Secure Endpoint Deployment Strategy

Last Updated: February 2, 2024

Cisco Systems, Inc.   www.cisco.com

Table of Contents

CHAPTER 1
PLANNING

This document will guide you through best practices to deploy Secure Endpoint for the first time. Following this strategy will increase your chances of a successful Secure Endpoint deployment and evaluation.

Before deployment you should gather as much information as possible about the environment to reduce post-install troubleshooting. To have an effective roll out of the connector for Windows, you must first identify your environment. To do that you must answer the following questions:

- How many computers is the connector for Windows being installed on?
- Which operating systems are the computers running?
- What are the hardware specifications for the computers?
- Do the operating systems and specifications meet the minimum requirements for the connector for Windows?
- Which applications are installed on the computers?
- Which custom applications or not widely deployed applications are installed on the computers?
- Do the computers connect to the Internet through a proxy?
- Will the connector be deployed on any Windows servers?
- What tool is being used to push software out to the endpoints?
- What security products (AV, HIDS, etc.) are installed on the computers?
- Do you want your users to see the connector user interface, desktop icon, program group and/or right-click menu?

Once you identify the environment you're working with then you can apply your first best practice of identifying candidates for an Alpha release. The best way to choose your candidates for Alpha is to choose a combination of three computers per operating system, three computers per custom application, three computers per proxy server, one computer per security product, and one computer per department. Your

Alpha release should probably contain a cross-section of approximately 100 computers.

System requirements and supported operating systems

Secure Endpoint Windows Connector

The following are the minimum system requirements for the Secure Endpoint Windows connector. The Secure Endpoint Windows connector supports both 32-bit and 64-bit versions of these operating systems on x86 processors. Additional disk space may be required when enabling certain connector features.

Desktop

- 1 GHz or faster processor
- 1 GB RAM
- 650 MB available hard disk space - Cloud-only mode
- 1 GB available hard disk space - TETRA

Server

- 2 GHz or faster processor
- 2 GB RAM
- 650 MB available hard disk space - Cloud only mode
- 1 GB available hard disk space - TETRA

See this article for operating system compatibility.

Incompatible software and configurations

The Secure Endpoint Windows connector is currently not compatible with the following software:

- ZoneAlarm by Check Point
- Carbon Black
- Res Software AppGuard

The connector does not currently support the following proxy configurations:

- Websense NTLM credential caching. The currently supported workaround for Secure Endpoint is either to disable NTLM credential caching in Websense or allow the connector to bypass proxy authentication through the use of authentication exceptions.
- HTTPS content inspection. The currently supported workaround is either to disable HTTPS content inspection or set up exclusions for the connector.
- Kerberos / GSSAPI authentication. The currently supported workaround is to use either Basic or NTLM authentication.

Secure Endpoint Mac connector

The following are the minimum system requirements for the Secure Endpoint Mac connector. The Secure Endpoint Mac connector only supports 64-bit Macs.

- 2 GB RAM
- 2 GB available hard disk space

See this article for operating system compatibility.

Incompatible Software and Configurations

The Secure Endpoint Mac connector does not currently support the following proxy configurations:

- Websense NTLM credential caching: The currently supported workaround for Secure Endpoint is either to disable NTLM credential caching in Websense or allow the connector to bypass proxy authentication through the use of authentication exceptions.
- HTTPS content inspection: The currently supported workaround is either to disable HTTPS content inspection or set up exclusions for the connector.
- Kerberos / GSSAPI authentication: The currently supported workaround is to use either Basic or NTLM authentication.

Secure Endpoint Linux connector

The following are the minimum system requirements for the Secure Endpoint Linux connector. The Secure Endpoint Linux connector only supports x64 architectures.

When using Linux-only ClamAV definitions:

- 2 GB of available RAM
- 2 GB available hard disk space in /opt. The connector will install and maintain temporary files in /opt/cisco/amp/.

When using full ClamAV definitions:

- 4 GB of available RAM
- 2 GB available hard disk space in /opt. The connector will install and maintain temporary files in /opt/cisco/amp/.

See this article for operating system compatibility. See this article for Ubuntu system requirements.

IMPORTANT! The Secure Endpoint Linux connector may not install properly on custom kernels. If you have a custom kernel, contact Support before attempting to install.

Incompatible software and configurations

The Secure Endpoint Linux connector is currently not compatible with the following software:

- F-Secure Linux Security
- Kaspersky Endpoint Security
- McAfee VSE for Linux
- McAfee Endpoint Security for Linux
- Sophos Server Security 9
- Symantec Endpoint Protection
- Trend Micro Deep Security Agent

The Secure Endpoint Linux connector may cause unmount failures with removable media or temporary file systems mounted in non-standard locations in Centos, Oracle Linux, and Red Hat Enterprise Linux versions 6.x. In accordance with the File System Hierarchy Standard, removable media such as USB storage, DVDs, and CD-ROMs should be mounted to `/media/` while temporarily mounted file systems such as NFS file system mounts should be mounted to `/mnt/`. Mounting removable media or temporary file systems to other directories can cause a conflict where unmount fails due to device busy. Upon encountering an unmount failure, the user must stop the cisco-amp service, retry the unmount operation, then restart cisco-amp.

```
sudo initctl stop cisco-amp
sudo umount {dir\device}
sudo initctl start cisco-amp
```

UEFI Secure Boot is supported starting with connector version 1.16.0 on operating systems running kernel versions 4.18 or later.

On systems with kernel version below 4.18, the Secure Endpoint Linux connector loads kernel modules which taints the kernel.To temporarily prevent the connector from influencing kernel taint, the Secure Endpoint service can be disabled, which prevents these kernel modules being loaded after the system restarts. This procedure should be used with caution, as disabling the Secure Endpoint service effectively disables Secure Endpoint protection on this system. To disable the Secure Endpoint service, run the commands:

```
sudo systemctl disable cisco-amp
sudo systemctl stop cisco-amp
```

A system restart is required to reload the kernel and reset the kernel taint value. To re-enable the Secure Endpoint service, run the commands:

```
sudo systemctl enable cisco-amp
sudo systemctl start cisco-amp
```

Secure Endpoint iOS

The following are the minimum system requirements for the Secure Endpoint iOS:

- The device must be running in supervised mode and managed using a Mobile Device Manager (MDM). See your MDM documentation for further requirements around device settings and configuration.
- 5 MB free space.

You will also have to set up MDM Integration in your Organization Settings between the Secure Endpoint Console and one of the following Mobile Device Managers:

- Meraki System Manager (SM) with API access enabled.
  - Only System Manager and Combined network types are supported.
- MobileIron Enterprise Mobility Management (EMM) On-Prem 9.4 or higher.
- AirWatch/Workspace ONE Mobility Management On-Prem and Cloud 9.2 or higher.

See this article for iOS version compatibility.

Gather information about endpoint security

Conflicts can arise when multiple security applications are running on a single computer. To prevent conflicts between applications you will need to create exclusions for Secure Endpoint in other security apps and exclude the security apps from Secure Endpoint

First, find out how many security applications are installed. Do different groups in the organization use different products? Find out the install, update, data, and quarantine path for each security product installed and make a note of it.

Next, decide on the install path for the connector (C:\Program Files\Sourcefire by default for versions up to 5.1.1 and C:\Program Files\Cisco\AMP for versions 5.1.1 and higher). You will need to exclude the connector directory from the other security applications, particularly antivirus products.

Create Secure Endpoint exclusions in other security products

You must create exclusions for the connector in antivirus products running on your endpoints to prevent conflicts. Consult your antivirus software documentation for instructions on excluding files, directories, and processes from being scanned.

See the Secure Endpoint Troubleshooting TechNotes for additional instructions on creating exclusions for the connector in various antivirus software.

Secure Endpoint Windows connector

Antivirus products must exclude the following directories and any files, directories, and executable files within them:

- `C:\Program Files\Cisco\AMP\`

IMPORTANT! This is the default install directory. If you have specified a custom install directory, that directory must be excluded.

For antivirus products that require a full path to the executable file for exclusions, you should exclude all binary files in the `C:\Program Files\Cisco\AMP\[connector version]\` directory.

For example:

- `C:\Program Files\Cisco\AMP\[connector version]\ConnectivityTool.exe`
- `C:\Program Files\Cisco\AMP\[connector version]\creport.exe`
- `C:\Program Files\Cisco\AMP\[connector version]\ipsupporttool.exe`
- `C:\Program Files\Cisco\AMP\[connector version]\iptray.exe`
- `C:\Program Files\Cisco\AMP\[connector version]\sfc.exe`
- `C:\Program Files\Cisco\AMP\[connector version]\uninstall.exe`
- `C:\Program Files\Cisco\AMP\[connector version]\updater.exe`

- `C:\Program Files\Cisco\AMP\clamav\[clam version]\freshclam.exe`
- `C:\Program Files\Cisco\AMP\clamav\[clam version]\freshclamwrap.exe`

Where `[connector version]` is in the most recently installed version number of the connector and `[clam version]` is the most recent version of the ClamAV engine.

It may also be necessary to exclude the connector UI log file:

- `C:\ProgramData\Cisco\AMP\IPTray.log`

Secure Endpoint Mac connector

Antivirus products must exclude the following directories and any files, directories, and executable files within them to be compatible with the Secure Endpoint Mac connector:

- `/Library/Application Support/Cisco/AMP for Endpoints Connector`
- `/opt/cisco/amp`

Secure Endpoint Linux connector

Antivirus products must exclude the following directories and any files, directories, and executable files within them to be compatible with the Secure Endpoint Linux connector:

- `/opt/cisco/amp`

If your antivirus product requires a full path to executable files, you should exclude all binary files in `/opt/cisco/amp/bin/` including:

- `/opt/cisco/amp/bin/ampdaemon`
- `/opt/cisco/amp/bin/ampupdater`
- `/opt/cisco/amp/bin/ampscansvc` (version 1.9.0 and later)
- `/opt/cisco/amp/bin/ampcli`
- `/opt/cisco/amp/bin/ampmon`
- `/opt/cisco/amp/bin/ampsupport`
- `/opt/cisco/amp/bin/ampsigncheck`

Gather information about custom apps

Custom applications can present a problem for initial deployment. Most widely-used applications have already been marked as clean files in the Secure Endpoint Cloud and tested with the connector. Custom applications are less likely to have this benefit, so extra precautions need to be taken with them. Find out if there are any custom or legacy applications running and the install path for each one and make a note of it. If only certain groups of users have the application installed, note which users they are. If the custom application has separate information stores, note the file path of those as well.

If possible, use a program like md5deep to calculate the SHA-256 value of the custom application’s executable files.

Gather information about proxy servers

If the computers in the organization use a proxy server to connect to the Internet you will need to gather some information about it including:

- Proxy host name
- Proxy port
- Type of proxy
- User name and password for authentication (if required)
- PAC file URL if they are used
- Whether the proxy server is used for DNS resolution
- If the proxy server will allow communications via TCP port 32137

Check firewall rules

To allow the connector to communicate with Cisco systems, the firewall must allow the clients to connect to certain servers over specific ports. There are three sets of servers depending on where you are located - one for the European Union, one for Asia Pacific, Japan, and Greater China, and one for the rest of the world.

IMPORTANT! If your firewall requires IP address exceptions see this Cisco TechNote.

Secure Endpoint Windows Firewall Exceptions

North America

Organizations located in North America must allow connectivity from the connector to the following servers over HTTPS (TCP 443):

- **Event Server** - intake.amp.cisco.com
- **Management Server** - mgmt.amp.cisco.com
- **Policy Server** - policy.amp.cisco.com
- **Error Reporting** - crash.amp.cisco.com
- **Endpoint IOC Downloads** - ioc.amp.cisco.com
- **Advanced Custom Signatures** - custom-signatures.amp.cisco.com
- **connector Upgrades** - upgrades.amp.cisco.com (TCP 80 and 443)
- **Remote File Fetch** - rff.amp.cisco.com

To allow the connector to communicate with Cisco cloud servers for file and network disposition lookups the firewall must allow the clients to connect to the following server over TCP 443:

- **Cloud Host** - cloud-ec.amp.cisco.com

For Secure Endpoint Windows version 5.0 and higher you will need to use the following Cloud Host address and enrollment server (both TCP 443) instead:

- **Cloud Host** - cloud-ec-asn.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.amp.cisco.com

If you have TETRA enabled on any of your connectors you must allow access to the following server over TCP 80 and 443 for signature updates:

- **Update Server** - tetra-defs.amp.cisco.com

To use Orbital on your Secure Endpoint connectors, you must allow access to the following servers over TCP 443:

- **Orbital Updates** - orbital.amp.cisco.com
- **Orbital Queries** - ncp.orbital.amp.cisco.com
- **Orbital Installer** - update.orbital.amp.cisco.com

European Union

Organizations located in the European Union must allow connectivity from the connector to the following servers over HTTPS (TCP 443):

- **Event Server** - intake.eu.amp.cisco.com
- **Management Server** - mgmt.eu.amp.cisco.com
- **Policy Server** - policy.eu.amp.cisco.com
- **Error Reporting** - crash.eu.amp.cisco.com
- **Endpoint IOC Downloads** - ioc.eu.amp.cisco.com
- **Advanced Custom Signatures** - custom-signatures.eu.amp.cisco.com
- **connector Upgrades** - upgrades.eu.amp.cisco.com (TCP 80 and 443)
- **Remote File Fetch** - rff.eu.amp.cisco.com

To allow the connector to communicate with Cisco cloud servers for file and network disposition lookups the firewall must allow the clients to connect to the following server over TCP 443 by default or TCP 32137:

- **Cloud Host** - cloud-ec.eu.amp.cisco.com

For Secure Endpoint Windows version 5.0 and higher, you will need to use the following Cloud Host address and enrollment server (both TCP 443) instead:

- **Cloud Host** - cloud-ec-asn.eu.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.eu.amp.cisco.com

If you have TETRA enabled on any of your connectors, you must allow access to the following server over TCP 80 and 443 for signature updates:

- **Update Server** - tetra-defs.eu.amp.cisco.com

To use Orbital on your Secure Endpoint connectors, you must allow access to the following servers over TCP 443:

- **Orbital Updates** - orbital.eu.amp.cisco.com
- **Orbital Queries** - ncp.orbital.eu.amp.cisco.com
- **Orbital Installer** - update.orbital.eu.amp.cisco.com

Asia Pacific, Japan, and Greater China

Organizations located in the Asia Pacific, Japan, and Greater China region must allow connectivity from the connector to the following servers over HTTPS (TCP 443):

- **Event Server** - intake.apjc.amp.cisco.com
- **Management Server** - mgmt.apjc.amp.cisco.com
- **Policy Server** - policy.apjc.amp.cisco.com
- **Error Reporting** - crash.apjc.amp.cisco.com

- **Endpoint IOC Downloads** - ioc.apjc.amp.cisco.com
- **Advanced Custom Signatures** - custom-signatures.apjc.amp.cisco.com
- **connector Upgrades** - upgrades.apjc.amp.cisco.com (TCP 80 and 443)
- **Remote File Fetch** - rff.apjc.amp.cisco.com

To allow the connector to communicate with Cisco cloud servers for file and network disposition lookups, the firewall must allow the clients to connect to the following server over TCP 443 by default or TCP 32137:

- **Cloud Host** - cloud-ec.apjc.amp.cisco.com

For Secure Endpoint Windows version 5.0 and higher, you will need to use the following Cloud Host address and enrollment server (both TCP 443) instead:

- **Cloud Host** - cloud-ec-asn.apjc.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.apjc.amp.cisco.com

If you have TETRA enabled on any of your connectors, you must allow access to the following server over TCP 80 and 443 for signature updates:

- **Update Server** - tetra-defs.apjc.amp.cisco.com

To use Orbital on your Secure Endpoint connectors, you must allow access to the following servers over TCP 443:

- **Orbital Updates** - orbital.apjc.amp.cisco.com
- **Orbital Queries** - ncp.orbital.apjc.amp.cisco.com
- **Orbital Installer** - update.orbital.apjc.amp.cisco.com

Secure Endpoint Mac Firewall Exceptions

North America

Organizations located in North America must allow connectivity from the connector to the following servers over HTTPS (TCP 443):

- **Event Server** - intake.amp.cisco.com
- **Management Server** - mgmt.amp.cisco.com
- **Policy Server** - policy.amp.cisco.com
- **Error Reporting** - crash.amp.cisco.com
- **connector Upgrades** - upgrades.amp.cisco.com (TCP 80 and 443)
- **Remote File Fetch** - rff.amp.cisco.com

To allow the connector to communicate with Cisco cloud servers for file and network disposition lookups, the firewall must allow the clients to connect to the following server over TCP 443 by default or TCP 32137:

- **Cloud Host** - cloud-ec.amp.cisco.com

For Secure Endpoint Mac version 1.2 and higher, you will need to use the following Cloud Host address and enrollment server (both TCP 443) instead:

- **Cloud Host** - cloud-ec-asn.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.amp.cisco.com

If you have ClamAV enabled on any of your Secure Endpoint Mac connectors you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - clam-defs.amp.cisco.com

European Union

Organizations located in the European Union must allow connectivity from the connector to the following servers over HTTPS (TCP 443):

- **Event Server** - intake.eu.amp.cisco.com
- **Management Server** - mgmt.eu.amp.cisco.com
- **Policy Server** - policy.eu.amp.cisco.com
- **Error Reporting** - crash.eu.amp.cisco.com
- **connector Upgrades** - upgrades.eu.amp.cisco.com (TCP 80 and 443)
- **Remote File Fetch** - rff.eu.amp.cisco.com

To allow the connector to communicate with Cisco cloud servers for file and network disposition lookups, the firewall must allow the clients to connect to the following server over TCP 443 by default or TCP 32137:

- **Cloud Host** - cloud-ec.eu.amp.cisco.com

For Secure Endpoint Mac version 1.2 and higher, you will need to use the following Cloud Host address and enrollment server (both TCP 443) instead:

- **Cloud Host** - cloud-ec-asn.eu.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.eu.amp.cisco.com

If you have ClamAV enabled on any of your Secure Endpoint Mac connectors, you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - clam-defs.eu.amp.cisco.com

Asia Pacific, Japan, and Greater China

Organizations located in the Asia Pacific, Japan and Greater China region must allow connectivity from the connector to the following servers over HTTPS (TCP 443):

- **Event Server** - intake.apjc.amp.cisco.com
- **Management Server** - mgmt.apjc.amp.cisco.com
- **Policy Server** - policy.apjc.amp.cisco.com
- **Error Reporting** - crash.apjc.amp.cisco.com
- **connector Upgrades** - upgrades.apjc.amp.cisco.com (TCP 80 and 443)
- **Remote File Fetch** - rff.apjc.amp.cisco.com

To allow the connector to communicate with Cisco cloud servers for file and network disposition lookups, the firewall must allow the clients to connect to the following server over TCP 443 by default or TCP 32137:

- **Cloud Host** - cloud-ec.apjc.amp.cisco.com

For Secure Endpoint Mac version 1.2 and higher, you will need to use the following Cloud Host address and enrollment server (both TCP 443) instead:

- **Cloud Host** - cloud-ec-asn.apjc.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.apjc.amp.cisco.com

If you have ClamAV enabled on any of your Secure Endpoint Mac connectors, you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - clam-defs.apjc.amp.cisco.com

Secure Endpoint Linux Firewall Exceptions

North America

Organizations located in North America must allow connectivity from the connector to the following servers over HTTPS (TCP 443):

- **Event Server** - intake.amp.cisco.com
- **Management Server** - mgmt.amp.cisco.com
- **Policy Server** - policy.amp.cisco.com
- **Error Reporting** - crash.amp.cisco.com
- **connector Upgrades** - upgrades.amp.cisco.com (TCP 80 and 443)

To allow the connector to communicate with Cisco cloud servers for file and network disposition lookups, the firewall must allow the clients to connect to the following servers over TCP 443:

- **Cloud Host** - cloud-ec-asn.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.amp.cisco.com

To use Orbital on your connectors, you must allow access to the following servers over TCP 443:

- **Orbital Updates** - orbital.amp.cisco.com
- **Orbital Queries** - ncp.orbital.amp.cisco.com
- **Orbital Installer** - update.orbital.amp.cisco.com

If you have ClamAV enabled on any of your Secure Endpoint Linux connectors, you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - clam-defs.amp.cisco.com

European Union

Organizations located in the European Union must allow connectivity from the connector to the following servers over HTTPS (TCP 443):

- **Event Server** - intake.eu.amp.cisco.com
- **Management Server** - mgmt.eu.amp.cisco.com
- **Policy Server** - policy.eu.amp.cisco.com
- **Error Reporting** - crash.eu.amp.cisco.com
- **connector Upgrades** - upgrades.eu.amp.cisco.com (TCP 80 and 443)

To allow the connector to communicate with Cisco cloud servers for file and network disposition lookups, the firewall must allow the clients to connect to the following servers over TCP 443:

- **Cloud Host** - cloud-ec-asn.eu.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.eu.amp.cisco.com

To use Orbital on your connectors, you must allow access to the following servers over TCP 443:

- **Orbital Updates** - orbital.eu.amp.cisco.com
- **Orbital Queries** - ncp.orbital.eu.amp.cisco.com
- **Orbital Installer** - update.orbital.eu.amp.cisco.com

If you have ClamAV enabled on any of your Secure Endpoint Linux connectors, you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - clam-defs.eu.amp.cisco.com

Asia Pacific, Japan, and Greater China

Organizations located in the Asia Pacific, Japan and Greater China region must allow connectivity from the connector to the following servers over HTTPS (TCP 443):

- **Event Server** - intake.apjc.amp.cisco.com
- **Management Server** - mgmt.apjc.amp.cisco.com
- **Policy Server** - policy.apjc.amp.cisco.com
- **Error Reporting** - crash.apjc.amp.cisco.com
- **connector Upgrades** - upgrades.apjc.amp.cisco.com (TCP 80 and 443)

To allow the connector to communicate with Cisco cloud servers for file and network disposition lookups the firewall must allow the clients to connect to the following servers over TCP 443:

- **Cloud Host** - cloud-ec-asn.apjc.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.apjc.amp.cisco.com

To use Orbital on your connectors, you must allow access to the following servers over TCP 443:

- **Orbital Updates** - orbital.apjc.amp.cisco.com
- **Orbital Queries** - ncp.orbital.apjc.amp.cisco.com
- **Orbital Installer** - update.orbital.apjc.amp.cisco.com

If you have ClamAV enabled on any of your Secure Endpoint Linux connectors you must allow access to the following server over TCP 80 for signature updates:

Update Server - clam-defs.apjc.amp.cisco.com

Secure Endpoint iOS Firewall Exceptions

North America

Organizations located in North America must allow connectivity from the Connector to the following servers over HTTPS (TCP 443):

- **Event Server** - intake.amp.cisco.com/event/
- **Management Server** - mgmt.amp.cisco.com/agent/v1/
- **Cloud Host** - cloud-ios-asn.amp.cisco.com
- **Enrollment Server** - cloud-ios-est.amp.cisco.com

European Union Firewall Exceptions

Organizations located in the European Union must allow connectivity from the connector to the following servers over HTTPS (TCP 443):

- **Event Server** - intake.amp.cisco.com/event/
- **Management Server** - mgmt.amp.cisco.com/agent/v1/
- **Cloud Host** - cloud-ios-asn.eu.amp.cisco.com
- **Enrollment Server** - cloud-ios-est.eu.amp.cisco.com

Asia Pacific, Japan, and Greater China Firewall Exceptions

Organizations located in the Asia Pacific, Japan, and Greater China region must allow connectivity from the connector to the following servers over HTTPS (TCP 443):

- **Event Server** - intake.amp.cisco.com/event/
- **Management Server** - mgmt.amp.cisco.com/agent/v1/
- **Cloud Host** - cloud-ios-asn.apjc.amp.cisco.com
- **Enrollment Server** - cloud-ios-est.apjc.amp.cisco.com

Selecting computers for evaluation deployment

Instead of installing the connector on a single computer, select a representative cross section of different users. If different operating systems and application sets are in use, try to deploy on at least one of each image type.

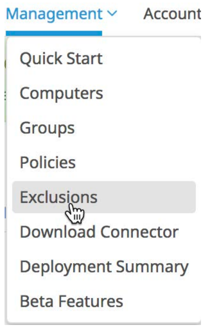
CHAPTER 2
PORTAL CONFIGURATION

Before deploying connectors there are tasks to complete in the Secure Endpoint portal based on the information you gathered.

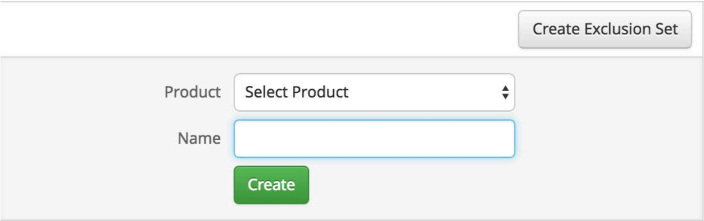
Create exclusions

To prevent conflicts between the connectors and antivirus or other security software, you must create exclusions so that the connector doesn't scan your antivirus directory and your antivirus doesn't scan the connector directory. This can create problems if antivirus signatures contain strings that the connector sees as malicious or cause issues with quarantined files.

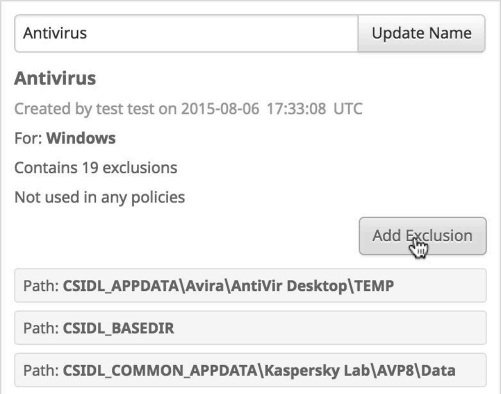
The first step is to create an exclusion by navigating to **Management > Exclusions** in the Secure Endpoint console.



Click on **Create Exclusion Set** to create a new list of exclusions. Enter a name for the list - for example, Desktop Exclusions - and click **Create**.



Next click **Add Exclusion** to add an exclusion to your list.



Antivirus

Antivirus

Created by test test on 2015-08-06 17:33:08 UTC

For: **Windows**

Contains 19 exclusions

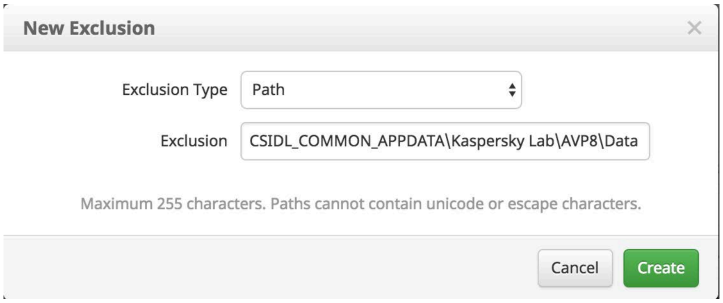
Not used in any policies

Path: **CSIDL_APPDATA\Avira\AntiVir Desktop\TEMP**

Path: **CSIDL_BASEDIR**

Path: **CSIDL_COMMON_APPDATA\Kaspersky Lab\AVP8\Data**

You will then be prompted to select an exclusion type. You can add a path, threat name, file extension, process, or use wild cards for file names, extensions, or paths. Select Path and enter the CSIDL of the security products you have installed on your endpoints then click **Create**.



Exclusion Type: Path

Exclusion: CSIDL_COMMON_APPDATA\Kaspersky Lab\AVP8\Data

Maximum 255 characters. Paths cannot contain unicode or escape characters.

IMPORTANT! You do not need to escape “space” characters in a path. For some non-English languages, different characters may represent path separators. The connectors will only recognize '\' characters as valid path separators for exclusions to take effect.

Repeat this procedure for each path associated with your security applications. More information about CSIDLs can be found here. See Best practices for AMP for Endpoint Exclusions for further information on creating exclusions and common exclusion paths.

IMPORTANT! CSIDLs are case sensitive.

Next create an exclusion set for your servers and another one for your Active Directory domain controllers. Make sure to exclude any security products as you did in your desktop exclusions above and also create exclusions based on your server roles (Active Directory, file server, DHCP, etc.) and installed software (Exchange, SQL, IIS, etc.). Microsoft has compiled a list of links to exclusions for their server products at http://social.technet.microsoft.com/wiki/contents/articles/953.microsoft-anti-virus-exclusion-list.aspx.

Create outbreak control lists

During the early stages of deployment you may encounter previously unseen malware on computers as well as false-positive detection of custom applications. To make sure the connector deals with these properly, you will want to create a Simple Custom Detection list and an Allowed Application list to associate with your policies.

To create a Simple Custom Detection list, go to **Outbreak Control > Simple**. Click **Create** to create a new Simple Custom Detection, name it Quick SCD (or a name that you prefer), and click on **Save**.

To create an Allowed Application list, go to **Outbreak Control > Application Control - Allowed Applications**. Next click **Create** to create a new list, name it, and click **Save**.

Create policies

For initial deployment we recommend you go to **Management > Policies** and create the following policies with specific configurations:

Audit Only

This policy puts the connector in a mode that will only detect malicious files but not quarantine them. Malicious network traffic is also detected but not blocked.

- This policy uses all the default policy settings but with **Modes and Engines > Files** set to **Audit**.
- The proxy server information gathered previously should be entered under **Proxy.**
- Associate the exclusion set you previously created with this policy.
- Associate the Quick SCD list you created with this policy.
- Associate the Quick WL list you created with this policy.

Protect

This is the standard policy for the connector that will quarantine malicious files and block malicious network connections. Once you have become familiar with the way the connector behaves you can tweak this policy to your own preferences.

- This policy uses all the default policy settings but with the **Modes and Engines > TETRA** unchecked.
- The proxy server information gathered previously should be entered under **Proxy**.
- Associate the exclusion set you previously created with this policy.
- Associate the Quick SCD list you created with this policy.
- Associate the Quick WL list you created with this policy.

Triage

This is an aggressive policy that enables the offline engine to scan computers that are suspected or known to be infected with malware.

- This policy uses all the default policy settings but with **Modes and Engines > TETRA** checked and with **Modes and Engines > Network** set to **Block**.

  IMPORTANT! If you enable TETRA you should never use this policy on an endpoint that already has another antivirus product installed.

- The proxy server information gathered previously should be entered under **Proxy**.
- Associate the exclusion set you previously created with this policy.
- Associate the Quick SCD list you created with this policy.
- Associate the Quick WL list you created with this policy.

Server

This is a lightweight policy for high availability computers and servers that require maximum performance and uptime.

- This policy uses all the default policy settings but with **Modes and Engines > Files** set to **Audit**.
- You can enable **Modes and Engings > TETRA** on your Server policy but it is highly recommended that you deploy it to a test server before rolling the policy out to your production servers. We also recommend using a local Secure Endpoint Update Server for your TETRA definition updates.

  WARNING! Running TETRA on a server without testing and proper Exclusions could significantly impact performance.

- If you do not want to run TETRA on your servers due to performance concerns you must make sure that **Modes and Engines > TETRA** is unchecked.

  WARNING! When installing the connector on a server without TETRA you must also use the /skiptetra command line switch along with this policy setting.

- If your servers host services or applications that require a large number of network connections (SMB, SQL, Exchange, etc.) it is recommended that **Modes and Engines > Network** be set to **Disabled**.

WARNING! When installing the connector on a server you must also use the /skipdfc command line switch along with this policy setting.

- The proxy server information gathered previously should be entered under **Proxy**.
- Associate the server exclusion set you previously created with this policy.
- Associate the Quick SCD list you created with this policy.
- Associate the Quick WL list you created with this policy.

Domain Controller

This is a lightweight policy for use on Active Directory Domain Controllers.

- This policy uses all the default policy settings but with the **Modes and Engines > Files** set to **Audit**.
- Because of authentication traffic from your network it is recommended that **Modes and Engines > Network** be set to **Disabled**.

WARNING! When installing the connector on a domain controller you must also use the /skipdfc command line switch along with this policy setting.

- You can enable **Modes and Engings > TETRA** on your Domain Controller policy but it is highly recommended that you deploy it to a test server before rolling the policy out to your production servers. We also recommend using a local Secure Endpoint Update Server for your TETRA definition updates.

WARNING! Running TETRA on a server without testing and proper Exclusions could significantly impact performance.

- If you do not want to run TETRA on your servers due to performance concerns you must make sure that **Modes and Engines > TETRA** is unchecked.

WARNING! When installing the connector on a server without TETRA you must also use the /skiptetra command line switch along with this policy setting.

- The proxy server information gathered previously should be entered under **Proxy**.
- Associate the domain controller exclusion set you previously created with this policy.

- Associate the Quick SCD list you created with this policy.
- Associate the Quick WL list you created with this policy.

IMPORTANT! If you have computers in multiple geographic locations using different proxy servers you will need to create the above policies for each location ie. Audit Only NYC and Audit Only London.

Create groups

Now that you have created the initial policies for your deployment you need to create groups to associate the policies with. Go to Management -> Groups and create the following groups:

Audit Only

- Associate this group with the Audit Only policy.
- This should be the first group that the workstations in your deployment belong to so that you can root out any false positive detections without the files being quarantined.
- You can also use the Audit Only group as a performance group for computers that require higher availability or perform intensive tasks like rendering graphics.

Protect

- Associate this group with the Protect policy.
- Once you are satisfied with the performance of the computers in your Audit Only group, you can move them to the Protect group for normal operation of the connector so that malicious files are quarantined and network threats are blocked.

Triage

- Associate this group with the Triage policy.
- Any computers with existing infections or computers you suspect of being heavily infected should be moved to the Triage group since this group has more aggressive malware scanning enabled.

Server

- Associate this group with the Server policy.
- All of your servers other than Active Directory domain controllers should be in this group.

Domain Controller

- Associate this group with the Domain Controller policy.

- All of your Active Directory domain controllers should be in this group.

IMPORTANT! If you created multiple policies for different geographic locations in the previous section, you will need to create multiple groups for each location as well ie. Protect NYC and Protect London.

Create Allowed Applications list from gold image

If you have a gold image available it is advisable to use it to add applications to an Allowed Applications list. You can use a tool like md5deep to generate SHA-256 values for all the applications and add them to your Application Control - Allowed Applications list.

Download installer

Now that you have created your policies and associated them with groups you can begin deploying the connector to the computers you identified in the information gathering stage. Go to **Management > Download connector** and download a redistributable installer for the Audit Only, Triage, Servers, and Domain Controllers groups.

All of your average user computers should initially use the Audit Only installer. This will allow you to make sure that all of the necessary applications have been allow listed and proper exclusions were created. Any detections will still trigger alerts in the Secure Endpoint console but nothing will be quarantined or blocked. This ensures that in the case of a false positive detection that there are no disruptions in regular operations. If you see a false positive detection, add the application in question to your Allowed Applications list. Once you are satisfied with the performance of the connector you can move computers from the Audit Only group into the Protect group. The Protect group has the same policy settings as the Audit Only group, except that malicious files will be quarantined and connections to malicious websites will be blocked.

Only use the Domain Controllers installer on your Active Directory domain controller servers. The policy for this group includes exclusions that are specific to servers that run directory services for your tree.

Use the Servers installer on all your other servers, such as file, SQL, and Exchange servers.

CHAPTER 3
DEPLOYING THE CONNECTOR

Now you are ready to begin deploying the connector to your evaluation computers.

Installer Command Line Switches

Administrators who have their own deployment software can use command line switches to automate the deployment. Here is a list of available switches:

- /R - For all connector versions 5.1.13 and higher this must be the first switch used.
- /S - Used to put the installer into silent mode.

IMPORTANT! This must be specified as the first parameter or the parameter immediately after /R.

- /desktopicon 0 - A desktop icon for the connector will not be created.
- /desktopicon 1 - A desktop icon for the connector will be created.
- /startmenu 0 - Start Menu shortcuts are not created.
- /startmenu 1 - Start Menu shortcuts are created.
- /contextmenu 0 - Disables Scan Now from the right-click context menu.
- /contextmenu 1 - Enables Scan Now in the right-click context menu.
- /remove 0 - Uninstalls the connector but leaves files behind useful for reinstalling later.
- /remove 1 - Uninstalls the connector and removes all associated files.
- /uninstallpassword [connector Protection Password] – Allows you to uninstall the connector when you have Connector Protection enabled in your policy. You must supply the **connector Protection** password with this switch.

- /skipdfc 1 - Skip installation of the DFC driver.

  IMPORTANT! Any connectors installed using this flag must be in a group with a policy that has **Modes and Engines > Network** set to **Disabled**.

- /skiptetra 1 - Skip installation of the TETRA driver.

  IMPORTANT! Any connectors installed using this flag must be in a group with a policy that has **Modes and Engines > TETRA** unchecked.

- /D=[PATH] - Used to specify which directory to perform the install. For example, /D=C:\tmp will install into C:\tmp.

  IMPORTANT! This must be specified as the last parameter.

- /temppath - Used to specify the path to use for temporary files created during connector install. For example, /temppath C:\somepath\temporaryfolder. This switch is only available in the Secure Endpoint Windows connector 5.0 and higher.

  IMPORTANT! The following switch for skipping registration and startup of connector is intended for use when creating a Windows operating image as a deployable golden image.

- /goldenimage 1 - Skip initial connector registration and startup on install.
- /goldenimage 0 - Do not skip initial connector registration and startup on install.

IMPORTANT! Starting with Secure Endpoint Windows connector version 6.3.1, if using any installer switch that contains a path argument (e.g. /temppath, /D switches) that contains a single quote character ('), you will need to enclose the entire path in double quotes ("). If not, the installer will incorrectly parse the argument and install the Connector in a different location than expected.

Running the command line installer without specifying any switches is equivalent to /desktopicon 0 /startmenu 1 /contextmenu 1 /skipdfc 0 /skiptetra 0.

There is a command line switch in Secure Endpoint Windows connector 5.1.3 and higher to enable users to opt in/out of migrating the install directory from “Sourcefire” to “Cisco” when upgrading from versions prior to 5.1.1 to versions 5.1.3 and higher. These are as follows:

- /renameinstalldir 1 will change the install directory from Sourcefire to Cisco.
- /renameinstalldir 0 will not change the install directory.

  IMPORTANT! By default /renameinstalldir 1 will be used.

Secure Endpoint Windows connector 6.0.5 and higher has a command line switch to skip the check for Microsoft Security Advisory 3033929.

- /skipexprevprereqcheck 1 - Skip the check for Microsoft Windows KB3033929.
- /skipexprevprereqcheck 0 - Check for Microsoft Windows KB3033929 (Default).

IMPORTANT! If you use this switch and do not have this KB installed, or other Windows Updates that enable SHA-2 code signing support for Windows 7 and Windows Server 2008 R2, you will encounter issues connecting to the Cisco Cloud.

Secure Endpoint Windows connector 6.0.7 and higher has a command line switch to set the registry key necessary to receive the Windows Security Update for KB 4072699.

- /kb4072699 1 - Set the registry key value.
- /kb4072699 0 - Do not set the registry key value (Default).

IMPORTANT! The registry key value can only be set using this command line switch. If you do not set this key either using the switch or manually, you will not receive the patch. See Cisco AMP for Endpoints Compatibility with Windows Security Update KB4056892 for a list of compatible versions.

Installer exit codes

Administrators who use the command line switches to install the connector should be aware of the exit codes. They can be found in immpro_install.log in the %TEMP% folder.

- 0 – Success.
- 1500 – Installer already running.
- 1618 – Another installation is already in progress.
- 1633 – Unsupported platform (i.e. installing 32 on 64 and vice versa).
- 1638 – This version or newer version of product already exists.
- 1801 – invalid install path.
- 3010 – Success (Reboot required – will only be used on upgrade).
- 16001 – Your trial install has expired.
- 16002 – A reboot is pending on the user’s computer that must be completed before installing.
- 16003 – Unsupported operating system (i.e. XP SP2, Win2000).
- 16004 – invalid user permissions (not running as admin).
- 16005 - Existing connector service was already stopped or uses connector Protection and the password was not supplied.
- 16006 - PoS OS specific features (Enhanced Write Filter (EWF) or File-Based Write Filter (FBWF)) are currently enabled which interfere with the Windows Connector. Disable the features and try again. Note that PoS OSes are not officially supported.
- 16007 - connector upgrade requires a reboot to complete, but the Block Reboot option has been configured in policy.

- 16008 - Connector upgrade blocked due to pending reboot already required on the computer.
- 16009 - SHA-2 Code signing support for Windows 7 and Windows Server 2008 R2 patch is missing (KB3033929).

Cisco Security Connector Monitoring Service

With versions of Secure Endpoint Windows connector lower than 6.3.1, the connector registers itself with Windows Security Center (WSC) when the TETRA engine is enabled and its definitions are up to date. Once it is successfully registered, Windows Defender will be disabled and Secure Endpoint will be designated as the active Virus and Threat Protection provider.

Starting with Windows Connector 6.3.1, the Cisco Security Monitoring Service will now be responsible for registering with WSC. As an anti-malware protected process light (AM-PPL) service, it will be able to communicate with WSC to enable or disable Windows Defender according to TETRA’s status.

Deployment

You can download the installer from **Management > Download Connector** and make the file available on a file share, use login scripts to install it, or distribute it using enterprise software deployment tools.

CHAPTER 4
TROUBLESHOOTING

This section describes some issues that may arise after the connector is installed and remediation steps.

Initial Configuration Failure

Under rare circumstances the initial configuration of your Secure Endpoint Private Cloud device may fail. If this occurs you will need to delete the Private Cloud device from your virtual machine console and import the OVA again. If the initial configuration fails again contact Support.

Performance

Secure Endpoint uses a filter driver to identify file copies, moves, and executes. This may cause additional file latency in some applications that have high I/O such as databases. To reduce latency you may need to determine what should be excluded from Secure Endpoint:

1. Identify where the application files exist.
2. Determine where the data files are being used.
3. Exclude both of those locations.
4. If there are still issues with the given application, turn on debug logging in the policy for the connector.
5. Use the logs to determine any temporary files being used.

Another helpful tip is that if you download the latest version of sqlite3 (http://www.sqlite.org/download.html), you can use that to query the history and see files that are continuously being written to, for example:

```
sqlite3.exe "C:\Program Files\Cisco\AMP\history.db"
SQLite version 3.7.16.2 2013-04-12 11:52:43
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .headers on
sqlite> select filename, count(filename) from history group by
filename order by
count(filename) desc limit 10;
filename|count(filename)
\\?\C:\WINDOWS\Tasks\User_Feed_Synchronization-{A1489466-0BD4-
42D2-A8B6-864FEA527577}.job|1706
\\?\C:\Documents and Settings\Administrator\Local
Settings\Application Data\Microsoft\Feeds\{5588ACFD-6436-411B-
A5CE-666AE6A92D3D}~\Internet Explorer Suggested Sites~.feed-
ms|341
\\?\C:\WINDOWS\Tasks\GoogleUpdateTaskUserS-1-5-21-839522115-
1229272821-725345543-500UA.job|222
...
```

The above data identifies some exclusions that may be worth implementing:

FilePath: CSIDL_WINDOWS\Tasks

FileExtension: *.feed-ms

Outlook performance

If you notice slow performance in Outlook with the connector installed, this may be from the high I/O on the .pst or .ost file. In this case, it is best to create an exclusion for all .pst and .ost files in the Secure Endpoint console. Go to **Management > Exclusions** and click **Edit** for the exclusion set you want. Click **Add Exclusion** and select **File Extension** from the Exclusion type drop down menu. Enter .pst in the field and click **Create**. Repeat this for the .ost file extension if you use Outlook with an Exchange server.

Cannot connect to the cloud

There can be any number of reasons why the connector cannot connect to the cloud. The most common two are that there is a firewall preventing the outbound connection or that the proxy server is not cooperating with the connection. In both cases, you want to start troubleshooting with these steps:

1. Make sure the sfc.exe process (or agent.exe for versions prior to 3.1.4) is running. Open the Task Manager, select Show processes from all users, and make sure there is an sfc.exe process (agent.exe for versions prior to 3.1.4) listed. If it is not, open the command prompt as an administrator and run `net start immunetprotect` for versions up to 5.1.1 and `net start ciscoamp_[version]` where [version] is the Connector version installed (such as 5.1.1).
2. Make sure that there is only one iptray.exe process listed in the Task Manager. If there is more than one iptray.exe process you will need to end both iptray.exe processes and restart the connector user interface.
3. Make sure you can connect to cloud-ec.amp.sourcefire.com over the correct port. A simple telnet test on TCP 443 should suffice if there is no proxy configured. If there is a proxy, see the Proxy section below.
4. If you're still unable to connect, then uninstall the connector and reboot the computer. Afterwards go to the policy that you're using and set **Advanced Settings > Administrative Features > Connector Log Level** to **Debug**. Then download the connector installer and re-install it. This will give additional information to send to diagnose the issue.

Copy, move, or execute events not in Device Trajectory

The copy, move, and execute events come up to the connector through the Immunet Protect driver. Then the connector passes this information off to the cloud servers to decide whether a file is malicious. Then the cloud server will load it into a database that Device Trajectory reads from. Therefore to troubleshoot what is going on:

1. Check if the driver is installed properly. If you run `fltmc instances` from the command line as an administrator, it will list the drivers installed and which drives it's bound with. What you want to see is the ImmunetProtectDriver bound to all of the local hard drives (ie. C:\, E:\, etc.).
2. Check to see if the policy has **Monitor File Copies and Moves** and **Monitor Process Execution** enabled under **Advanced Settings > File and Process Scan**. Without these enabled, we will not monitor these file operations.
3. Check to see if you can connect to the cloud.
4. In your policy, set **Advanced Settings > Administrative Features > Connector Log Level** to **Debug** to make sure that you are getting disp=1 or disp=3 in your logs. A disp=4 means it failed to look up the file to the cloud. That could be an unsupported file type or other reason.
5. If you're connected to the cloud and seeing the dispositions of 1 or 3 coming back from the cloud, then take a support diagnostic and attach it along with your external IP address to a support case.

Network events not in Device Trajectory

The network information is picked up by the DFC driver and sent to the connector. The connector passes this information off to the cloud server to see whether or not that connection is malicious. In order to troubleshoot what is going on:

1. Check to see if the policy has **Modes and Engines > Network** set to **Block** or **Audit**.
2. Set the **Advanced Settings > Administrative Features > Connector Log Level** to **Debug** if you can see events that list the IP and port information.

IMPORTANT! Secure Endpoint only monitors a limited number of connections after process execution. Therefore you need to make sure that you execute a new process after you start the connector. Internet Explorer will re-use processes for each new tab whereas Chrome will start a new process upon tab creation.

Policy not updating

When a connector fails to receive policy updates the most common causes are network connectivity or proxy configuration. For network connectivity issues, see Proxy and Cannot connect to the cloud. If the proxy settings in the policy were mis-configured then most often you will have to uninstall the connector, reboot the computer, fix the proxy settings in the policy, download the connector installer again, then reinstall it. However, if you already have one computer installed in a group (you can move a computer into that group just for this purpose), then you can:

1. Go to **Management > Policies**.
2. Find the policy you're looking for and click on it (DO NOT click Edit) so that you see the preview on the right hand side and click the **Download XML** button. Once the XML file has been downloaded:
   - Stop the connector by typing `sfc.exe -k “password”` into a command prompt as an administrator from your connector install folder. You will only need to enter the password if you have connector protection enabled and the password must be in quotes.
   - In the install folder (C:\Program Files\Sourcefire\FireAMP by default for versions up to 5.1.1 and C:\Program Files\Cisco\AMP for versions 5.1.1 and higher), rename the existing policy.xml to policy.xml.bak
   - Copy the policy.xml that you downloaded to that folder and rename it policy.xml
   - Open the policy.xml in the file you downloaded and note the serial number.
   - Start the connector by running `net start immunetprotect` for versions up to 5.1.1 and `net start ciscoamp_[version]` where [version] is the Connector version installed (such as 5.1.1), from a command prompt as an administrator.
   - Wait the duration of the policy's heartbeat time before again stopping the connector by typing `sfc.exe -k “password”` into a command prompt as an administrator from your connector install folder. Check to see if the serial number has changed.

Proxy

Not every organization allows direct outbound connections to the Internet but instead routes connections through a proxy so that they can filter and scan traffic. Secure Endpoint supports proxies, but it is important to make sure the policies are configured correctly. In this case, it's probably best to start the connector with **Advanced Settings > Administrative Features > Connector Log Level** set to **Debug** in the policy. If there aren't any obvious errors in the logs:

- Stop the connector by typing `sfc.exe -k “password”` into a command prompt as an administrator from your connector install folder. You will only need to enter the password if you have connector protection enabled and the password must be in quotes.
- Close any unnecessary applications then install and run Wireshark on the computer you're troubleshooting.
- Try to get a packet capture started between the proxy server and the outbound Internet connection using Wireshark.
- Make sure that the browser on your computer is configured with the same proxy configuration as the browser on the computer you're troubleshooting. Test to make sure you can get to https://console.amp.cisco.com.
- Install curl from http://curl.haxx.se/download.html. Download FireAMP_Helper.vbs from http://immunet-janus-helpdoc.s3.amazonaws.com/FireAMP_Helper/FireAMP_Helper.vbs. Open the .vbs file and modify:
  - CURL_APP = "curlpath\curl.exe"

    Where curlpath is the path to your curl install directory.
  - PROXY_SERVER = "http://x.x.x.x:yyyy"

    Where x.x.x.x is the IP address of your proxy server and yyyy is the port used (normally 8080).
  - PROXY_USER_PASS = "Domain\username:password"

    Where Domain\username and password are the username and password you use to authenticate to the proxy server. If your proxy doesn't require authentication you can leave this field empty.

  Then you can run:

  ```
  cscript FireAMP_Helper.vbs testproxy
  ```
- Start the connector by running `net start immunetprotect` for versions up to 5.1.1 and `net start ciscoamp_[version]` where [version] is the Connector version installed (such as 5.1.1), from a command prompt as an administrator.
- Let the connector run for approximately 5 minutes to generate traffic.
- Get a Secure Endpoint diagnostics, the PCAP from the connector to the proxy, and the PCAP from the proxy to the Internet and attach them to a support case.

Duplicate connectors

Under some circumstances you may see duplicate entries on the Computers page of the Secure Endpoint Console. Determine the cause of the duplicate entries first, then you can proceed to delete them.

Causes

There are three common reasons for duplicate connectors appearing in your Organization.

Gold Standard Image

When you deploy endpoints using a gold standard image that includes the connector, each time you deploy an endpoint a duplicate connector will appear in your Secure Endpoint Console. If you deploy endpoints using a gold standard image, you can refer to this article or contact support for help on preventing duplicate connectors.

Re-image

When you re-image an endpoint there will always be a duplicate connector entry. This is because a new Device Trajectory is started for the re-imaged connector and the old connector Device Trajectory is maintained. If the computer was re-imaged because of a compromise this lets you further examine the possible cause. If you no longer need the old Device Trajectory the older connector can be deleted.

Virtual Environments

Virtual environments can also cause duplicate connector entries when new virtual sessions are started or when a virtual computer is re-imaged. In most cases you can refer to this article or contact support for help on preventing duplicate connectors.

Delete Duplicate connectors

Deleting duplicate connectors within the management console is a manual process. To manage duplicates, go to **Management > Computers** expand the **Filters** section at the top of the page, configure the **Last Seen** drop down to the desired range and click **Apply Filter**. The filtered view will show all connectors that were Last Seen over the time period selected. You can select all computers and delete them from the list. If you delete a computer that still has a connector installed, it will re-register with the management console when the service is restarted such as on a reboot of the computer.

Simple Custom Detections

Simple Custom Detections allow you to manually blocklist files for detection. If **Modes and Engines > Files** is set to **Audit**, you'll just be notified of the detection but if it's set to **Quarantine**, the file will be quarantined. The most common issue is that you found a file, you copied it on your machine, you add it to a Simple Custom Detection, and then you can't understand why it's not being detected. There could be a few reasons:

1. The file is being excluded. Compare the path you're running from with the path in your exclusions listed in the policy.xml. Don't forget to look at file extension exclusions as well.
2. The file is in a signed Microsoft or Verisign Class 3 certificate. Right-click on the file and look at the properties. Check to see if there is a Digital Signature associated with it and who the issuer is. If it is Verisign and you're sure it's malware, upload it to Virus Total and then contact Support.

3. The file is not associated with the correct policy. Make sure the SHA-256 for the file is in the correct Simple Custom Detection list. Make sure that Simple Custom Detection list is associated with the policy that the connector is using.
4. The file has been cached. This is by far the most common issue. When you copied it onto your computer, you created a record for it in your cache.db. To remove this:
   - Stop the connector by typing `sfc.exe -k “password”` into a command prompt as an administrator from your connector install folder. You will only need to enter the password if you have connector protection enabled and the password must be in quotes.
   - Go to the install directory (C:\Program Files\Sourcefire\FireAMP by default for versions up to 5.1.1 and C:\Program Files\Cisco\AMP for versions 5.1.1 and higher) and remove the cache.* files.
   - Start the connector by running `net start immunetprotect` for versions up to 5.1.1 and `net start ciscoamp_[version]` where [version] is the Connector version installed (such as 5.1.1), from a command prompt as an administrator.
   - Now re-copy the file in question and make sure it is detected.

Allowed Applications

The Allowed Applications list allows you to allow a file to avoid detection. This can be done as part of collecting all files from a “Golden Image” or in the case of a false positive. The most common issue here is caching because you had it previously on your computer and need to clear your cache.db:

1. Stop the connector by typing `sfc.exe -k “password”` into a command prompt as an administrator from your connector install folder. You will only need to enter the password if you have connector protection enabled and the password must be in quotes.
2. Go to the install directory (C:\Program Files\Sourcefire\FireAMP by default for versions up to 5.1.1 and C:\Program Files\Cisco\AMP for versions 5.1.1 and higher) and remove the cache.* files.
3. Start the connector by running `net start immunetprotect` for versions up to 5.1.1 and `net start ciscoamp_[version]` where [version] is the Connector version installed (such as 5.1.1), from a command prompt as an administrator.
4. Now re-copy the file you created and make sure it’s not detected.

Another possible issue is that the Allow List is not associated with the correct policy or that the file SHA-256 is not on that list.

Application Blocking

Application Blocking allows you stop a file from executing without quarantining the file. If you add a SHA-256 to an Application Blocking list and it still executes, there could be a few reasons why this may occur:

1. The file is being excluded. Compare the path you're running from with the path in your exclusions listed in the policy.xml. Don't forget to look at file extension exclusions as well.
2. The file is not associated with the correct policy. Make sure the SHA-256 for the file is in the correct Simple Custom Detection list. Make sure that Simple Custom Detection list is associated with the policy that the connector is using.
3. The file has been cached. This is by far the most common issue. When you copied it onto your computer, you created a record for it in your cache.db. To remove this:
    - Stop the connector by typing `sfc.exe -k “password”` into a command prompt as an administrator from your connector install folder. You will only need to enter the password if you have connector protection enabled and the password must be in quotes.
    - Go to the install directory (C:\Program Files\Sourcefire\FireAMP by default for versions up to 5.1.1 and C:\Program Files\Cisco\AMP for versions 5.1.1 and higher) and remove the cache.* files.
    - Start the connector by running `net start immunetprotect` for versions up to 5.1.1 and `net start ciscoamp_[version]` where [version] is the Connector version installed (such as 5.1.1), from a command prompt as an administrator.
    - Now re-copy the file in question and make sure it does not execute.

Contacting Support

If you have not had success with other troubleshooting measures, you may need to contact Support to resolve your issue. In order to speed up turnaround time for your support case it is helpful to provide some information when opening the case.

1. Go to **Management > Policies** and edit the policy the connector you're troubleshooting is in.
2. Set **Advanced Settings > Administrative Features > Connector Log Level** to **Debug**.
3. On the connector go to **Settings** and click **Sync Policy**.

    If you installed the connector using the command line switch to disable the Start Menu items you can force a policy sync by opening a command prompt and entering:

    ```
    %PROGRAMFILES%\Sourcefire\FireAMP\x.x.x\iptray.exe -f
    ```

    Where x.x.x is the connector version number.
4. After the policy has synced allow the connector to run for 5-10 minutes or perform the specific actions that are causing errors.

5. Open the Windows Start Menu and go to connector and click Support Diagnostic Tool. This will create a file on your desktop named Sourcefire_Support_Tool_2013_XX_XX_XX_XX_XX.7z where XX will represent the month, day, and time you ran the tool.

   If you installed the connector using the command line switch to disable the Start Menu items you can run the Support Diagnostic tool by opening a command prompt and entering:

   ```
   %PROGRAMFILES%\Sourcefire\FireAMP\x.x.x\ipsupporttool.exe
   ```

   Where x.x.x is the connector version number.

6. If you are having connectivity issues with the connector, take a PCAP of any network activity.
7. Upload the diagnostic file and PCAP to the Support Case Manager at https://mycase.cloudapps.cisco.com/case and make sure to note the filenames when contacting support.
8. If the issue is a user interface bug or a problem with the Secure Endpoint console, take a screenshot of the problem and attach it to the email you send.
9. Contact Support with all relevant information to the issue, the filenames of any files you uploaded, and attach your screenshots if required. Also make sure to include information on the type of proxy and firewall you are using in the case of connectivity issues.

APPENDIX A
THREAT DESCRIPTIONS

Secure Endpoint has unique network detection event types and Indications of Compromise. Descriptions of these detection types are found in this section.

IMPORTANT! For descriptions of threat names, see AMP Naming Conventions.

File Disposition

Files observed by your connectors are divided into three disposition types:

- Clean - the file is known to be clean or signed with a trusted certificate.
- Malicious - the file is known malware or harmful.
- Unknown - there is insufficient data to make a determination.

Indications of Compromise

Secure Endpoint calculates devices with Trajectory Indications of Compromise based on events observed over the last 7 days. A single Cloud IOC will only be reported once every four hours per endpoint. Events such as malicious file detections, a parent file repeatedly downloading a malicious file (Potential Dropper Infection), or multiple parent files downloading malicious files (Multiple Infected Files) are all contributing factors. Indications of compromise include:

- Threat Detected - One or more malware detections were triggered on the computer.
- Potential Dropper Infection - Potential dropper infections indicate a single file is repeatedly attempting to download malware onto a computer.
- Multiple Infected Files - Multiple infected files indicate multiple files on a computer are attempting to download malware.

- Executed Malware - A known malware sample was executed on the computer. This can be more severe than a simple threat detection because the malware potentially executed its payload.
- Suspected botnet connection - The computer made outbound connections to a suspected botnet command and control system.
- [Application] Compromise - A suspicious portable executable file was downloaded and executed by the application named, for example Adobe Reader Compromise.
- [Application] launched a shell - The application named executed an unknown application, which in turn launched a command shell, for example Java launched a shell.
- Generic IOC - Suspicious behavior that indicates possible compromise of the computer.
- Suspicious download - Attempted download of an executable file from a suspicious URL. This does not necessarily mean that the URL or the file is malicious, or that the endpoint is definitely compromised. It indicates a need for further investigation into the context of the download and the downloading application to understand the exact nature of this operation.
- Suspicious Cscript Launch - Internet Explorer launched a Command Prompt, which executed cscript.exe (Windows Script Host). This sequence of events is generally indicative of a browser sandbox escape ultimately resulting in execution of a malicious Visual Basic script.
- Suspected ransomware - File names containing certain patterns associated with known ransomware were observed on the computer. For example, files named help_decrypt.<filename> were detected.
- Possible webshell - the IIS Worker Process (w3wp) launched another process such as powershell.exe. This could indicate that the computer was compromised and remote access has been granted to the attacker.
- Global threat alert - global threat alerts uses advanced algorithms, machine learning, and artificial intelligence to correlate network traffic generated by your users and network devices to identify command-and-control traffic, data exfiltration, and malicious applications. A global threat alert indication of compromise event is generated when suspicious or anomalous traffic is detected in your organization. Only threats that global threat alerts has assigned a severity of 7 or higher are sent to Secure Endpoint.

IMPORTANT! In certain cases the activities of legitimate applications may trigger an indication of compromise. The legitimate application is not quarantined or blocked, but to prevent another Indication of Compromise being triggered on future use you can add the application to Application Control - Allowed Applications.

Device Flow Correlation Detections

Device flow correlation allows you to flag or block suspicious network activity. You can use Policies to specify Secure Endpoint Secure Endpoint connector behavior when a suspicious connection is detected and also whether the connector should use addresses in the Cisco Intelligence Feed, custom IP lists you create, or a combination of both. Device flow correlation detections include:

- DFC.CustomIPList - The computer made a connection to an IP address you have defined in a device flow correlation IP blocked list.
- Infected.Bothost.LowRisk - The computer made a connection to an IP address thought to belong to a computer that is a known participant in a botnet.
- CnC.Host.MediumRisk - The computer made a connection to an IP address that was previously known to be used as a bot command and control channel. Check the Device Trajectory for this computer to see if any files were downloaded and subsequently executed from this host.
- ZeroAccess.CnC.HighRisk - The computer made a connection to a known ZeroAccess command and control channel.
- Zbot.P2PCnC.HighRisk - The computer made a connection to a known Zbot peer using its peer-to-peer command and control channel.
- Phishing.Hoster.MediumRisk - The computer made a connection to an IP address that may host a phishing site. Often, computers phishing sites also host many other websites and the connection may have been made to one of these other benign sites.

IMPORTANT! Device flow correlation is incompatible with applications that do network tunneling, like VPN.

APPENDIX D
SUPPORTING DOCUMENTS

The following supporting documents are available for download.

Cisco Secure Endpoint User Guide

The current version of the User Guide can be downloaded here.

Download the User Guide

Cisco Secure Endpoint Deployment Strategy Guide

This guide provides a more detailed look at preparing and planning for a production deployment of Secure Endpoint along with best practices and troubleshooting tips.

Download the Deployment Strategy Guide

Cisco Secure Endpoint Support Documentation

TechNotes for configuring, maintaining, and troubleshooting Secure Endpoint.

Support Documentation

Cisco Endpoint IOC Attributes

The Endpoint IOC Attributes document details IOC attributes supported by the Endpoint IOC scanner included in the Secure Endpoint connector. Sample IOC documents that can be uploaded to your Secure Endpoint console are also included.

Download the Endpoint IOC Attributes

Cisco Secure Endpoint API Documentation

The API allows you to access your Secure Endpoint data and events without logging into the console. The documentation provides descriptions of available interfaces, parameters, and examples.

View the API documentation

Cisco Secure Endpoint Release Notes

The Release Notes contain the Secure Endpoint change log.

Download the Release Notes

Cisco Secure Endpoint Demo Data Stories

The Demo Data stories describe some of the samples that are shown when Demo Data is enabled in Secure Endpoint.

Download the Device Control document

Download the WMIPRVSE document

Download the FriedEx document

Download the WannaCry Ransomware document

Download the Cognitive Threat Analytics (CTA) document

Download the Command Line Capture document

Download the Low Prevalence Executable document

Download the Cryptowall document

Download the PlugX document

Download the Upatre document

Download the CozyDuke document

Download the SFEICAR document

Download the ZAccess document

Download the ZBot document

Cisco Universal Cloud Agreement

Cloud Offer Terms