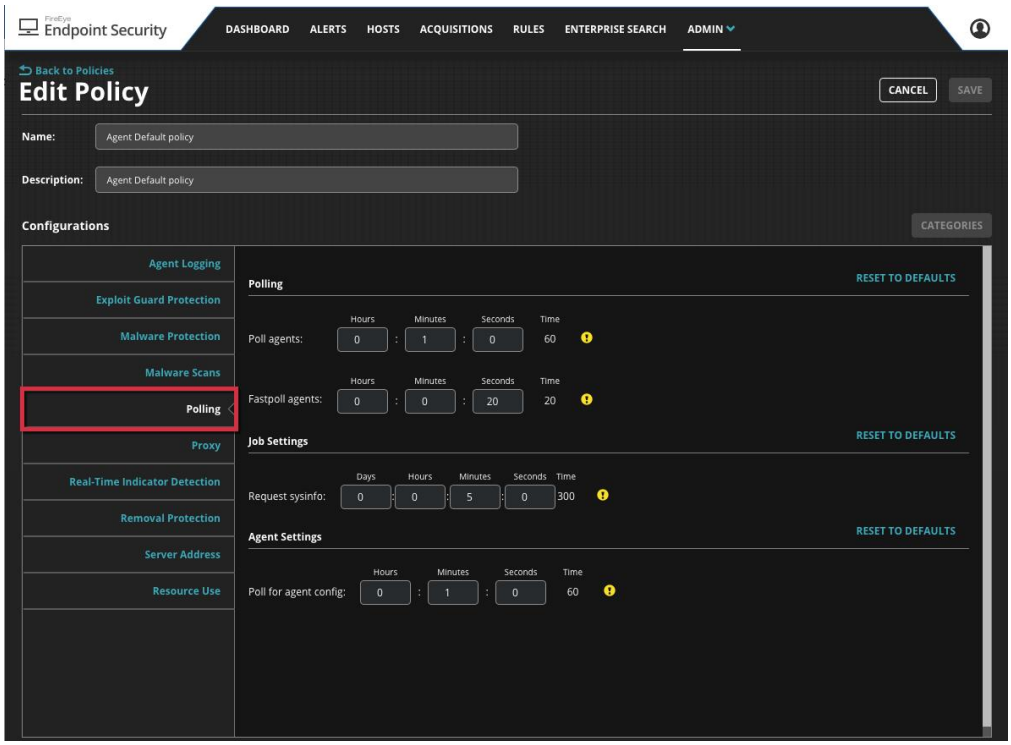
- Admin access to the Web UI

Configuring the System Information Request Frequency for All Endpoints

This section describes how to modify the Agent Default Policy to configure the system information request frequency for all host sets.

To configure the system information request frequency for all host endpoints:

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. From the Policies table, click the **Agent Default Policy** link to go to the **Edit Policy** page.
4. Select the **Polling** tab.



5. In the **Request sysinfo every:** fields, enter the system information request frequency **(hours, minutes, and seconds)**. Valid values range from 300 to 604800 seconds (five minutes to seven days). The default is 14400 seconds (four hours).
6. Click **Save**.

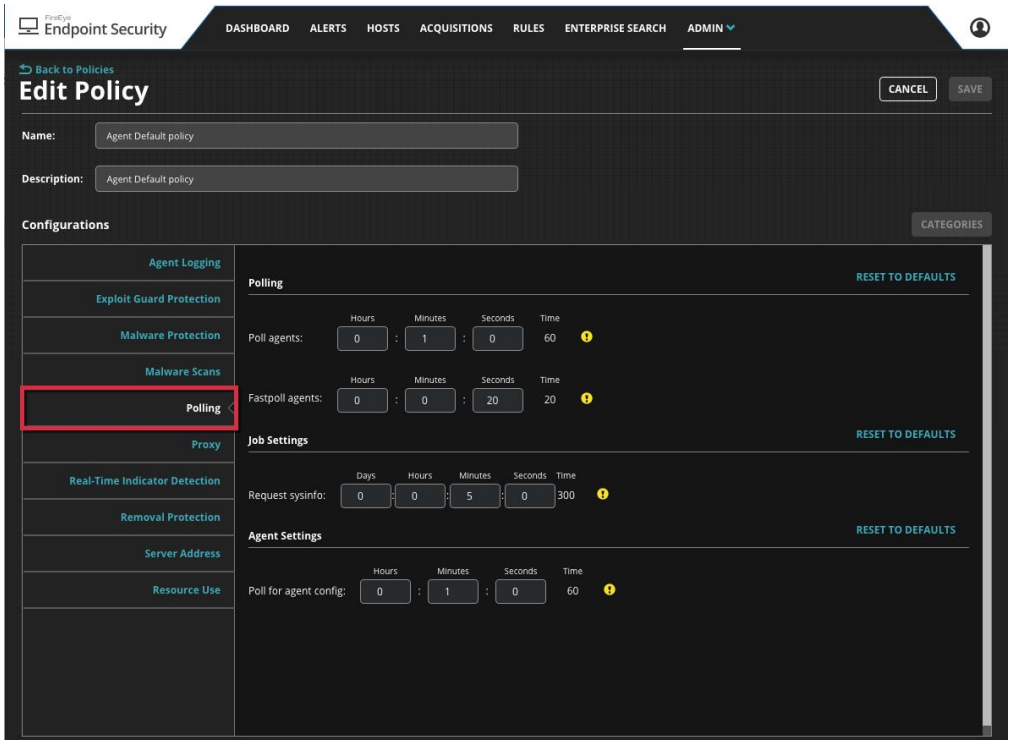
Click **Reset to defaults** to revert the request interval to the default setting.

Configuring the System Information Request Frequency for a Custom Policy

To configure the system information request frequency for selected host sets:

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. In the Policies table, click the link for the custom policy you want to modify.

4. Select the **Polling** tab.



5. In the **Request sysinfo:** fields, enter the system information request frequency **(hours, minutes, and seconds)**. Valid values range from 300 to 604800 seconds (five minutes to seven days). The default is 14400 seconds (four hours).
6. Click **Save**.

> **NOTE:** Click **Reset to defaults** to revert the request interval to the default setting.

Now you can assign host sets to the custom policy and set the policy priority level. See "Assigning Host Sets to Agent Policies" and "Configuring Policy Priority Using the Web UI" in the *Endpoint Security Agent Administration Guide* for more information.

Configuring the System Information Task-Timeout Period

To configure the system information request timeout period using the CLI:

1. Enable the CLI configuration mode:

```
hostname > enable
hostname (config) # configure terminal
```

2. Enter the number of seconds for the new system information request timeout period. Valid values range from 0 to 31536000 seconds (1 year). The default timeout period is 43200 seconds (12 hours).

```
hostname (config) # hx server sysinfo task-timeout <seconds>
```

To restore the default system information timeout period of 43200 seconds (12 hours):

```
hostname (config) # no hx server sysinfo task-timeout <seconds>
```

3. Verify updated sysinfo settings:

```
hostname (config) # show hx server general
```

4. Save your settings:

```
hostname (config) # write mem
```

Configuring the Malware Protection Indicator Download Channel

Malware protection indicators are used by the Endpoint Security malware protection engine during malware detection scans. Malware definitions, which include malware protection indicators, are transferred through the channel you select.

The **Malware Protection indicator download channel** drop-down allows you to select which channel you want to use to download the latest malware definitions, which include malware protection indicators, to the Endpoint Security Agent. The table below lists the available channels. The Internet is the default channel.

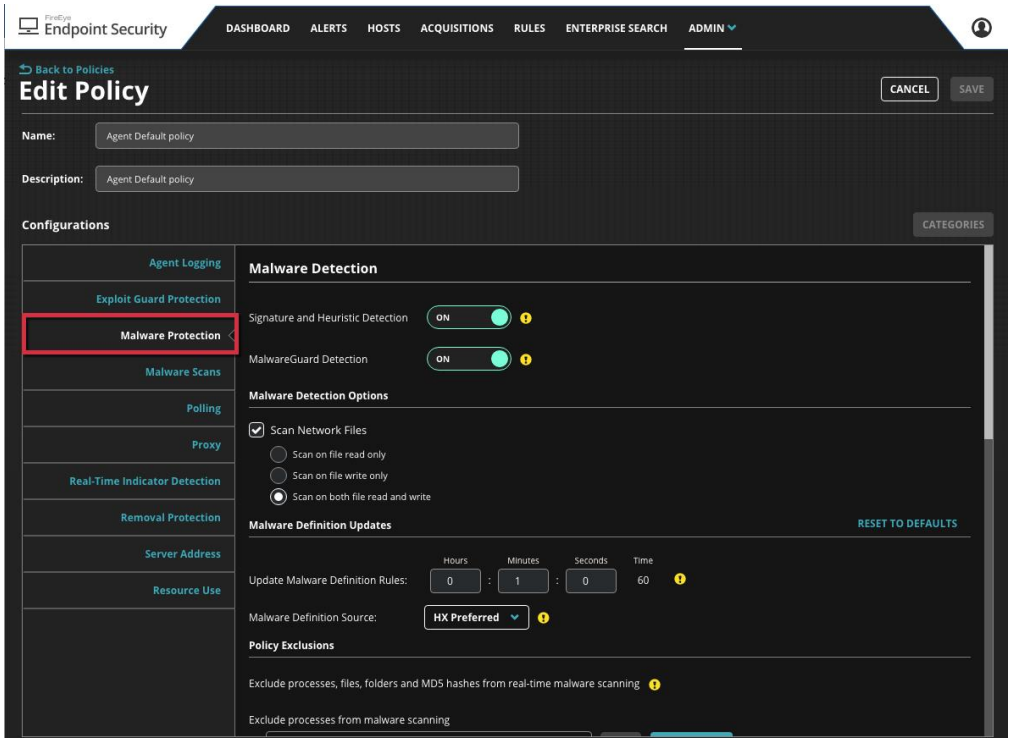
Indicator Source	Description
Internet	Malware protection indicator updates are downloaded directly from the Internet.
HX-Preferred	Malware protection indicator updates are downloaded from the Endpoint Security server. If the Endpoint Security server is unavailable, malware protection indicator updates are downloaded from the Internet.
HX-Only	Malware protection indicator updates are downloaded from the Endpoint Security server only.

When you first enable malware protection, the latest malware definitions are downloaded to your agents. By default, this initial download can take up to four hours to complete. Malware protection will not start until these definitions have been downloaded. To verify that the data has downloaded successfully, review the Host Details tab in the Endpoint Security Web UI for a Windows host. Verify the values in the Content Version and Last Updated fields under Malware Protection on the tab. For more information, see the *Endpoint Security Server User Guide*.

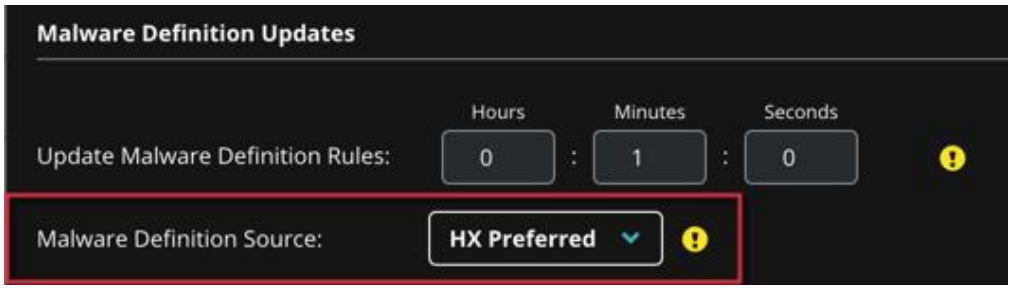
Configuring the Malware Protection Indicator Download Channel

To configure the download channel for malware protection indicators for all host endpoints:

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select Policies to access the **Policies** page.
3. In the Policies table, click the **Agent Default Policy** link to access the **Edit Policy** page.
4. Select the **Malware Protection** tab.



5. In the Malware Detection section, verify that the **Signature and Heuristic Detection** ON/OFF switch is set to **ON**.
6. In the **Malware Definition Updates** section, click the **Malware Definition Source** drop-down and select which connection channel the agent should use to receive the latest malware protection indicators. Valid options include Internet (default), HX only, and HX Preferred.

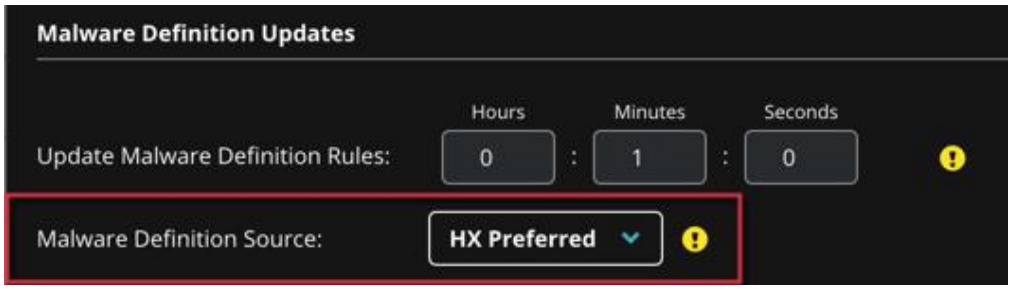


7. Click **Save**.

To set the update interval for the malware protection indicators for selected host sets:

See "Creating a Custom Policy" in the *Endpoint Security Agent Administration Guide* for more information about using the Web UI to create a custom policy.

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select Policies to access the **Policies** page.
3. In the Policies table, click the link for the custom policy you want to modify.
4. Select the **Malware Protection** tab.
5. In the **Malware Definition Updates** section, click the **Malware Definition Source** drop-down and select which connection channel the agent should use to receive the latest malware protection indicators. Valid options include Internet (default), HX only, and HX Preferred.



6. Click **Save**.

After you save, click **Reset to defaults** to revert the **Malware Definition Source** and the **Update Malware Definition Rules** settings to the default settings.

Now you can assign host sets to the custom policy and set the policy priority level. See "Assigning Host Sets to Agent Policies" and "Configuring Policy Priority Using the Web UI" in the *Endpoint Security Agent Administration Guide* for more information.

Configuring the Update Interval for Malware Protection Indicators

Using the Endpoint Security Web UI or the API, you can specify the interval, in seconds, at which the latest malware definitions that include malware protection indicators should be retrieved and downloaded to the agents on all of your host endpoints or select host sets in your environment.

NOTE: Malware definition rule updates are available for Windows agents version 24 or later only.

When Endpoint Security Agent starts an update, it picks a random interval for the content download between 0 and the configured polling interval, which by default is 14400 seconds (4 hours). If the download does not succeed or the content is corrupt, Endpoint Security Agent attempts the download again using another random interval. Once the download succeeds, the update process stops until the next update interval.

IMPORTANT: When you first enable malware protection, the latest malware definitions are downloaded to your agents. By default, this initial download can take up to four hours to complete. Malware protection will not start until these definitions have been downloaded. To verify that the data has downloaded successfully, review the Host Details tab in the Endpoint Security Web UI for a Windows host. Verify the values in the Content Version and Last Updated fields under Malware Protection on the tab. For more information, see the *Endpoint Security Server User Guide*.

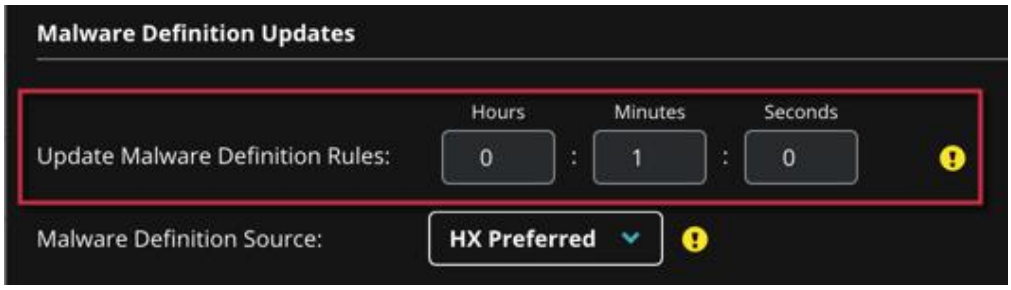
This section describes how to configure the update interval for all of your host endpoints and for selected host sets in your environment using the Web UI. See the *Endpoint Security REST API Guide* for information on using the API to define the update interval for malware protection indicators.

Configuring the Update Interval for All Host Endpoints

To set the update interval for the malware protection indicators for all host endpoints:

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select Policies to access the **Policies** page.
3. In the Policies table, click the Agent Default Policy link to access the **Edit Policy** page.

4. Select the **Malware Protection** tab.
5. In the **Malware Definition Updates** section, enter the malware protection indicators update frequency in the **Update Malware Definition Rules** fields. Valid values range from 1800 to 86400 seconds (30 minutes to one day). The default is 14400 seconds (four hours).



6. Click **Save**.

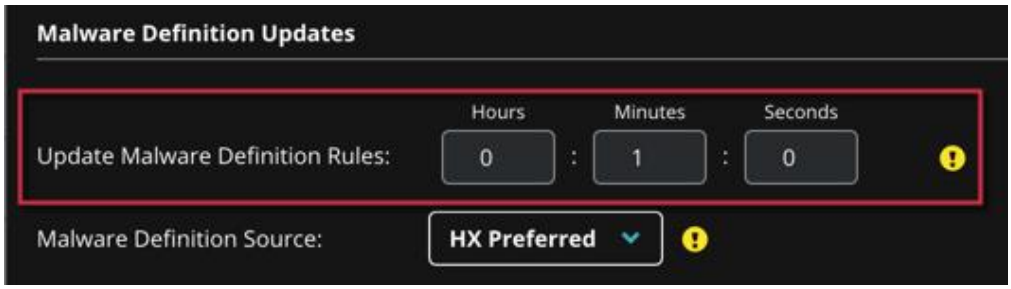
After you save, click **Reset to defaults** to revert the **Malware Definition Source** and the **Update Malware Definition Rules** settings to the default settings.

Configuring the Update Interval for Selected Host Sets

To set the update interval for the malware protection indicators for selected host sets:

NOTE: See "Creating a Custom Policy: in the *Endpoint Security Agent Administration Guide* for more information about using the Web UI to create a custom policy.

1. Log in to the Web UI as an administrator.
2. From the **Admin** menu, select Policies to access the **Policies** page.
3. In the Policies table, click the link for the custom policy you want to modify.
4. Select the **Malware Protection** tab.
5. In the **Malware Definition Updates** section, enter the malware protection indicators update frequency in the **Update Malware Definition Rules** fields. Valid values range from 1800 to 86400 seconds (30 minutes to one day). The default is 14400 seconds (four hours).



6. Click **Save**.

NOTE: After you save, click **Reset to defaults** to revert the **Malware Definition Source** and the **Update Malware Definition Rules** settings to the default settings.

CHAPTER 14: Performance Considerations

This section describes performance considerations for deploying and managing Endpoint Security Agents in your environment.

CPU Limiting

Every endpoint population is unique. Trellix recommends that you test CPU limiting values on machines representative of your production environment and workloads before you deploy the limit to all agents throughout your enterprise. Finding the right balance between CPU limits, system performance, and agent performance requires tuning, and preferences vary by customer.

At minimum, Trellix Endpoint Security Agent version 35.30.0 requires a computer with a Pentium-class processor. In addition, Trellix Endpoint Security Agent version 11.8 and later require that the processor support Intel SIMD (Single Instruction, Multiple Data) processor supplementary instruction set SSE2.

If you are using Endpoint Security Agent version 20 or later, CPU limits can be set for the entire agent population or a subset of the population. Limits can be set using Web UI, using the API, or in the agent configuration file.

IMPORTANT: CPU limiting only impacts main agent processes and the acquisition process. It does not apply to real-time event monitoring, the AV engine, or MalwareGuard engine detection processes as this would increase the risk of missed detections.

NOTE: The imposed CPU limit is measured as an average over a period of a few seconds. Actual CPU usage may rise above the limit for a short time.

IMPORTANT: A physical processor can simultaneously run a limited number of threads. Trellix recommends setting a CPU limit greater than the quotient of 1/# of threads. For example, for an Intel i5 processor, which can run 4 threads at a time, set the CPU limit to 25% (1/4) or higher. If you set the CPU limit below this guideline, the Full Disk and Full Memory data acquisitions may not have enough resources to complete.

In addition to testing before enterprise-wide deployment, the following information about how the agent's CPU limiting feature works may help you determine what values to set and the expected behavior.

Operating System Differences in CPU Limiting

The behavior of CPU limiting depends on the version of Windows you are running. This is due to differences in the underlying operating system.

In Windows 8 and later environments, the CPU limit set on the Endpoint Security server applies to the main agent processes and the acquisition process. This limit is enforced across two measures of CPU use:

- Cumulative user time of all agent processes
- Combined user and kernel time for an individual audit process

In Windows 7 and earlier environments, the CPU limit set on the Endpoint Security server is applied per agent process. The combined user and kernel CPU use per process is limited. The combined CPU use of all agent processes may exceed the CPU limit.

NOTE: macOS and Linux environments do not support CPU limiting.

Effect of CPU Limiting on Agent Performance

There is an inherent trade-off between the CPU limit set for an agent and the amount of time it takes the agent to perform tasks such as data acquisitions, Enterprise Searches, and triages. In most cases, a lower CPU limit setting will increase the expected time for the agent to complete tasks.

Agent Full Poll Interval Setting

Generally, sites with fewer agents can set the agent full poll interval lower than sites with many agents. However, performance issues can occur if the full poll interval is set too low. If agent performance seems slow in your environment, consider increasing the full poll interval.

The full poll interval distributed with the Endpoint Security Agent software is 600 seconds (10 minutes).

You can set the full poll interval using the Web UI or the API. See Configuring the Full Poll Interval on page 106.

System Information Frequency Setting

Generally, sites with fewer agents can set the sysinfo frequency lower than sites with many agents. However, performance issues can occur if the sysinfo frequency is set too low. If Endpoint Security server performance seems slow in your environment, consider increasing the sysinfo frequency.

The frequency initially distributed with the Endpoint Security software is 14,400 seconds (4 hours).

If your organization has upgraded from early versions of the agent, check this frequency setting. Early versions of the agent software were distributed with this frequency set to 30 minutes. The distributed setting was changed with Endpoint Security version 2.6.

You can set the sysinfo frequency using the Web UI. See Configuring the System Information Request on page 115.

Optimizing Event Storage Disk I/O

If your host endpoints experience a degradation in I/O processing times, use the `storage_mode` setting in the agent configuration file to optimize event storage I/O handling and reduce the physical disk I/O use.

NOTE: The storage_mode setting is only available for agents running Endpoint Security Agent version 21.33.7 or later.

In Endpoint Security version 26 or later, databases operate more reliably and allow for automatic recovery whenever possible.

Changing storage mode may lead to the loss of historical data. Complete all incident response investigations on your host endpoint before changing the storage mode.

The table below describes the available storage modes.

Storage Mode	Description	Configuration
Conventional	This is the *default* storage mode. This storage mode stores write events in batches before writing them to the events database on disk. **IMPORTANT:** Use one of the other storage modes only if your endpoints experience a degradation in I/O processing times.	To select the default storage mode, remove the `storage_mode` key from the configuration file.

Storage Mode	Description	Configuration
Memory-mapped I/O with log	This is the recommended memory-mapped storage mode. In this storage mode, read and write operations are backed by memory and backed by an on-disk journal file. Write transactions are written to the Write Ahead Log file (`events.db-wal`) then committed to the events database. The journal file prevents database corruption caused by unexpected restarts. This mode produces efficient disk I/O performance because read transactions are in memory. Memory-mapped I/O with log mode improves disk I/O performance for two reasons. • Event processing does not need to transition to kernel mode to read and write data. • Event data is stored in memory as much as possible and is written to the events database only when necessary. Before changing to this storage mode in your production environment, you should first determine the impact of the change in a test environment.	To select this storage mode, set the storage_mode key to `mmapiowithlog`.

Storage Mode	Description	Configuration
In-memory	This storage mode stores the events database in memory. This mode increases memory usage, but improves disk I/O performance. Consider the following caveats before switching to in-memory storage mode. • The in-memory events database is volatile. Events in the in-memory database are lost when the agent restarts or when event processing is restarted. Consequently, in-memory mode is best used for machines that remain running for long periods (such as servers). • Any previous events database on disk remains untouched and unmodified. Events stored in it are not transferred to the in-memory database. If you switch back to the default storage mode, your agent resumes updating the events database on disk and the events in the in-memory database are lost.	To select this storage mode, set the `storage_mode` key to `inmemory`.
Memory-mapped I/O NOT RECOMMENDED	Use of this storage mode is not recommended because it may cause failure of Real-time Event storage and functionality. Please use MMAPIOWITHLOG. This storage mode uses memory mappings to back up read and write operations, and uses paging to optimize the read and write operations.	To select this storage mode, set the `storage_mode` key to `mmapio`.

For information on making agent configuration file changes, see "Modifying Agent Configuration Settings" in the *Endpoint Security Agent Administration Guide*.

Performance Log Messages

Messages are logged that provide performance statistics for the agent. These messages include a performance area and statistic title for each value. This section describes the performance statistics found in the log messages.

Performance Area	Statistic Title	Description
CPU	Average Usage	The average CPU used by processes running in kernel mode and in user mode. The CPU average does not take into account the number of processors in the system. To obtain an accurate value, divide the average shown in the log message by the number of logical processors in the system. The times that each thread of the process ran in kernel or user mode is determined and totaled for each mode. These times can exceed the amount of real time elapsed if the process executes across multiple CPU cores. After these total times are calculated, the average CPU use is calculated for kernel mode and user mode. The difference between the current and previous kernel or user mode time is divided by elapsed time. This value is shown in the log message.
	Total Usage	The number of seconds the agent ran in kernel mode and in user mode since the process started. The total time since the process started is given in parentheses.

Performance Area	Statistic Title	Description
IO	The counters in this section include all operations performed by all processes that have ever been associated with the job object. See Microsoft's IO_COUNTERS structure.	
	BytesPerSec	The number of bytes per second read and written. These values represent the average over the number of seconds shown in parentheses in the message.
	Process IOPS	The number of read and write operations performed. These values represent the average over the number of seconds shown in parentheses in the message.
	Process TotalBytes	The total number of bytes read and written. The total time since the process started is given in parentheses.
KERN	The statistics in this section relate to Microsoft's PERFORMANCE_INFORMATION structure.	
	HandleCount	The current number of open handles.
	Nonpaged	The memory currently in the nonpaged kernel pool, in pages.
	Paged	The memory currently in the paged kernel pool, in pages.
	ProcessCount	The current number of processes.
	ThreadCount	The current number of threads.
	Total	The sum of the memory currently in the paged and nonpaged kernel pools, in pages.

Performance Area	Statistic Title	Description
PROC	The statistics in this section relate to Microsoft's PROCESS_MEMORY_COUNTERS_EX structure.	
	PageFaultCount	The number of page faults.
	PagefileUsage	The commit charge value, in bytes, for this process. Commit charge is the total amount of memory that the memory manager has committed for a running process.
	PeakPagefileUsage	The peak value, in bytes, of the commit charge during the lifetime of this process.
	PeakWorkingSetSize	The peak working set size, in bytes.
	Pool Usage: NonPaged	The current nonpaged pool usage, in bytes.
	Pool Usage: PeakNonPaged	The peak nonpaged pool usage, in bytes.
	Pool Usage: PeakPaged	The peak paged pool usage, in bytes.
	Pool Usage: QuotaPaged	The current paged pool usage, in bytes.
	WorkingSetSize	The current working set size, in bytes.

Performance Area	Statistic Title	Description
SYS	The statistics in this section relate to Microsoft's PERFORMANCE_INFORMATION structure.	
	CommitLimit	The current maximum number of pages that can be committed by the system without extending the paging files.
	CommitPeak	The maximum number of pages that were simultaneously in a committed state since the last system reboot.
	CommitTotal	The number of pages currently committed by the system.
	PageSize	The size of a page, in bytes.
	PhysicalTotal	The amount of actual physical memory, in pages.
	SystemCache	The amount of system cache memory, in pages. This is the size of the standby list plus the system working set.

CHAPTER 15: Troubleshooting Endpoint Security Agent Issues

This section describes troubleshooting steps you should follow to resolve issues installing or using Endpoint Security Agent version 22 or later.

Proxy Server Configuration Errors

Direct HTTPS proxy support for Internet access is supported in Endpoint Security Agent version 25 or later. If your enterprise uses an HTTPS proxy server to allow endpoints on your network to access the Endpoint Security server or the Internet, a proxy server configured incorrectly will cause the Endpoint Security Agent installation process to fail.

Follow the troubleshooting steps below, if the installation of Endpoint Security Agent version 25 or later fails after one minute.

To correct the system proxy server settings:

1. Open a command line prompt on the host endpoint currently running Endpoint Security Agent version 25 or later as an administrator.
2. Enter the registry export command below:

   ```
   reg export “HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections” current.txt
   ```

3. Enter the command below to open the `current.txt` file in notepad:

   ```
   current.txt
   ```

4. Replace the contents of line 3 with the text below:

   ```
    [HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections]
   ```

5. Save the file and exit notepad.
6. Enter the registry import command below:

   ```
   reg import current.txt
   ```

7. Start the installation again either from the command line or from Endpoint Security Server.

Collecting Agent Diagnostic Information

If you experience problems with Endpoint Security on your host endpoint, collect diagnostic information to help troubleshoot the problem. This section describes the types of data you should collect.

Export a Copy of Your Log File

Exporting a copy of your log file might help you diagnose the problem. To export a copy of the host log file, enter the following command on the command line:

```
xagt --log-export <filename>
```

The log file is exported using the specified file name from the agent database and decrypted.

Export a Copy of Your Configuration File

Exporting a copy of your configuration file might help you diagnose the problem. To export a copy of the host configuration file, enter the following command on the command line:

```
xagt --cfg-export <filename>
```

The configuration file is exported using the specified file name and decrypted.

Acquire Agent Diagnostics Data from the Endpoint Security Server

If you decide to contact FireEye Technical Support with your problem, you should acquire agent diagnostics data from the Endpoint Security server. This report will help your FireEye technician help you diagnose problems.

To acquire agent diagnostics data from the Endpoint Security server:

1. Log in to the Web UI as an administrator.
2. Select **Hosts** at the top of the Web UI to access the Hosts page.
3. Select the **All Hosts** tab and locate the host for which you want diagnostics.
4. Select the checkbox to the left of the host line.
5. In the Actions menu above the host list, select **Acquire: Agent Diagnostics** to request the agent diagnostics.

6. Select **Acquisitions** at the top of the Web UI.
7. Locate and select your acquisition on the Acquisitions page. Details about the acquisition appear in the Acquisition Detail pane.
8. When the acquisition status has changed to **Acquired**, click **Download** in the Acquisition Detail pane. The acquisition `.zip` file is downloaded to your computer.

PART V: Appendix

APPENDIX 15: macOS Agent JAMF Deployment

You can use an enterprise-wide software deployment tool to install the Endpoint Security Agent software on your macOS endpoints. This section describes how to use JAMF Suite to capture and create a deployment package for Endpoint Security Agent version 22 or later and deploy the package to your macOS endpoints.

The instructions provided in this section are sample instructions only, written using JAMF versions 9.91 and 9.97. The deployment steps you use may vary depending on the version of JAMF you use and your macOS endpoint environment.

JAMF deployments set the INSTALLSERVICE installation option to 2. When INSTALLSERVICE is set to 2 in macOS environments, host endpoint containment notifications do not work until the endpoint user logs off and logs in again.

To correctly use JAMF to install the Endpoint Security Agent software on your macOS endpoints, do not install the agent on the reference machine directly. Instead, extract the contents of the agent installation `.dmg` file and use JAMF to push the files to your endpoints. Next, run a script that installs the agent files on the macOS endpoints. For more information about using JAMF to deploy and install the Endpoint Security Agent software on your macOS endpoints, see this community article.

Prerequisites

- A JAMF Nation customer account that is linked to your organization.
- A compatible version of JAMF Nation's JAMF Suite for your macOS endpoint environment.
- A dedicated macOS, with a compatible version of JAMF Suite installed, to use for JAMF deployments.

Perform the following steps to deploy agent software to your macOS hosts using JAMF.

Task	Instructions
1. Prepare a JAMF build system to use for software deployment.	See Preparing the JAMF Build System below.
2. Create a JAMF package from the Endpoint Agent macOS installation image.	See Capturing and Installing the Endpoint Security Agent JAMF Package on page 142.
3. Deploy the JAMF package to your macOS endpoint hosts using a JAMF policy.	See Deploying the OS X Agent JAMF Package on page 146.

Preparing the JAMF Build System

A JAMF build system is required in order to use JAMF to deploy the Endpoint SecurityAgent software to your macOS endpoints. This section describes how to prepare your JAMF build system by using your JAMF Nation account to access, download, and install the JAMF Suite .

Prepare your JAMF build system by performing the following steps:

- Obtain a version of the JAMF Suite software that is compatible with your macOS production environment.
- Install the JAMF Suite software on an macOS system or macOS virtual machine that you plan to use for software deployment.

  IMPORTANT: The JAMF Suite software must be installed on a "vanilla" macOS system or macOS virtual machine, a system or machine in its original state that has not received any customized configurations or software updates. The macOS system you select should be used for JAMF deployments only.

- Download the Endpoint Security Agent version 23.10.0 or above from Trellix's Dynamic Threat Intelligence (DTI) offline portal.

NOTE: Only Endpoint Security Agent versions 23.10.0 and above can run on macOS platforms. See System Requirements on page 11 for a full list of supported macOS versions.

Downloading and Installing the JAMF Suite

To obtain the JAMF Suite version, you must have an account on JAMF Nation that is linked to your organization. Contact JAMF Nation at https://www.jamf.com/contact for assistance setting up a JAMF Nation account.

To download and install the JAMF Suite on your macOS system:

1. From the macOS system or macOS virtual machine that you plan to use for software deployment, log in to your JAMF Nation account.
2. From the **Profile** drop-down menu, click **My Assets**.
3. Identify and download the JAMF Suite software version that is compatible with your macOS production environment.

   NOTE: This procedure was tested against JAMF Suite software versions 9.91 and 9.97. You can access additional versions of the JAMF Suite software by clicking **Show Previous Releases** under the **JAMF Suite Download** link.

4. Install the JAMF Suite software. See JAMF Nation's Product Documentation for JAMF Suite installation instructions.

   IMPORTANT: The JAMF Suite software must be installed on a "vanilla" macOS system or macOS virtual machine, a system or machine in its original state that has not received any customized configurations or software updates. The macOS system you select should be used for JAMF deployments only.

Retrieving the Agent Installation Software and Uploading it to the Endpoint Security Server

You can manually retrieve the Endpoint Security Agent `.dmg` (macOS) file directly from Trellix DTI. The section describes how to obtain the Endpoint Security Agent installation package for Trellix's DTI cloud and upload it to your Endpoint Security Server.

Before using JAMF to capture and deploy the Trellix Endpoint Security Agent installation package to your macOS endpoints, you must upload the Endpoint Security Agent software package to your Endpoint Security Server to ensure the installation package obtains the agent configuration file and certificates required to provision your Endpoint Security Server with the agent.

To obtain and upload an agent installation package from the DTI cloud:.

1. Using the SSH protocol, log in to the Endpoint Security Server using the management interface's IP address or hostname.

   ```
   $ ssh <username>@<ipAddress>
   ```

   Or

   ```
   $ ssh <username>@<ipAddress> | <hostname>
   ```

2. Enter the password at the prompt.
3. Enable CLI configuration mode for your Endpoint Security Server:

   ```
   hostname > enable
   hostname # configure terminal
   ```

4. Check whether any new agent images are available on the DTI:

   ```
   hostname (config) # fenet hx-agent image check
   ```

   Alternatively, you can use the following command to refresh the agent metadata available on the DTI.

   ```
   hostname (config) # fenet hx-agent metadata refresh
   ```

5. List all agent images available on the DTI, fetched from the DTI, or available on the local server:

   ```
   hostname (config) # show fenet hx-agent image available
   ```

   This command lists supported operating systems, Trellix Endpoint Security Agent versions, and the content IDs associated with each agent image available.

6. Retrieve the .dmg (macOS) agent image from the DTI:

   ```
   hostname (config) # fenet hx-agent image fetch content-id <content-id>
   ```

   where <content-id> is the content ID associated with the Trellix Endpoint Security Agent image you want to retrieve.

   You can also simply retrieve the latest agent image from the DTI with the following command:

   ```
   hostname (config) # fenet hx-agent image fetch latest
   ```

7. Verify and upload the agent image to the Endpoint Security Server:

   ```
   hostname (config) # fenet hx-agent image apply content-id <content-id>
   ```

   where <content-id> is the ID associated with the Trellix Endpoint Security Agent image you want to upload.

If you retrieved the latest agent image in Step 4, you can upload it to the Endpoint Security Server using the following command:

```
hostname (config) # fenet hx-agent image apply latest
```

Export the Agent Installation Software Image

After uploading the Endpoint Security Agent software to your Endpoint Security Server, you need to download the installation package to the macOS system or macOS virtual machine you are using for the JAMF deployment.

1. Log in to the Web UI from the macOS system or macOS virtual machine with the installed JAMF software.
2. From the **Admin** menu, select **Agent Versions**.
3. Locate the Endpoint Security Agent installation `.dmg` image file you uploaded to the Endpoint Security Server in Retrieving the Agent Installation Software and Uploading it to the Endpoint Security Server on page 140and click the **DOWNLOAD AGENT INSTALLER** button to download the file to a location on your macOS system.

Capturing and Installing the Endpoint Security Agent JAMF Package

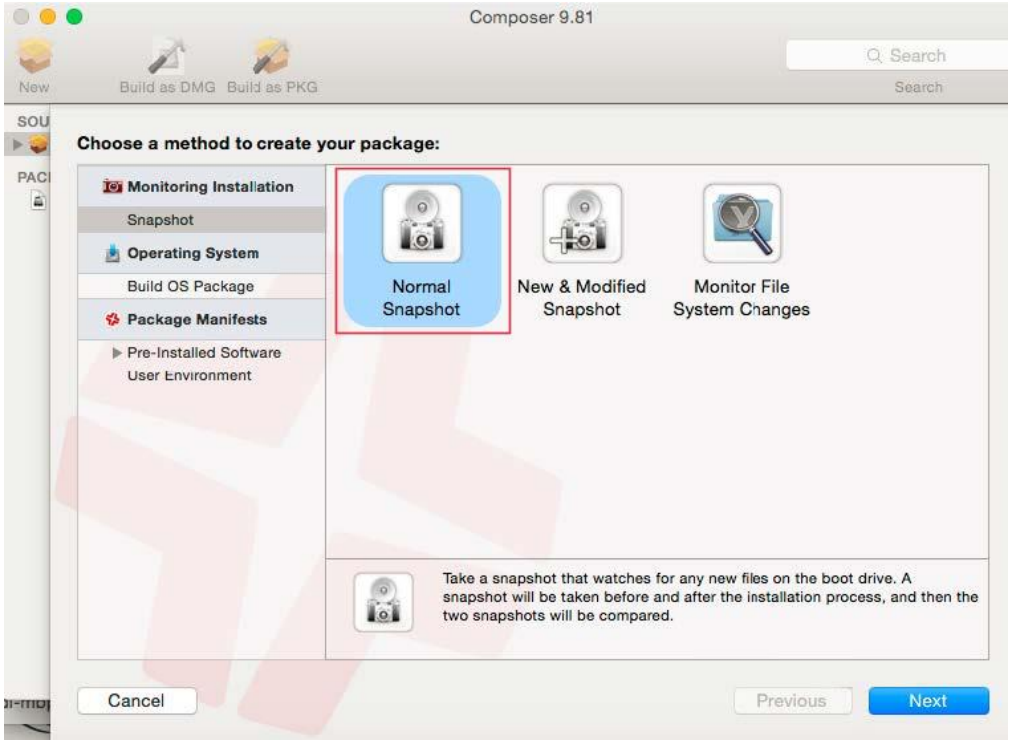
You must create an agent package before you can deploy the macOS agent to your macOS endpoints using JAMF. This section describes how to capture, create, and install the macOS agent installation package using JAMF.

Creating the Source Package

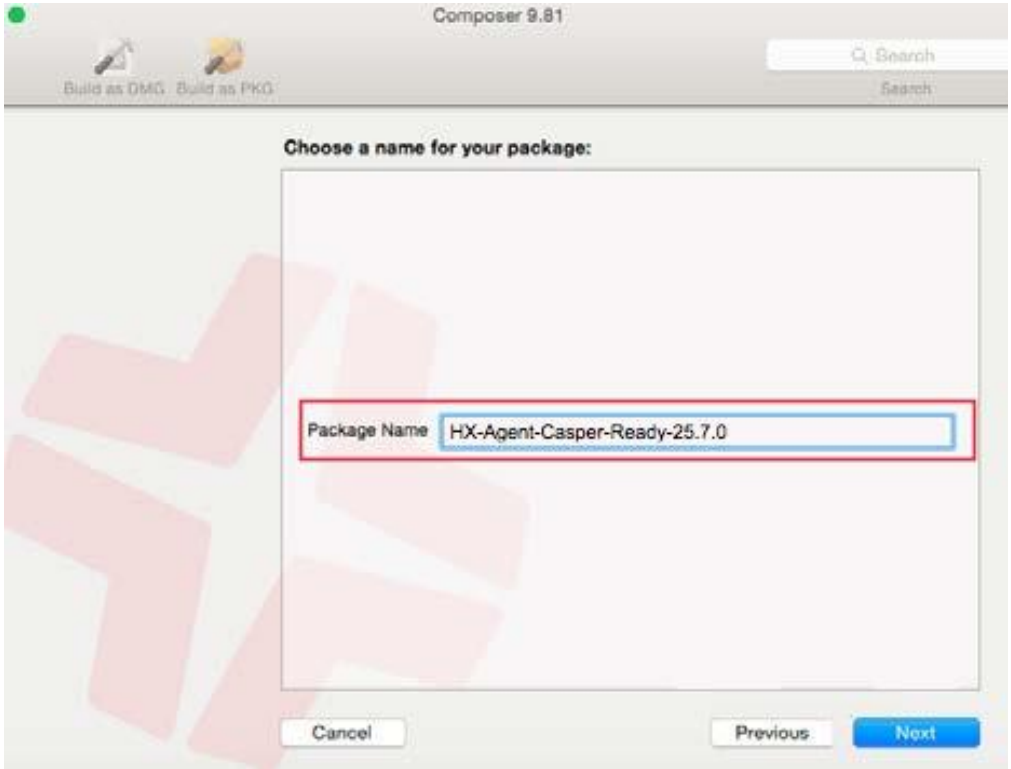
JAMF Composer allows you to create software packages to meet your deployment requirements. This section describes how to create the source package for your Endpoint Security Agent software deployment using JAMF Composer.

To create an agent package in JAMF:

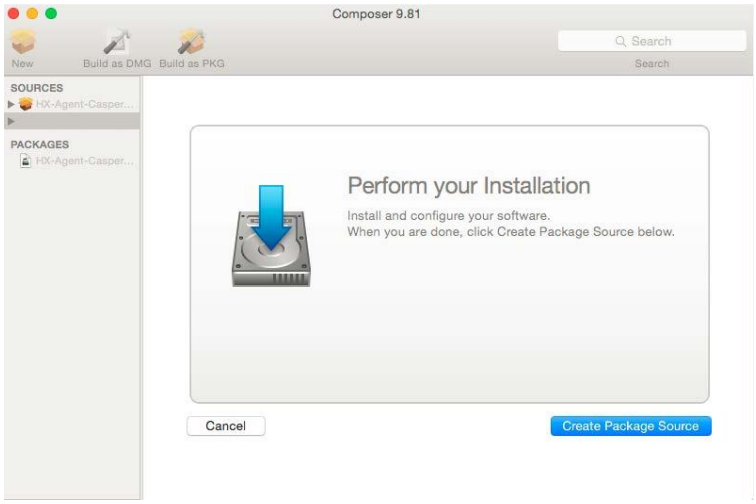
1. Launch the **JAMF Composer** and click **New**.
2. Click **Normal Snapshot** to capture a snapshot of your system before and after the installation. Click **Next**.



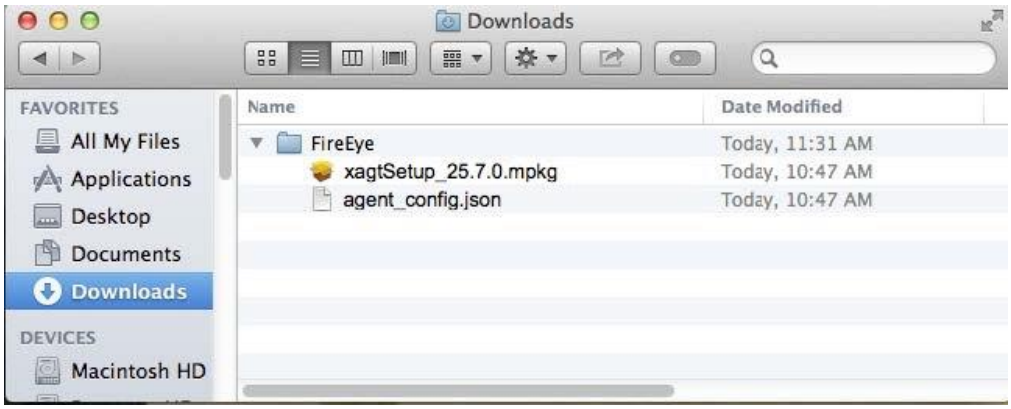
3. Enter a name in the **Package Name** field for the agent package you are capturing. The example below shows `Agent-25.7.0` in the **Package Name** field.



4. Click Next. The system creates a snapshot of your system before any further processing occurs. When the snapshot is complete, the following screen appears:



5. Open the agent installation file by double-clicking the `.dmg` file you downloaded.
6. Create a temporary folder and copy the contents of the `.dmg` file in to the folder. In the example below, the `.dmg` file contents were copied to a `FireEye` folder that resides in the `Downloads` directory.



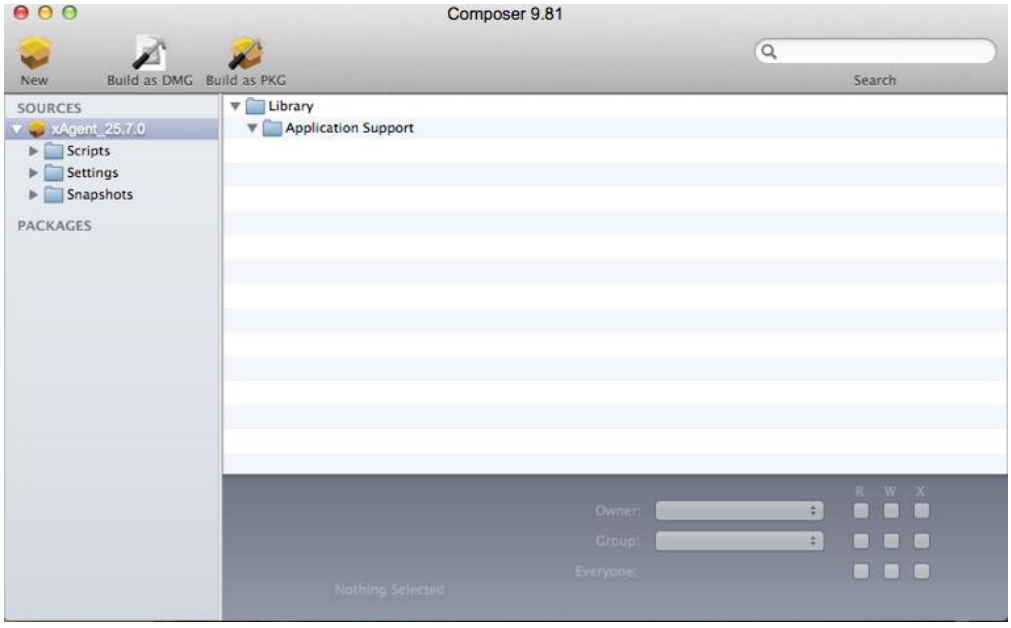
7. Click the **Create Package Source** button in Composer and select the **xAgent package source name** in the left pane.

Creating New Directories for File Copying

You need to create new directories and copy the xAgent source package in to your new directory.

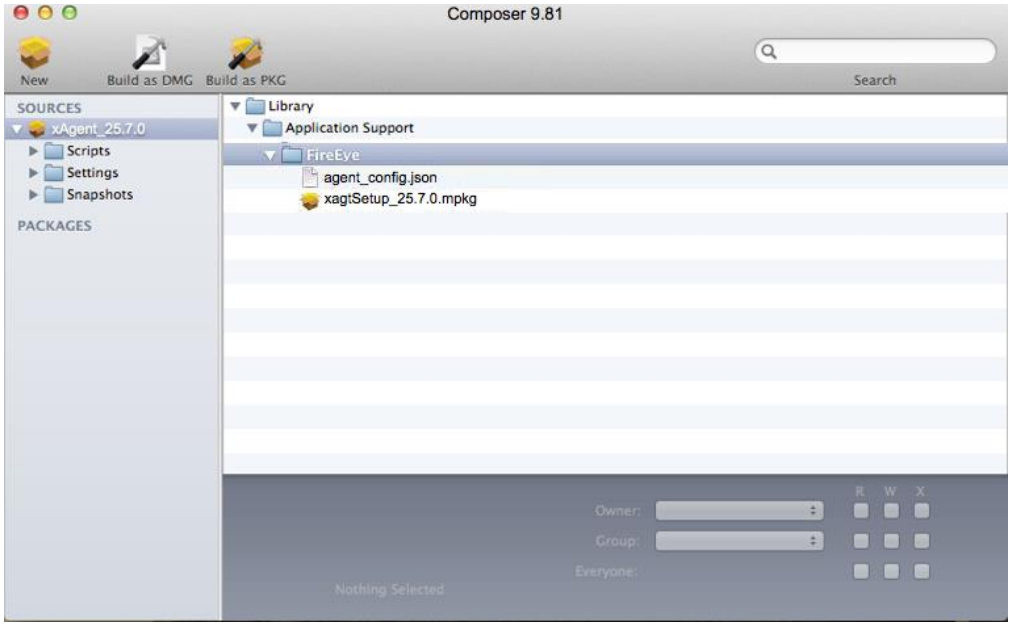
To create the source directories and copy the source package:

1. In the right pane, delete any directories or files.
2. Create a new directory called `Library` and create a new directory under `Library` called `Application Support`.



3. Right-click in the right pane and select **Create New Directories** from the drop-down menu.

4. In the Finder, copy the entire folder that you created in Creating the Source Package on page 142 to the `Application Support` directory in Composer. The screen will look similar to this:



Building the Package for Deployment

The .pkg file you create in this section will be used to deploy the Endpoint Security Agent software to all of your macOS endpoints enrolled in JAMF.

To create the build package:

1. Click the **Build as PKG** button at the top of the Composer screen.
2. Save the .pkg file to a location on your Endpoint Security server system.

Deploying the OS X Agent JAMF Package

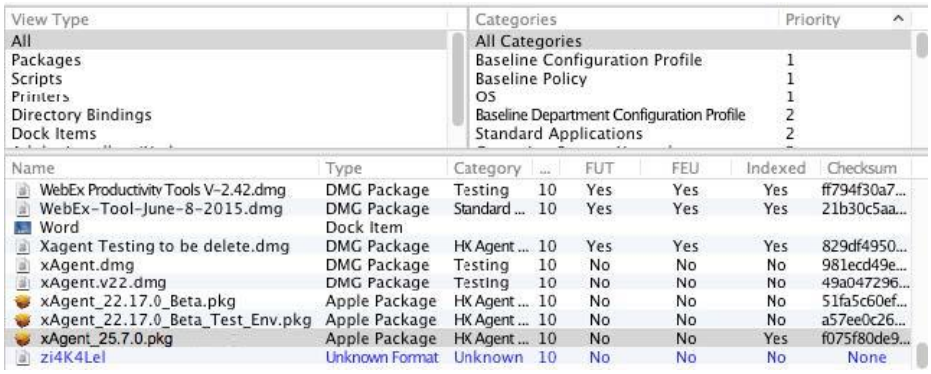
After you create the JAMF package for the Endpoint Security software, you can deploy it to any OS X endpoints that have been enrolled in JAMF. Deploying the agent software involves setting up a policy in JAMF. This section describes how to set up this policy, create a script to start agent services on your endpoints, add the script to the deployment policy, and deploy the agent software to specific systems.

Setting up a JAMF Deployment Policy

JAMF deployment policies allow you to identify the OS X endpoints and host groups that should receive the policy and associate the agent JAMF package with a JAMF script and use the script to run the software on the assigned endpoints.

To set up the policy and deploy the agent software to your Endpoint Security server host endpoints:

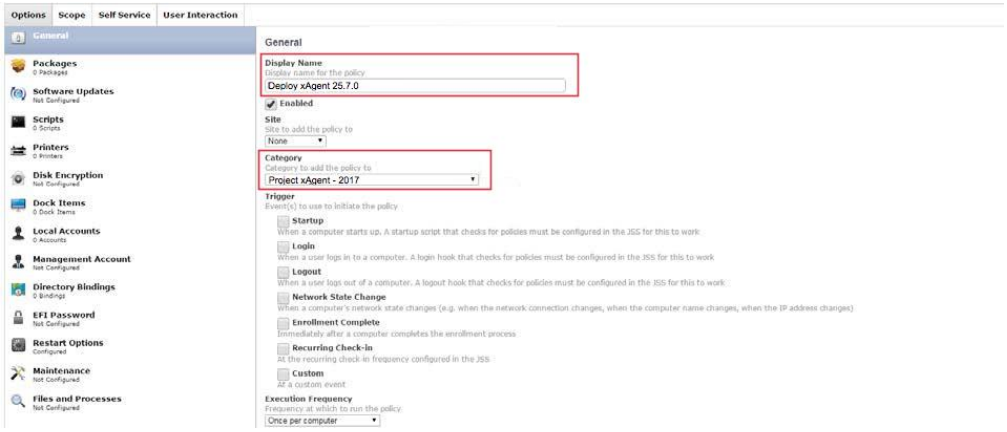
1. Open **JAMF Admin**.
2. Using JAMF Admin, upload the `.pkg` file you created and saved in Building the Package for Deployment on the previous page by completing the following steps:
   a. Drag and drop the `.pkg` file into JAMF Admin.
   b. Assign the package to a category.
   c. Select **File > Save** to save the file in your JAMF environment.



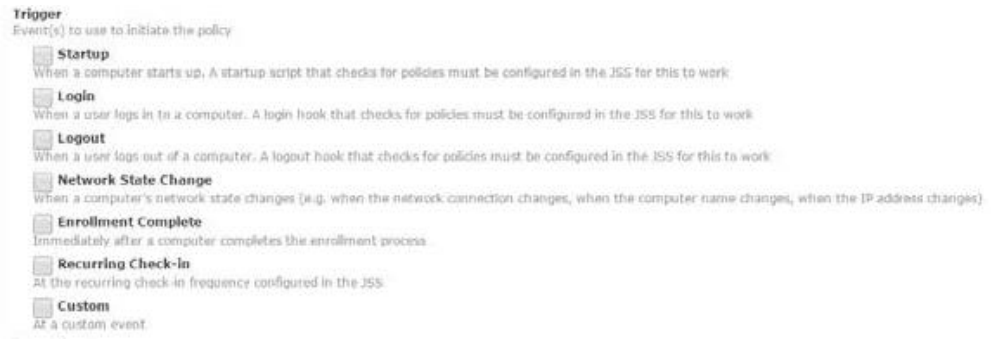
3. Log in to the **JAMF Web Console** and click on **Computers** and then **Policies**.
4. Click **New** to create a policy to push the package to your Endpoint Security server host endpoints that are managed by JAMF.

5. From the **Options** tab, select **General** and enter an appropriate display name in the Display Name field.

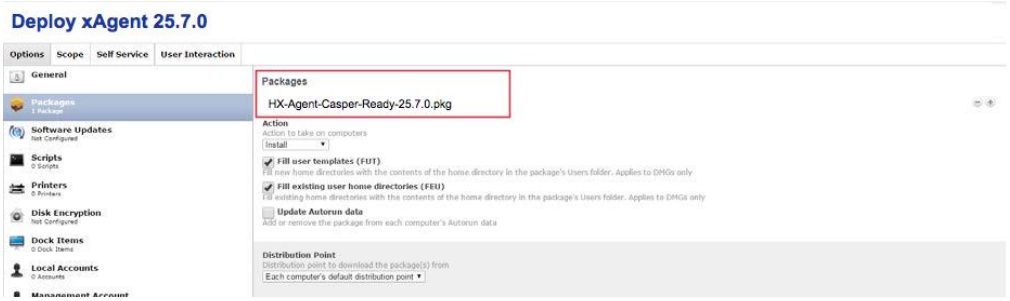
6. From the **Category Field** drop-down menu, select a JAMF category to add to the policy.



7. Under the **Trigger** section, select the trigger options that are required for your environment and deployment plan. For example, the agent software package is made available in Self Service later in these steps, so no trigger options are set in the screen below.



8. From the **Options** tab, select **Packages** and add the package you uploaded in step 2 in the **Packages** pane on the right side of the screen.



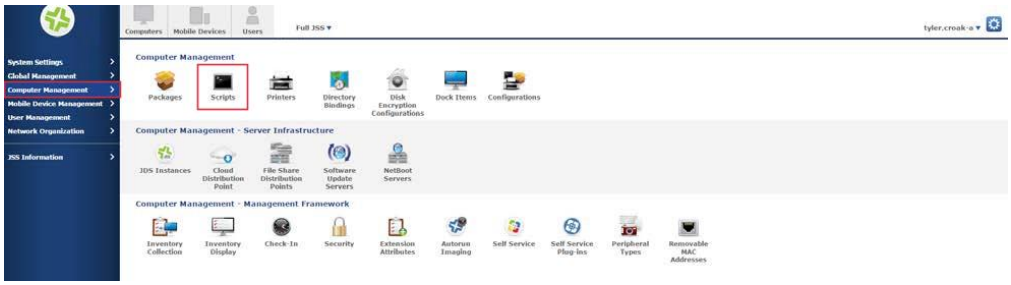
9. Select the **Self Service** tab and select **Make the policy available in Self Service**.

10. Click **Save**.

Creating a Script to Start xAgent Services

After deploying the Endpoint Security software package to your OS X endpoints, you need to start the agent services on your Endpoint Security server endpoints. The JAMF Web Console allows you to create a script that will install the agent software package after the policy deploys the package to an endpoint and start agent services.

1. In the JAMF Web Console, click the **Gear button** (settings).
2. Click the **Computer Management** tab in the left pane and click the **Scripts** icon in the right pane



3. Create and name the new script. For example, the Display Name for the script shown below is *Start xAgent Service*.

4. Select the **Script** tab and add the code below. Be sure to replace `xagtSetup_27.x.x.mpkg` with the actual name of your .mpkg file. For example, `xagtSetup_27.3.0.mpkg`).

```
#!/bin/sh

DIR1="/Library/Application Support/FireEye/"
FILE1="xagtSetup_27.x.x.mpkg"
FILE2="agent_config.json"
installer -pkg "$DIR1$FILE1" -target /
sleep 30
rm "$DIR1$FILE1"
rm "$DIR1$FILE2"
```

5. Click **Save**.

Adding the Script to the Deployment Policy

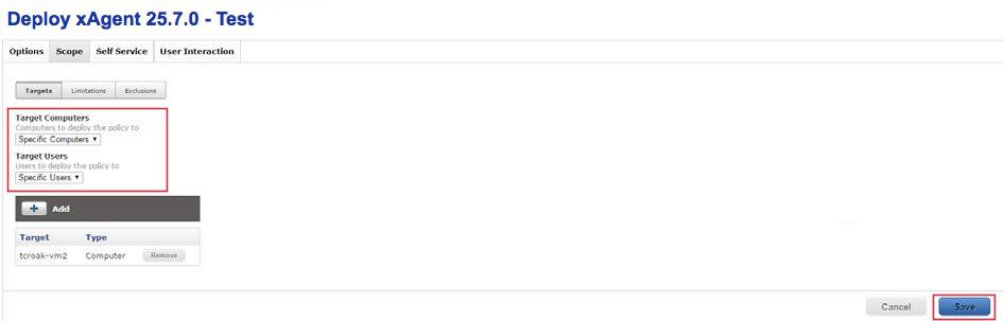
This section describes how to add the script you created in Creating a Script to Start xAgent Services on the previous page to the deployment policy you created in Setting up a JAMF Deployment Policy on page 147

To add the script to your deployment policy:

1. Locate the policy you created in Setting up a JAMF Deployment Policy on page 147 step 4 and click **Edit**.
2. From the **Options** tab, select **Scripts** and add the script you created in Creating a Script to Start xAgent Services on the previous page step 3 in the **Scripts** pane.

3. Select the **Scope** tab and click **Targets**.

   From the **Target Computer**s drop-down menu, add the OS X endpoints that you want to apply the policy to in **Self Service**. I



4. From the **Target Users** drop-down menu, add the users or user groups that you want to apply the policy to in **Self Service**.
5. Click **Add** and **Save** to deploy the Endpoint Security software to your assigned endpoints and user groups.

Installing the Agent Software on OS X Endpoints

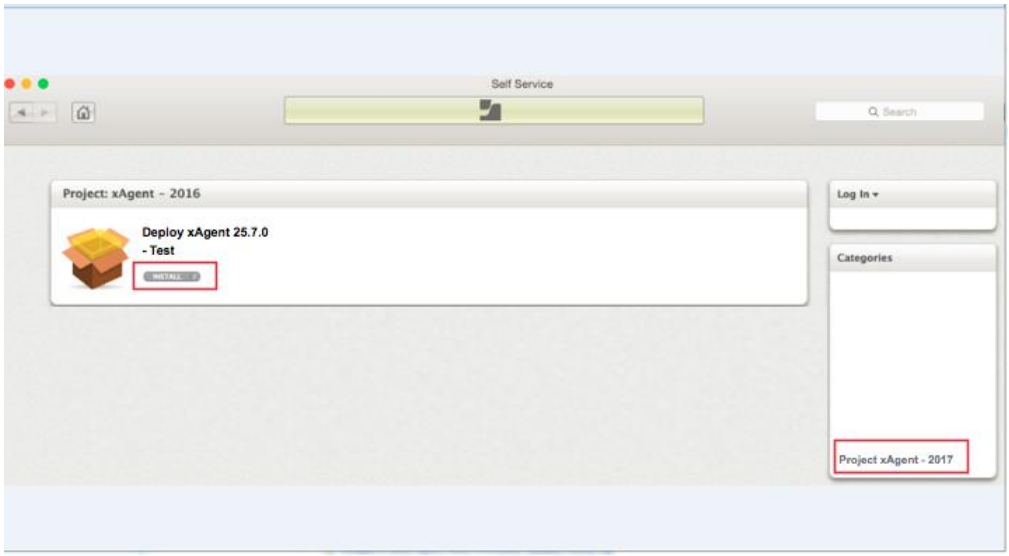
Users with endpoints assigned the deployment policy can now install the Endpoint Security software and start agent services using the JAMF's Self Service tool.

To completely automate the Endpoint Security software installation on the endpoint, set a trigger option for "Recurring Check-In" and remove the "Make Available in Self Service" condition from the deployment policy.

To install Endpoint Security software on your endpoint:

1. Log into a host endpoint that has the deployment policy assigned.
2. Launch **JAMF's Self Service** tool.

3. Go to the JAMF category where the policy is located and click **Install**.



The agent software is now installed on that OS X endpoint.

Technical Support

For technical support, contact Trellix through the Support portal:

https://www.trellix.com/en-us/support.html

Documentation

Documentation for all Trellix products is available on the Trellix Documentation Portals (login required):

https://docs.fireeye.com/

https://docs.mcafee.com/

Trellix | 601 McCarthy Blvd. | Milpitas, CA | 1.408.321.6300 | 1.877.347.3393 | www.trellix.com