



Private Cloud Deployment Strategy

Last Updated: May 9, 2019

Chapter 1:	Planning	3
	System requirements and supported operating systems	4
	FireAMP Windows Connector	4
	FireAMP Mac Connector	5
	FireAMP Linux Connector	5
	Incompatible software and configurations	6
	Gather information about endpoint security	6
	Create exclusions for FireAMP in other security products	6
	Creating Exclusions in McAfee Products	6
	Creating Exclusions in Symantec Products	7
	Creating Exclusions in Microsoft Security Essentials	8
	Gather information about custom apps	8
	Gather information about proxy servers	9
	Check firewall rules	9
	European Union	9
	Selecting computers for evaluation deployment	10
 Chapter 2:	 Portal Configuration	 11
	Create exclusions	11
	Create outbreak control lists	13
	Create policies	14
	Create groups	16
	Create whitelist from gold master	17
	Download installer	17
 Chapter 3:	 Deploying the FireAMP Connector	 18
	Command line switches	18
	Installer exit codes	19
	Deployment	19
	Microsoft System Center Configuration Manager	20
 Chapter 4:	 Troubleshooting	 26
	Initial Configuration Failure	26
	Performance	26
	Outlook performance	27
	Copy, move, or execute events not in Device Trajectory	27
	Network events not in Device Trajectory	28
	Policy not updating	28
	Simple Custom Detections	29
	Custom Whitelists	29
	Application Blocking	30

	Contacting Support.....	30
Appendix A:	Threat Descriptions	32
	Indications of Compromise	32
	DFC Detections.....	33
Appendix B:	Supporting Documents	34
	Cisco FireAMP Private Cloud Console User Guide	34
	Cisco FireAMP Private Cloud User Guide	34
	Cisco FireAMP Private Cloud Quick Start Guide	34
	Cisco FireAMP Private Cloud Deployment Strategy Guide.....	34
	Cisco Endpoint IOC Attributes	35
	Cisco FireAMP Private Cloud Release Notes	35
	Cisco FireAMP Demo Data Stories.....	35

CHAPTER 3

PLANNING

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

- How many computers is the FireAMP 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 FireAMP 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 FireAMP 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 FireAMP 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 Connector based on the operating system. Operating systems not listed here are not currently supported.

FireAMP Windows Connector

The FireAMP Windows Connector supports both 32-bit and 64-bit versions of these operating systems. Additional disk space may be required when enabling certain Connector features.

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 FireAMP Windows 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 FireAMP Windows 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 and 2012 R2 (requires FireAMP Windows 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

Microsoft Windows Server 2016 (requires FireAMP Windows Connector 6.0.9 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

FireAMP Mac Connector

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

Apple OS X 10.11 (requires FireAMP Mac Connector 1.0.7 or later)

- 2 GB RAM
- 1.5 GB available hard disk space

Apple OS X 10.12 (requires FireAMP Mac Connector 1.2.4 or later)

- 2 GB RAM
- 1.5 GB available hard disk space

Apple macOS 10.13 (requires FireAMP Mac Connector 1.5.0 or later)

- 2 GB RAM
- 1.5 GB available hard disk space

FireAMP Linux Connector

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

RHEL/CentOS 6.8 (requires FireAMP Linux Connector 1.5.1 or later)

- 2 GB RAM
- 1.5 GB available hard disk space

RHEL/CentOS 6.9 (requires FireAMP Linux Connector 1.5.1 or later)

- 2 GB RAM
- 1.5 GB available hard disk space

RHEL/CentOS 7.3 (requires FireAMP Linux Connector 1.5.1 or later)

- 1 GB RAM
- 1.5 GB available hard disk space

RHEL/CentOS 7.4 (requires FireAMP Linux Connector 1.5.1 or later)

- 2 GB RAM
- 1.5 GB available hard disk space

IMPORTANT! The FireAMP 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 FireAMP Connector is currently not compatible with the following software:

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

The FireAMP Connector does not currently support the following proxy configurations:

- [Websense NTLM](#) credential caching. The currently supported workaround for FireAMP is either to disable NTLM credential caching in Websense or allow the FireAMP 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 FireAMP Connector.
- Kerberos / GSSAPI authentication. The currently supported workaround is to use either Basic or NTLM authentication.

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 FireAMP in other security apps and exclude the security apps from FireAMP

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 FireAMP Connector. By default this is C:\Program Files\Sourcefire. You will need to exclude the FireAMP Connector directory from the other security applications, particularly antivirus products.

Create exclusions for FireAMP 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 FireAMP Connector install (C:\Program Files\Sourcefire 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.

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 FireAMP Connector install directory (C:\Program Files\Sourcefire 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 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 FireAMP 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 FireAMP Connector installation folder (C:\Program Files\Sourcefire\FireAMP 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 FireAMP Connector installation folder (C:\Program Files\Sourcefire\FireAMP by default) 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 FireAMP Connector installation folder (C:\Program Files\Sourcefire\FireAMP 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 or agent.exe file (C:\Program Files\Sourcefire\FireAMP\x.x.x\sfc.exe by default where x.x.x is the FireAMP 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 FireAMP 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 FireAMP Cloud and tested with the FireAMP 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 your FireAMP Connectors to communicate with your Private Cloud device, you will need to allow access through any firewalls between the Connectors and the Cloud Proxy interface of the Private Cloud device. Refer to your FireAMP Private Cloud device configuration for the host name and port used for the Disposition Server and FireAMP interface.

(Cloud proxy and standalone-connected modes only) The firewall must allow connectivity from the Private Cloud device to the following servers on either TCP port 443 or 32137 depending on what you specify in the administration console:

- **Disposition lookups** - cloud-pc.amp.cisco.com
- **Disposition lookups, extended protocol** - cloud-pc-asn.amp.cisco.com
- **Disposition server, EP registration** - cloud-pc-est.cisco.com

To allow the Private Cloud device to perform content and software updates you must allow access to the following servers on TCP port 443:

- **Private Cloud version 2.0 and higher** - packages-v2.amp.sourcefire.com
- **Private Cloud versions prior to 2.0** - packages.amp.sourcefire.com

If you want to allow Cisco Support to connect for remote support sessions, you must allow access to the following server on TCP port 22:

- **Support server** - support-sessions.amp.sourcefire.com

European Union

(Cloud proxy and standalone-connected modes only) The firewall must allow connectivity from the Private Cloud device to the following servers on either TCP port 443 or 32137 depending on what you specify in the administration console:

- **Disposition lookups** - cloud-pc.eu.amp.cisco.com
- **Disposition lookups, extended protocol** - cloud-pc-asn.eu.amp.cisco.com
- **Disposition server, EP registration** - cloud-pc-est.eu.amp.cisco.com

To allow the Private Cloud device to perform content and software updates you must allow access to the following servers on TCP port 443:

- **Private Cloud version 2.0 and higher** - packages-v2.amp.sourcefire.com
- **Private Cloud versions prior to 2.0** - packages.amp.sourcefire.com

If you want to allow Cisco Support to connect for remote support sessions, you must allow access to the following server on TCP port 22:

- **Support server** - support-sessions.amp.sourcefire.com

Selecting computers for evaluation deployment

Instead of installing the FireAMP 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 4

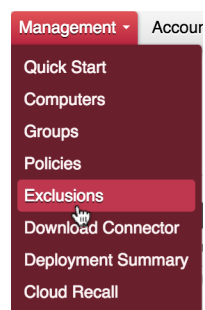
PORTAL CONFIGURATION

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

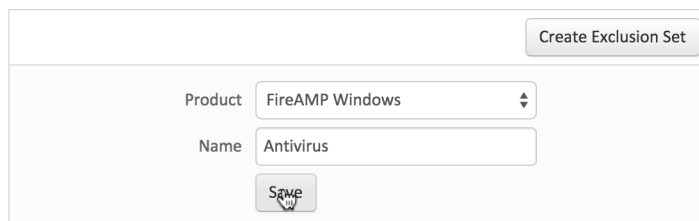
Create exclusions

To prevent conflicts between the FireAMP 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.

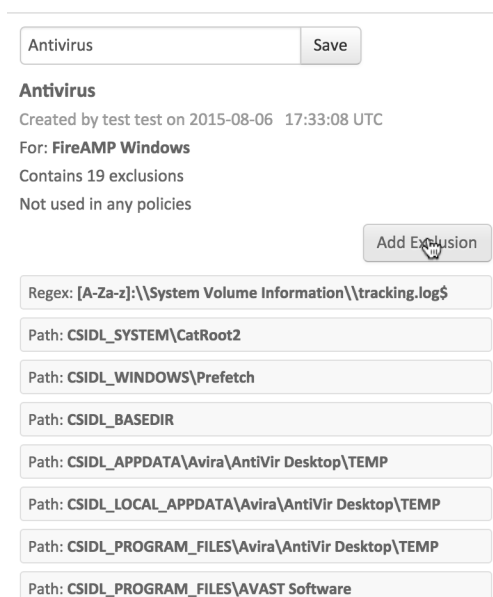
The first step is to create an exclusion by navigating to **Management > Exclusions** in the FireAMP console.



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



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



Antivirus

Save

Antivirus
Created by test test on 2015-08-06 17:33:08 UTC
For: **FireAMP Windows**
Contains 19 exclusions
Not used in any policies

Add Exclusion

Regex: [A-Za-z]:\\System Volume Information\\tracking.log\$

Path: CSIDL_SYSTEM\CatRoot2

Path: CSIDL_WINDOWS\Prefetch

Path: CSIDL_BASEDIR

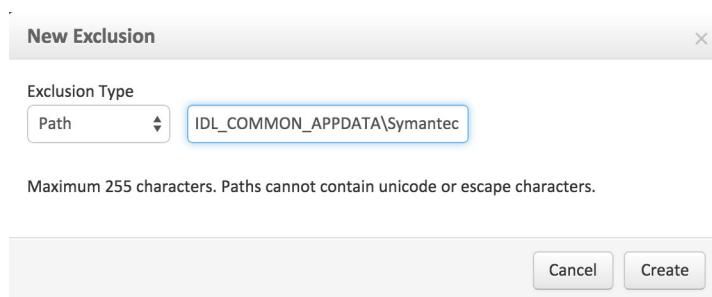
Path: CSIDL_APPDATA\Avira\AntiVir Desktop\TEMP

Path: CSIDL_LOCAL_APPDATA\Avira\AntiVir Desktop\TEMP

Path: CSIDL_PROGRAM_FILES\Avira\AntiVir Desktop\TEMP

Path: CSIDL_PROGRAM_FILES\AVAST Software

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**.



New Exclusion

Exclusion Type

Path IDL_COMMON_APPDATA\Symantec

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

Cancel Create

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 FireAMP 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 FireAMP 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 the **File > Modes > File Conviction Mode** set to **Audit**.
- The proxy server information gathered previously should be entered under **General > Proxy Settings**.
- 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 FireAMP Connector that will quarantine malicious files and block malicious network connections. Once you have become familiar with the way the FireAMP Connector behaves you can tweak this policy to your own preferences.

- This policy uses all the default policy settings.
- The proxy server information gathered previously should be entered under **General > Proxy Settings**.
- 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 the **File > Engines > Offline Engine** set to **TETRA** and with **Network > Device Flow Correlation (DFC) > Detection Action** set to **Block**.
- The proxy server information gathered previously should be entered under **General > Proxy Settings**.
- 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 the **File > Modes > File Conviction Mode** set to **Audit**.
- If your servers are running Windows 2008 you must make sure that **File > Engines > Offline Engine** is set to **Disabled**.

WARNING! When installing the FireAMP 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 **Network > Device Flow Correlation (DFC) > Enable DFC** be unchecked.

WARNING! When installing the FireAMP 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 **General > Proxy Settings**.
- 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 **File > Modes > File Conviction Mode** set to **Audit**.
- Because of authentication traffic from your network it is recommended that **Network > Device Flow Correlation (DFC) > Enable DFC** be unchecked.

WARNING! When installing the FireAMP 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 **File > Engines > Offline Engine** is set to **Disabled**.

WARNING! When installing the FireAMP 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 **General > Proxy Settings**.
- 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 FireAMP 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 FireAMP 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 FireAMP 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 FireAMP 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 5

DEPLOYING THE FIREAMP CONNECTOR

Now you are ready to begin deploying the FireAMP 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:

- /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 **Network > Device Flow Correlation (DFC) > Enable DFC** unchecked.

- /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 **File > Engines > Offline Engine** set to **Disabled**.

- /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.

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

Installer exit codes

Administrators who use the command line switches to install the FireAMP 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).

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 FireAMP 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 a FireAMP 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 FireAMP 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.

The screenshot shows the 'Create Application Wizard' window with the 'General Information' tab selected. The window title is 'Create Application Wizard'. On the left is a navigation pane with 'General Information' highlighted. The main area is titled 'Specify information about this application'. It contains several input fields: 'Name' (FireAMP Protect), 'Administrator comments' (FireAMP Connector for members of Protect group), 'Manufacturer' (Sourcefire), 'Software version' (3.1.4), 'Optional reference' (empty), 'Administrative categories' (Security), 'Date published' (6/19/2013), and a checkbox for 'Allow this application to be installed from the Install Application task sequence action without being deployed'. Below these are fields for 'Owners' and 'Support contacts', both set to 'administrator', with 'Browse...' buttons. At the bottom are '< Previous', 'Next >', 'Summary', and 'Cancel' buttons.

Field	Value
Name	FireAMP Protect
Administrator comments	FireAMP Connector for members of Protect group
Manufacturer	Sourcefire
Software version	3.1.4
Optional reference	
Administrative categories	Security
Date published	6/19/2013
Allow installation without deployment	<input type="checkbox"/>
Owners	administrator
Support contacts	administrator

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

The screenshot shows the 'Create Application Wizard' dialog box, specifically the 'Application Catalog' step. The left sidebar contains a tree view with 'General' (sub-items: General Information, Application Catalog, Deployment Types, Summary, Progress, Completion) selected. The main area is titled 'Specify the Configuration Manager Application Catalog entry'. It contains a 'Selected language:' dropdown set to 'English (United States) default' with an 'Add/Remove...' button. Below this is a section for application details: 'Localized application name:' (text box with 'FireAMP Protect'), 'User categories:' (text box with 'Security' and an 'Edit...' button), 'User documentation:' (text box with a 'Browse...' button), 'Link text:' (text box), 'Localized description:' (text area with 'FireAMP Connector for members of the Protect group.'), 'Keywords:' (text box), and 'Icon:' (icon button with a 'Browse...' button). At the bottom are navigation buttons: '< Previous', 'Next >', 'Summary', and 'Cancel'.

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.

The screenshot shows the 'Create Deployment Type Wizard' dialog box with the 'General Information' tab selected. The left sidebar lists the following steps: General, General Information (selected), Content, Detection Method, User Experience, Requirements, Dependencies, Summary, Progress, and Completion. The main area is titled 'Specify general information for this deployment type' and contains the following fields:

- Name:** A text box containing 'FireAMP'.
- Administrator comments:** A text box with a vertical scrollbar.
- Languages:** A dropdown menu showing 'English' with a 'Select...' button to its right.

At the bottom of the dialog, there are four buttons: '< Previous', 'Next >', 'Summary', and 'Cancel'. A help icon (?) is located at the bottom left of the main area.

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\3.1.4\uninstall.exe by default). Click Next to continue.

Create Deployment Type Wizard

Content

General
General Information
Content
Detection Method
User Experience
Requirements
Dependencies
Summary
Progress
Completion

Specify information about the content to be delivered to target devices

Specify the location of the deployment type's content and other settings that control how content is delivered to target devices. All the contents in the path specified will be delivered.

Content location:

☐ Persist content in the client cache

☒ Allow clients to share content with other clients on the same subnet

This option allows clients that use Windows BranchCache to download content from on-premises distribution points. Content downloads from cloud-based distribution points can always be shared by clients that use Windows BranchCache.

Specify the command used to install this content.

Installation program:

Installation start in:

Configuration Manager can remove installations of this content if an uninstall program is specified below.

Uninstall program:

Uninstall start in:

☐ Run installation and uninstall program as 32-bit process on 64-bit clients.

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 FireAMP Connector on your endpoints (C:\Program Files\Sourcefire\FireAMP\3.1.4 by default), then enter sfc.exe in the File or folder name field. Click OK, then click Next on the Detection Method page.

Detection Rule

Create a rule that indicates the presence of this application.

Setting Type: File System

Specify the file or folder to detect this application.

Type: File

Path: C:\Program Files\Sourcefire\FireAMP\3.1.4

File or folder name: sfc.exe

☐ This file or folder is associated with a 32-bit application on 64-bit systems.

☒ The file system setting must exist on the target system to indicate presence of this application

☐ The file system setting must satisfy the following rule to indicate the presence of this application

Property: Date Modified

Operator: Equals

Value:

OK Cancel

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.

Create Deployment Type Wizard

User Experience

General
General Information
Content
Detection Method
User Experience
Requirements
Dependencies
Summary
Progress
Completion

Specify user experience settings for the application

Installation behavior: Install for system

Logon requirement: Only when a user is logged on

Installation program visibility: Normal

☒ Allow users to view and interact with the program installation

Specify the maximum run time and estimated installation time of the deployment program for this application. The estimated installation time displays to the user when the application installs.

Maximum allowed run time (minutes): 120

Estimated installation time (minutes): 0

< Previous Next > Summary Cancel

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 6

TROUBLESHOOTING

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

Initial Configuration Failure

Under rare circumstances the initial configuration of your FireAMP 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

FireAMP 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 FireAMP:

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 FireAMP 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\Sourcefire\fireAMP\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 FireAMP 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 FireAMP 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.

Copy, move, or execute events not in Device Trajectory

The copy, move, and execute events come up to the Connector through the Immundet Protect driver. Then the Connector passes this information off to the disposition server to decide whether a file is malicious. Then the disposition 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 ImmuneNetProtectDriver 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 **File > Modes**. 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 **General > 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 FireAMP Connector. The Connector passes this information off to the disposition 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 "Enable DFC" on
2. Enable the "Connector Log Level" of Debug if you can see events that list the IP and port information.

IMPORTANT! FireAMP 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 FireAMP 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. If the proxy settings in the policy were mis-configured then most often you will have to uninstall the FireAMP Connector, reboot the computer, fix the proxy settings in the policy, download the FireAMP 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 Policy XML File** button. Once the XML file has been downloaded:

- Stop the FireAMP Connector by running `net stop immunetprotect` from a command prompt as an administrator.
- In the install folder (C:\Program Files\Sourcefire\FireAMP\), 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 FireAMP Connector by running `net start immunetprotect` 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 FireAMP Connector Settings screen. Wait approximately 2 minutes then check to see if the serial number has changed.

Simple Custom Detections

Simple Custom Detections allow you to manually blacklist files for detection. If **File > Modes > File Conviction Mode** 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 FireAMP Connector by running `net stop immunetprotect` from a command prompt as an administrator.
 - Go to the install directory (C:\Program Files\Sourcefire\FireAMP) and remove the `cache.*` files.
 - Start the FireAMP Connector by running `net start immunetprotect` 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 FireAMP Connector by running `net stop immunetprotect` from a command prompt as an administrator.
2. Go to the install directory (C:\Program Files\Sourcefire\FireAMP) and remove the cache.* files.
3. Start the FireAMP Connector by running `net start immunetprotect` 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 FireAMP Connector by running `net stop immunetprotect` from a command prompt as an administrator.
 - Go to the install directory (C:\Program Files\Sourcefire\FireAMP) and remove the cache.* files.
 - Start the FireAMP Connector by running `net start immunetprotect` 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 FireAMP Connector you're troubleshooting is in.
2. Under **General > Administrative Features** set **Connector Log Level** to **Debug**.

3. On the FireAMP 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 FireAMP 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 FireAMP 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 FireAMP Connector version number.
6. If you are having connectivity issues with the FireAMP 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/ed14f406d34f0fd7c1af84fe024bd1d> and make sure to note the filenames when contacting support.
8. If the issue is a user interface bug or a problem with the FireAMP 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

FireAMP 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

FireAMP 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 - An executable file was downloaded from an IP address using a non-standard port. This is often indicative of malware droppers.
- 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.

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 FireAMP 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 FireAMP Private Cloud Console User Guide

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

[Download the User Guide](#)

Cisco FireAMP Private Cloud User Guide

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

[Download the Administration Portal User Guide](#)

Cisco FireAMP Private Cloud Quick Start Guide

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

[Download the Quick Start Guide](#)

Cisco FireAMP Private Cloud Deployment Strategy Guide

This guide provides a more detailed look at preparing and planning for a production deployment of FireAMP 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 FireAMP Connector. Sample IOC documents that can be uploaded to your FireAMP Console are also included.

[Download the Endpoint IOC Attributes](#)

Cisco FireAMP Private Cloud Release Notes

The Release Notes contain the FireAMP change log.

[Download the Release Notes](#)

Cisco FireAMP Demo Data Stories

The Demo Data stories describe some of the samples that are shown when [Demo Data](#) is enabled in FireAMP.

[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](#)