AMP for Endpoints Deployment Strategy

Last Updated: December 4, 2017

Table of Contents

CHAPTER 1
PLANNING

This document will guide you through best practices to deploy AMP for Endpoints for the first time. Following this strategy will increase your chances of a successful AMP for Endpoints 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 AMP for Endpoints Connector for Windows, you must first identify your environment. To do that you must answer the following questions:

- How many computers is the AMP for Endpoints 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 AMP for Endpoints 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 AMP for Endpoints 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 AMP for Endpoints 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

The following are the minimum system requirements for the AMP for Endpoints Connector Connector based on the operating system. Operating systems not listed here are not currently supported.

AMP for Endpoints Windows Connector

The AMP for Endpoints Windows Connector supports both 32-bit and 64-bit versions of these operating systems.

Currently Supported Versions

Microsoft Windows 7

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

Microsoft Windows 8 and 8.1 (requires AMP for Endpoints Connector 3.1.4 or later)

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

Microsoft Windows 10 (requires AMP for Endpoints Connector 4.3.0 or later)

- 1 GHz or faster processor
- 1 GB RAM (32-bit) or 2 GB RAM (64-bit)
- 650 MB available hard disk space - Cloud-only mode
- 1 GB available hard disk space - TETRA

Microsoft Windows Server 2008 R2

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

Microsoft Windows Server 2012 (requires AMP for Endpoints Connector 3.1.9 or later)

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

Previously Supported Versions

Microsoft Windows XP with Service Pack 3 or later (requires AMP for Endpoints Windows Connector versions 5.x.x or lower)

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

Microsoft Windows Vista with Service Pack 2 or later (requires AMP for Endpoints Windows Connector versions 5.x.x or lower)

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

Microsoft Windows Server 2003 (requires AMP for Endpoints Windows Connector versions 5.x.x or lower)

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

Microsoft Windows Server 2008 (requires AMP for Endpoints Windows Connector versions 5.x.x or lower)

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

Incompatible software and configurations

The AMP for Endpoints Windows Connector is currently not compatible with the following software:

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

The AMP for Endpoints Connector does not currently support the following proxy configurations:

- Websense NTLM credential caching. The currently supported workaround for AMP for Endpoints is either to disable NTLM credential caching in Websense or allow the AMP for Endpoints 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 AMP for Endpoints Connector.

- Kerberos / GSSAPI authentication. The currently supported workaround is to use either Basic or NTLM authentication.

AMP for Endpoints Mac Connector

The following are the minimum system requirements for the AMP for Endpoints Mac Connector based on the operating system. The AMP for Endpoints Mac Connector only supports 64-bit Macs.

Apple OS X 10.8

- 2 GB RAM
- 65 MB available hard disk space

Apple OS X 10.9

- 2 GB RAM
- 65 MB available hard disk space

Apple OS X 10.10 (requires AMP for Endpoints Mac Connector 1.0.6 or later)

- 2 GB RAM
- 65 MB available hard disk space

Apple OS X 10.11 (requires AMP for Endpoints Mac Connector 1.0.7 or later)

- 2 GB RAM
- 65 MB available hard disk space

Apple OS X 10.12 (requires AMP for Endpoints Mac Connector 1.2.4 or later)

- 2 GB RAM
- 65 MB available hard disk space

Apple macOS 10.13 (requires AMP for Endpoints Mac Connector 1.5.0 or later)

- 2 GB RAM
- 65 MB available hard disk space

Incompatible Software and Configurations

The AMP for Endpoints Mac Connector does not currently support the following proxy configurations:

- Websense NTLM credential caching: The currently supported workaround for AMP for Endpoints is either to disable NTLM credential caching in Websense or allow the AMP for Endpoints 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 AMP for Endpoints Connector.
- Kerberos / GSSAPI authentication: The currently supported workaround is to use either Basic or NTLM authentication.

AMP for Endpoints Linux Connector

The following are the minimum system requirements for the AMP for Endpoints Linux Connector based on the operating system. The AMP for Endpoints Linux Connector only supports x64 architectures.

CentOS 6.4/6.5/6.6/6.7/6.8/7.2/7.3

- 1 GB RAM
- 400 MB available hard disk space

CentOS 6.9 (requires AMP for Endpoints Linux Connector 1.5.0 or later)

- 1 GB RAM
- 400 MB available hard disk space

Red Hat Enterprise Linux 6.5/6.6/6.7/6.8/7.2/7.3

- 1 GB RAM
- 400 MB available hard disk space

Red Hat Enterprise Linux 6.9 (requires AMP for Endpoints Linux Connector 1.5.0 or later)

- 1 GB RAM
- 400 MB available hard disk space

IMPORTANT! The AMP for Endpoints 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 AMP for Endpoints 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

The AMP for Endpoints Linux Connector may cause unmount failures with removable media or temporary file systems mounted in non-standard locations in Centos 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
```

The AMP for Endpoints Linux Connector does not support UEFI Secure Boot.

The AMP for Endpoints Linux Connector uses kernel modules that when loaded in Red Hat Enterprise Linux 7.x or CentOS 7.x taints the kernel. To temporarily prevent AMP from influencing kernel taint, the AMP 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 AMP service effectively disables AMP protection on this system. To disable the AMP 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 AMP service, run the commands:

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

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 AMP for Endpoints in other security apps and exclude the security apps from AMP for Endpoints

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 AMP for Endpoints 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 AMP for Endpoints Connector directory from the other security applications, particularly antivirus products.

Create exclusions for AMP for Endpoints in other security products

Creating Exclusions in McAfee Products

ePolicy Orchestrator 4.6

1. Log in to ePolicy Orchestrator.
2. Select Policy > Policy Catalog from the Menu.

3. Select the appropriate version of VirusScan Enterprise from the Product pulldown.
4. Edit your On-Access High-Risk Processes Policies.
5. Select the Exclusions tab click the Add button.
6. In the By Pattern field enter the path to your AMP for Endpoints Connector install (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) and check the Also exclude subfolders box.
7. Click OK.
8. Click Save.
9. Edit your On-Access Low-Risk Processes Policies.
10. Repeat steps 5 through 8 for this policy.

VirusScan Enterprise 8.8

1. Open the VirusScan Console.
2. Select On-Access Scanner Properties from the Task menu.
3. Select All Processes from the left pane.
4. Select the Exclusions tab.
5. Click the Exclusions button.
6. On the Set Exclusions dialog click the Add button.
7. Click the Browse button and select your AMP for Endpoints Connector install directory (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) and check the Also exclude subfolders box.
8. Click OK.
9. Click OK on the Set Exclusions dialog.
10. Click OK on the On-Access Scanner Properties dialog.

Creating Exclusions in Symantec Products

Managed Symantec Enterprise Protection 12.1

1. Log into Symantec Endpoint Protection Manager.
2. Click Policies in the left pane.
3. Select the Exceptions entry under the Policies list.
4. You can either add a new Exceptions Policy or edit an existing one.
5. Click Exceptions once you have opened the policy.
6. Click the Add button, select Windows Exceptions from the list and choose Folder from the submenu.

7. In the Add Security Risk Folder Exception dialog choose [PROGRAM_FILES] from the Prefix variable dropdown menu and enter Cisco in the Folder field. Ensure that Include subfolders is checked.
8. Under Specify the type of scan that excludes this folder menu select All.
9. Click OK.
10. Make sure that this Exception is used by all computers in your organization with the AMP for Endpoints Connector installed.

Unmanaged Symantec Enterprise Protection 12.1

1. Open SEP and click on Change Settings in the left pane.
2. Click Configure Settings next to the Exceptions entry.
3. Click the Add button on the Exceptions dialog.
4. Select Folders from the Security Risk Exception submenu.
5. Select your AMP for Endpoints Connector installation folder (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) from the dialog and click OK.
6. Click the Add button on the Exceptions dialog.
7. Select Folder from the SONAR Exception submenu.
8. Select your AMP for Endpoints Connector installation folder (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) from the dialog and click OK.
9. Click the Close button.

Creating Exclusions in Microsoft Security Essentials

1. Open Microsoft Security Essentials and click on the Settings tab.
2. Select Excluded files and locations in the left pane.
3. Click the Browse button and navigate to your AMP for Endpoints Connector installation folder (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) and click OK.
4. Click the Add button then click Save changes.
5. Select Excluded processes in the left pane.
6. Click the Browse button and navigate to the sfc.exe or agent.exe file (C:\Program Files\Sourcefire\FireAMP\x.x.x\sfc.exe by default for versions up to 5.1.1 and C:\Program Files\Cisco\AMP\x.x.x\sfc.exe for versions 5.1.1 and higher)and where x.x.x is the AMP for Endpoints Connector version number) and click OK.

7. Click the Add button then click Save changes.

IMPORTANT! Because the process exclusions in Microsoft Security Essentials require a specific path to the sfc.exe file you will need to update this exclusion whenever you upgrade to a new version of the AMP for Endpoints Connector.

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 AMP for Endpoints Cloud and tested with the AMP for Endpoints 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 AMP for Endpoints 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.

AMP for Endpoints Windows Firewall Exceptions

North America

The firewall 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.immunet.com
- **Endpoint IOC Downloads** - ioc.amp.cisco.com
- **Advanced Custom Signatures** - custom-signatures.amp.cisco.com
- **Connector Upgrades** - upgrades.amp.cisco.com
- **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 AMP for Endpoints 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 AMP for Endpoints Connectors you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - update.amp.cisco.com

European Union

Companies located in the European Union must allow connectivity from the Connector to the following servers over HTTPS:

- **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.sourcefire.com
- **Endpoint IOC Downloads** - ioc.eu.amp.cisco.com
- **Advanced Custom Signatures** - custom-signatures.eu.amp.cisco.com
- **Connector Upgrades** - upgrades.amp.cisco.com
- **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 AMP for Endpoints 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 AMP for Endpoints Connectors you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - update.amp.cisco.com

Asia Pacific, Japan, and Greater China

Companies located in the Asia Pacific, Japan, and Greater China region must allow connectivity from the Connector to the following servers over HTTPS:

- **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.sourcefire.com
- **Endpoint IOC Downloads** - ioc.apjc.amp.cisco.com
- **Advanced Custom Signatures** - custom-signatures.apjc.amp.cisco.com
- **Connector Upgrades** - upgrades.amp.cisco.com
- **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 AMP for Endpoints 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 AMP for Endpoints Connectors you must allow access to the following server over TCP 80 for signature updates:

Update Server - update.amp.cisco.com

AMP for Endpoints Mac Firewall Exceptions

North America

The firewall 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.sourcefire.com
- **Connector Upgrades** - upgrades.amp.cisco.com
- **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 AMP for Endpoints 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 AMP for Endpoints Mac Connectors you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - defs.amp.sourcefire.com

European Union

Companies located in the European Union must allow connectivity from the Connector to the following servers over HTTPS:

- **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.sourcefire.com
- **Connector Upgrades** - upgrades.amp.cisco.com
- **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 AMP for Endpoints 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 AMP for Endpoints Mac Connectors you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - defs.amp.sourcefire.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:

- **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.sourcefire.com
- **Connector Upgrades** - upgrades.amp.cisco.com
- **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 AMP for Endpoints 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 AMP for Endpoints Mac Connectors you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - defs.amp.sourcefire.com

AMP for Endpoints Linux Firewall Exceptions

North America

The firewall 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

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

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

- **Update Server** - defs.amp.sourcefire.com

European Union

Companies located in the European Union must allow connectivity from the Connector to the following servers over HTTPS:

- **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.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 servers over TCP 443:

- **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 AMP for Endpoints Linux Connectors you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - defs.amp.sourcefire.com

Asia Pacific, Japan, and Greater China

Organizations located in the European Union must allow connectivity from the Connector to the following servers over HTTPS:

- **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.sourcefire.com
- **Connector Upgrades** - upgrades.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 servers over TCP 443:

- **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 AMP for Endpoints Linux Connectors you must allow access to the following server over TCP 80 for signature updates:

Update Server - defs.amp.sourcefire.com

Selecting computers for evaluation deployment

Instead of installing the AMP for Endpoints 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.

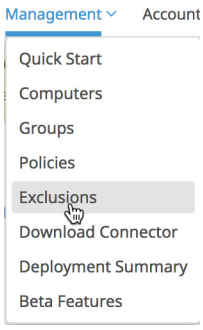
CHAPTER 2
PORTAL CONFIGURATION

Before deploying AMP for Endpoints Connectors there are tasks to complete in the AMP for Endpoints portal based on the information you gathered.

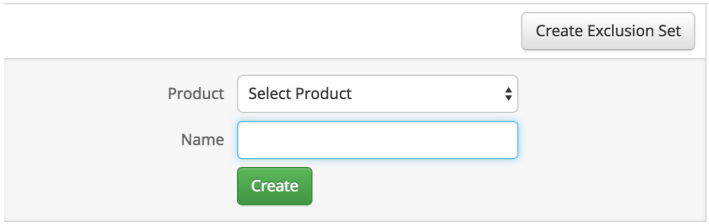
Create exclusions

To prevent conflicts between the AMP for Endpoints Connector 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.

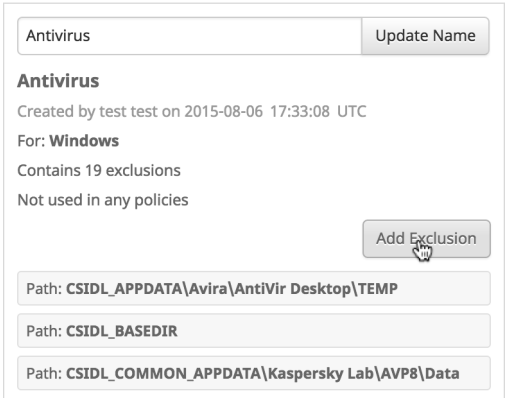
The first step is to create an exclusion by navigating to **Management > Exclusions** in the AMP for Endpoints Console.



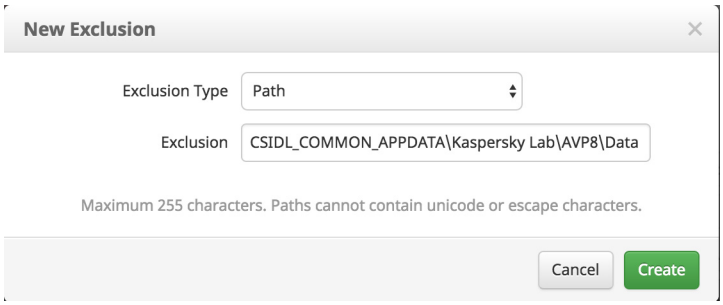
Click on **Create Exclusion Set** to create a new list of exclusions. Enter a name for the list - for example, Desktop Exclusions - and click **Create**.



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



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**.



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. Common CSIDLs are:

Symantec Endpoint Protection:

- CSIDL_COMMON_APPDATA\Symantec
- CSIDL_PROGRAM_FILES\Symantec\Symantec End Point Protection
- CSIDL_PROGRAM_FILESx86\Symantec\Symantec Endpoint Protection
- CSIDL_COMMON_APPDATA\Symantec

McAfee VirusScan Enterprise:

- CSIDL_COMMON_APPDATA\VSE
- CSIDL_PROGRAM_FILES\VSE

Trend Micro

- CSIDL_PROGRAM_FILES\Trend Micro
- CSIDL_PROGRAM_FILESX86\Trend Micro

Microsoft ForeFront

- CSIDL_PROGRAM_FILES\Microsoft Forefront
- CSIDL_PROGRAM_FILESX86\Microsoft Forefont

Microsoft Security Client

- CSIDL_PROGRAM_FILES\Microsoft Security Client
- CSIDL_PROGRAM_FILESX86\Microsoft Security Client

Sophos

- CSIDL_PROGRAM_FILES\Sophos
- CSIDL_PROGRAM_FILESX86\Sophos

Splunk:

- CSIDL_PROGRAM_FILES\Splunk

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 AMP for Endpoints Connector deals with these properly, you will want to create a Simple Custom Detection list and a Custom Whitelist 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 a Custom Whitelist, go to **Outbreak Control > Whitelisting**. Next click **Create** to create a new Custom Whitelist, name it Quick WL (or a name that you prefer), and click **Save**.

Create policies

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

Audit Only

This policy puts the AMP for Endpoints 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 AMP for Endpoints Connector that will quarantine malicious files and block malicious network connections. Once you have become familiar with the way the AMP for Endpoints 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**.
- 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**.
- If your servers are running Windows 2008 you must make sure that **Modes and Engines > TETRA** is unchecked.

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

- If your servers are running Windows 2008 you must make sure that **Modes and Engines > TETRA** is unchecked.

  WARNING! When installing the AMP for Endpoints Connector on a domain controller 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 AMP for Endpoints 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 whitelist from gold master

If you have a gold master image available it is advisable to use it to whitelist applications. You can use a tool like md5deep to generate SHA-256 values for all the applications and add them to your Quick WL whitelist.

Download installer

Now that you have created your policies and associated them with groups you can begin deploying the AMP for Endpoints 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 whitelisted and proper exclusions were created. Any detections will still trigger alerts in the AMP for Endpoints 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 whitelist. Once you are satisfied with the performance of the AMP for Endpoints 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 AMP FOR ENDPOINTS CONNECTOR

Now you are ready to begin deploying the AMP for Endpoints Connector to your evaluation computers.

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.

  WARNING! 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.

  WARNING! 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.

- /overridepolicy 1 - Replace existing policy.xml file when installing over a previous Connector install.
- /overridepolicy 0 - Do not replace existing policy.xml file when installing over a previous Connector install.
- /temppath - Used to specify the path to use for temporary files created during installation. For example, /temppath (c:\somepath\my temporary folder). This switch is only available in AMP for Endpoints Windows 5.0 and higher.

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 AMP for Endpoints 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.

AMP for Endpoints 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.

Installer exit codes

Administrators who use the command line switches to install the AMP for Endpoints 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 AMP for Endpoints 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).

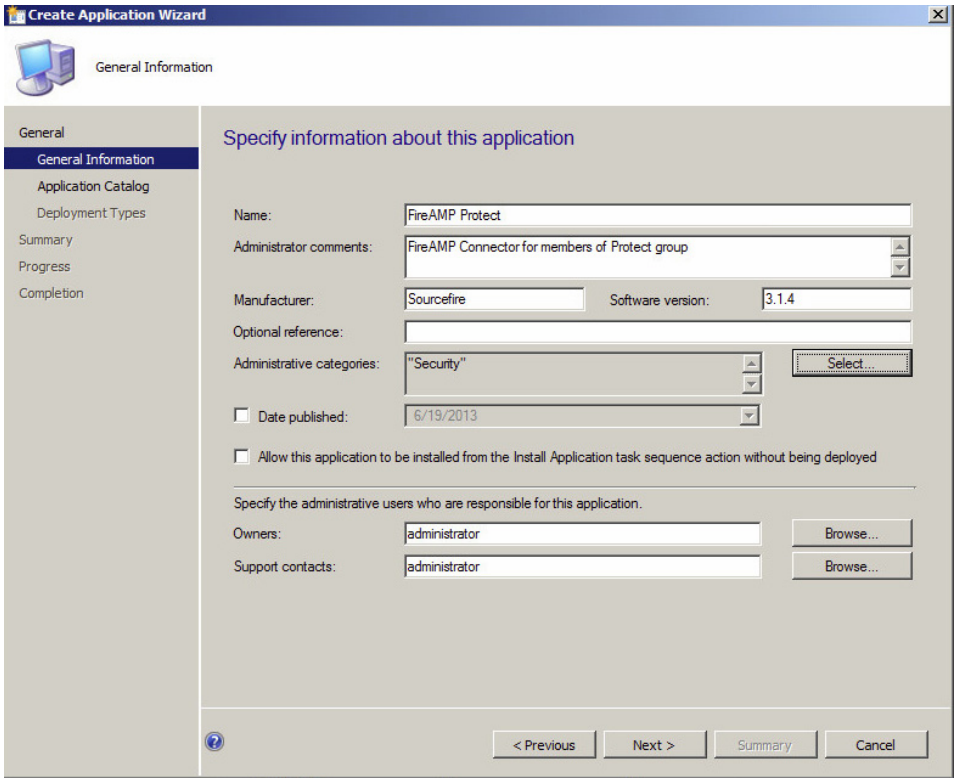
Deployment

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.

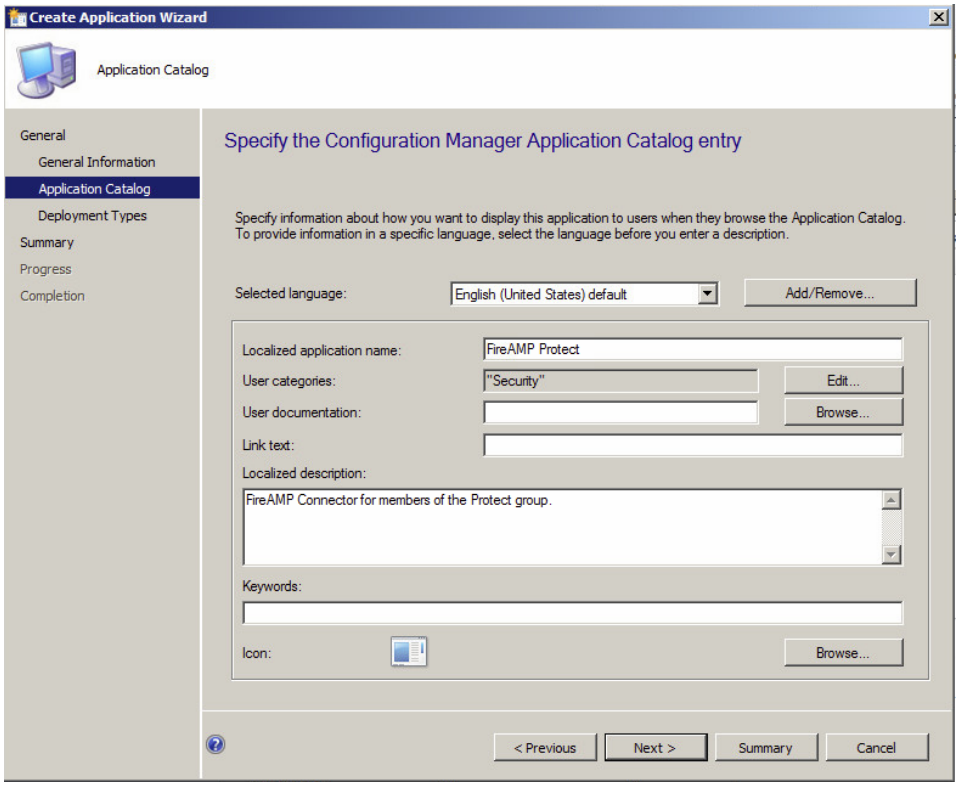
Microsoft System Center Configuration Manager

To install the AMP for Endpoints Connector using Microsoft System Center Configuration Manager (SCCM) you will first need to download the redistributable installer for each of your groups.

1. Go to **Management > Download Connector** and select one of your groups, make sure to check the **Create Redistributable Installer** box, then click **Download**. The downloaded file will include the name of the group to make it easily identifiable, for example Protect-FireAMPSetup.exe.
2. Create an AMP for Endpoints folder in the shared source file directory on your SCCM server and copy the installer files to that folder.
3. Next, open your Configuration Manager Console and navigate to Software Library > Overview > Application Management > Applications and click Create Application.
4. On the first screen of the Create Application Wizard, select “Manually specify the application information” and click Next.
5. Enter identifying information for your application package. If you plan to deploy multiple group versions of the AMP for Endpoints Connector it is a good idea to use the group name to easily differentiate them in your software library. When you have entered the necessary information, click Next.

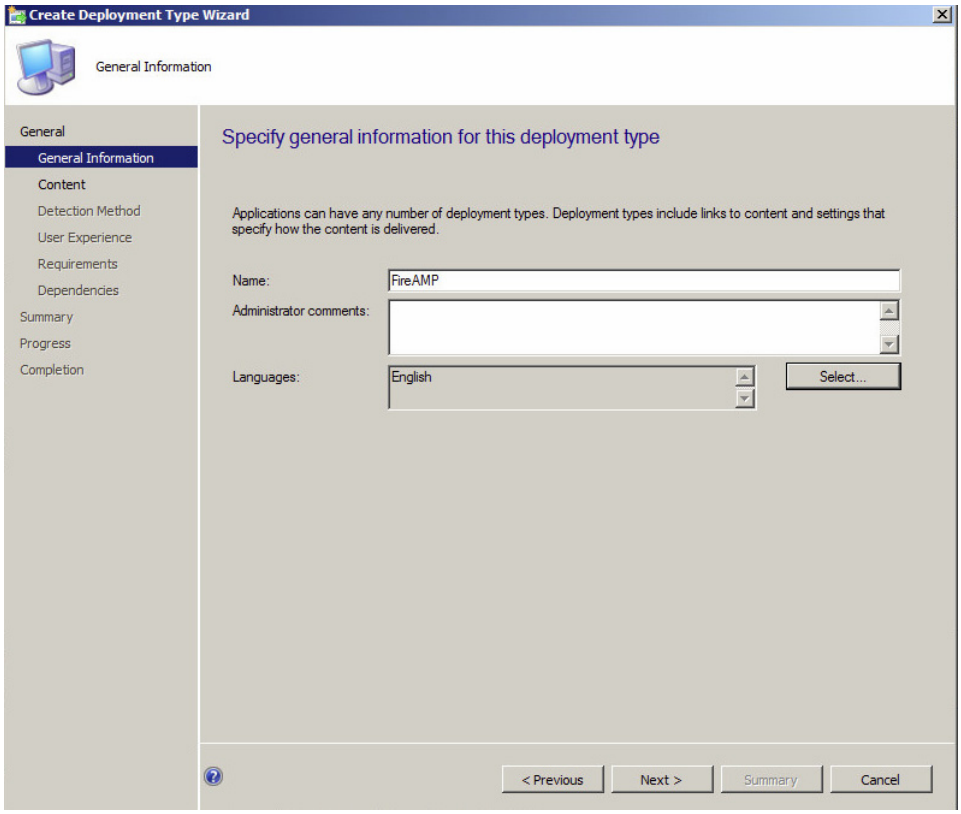


6. Enter the information available to your users in the Application Catalog. When you have entered the necessary information, click Next.

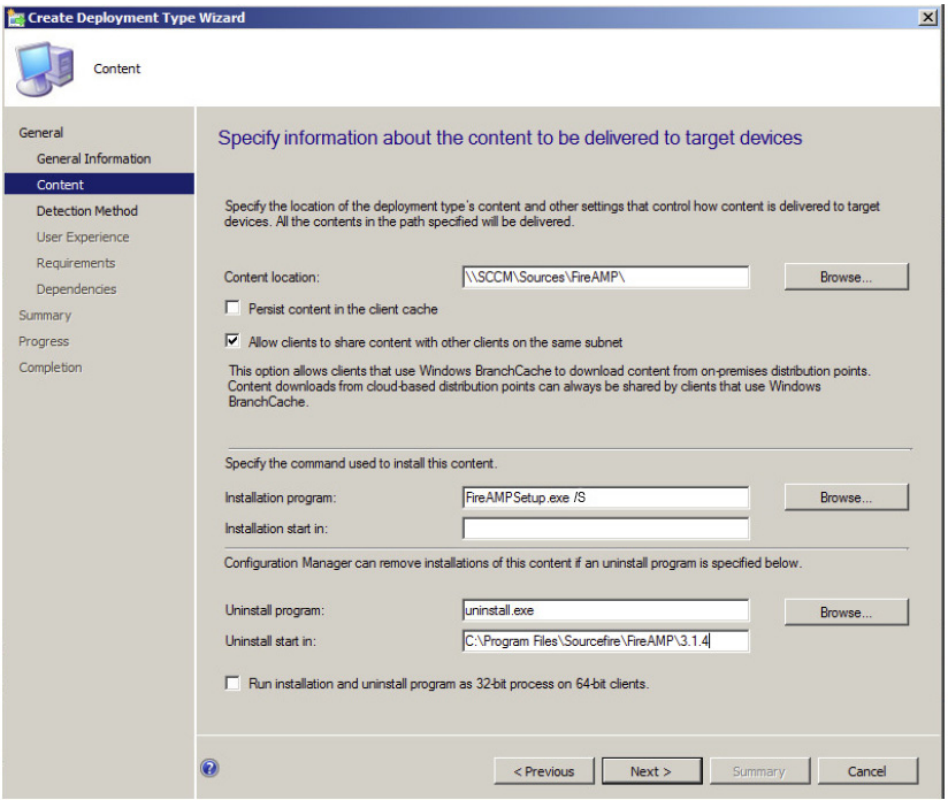


7. On the Deployment Types screen click the Add button to launch the Create Deployment Type wizard.
8. Select “Manually specify the deployment type information” and click Next.

9. Enter the application name and select languages then click Next.

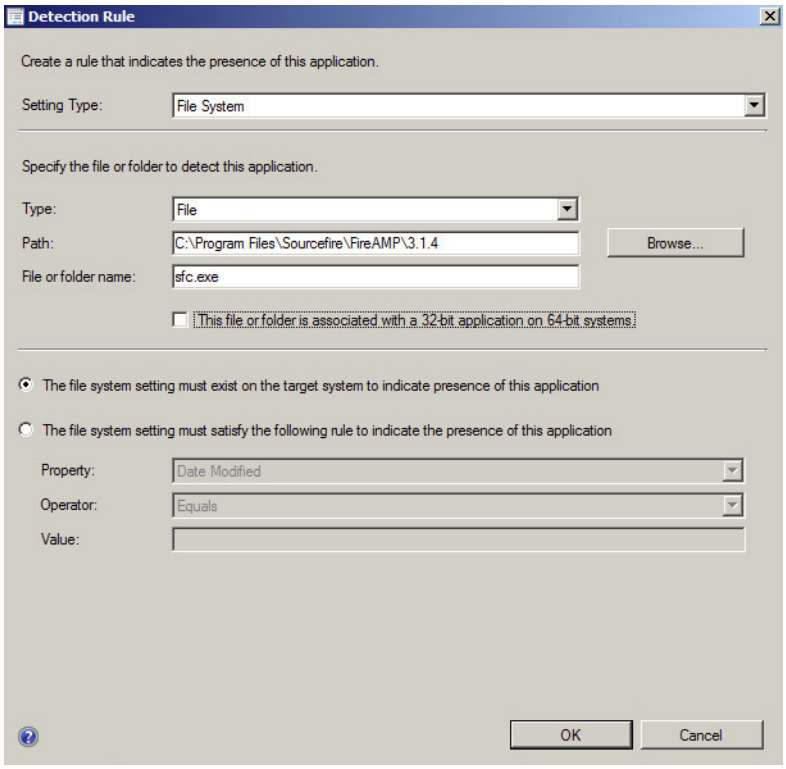


10. Enter the path to the installer files you downloaded for each of your groups in the Content location field. Enter the name of your executable installer file along with any command line switches you want to use in the Installation program field. You can also specify the Uninstall program and path (C:\Program Files\Sourcefire\FireAMP\[version]\uninstall.exe by default for versions up to 5.1.1 and C:\Program Files\Cisco\AMP\[version]\uninstall.exe for versions 5.1.1 and higher, where [version] is the Connector version installed (such as 5.1.1). Click Next to continue.

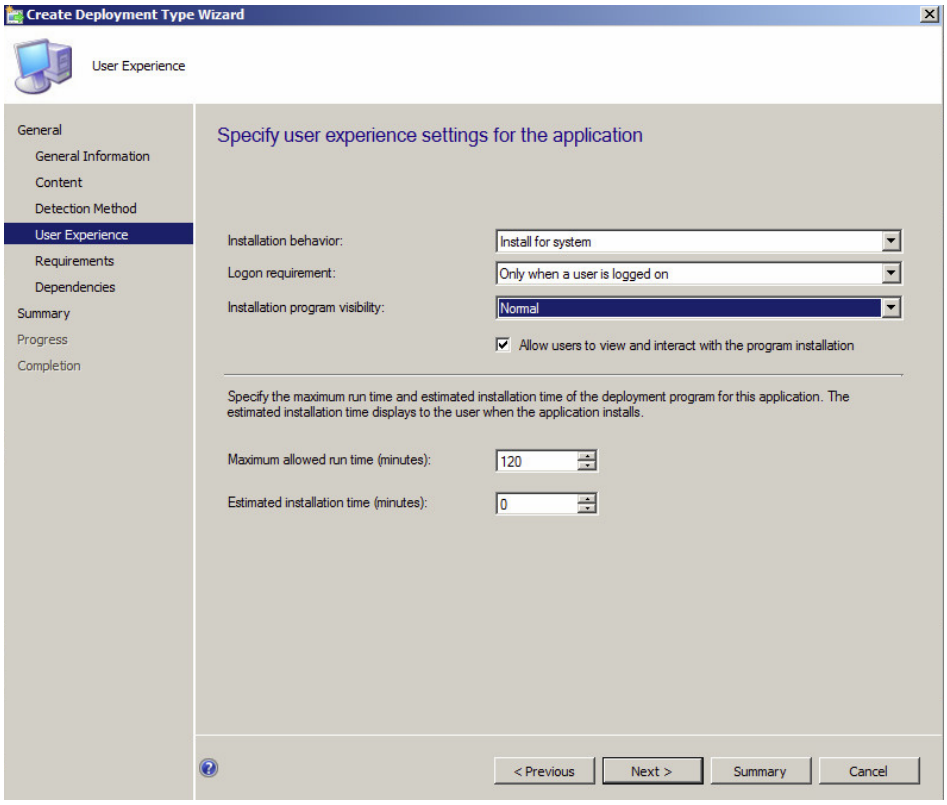


11. Click Add Clause on the Detection Method screen.

12. Select File System as the Setting Type, then File as the Type. Enter the path to where you plan on installing the AMP for Endpoints Connector on your endpoints (C:\Program Files\Sourcefire\FireAMP\[version] by default for versions up to 5.1.1 and C:\Program Files\Cisco\AMP\[version] for versions 5.1.1 and higher, where [version] is the Connector version installed (such as 5.1.1), then enter sfc.exe in the File or folder name field. Click OK, then click Next on the Detection Method page.



13. Select Install for system as the Installation behavior and Only when a user is logged on for the Logon requirement. Select the Installation program visibility setting you want, then check Allow users to view and interact with the program installation. Click Next.



14. You can choose to specify any installation requirements or simply click Next on the Requirements screen.
15. Click Next on the Dependencies screen.
16. Review your settings on the Summary screen and if you are satisfied click Next.
17. Once the wizard has completed successfully click Close to return to the Create Application Wizard. Click Next.
18. Review your settings on the Summary screen and if you are satisfied click Next.
19. Once the wizard has completed successfully click Close.

Your application will now be listed in the Software Library. Deploy the content to your Deployment Point and select whether to deploy it to Users and Groups or Devices.

CHAPTER 4
TROUBLESHOOTING

This section describes some issues that may arise after the AMP for Endpoints Connector is installed and remediation steps.

Initial Configuration Failure

Under rare circumstances the initial configuration of your AMP for Endpoints 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

AMP for Endpoints 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 AMP for Endpoints:

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 AMP for Endpoints 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 AMP for Endpoints 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 AMP for Endpoints 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 AMP for Endpoints 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 AMP for Endpoints 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 AMP for Endpoints 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 AMP for Endpoints 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! AMP for Endpoints only monitors the first 100 connections after process execution. Therefore you need to make sure that you execute a new process after you start the AMP for Endpoints 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 AMP for Endpoints Connector, reboot the computer, fix the proxy settings in the policy, download the AMP for Endpoints 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 AMP for Endpoints Connector by typing `sfc.exe -k "password"` into a command prompt as an administrator from your AMP for Endpoints 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
    - Start the AMP for Endpoints 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.

- Open the policy.xml in the file you downloaded and note the serial number.
- Change something on the policy in the portal then click Sync Policy in the AMP for Endpoints Connector Settings screen. Wait approximately 2 minutes then 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. AMP for Endpoints supports proxies, but it is important to make sure the policies are configured correctly. In this case, it's probably best to start the AMP for Endpoints 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 AMP for Endpoints Connector by typing `sfc.exe -k "password"` into a command prompt as an administrator from your AMP for Endpoints 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 AMP for Endpoints 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 an AMP for Endpoints diagnostics, the PCAP from the AMP for Endpoints 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 AMP for Endpoints 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 Business.

Gold Standard Image

When you deploy endpoints using a gold standard image that includes the AMP for Endpoints Connector, each time you deploy an endpoint a duplicate Connector will appear in your AMP for Endpoints 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 blacklist 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 AMP for Endpoints Connector by typing `sfc.exe -k "password"` into a command prompt as an administrator from your AMP for Endpoints 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 AMP for Endpoints 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.

Custom Whitelists

The Custom Whitelist allows you to whitelist 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 AMP for Endpoints Connector by typing `sfc.exe -k "password"` into a command prompt as an administrator from your AMP for Endpoints 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 AMP for Endpoints 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 Custom Whitelist 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 AMP for Endpoints Connector by typing `sfc.exe -k "password"` into a command prompt as an administrator from your AMP for Endpoints 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 AMP for Endpoints 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 AMP for Endpoints Connector you're troubleshooting is in.
2. Set **Advanced Settings > Administrative Features > Connector Log Level** to **Debug**.
3. On the AMP for Endpoints 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 AMP for Endpoints 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 AMP for Endpoints 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 AMP for Endpoints Connector version number.
6. If you are having connectivity issues with the AMP for Endpoints Connector, take a PCAP of any network activity.
7. Upload the diagnostic file and PCAP to the Cisco SSL server at https://uploads.sourcefire.com/uploads/ed14f406d34f0fbd7c1af84fe024bd1d and make sure to note the filenames when contacting support.
8. If the issue is a user interface bug or a problem with the AMP for Endpoints 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

AMP for Endpoints 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.

Indications of Compromise

AMP for Endpoints calculates devices with Indications of Compromise based on events observed over the last 7 days. 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.
- Cognitive Threat - Cisco Cognitive Threat Analytics 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 Cognitive Threat Indication of Compromise event is generated when suspicious or anomalous traffic is detected in your organization. Only threats that CTA has assigned a severity of 7 or higher are sent to AMP for Endpoints.

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 - Whitelisting.

DFC Detections

Device Flow Correlation allows you to flag or block suspicious network activity. You can use Policies to specify AMP for Endpoints 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. DFC detections include:

- DFC.CustomIPList - The computer made a connection to an IP address you have defined in a DFC IP Black 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.

APPENDIX B
SUPPORTING DOCUMENTS

The following supporting documents are available for download.

Cisco AMP for Endpoints User Guide

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

Download the User Guide

Cisco AMP for Endpoints Quick Start Guide

This guide walks through setting up groups, policies, and exclusions then deploying AMP for Endpoints Connectors. This guide is useful for evaluating AMP for Endpoints.

Download the Quick Start Guide

Cisco AMP for Endpoints Deployment Strategy Guide

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

Download the Deployment Strategy Guide

Cisco Endpoint IOC Attributes

The Endpoint IOC Attributes document details IOC attributes supported by the Endpoint IOC scanner included in the AMP for Endpoints Connector. Sample IOC documents that can be uploaded to your AMP for Endpoints Console are also included.

Download the Endpoint IOC Attributes

Cisco AMP for Endpoints API Documentation

The API allows you to access your AMP for Endpoints data and events without logging into the Console. The documentation provides descriptions of available interfaces, parameters, and examples.

View the API documentation

Cisco AMP for Endpoints Release Notes

The Release Notes contain the AMP for Endpoints change log.

Download the Release Notes

Cisco AMP for Endpoints Demo Data Stories

The Demo Data stories describe some of the samples that are shown when Demo Data is enabled in AMP for Endpoints.

Download the SFEICAR document

Download the ZAccess document

Download the ZBot document

Download the CozyDuke document

Download the Upatre document

Download the PlugX document

Download the Cryptowall document

Download the Low Prevalence Executable document

Download the Command Line Capture document

Download the Cognitive Threat Analytics (CTA) document

Download the WannaCry Ransomware document

Single Sign-On Configurations

Some identity providers require additional configuration steps to enable single sign-on with the AMP for Endpoints Console. See the documents below for instructions.

Download the Active Directory setup guide

Download the Okta setup guide

Download the Ping Federate setup guide

Cisco Universal Cloud Agreement

Cloud Offer Terms