



AMP for Endpoints Quick Start

Last Updated: December 4, 2017

Chapter 1:	Introduction.....	3
	First Use Wizard	3
	Dashboard	3
	Creating Exclusions for Antivirus Products.....	4
	Creating Antivirus Exclusions in the AMP for Endpoints Windows Connector..	4
	Creating Exclusions for the AMP for Endpoints Connector in Antivirus Software	6
	Configuring a Policy	9
	Creating Groups	9
	Deploying a Connector	10
	Downloading the Connector Installer.....	11
	Installing the Connector	11
	Firewall Connectivity	15
	Firewall Exceptions	15
	European Union Firewall Exceptions.....	16
	Asia Pacific, Japan, and Greater China Firewall Exceptions	16
	Proxies	17
Chapter 2:	Exploring AMP for Endpoints	18
	Console Menu	18
	Events.....	19
	Detections / Quarantine	20
	Restore a File From Quarantine	20
	Outbreak Control	21
	Application Control - Whitelisting.....	21
	Custom Detections - Simple.....	22
	Custom Detections - Advanced	23
	Creating Additional User Accounts	24
	Filters and Subscriptions.....	25
	Demo Data	26
Appendix A:	Threat Descriptions.....	27
	Indications of Compromise.....	27
	DFC Detections.....	28
Appendix B:	Supporting Documents	30
	Cisco AMP for Endpoints User Guide.....	30

Cisco AMP for Endpoints Quick Start Guide	30
Cisco AMP for Endpoints Deployment Strategy Guide	30
Cisco Endpoint IOC Attributes	31
Cisco AMP for Endpoints API Documentation	31
Cisco AMP for Endpoints Release Notes	31
Cisco AMP for Endpoints Demo Data Stories.....	31
Single Sign-On Configurations.....	31
Cisco Universal Cloud Agreement	32

CHAPTER 1

INTRODUCTION

AMP for Endpoints not only detects viruses, but also gives you features to clean up viruses that were missed by us and other vendors. You can create Custom Whitelists to avoid False Positives (FPs), Simple Custom Detections to control malware outbreaks, and Advanced Custom Detections for writing your own detections for tracking and removing Advanced Persistent Threats. The reporting lets you know the general security health of your computers, highlights the source of viruses entering your network and attempts to surface security issues in your environment. You can also track a series of different file types traversing your systems to provide powerful timelines for understanding the impact of malware outbreaks in your environment.

To get started with AMP for Endpoints you will need to log in at <https://console.amp.cisco.com>, download a Connector, and configure a policy. Afterwards, you may want to explore the Console's abilities to restore quarantined files, add to Custom Whitelists, create Simple Custom Detections, and push installs of Connectors to your computers.

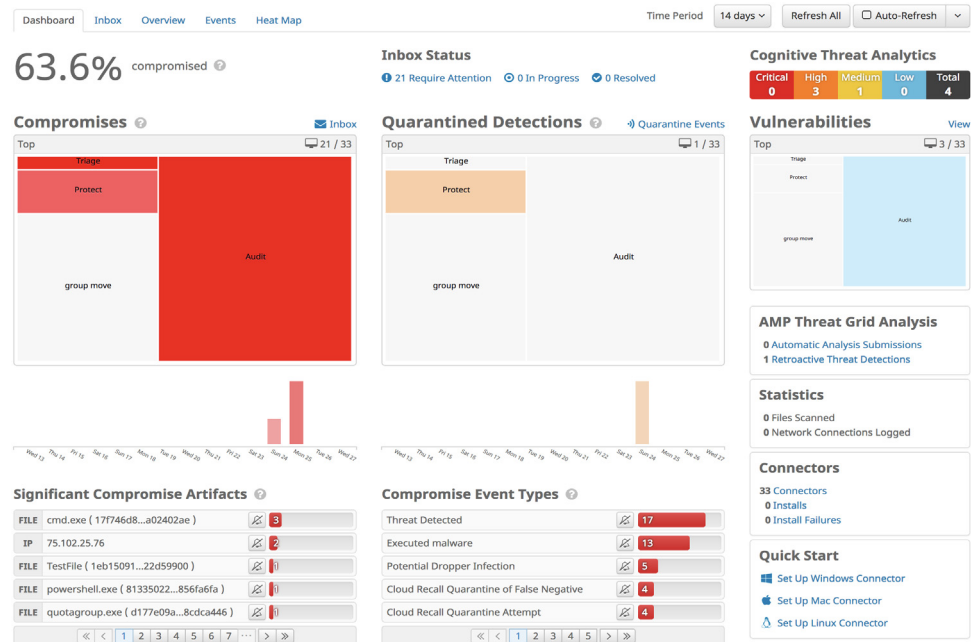
First Use Wizard

The first time you log into the AMP for Endpoints Console you will be presented with the first use wizard. This wizard can walk you through some of the steps to quickly configure your AMP for Endpoints environment by [Creating Exclusions for Antivirus Products](#), setting up [Proxies](#), [Configuring a Policy](#), and [Creating Groups](#).

Dashboard

The AMP for Endpoints Dashboard gives you a quick overview of trouble spots on devices in your environment along with updates about malware and network threat detections. From the

dashboard page you can drill down on events to gather more detailed information and remedy potential compromises.

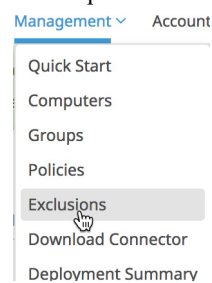


Creating Exclusions for Antivirus Products

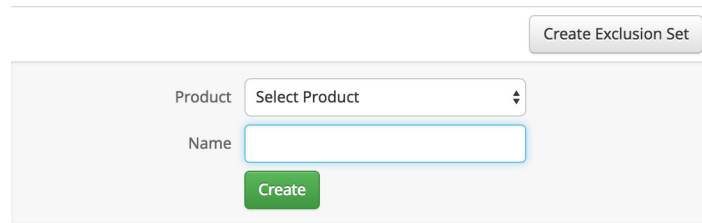
To prevent conflicts between the AMP for Endpoints Windows Connector and antivirus or other security software, you must create exclusions so that the Connector doesn't scan your antivirus directory and your antivirus doesn't scan the Connector directory. This can create problems if antivirus signatures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

Creating Antivirus Exclusions in the AMP for Endpoints Windows Connector

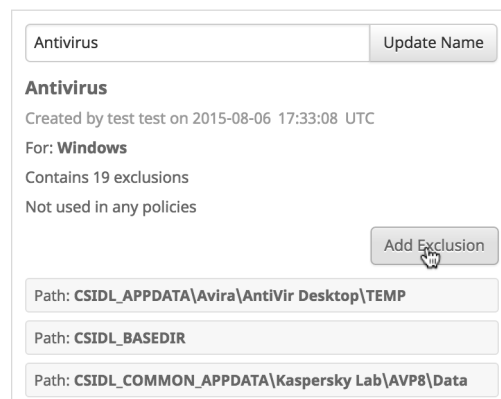
The first step is to create an exclusion by navigating to **Management > Exclusions** in the AMP for Endpoints Console.



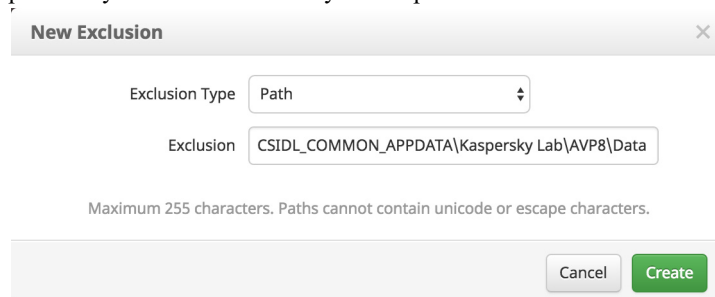
Click on **Create Exclusion Set** to create a new list of exclusions. Enter a name for the list, select whether it will be for AMP for Endpoints Windows or AMP for Endpoints Mac Connectors, and click **Create**.



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



You will then be prompted to enter a path for the exclusion. Enter the CSIDL of the security products you have installed on your endpoints then click **Create**.



IMPORTANT!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. Common CSIDLs are:

Kaspersky

- CSIDL_COMMON_APPDATA\Kaspersky Lab\AVP8\Data

McAfee VirusScan Enterprise

- CSIDL_PROGRAM_FILES\McAfee
- CSIDL_PROGRAM_FILESX86\McAfee
- CSIDL_PROGRAM_FILES\Common Files\McAfee
- CSIDL_COMMON_APPDATA\McAfee
- CSIDL_PROGRAM_FILES\VSE
- CSIDL_COMMON_APPDATA\VSE
- CSIDL_PROGRAM_FILES\Common Files\VSE

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
- CSIDL_COMMON_APPDATA\Sophos\Sophos Anti-Virus\

Splunk

- CSIDL_PROGRAM_FILES\Splunk

Symantec Endpoint Protection

- CSIDL_COMMON_APPDATA\Symantec
- CSIDL_PROGRAM_FILES\Symantec\Symantec End Point Protection
- CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection

Once you have added all the necessary exclusions for your endpoints, you will need to add the exclusion set to a policy.

IMPORTANT! CSIDLs are case sensitive.

Creating Exclusions for the AMP for Endpoints Connector in Antivirus Software

In addition to creating exclusions for antivirus products in the AMP for Endpoints Connector, you must also create exclusions for the AMP for Endpoints Connector in antivirus products running on your endpoints. The following are the steps for doing this in common antivirus products.

Creating Exclusions in McAfee 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\Cisco for versions 5.1.1 and higher or C:\Program Files\Sourcefire for previous versions by default) 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.

Creating Exclusions in McAfee 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\Cisco for versions 5.1.1 and higher or C:\Program Files\Sourcefire for previous versions by default) 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 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.

Creating Exclusions in 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\Cisco for versions 5.1.1 and higher or C:\Program Files\Sourcefire for previous versions by default) 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\Cisco for versions 5.1.1 and higher or C:\Program Files\Sourcefire for previous versions by default) from the dialog and click OK.
9. Click the Close button.

Creating Exclusions for the AMP for Endpoints Connector in Microsoft Security Essentials

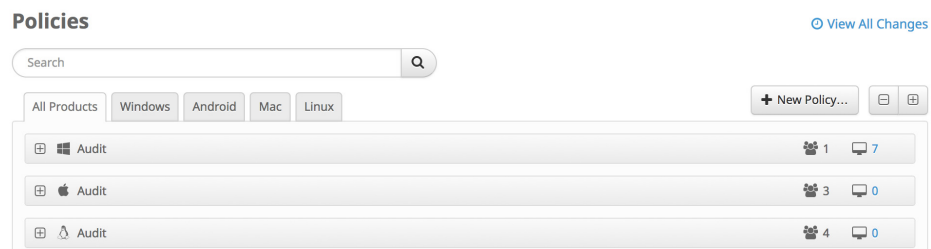
1. Open Microsoft Security Essentials and click on the Settings tab.
2. Select Excluded files and locations in the left pane.
3. Click the Browse button and navigate to your AMP for Endpoints Connector installation folder (C:\Program Files\Cisco for versions 5.1.1 and higher or C:\Program Files\Sourcefire for previous versions by default) 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 file (C:\Program Files\Cisco\AMP\x.x.x\sfc.exe for versions 5.1.1 and higher or C:\Program Files\Sourcefire\FireAMP\x.x.x\sfc.exe for previous versions by default 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.

Configuring a Policy

Policies are configuration settings that are set up for each group that you deploy the AMP for Endpoints Connector to. From the menu select **Management > Policies** to be taken to the Policy creation and configuration page.



Click **New Policy...** to create a new policy or **Duplicate** to create a new policy based on an existing one. After selecting the new policy's platform and clicking **New Policy**, you will be taken to the first of a series of configuration pages that you must complete before you can save your new policy. Fill in the settings and click **Next** to advance through the pages. Make sure to add the Custom Exclusion Set you created with your antivirus exclusions to this policy. For detailed information see our [online documentation](#).

After you have chosen your configuration settings click the **Save** button to create the policy.

Creating Groups

Now that you have a policy you can create a group that the policy will apply to. Groups allow the computers in an organization to be managed according to their function, location, or other criteria determined by the administrator.

Click **Create Group** to create a new group. Assign the group a name and give it a description, then make sure to assign the policy you previously created to it.

Name

Description

Parent Group

Windows Policy

Android Policy

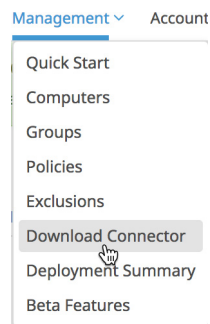
Mac Policy

Linux Policy

You can repeat this for as many groups as you would like to have in your deployment.

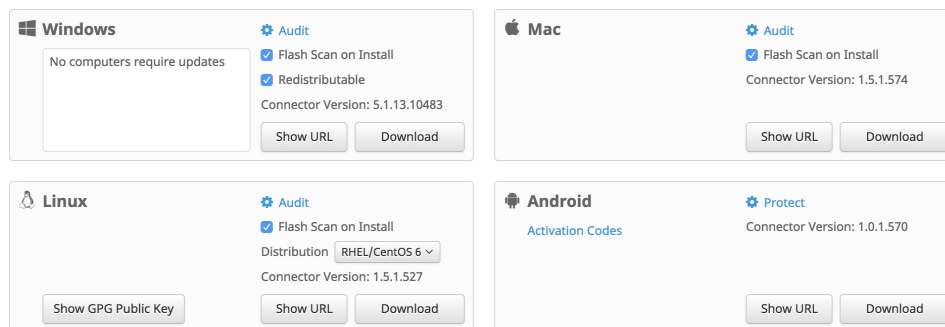
Deploying a Connector

To deploy the AMP for Endpoints Windows Connector on endpoints use the AMP for Endpoints Connector Installer. Access the installer by going to **Management > Download Connector**.



Downloading the Connector Installer

This takes you to the Download the Connector screen. Select one of the Groups you created in the previous step and click on the **Download** button to download the AMP for Endpoints Windows Installer.



IMPORTANT!For instructions on installing the AMP for Endpoints Mac, AMP for Endpoints Linux, and AMP for Endpoints Android Connectors see the [AMP for Endpoints User Guide](#).

Flash Scan on Install

Checking this option will have the AMP for Endpoints Windows Connector automatically perform a Flash Scan after it is installed and connected to the cloud. The Flash Scan is a quick scan of running processes and associated registry entries.

Redistributable

Download an installer that contains both 32-bit and 64-bit versions of the AMP for Endpoints Windows Connector. This file can be placed on a network share or pushed to all the computers in a group via a tool like System Center Configuration Manager in order to install the Connector on multiple computers.

Click the **Download** button once you have selected the Installer options. Save the file to the local computer or a network share accessible by the computers you want to install the Connector on.

IMPORTANT!When using Microsoft System Center Configuration Manager (SCCM) to deploy the Connector to Windows XP computers, you must perform an additional step. Right-click on the AMP for Endpoints Connector installer and select Properties from the context menu. Under the Environment tab, check the Allow users to interact with this program box and click OK.

Installing the Connector

Double-click the installer from the computer you want to install the Connector on. If you have your own deployment software, you may want to use command line switches to automate the deployment. Here are the available switches:

- /S - Used to put the installer into silent mode.

IMPORTANT! This must be specified as the first parameter.

- /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.

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.

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

AMP for Endpoints Windows Connector 6.0.5 and higher has a command line switch to skip the check for [Microsoft Security Advisory 3033929](#).

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

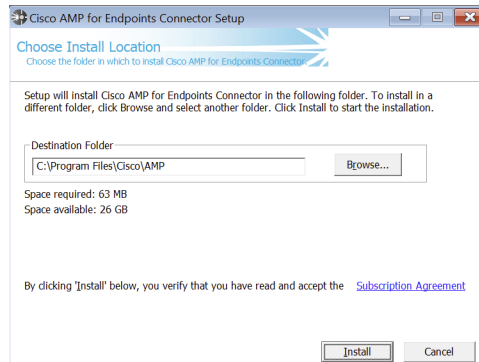
IMPORTANT!If you use this switch and do not have this KB installed, or other Windows Updates that enable SHA-2 code signing support for Windows 7 and Windows Server 2008 R2, you will encounter issues connecting to the Cisco Cloud.

If you use the command line switches to install the AMP for Endpoints Connector you should also be aware of the exit codes. They can be found in the `immpro_install.log` file in the `%TEMP%` folder.

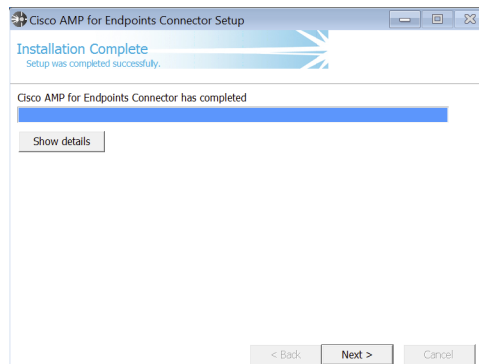
- 0 – Success
- 1500 – Installer already running
- 1618 – Another installation is already in progress.
- 1633 – Unsupported Platform (i.e. installing 32 on 64 and vice versa)
- 1638 – This version or newer version of product already exists.
- 1801 – invalid install path
- 3010 – Success (Reboot required – will only be used on upgrade)
- 16001 – Your trial install has expired.
- 16002 – A reboot is pending on the users' system 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](#)).

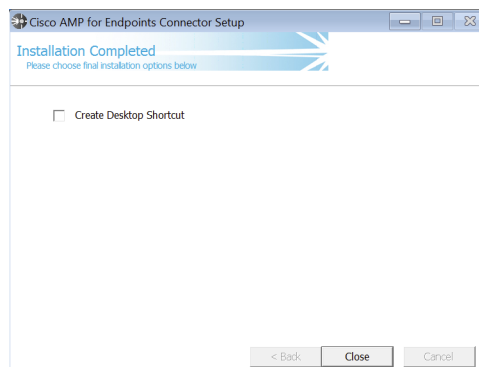
If Windows User Access Control (UAC) is enabled, the user will be presented with a prompt. Click on **Yes** to continue.



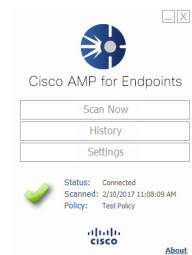
Next the user is presented with the install location dialog. In most cases the default location is the best choice. Links to the Connector End User License Agreement and Privacy Policy are also presented. Click **Install** to continue.



When the install is complete, click the **Next** button to continue.



You can leave the box checked to have an icon for the Connector created on the desktop. Click the **Close** button to complete the install. If the option to run a Flash Scan on install was selected, that scan will now execute. The Windows System Tray icon will also indicate that you are now connected to the Cisco Cloud if you selected Cloud Notifications in the policy applied to the Connector.



IMPORTANT! At this point it is extremely important to make sure you have created folder exclusions in all installed security products such as antivirus, intrusion prevention, etc. for the AMP for Endpoints Connector directories. See your antivirus software documentation for instructions. Conversely, exclusions should be created within the AMP for Endpoints Connector by adding Custom Exclusion Sets to the AMP for Endpoints Default Policy for all security and backup applications.

Firewall Connectivity

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](#).

Firewall Exceptions

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** - console.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 Firewall Exceptions

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** - console.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 Firewall Exceptions

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** - console.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

Proxies

The Connector is able to use multiple mechanisms to support proxy servers. A specific proxy server or path to a proxy auto-config (PAC) file can be defined in policy, or the Connector can discover the endpoint proxy settings from the Windows registry.

The AMP for Endpoints Connector can be set to discover endpoint proxy settings automatically. Once the Connector detects proxy setting information it attempts to connect to the AMP for Endpoints Management Server to confirm the proxy server settings are correct. The Connector will first use the proxy settings specified in the policy. If the Connector is unable to establish a connection to sourcefire.com it will attempt to retrieve proxy settings from the Windows registry on the endpoint. The Connector will attempt to retrieve the settings only from system-wide settings and not per-user settings.

If the Connector is unable to retrieve proxy settings from the Windows registry, it attempts to locate the proxy auto-configuration (PAC) file. This can be specified in policy settings or determined using Web Proxy Auto-Discovery protocol (WPAD). If the PAC file location is specified in policy it has to begin with http or https. Note that PAC files supported are only ECMAScript-based. Since all Connector communications are already encrypted, https proxy is not supported. For version 3.0.6 of the Connector, a socks proxy setting cannot be specified using a PAC file.

The Connector will attempt to rediscover proxy settings after a certain number of cloud lookups fail. This is to ensure that when laptops are outside of the enterprise network the Connector is able to connect when network proxy settings are changed.

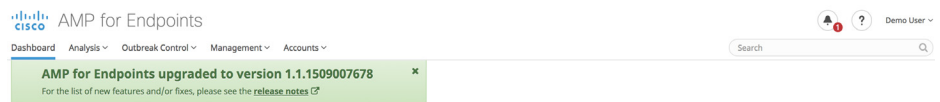
CHAPTER 2

EXPLORING AMP FOR ENDPOINTS

Now that you have configured a policy and installed a Connector we will highlight some of the other AMP for Endpoints features.

Console Menu

The menu bar at the top indicates the total number of installs and the number of malware detections in the last 7 days. The current number of system announcements is also shown at the top of the page along with a link to view previous announcements. Menu items take you to the Dashboard, Analysis, Outbreak Control, Reports, Management, and Accounts as indicated below. It also has a link to [contact Support](#), the Help system and a Logout link to end your session. The My Account link will take you directly to the Users page for your account so you can make changes.



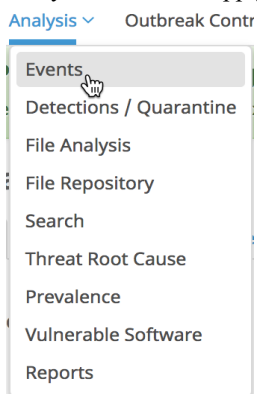
You can perform a [Search](#) from any page using the menu bar search box. There is also a global Group Filter to present a more granular view on the Dashboard Overview and Heat Map tabs, Threat Root Cause, and Deployment Summary pages.

- **Dashboard** - The Dashboard provides current information about malicious file detections and quarantines occurring within your AMP for Endpoints Connector deployment.
- **Analysis** - The Analysis menu contains items related to analysis of threats in your environment.

- **Outbreak Control** - The Outbreak Control section provides tools an administrator will need to manage malicious file outbreaks that are occurring within your AMP for Endpoints deployment.
- **Reports** - The Reports link allows you to create PDF reports based on your data.
- **Management** - The Management menu contains items that allow you to manage your AMP for Endpoints Connectors.
- **Accounts** - The purpose of the Accounts section is for managing users that have access to the AMP for Endpoints Web Interface.

Events

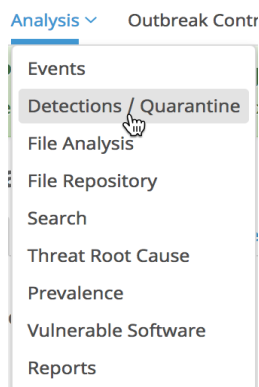
Events refer to all activity within your AMP for Endpoints deployment that is being tracked and recorded. Information such as detections, quarantines, and software installs can be viewed here. This information is also the basis for much of the reporting functionality that exists within the system. You can apply filters to the events to narrow your view.



From the menu select **Analysis > Events** and you will be taken to the Event View page.

Detections / Quarantine

Detections and Quarantines are a specific type of Event that tracks each time a malicious file is detected within your deployment. It will also show you whether or not the quarantine attempt of the malicious file succeeded or failed. You can apply filters to the list to narrow your view.



From the menu select **Analysis > Detections / Quarantine** and you will be taken to the Detections and Quarantine Events Page.

Restore a File From Quarantine

Once a malicious file detection and quarantine has occurred it may be necessary to restore the file if the detection was a false positive. This can only be done from the AMP for Endpoints Web Interface.

An example event is shown below.

Event ID	Detection	Status	Timestamp
Win7-pmr2	detected np_bad_15sept1.exe as PMRQASept15-1_NP.exe	Quarantine: Successful	2014-09-15 19:06:04 UTC
Win7-pmr2	detected np.exe as PMRQA_NP.exe	Quarantine: Successful	2014-09-13 17:34:39 UTC
Win7-pmr2	detected np.exe as PMRQA_NP.exe	Quarantine: Successful	2014-09-13 03:41:53 UTC

Clicking on the event shows the specific details of the quarantined file. Clicking on the event shows the specific details of the quarantined file.

Event ID	Detection	Status	Timestamp
Win7-pmr2	detected np_bad_15sept1.exe as PMRQASept15-1_NP.exe	Quarantine: Successful	2014-09-15 19:06:04 UTC

Field	Value
File Detection	Detection
Connector Info	Fingerprint (SHA-256)
Comments	Filename
	Filepath
	File Size (bytes)
	Parent

Unanalyzed File | Analyze | **Restore File** | All Computers | Add to Whitelist | File Trajectory

In order to restore the file on the computer named in the even, click on **Restore File** in the event entry. To restore the file on all computers that have quarantined the file, click **Restore**

File on all Computers. Files are kept in quarantine for 30 days. After that they cannot be restored.

IMPORTANT! There is a time lag of up to 30 minutes between submitting the restore request and when the file is actually restored on the computer.

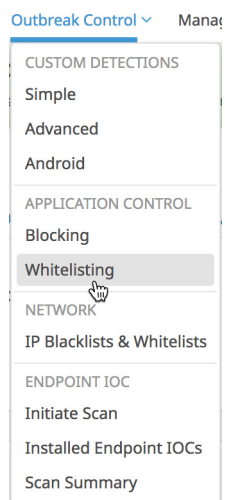
Outbreak Control

AMP for Endpoints offers a variety of lists, classified as Outbreak Control, that allow you to customize it to your needs. The main lists are Simple Custom Detections, Application Blocking, Application Whitelists, Advanced Custom Detections, and IP Blacklists and Whitelists.

Application Control - Whitelisting

Application Whitelists are user defined lists of files that the AMP for Endpoints system is instructed to assume as safe or not malicious.

Select **Outbreak Control > Whitelisting** to be taken to the Application Whitelist creation and configuration screen.



To create an Application Whitelist click the **Create** button seen below, fill in the Name information and click **Save**.

A screenshot of a form for creating an Application Whitelist. The form has a light grey background. At the top right, there is a blue 'Create' button. Below it, there is a text input field labeled 'Name' with a green 'Save' button to its right.

Click **Edit** to configure the Whitelist. The options below show the configuration selections for the Whitelist.

Test

Add SHA-256

Add a file by entering the SHA-256 of that file

SHA-256

Note

Files included

You have not added any files to this list

If you want to create a baseline of files on your computers to be whitelisted, use an application like sha256deep to extract the hashes to a file that you can upload. Suggested usage is:

```
sha256deep.exe -q -s -r -oe c:\*.*
```

Custom Detections - Simple

A Simple Custom Detection list is synonymous to a blacklist. These are files that a user wants to quarantine. Not only will an entry on the Simple Custom Detection quarantine future files, but through Retrospective it will quarantine the file on the PCs that the service has already seen it on.

To create a Simple Custom Detection list, go to **Outbreak Control > Simple**. Once there click **Create** to create a new Simple Custom Detection, give it a name, and click on **Save**.

Name

Click **Edit** to add detections to your list. The options below show the configuration selections for your Simple Custom Detection.

The screenshot shows a configuration interface for a Simple Custom Detection. At the top, there is a text input field containing the word "Test" and an "Update Name" button to its right. Below this, there are three buttons: "Add SHA-256", "Upload File", and "Upload Set of SHA-256s". A horizontal line separates these buttons from the main configuration area. The main area contains the instruction "Add a file by entering the SHA-256 of that file". Below this instruction are two text input fields: "SHA-256" and "Note". At the bottom of this section is an "Add" button. Another horizontal line separates this section from the "Files included" section. The "Files included" section has the heading "Files included" and the text "You have not added any files to this list".

Custom Detections - Advanced

Advanced Custom Detections are like traditional antivirus signatures, but they are written by the user. These signatures can inspect various aspects of a file and have different signature formats. Some of the available signature formats are:

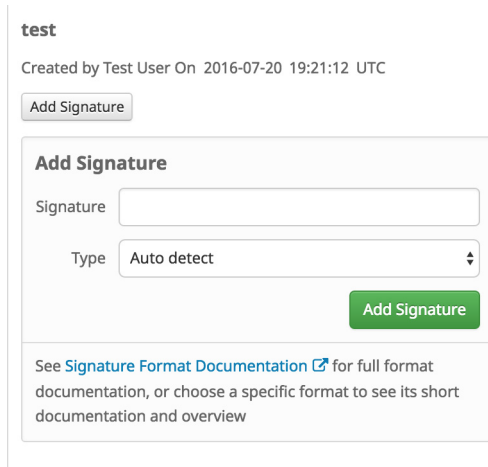
- MD5 Signatures
- MD5, PE section based Signatures
- File Body-based Signatures
- Extended Signature Format (offsets, wildcards, regular expressions)
- Logical Signatures
- Icon Signatures

For information on signature formats, please look at <http://www.clamav.net/doc/latest/signatures.pdf>. These signatures are compiled into a file downloaded to the endpoint.

In order to create Advanced Custom Detections, go to **Outbreak Control > Advanced**. Once there click on **Create Signature Set** to create a new Advanced Custom Detection set, give it a name, and click **Create**.

The screenshot shows a form for creating a signature set. It features a large empty text input field at the top right with a "Create" button. Below this, there is a "Name" label followed by a text input field and a green "Save" button.

After you create the Advanced Custom Detection set, click on **Edit** and you will see the **Add a signature** link. Enter the name of your signature and click **Create**.



The screenshot shows a web interface for adding a signature. At the top, it says "test" and "Created by Test User On 2016-07-20 19:21:12 UTC". Below this is a button labeled "Add Signature". The main form is titled "Add Signature" and contains a text input field for "Signature", a dropdown menu for "Type" currently set to "Auto detect", and a green "Add Signature" button. At the bottom of the form, there is a link to "Signature Format Documentation" with a note about full and short documentation.

Once all your signatures are listed, select **Build a Database from Signature Set**. If you accidentally add a signature you didn't want, you can delete it by clicking **Remove**.

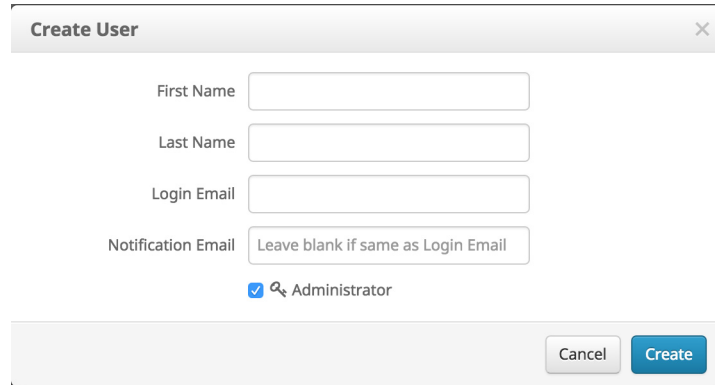
IMPORTANT! Any time you add or remove a signature you **MUST** click on **Build a Database from Signature Set**.

Creating Additional User Accounts

The Users screen allows you to manage accounts and view notifications and subscriptions for that account as well as create additional user accounts. To create a new user go to **Accounts > Users** from the menu.

Click on New User to create a new AMP for Endpoints Console user account. A valid email address is required for them to receive an account activation email. You can also add a different email address to receive notifications, for example if you want all notifications you create to go to a distribution list You must also decide if the user will be an Administrator or an unprivileged user. An Administrator has full control over all groups in the organization. If you

uncheck the Administrator box the user will only be able to view data for groups you assign to them. You can also change the user's privileges and group access later by editing their account.

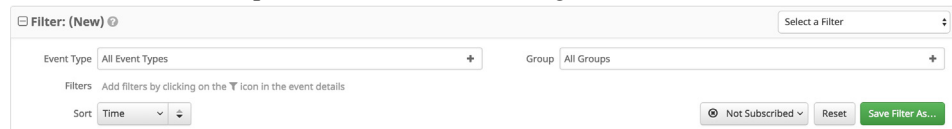


The new user should receive an activation email asking them to click on a link to activate the account and set up their password.

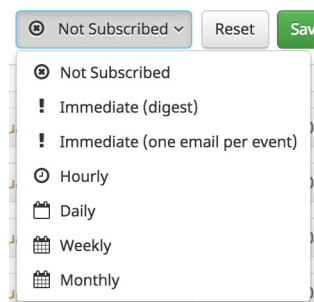
Filters and Subscriptions

The filters are shown at the top of the Events tab. You can select a previously saved filter from the drop down on the right side or add event types, groups, or specific filters from existing events. To remove a filter criteria, click the x next to the item you want to remove. You can also sort the Events list in ascending or descending order based on criteria from the drop down list. Click the **Reset** button to remove all filter criteria or click the **Save Filter As** button to save the current filtered view.

When viewing a saved filter you can update the filter and click **Save New** to save the changes as a new filter or click **Update** to overwrite the existing filter.



To subscribe to a filter view click the Not Subscribed button to show a menu with subscription timing options. You can subscribe to events with immediate, hourly, daily, weekly, or monthly notifications.



Once you have selected the notification frequency click Update to save your settings. If you no longer want to receive notifications for a filter view, switch the notification frequency to Not Subscribed and click Update.

Demo Data

Demo Data allows you to see how AMP for Endpoints works by populating your Console with replayed data from actual malware infections. This is useful for evaluating the product and demonstrating its capabilities without having to infect computers yourself.

Enabling Demo Data will add computers and events to your AMP for Endpoints Console so you can see how the Dashboard, File Trajectory, Device Trajectory, Threat Root Cause, Detections, and Events behave when malware is detected. Demo Data can coexist with live data from your AMP for Endpoints deployment, however, because of the severity of some of the Demo Data malware it may obscure real events in certain views such as the Dashboard Indications of Compromise widget.

Click on **Enable Demo Data** to populate your Console with the Demo Data.

When the Demo Data has been enabled you can click **Disable Demo Data** to remove it again.

Refresh Demo Data is similar to enabling it. When the Demo Data is enabled, refreshing it will simply refresh all the events so that they appear in the current day's events.

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.Hosted.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](#)