



File Policies and Malware Protection

The following topics provide an overview of file control, file policies, file rules, Advanced Malware Protection (AMP), cloud connections, and dynamic analysis connections.

- [About File Policies and Advanced Malware Protection, on page 1](#)
- [Requirements and Prerequisites for File Policies, on page 2](#)
- [License Requirements for File and Malware Policies, on page 3](#)
- [Best Practices for File Policies and Malware Detection , on page 3](#)
- [How to Configure Malware Protection, on page 6](#)
- [Cloud Connections for Malware Protection, on page 10](#)
- [File Policies and File Rules, on page 19](#)
- [Retrospective Disposition Changes, on page 34](#)
- [\(Optional\) Malware Protection with AMP for Endpoints, on page 34](#)
- [History for File Policies and Malware Protection, on page 39](#)

About File Policies and Advanced Malware Protection

To detect and block malware, use file policies. You can also use file policies to detect and control traffic by file type.

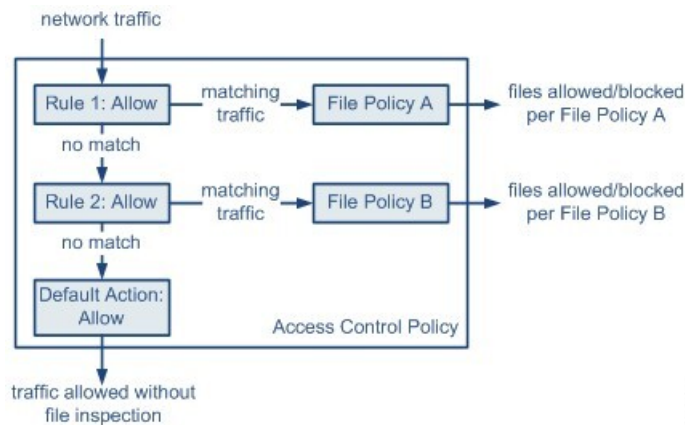
Advanced Malware Protection (AMP) for Firepower can detect, capture, track, analyze, log, and optionally block the transmission of malware in network traffic. In the Firepower Management Center web interface, this feature is called *AMP for Networks*, formerly called *AMP for Firepower*. Advanced Malware Protection identifies malware using managed devices deployed inline and threat data from the Cisco cloud.

You associate file policies with access control rules that handle network traffic as part of your overall access control configuration.

When the system detects malware on your network, it generates file and malware events. To analyze file and malware event data, see [File/Malware Events and Network File Trajectory](#).

File Policies

A file policy is a set of configurations that the system uses to perform malware protection and file control, as part of your overall access control configuration. This association ensures that before the system passes a file in traffic that matches an access control rule's conditions, it first inspects the file. Consider the following diagram of a simple access control policy in an inline deployment.



371859

The policy has two access control rules, both of which use the Allow action and are associated with file policies. The policy's default action is also to allow traffic, but without file policy inspection. In this scenario, traffic is handled as follows:

- Traffic that matches Rule 1 is inspected by File Policy A.
- Traffic that does not match Rule 1 is evaluated against Rule 2. Traffic that matches Rule 2 is inspected by File Policy B.
- Traffic that does not match either rule is allowed; you cannot associate a file policy with the default action.

By associating different file policies with different access control rules, you have granular control over how you identify and block files transmitted on your network.

Requirements and Prerequisites for File Policies

Model Support

Any

Supported Domains

Any

User Roles

- Admin
- Access Admin

License Requirements for File and Malware Policies

To Do This	License Required	File Rule Action
Block or allow all files of a particular type (for example, block all .exe files)	Threat (for FTD devices) Protection (for Classic devices)	Allow, Block, Block with Reset
Selectively allow or block files based on a judgment that it contains or is likely to contain malware	Threat (for FTD devices) Protection (for Classic devices) Malware	Malware Cloud Lookup, Block Malware
Store files	Threat (for FTD devices) Protection (for Classic devices) Malware	Any file rule action with Store Files selected

For details about Malware licenses, see:

- [Malware Licenses for Firepower Threat Defense Devices](#)
- [Malware Licenses for Classic Devices](#)

Best Practices for File Policies and Malware Detection

In addition to the items described below, follow the steps in [How to Configure Malware Protection, on page 6](#) and referenced topics.

File Rule Best Practices

Note the following guidelines and limitations when configuring file rules:

- A rule configured to block files in a passive deployment does not block matching files. Because the connection continues to transmit the file, if you configure the rule to log the beginning of the connection, you may see multiple events logged for this connection.
- A policy can include multiple rules. When you create the rules, ensure that no rule is "shadowed" by a previous rule.
- The file types supported for dynamic analysis are a subset of the file types supported for other types of analysis. To view the file types supported for each type of analysis, navigate to the file rule configuration page, select the **Block Malware** action, and select the checkboxes of interest.

To ensure that the system examines all file types, create separate rules (within the same policy) for dynamic analysis and for other types of analysis.

- If a file rule is configured with a **Malware Cloud Lookup** or **Block Malware** action and the Firepower Management Center cannot establish connectivity with the AMP cloud, the system cannot perform any configured rule action options until connectivity is restored.
- Cisco recommends that you enable **Reset Connection** for the **Block Files** and **Block Malware** actions to prevent blocked application sessions from remaining open until the TCP connection resets. If you do not reset connections, the client session will remain open until the TCP connection resets itself.
- If you are monitoring high volumes of traffic, do **not** store all captured files, or submit all captured files for dynamic analysis. Doing so can negatively impact system performance.
- You cannot perform malware analysis on all file types detected by the system. After you select values from the **Application Protocol**, **Direction of Transfer**, and **Action** drop-down lists, the system constrains the list of file types.

File Detection Best Practices

Consider the following notes and limitations for file detection:

- If adaptive profiling is not enabled, access control rules cannot perform file control, including AMP.
- If a file matches a rule with an application protocol condition, file event generation occurs after the system successfully identifies a file's application protocol. Unidentified files do not generate file events.
- FTP transfers commands and data over different channels. In a passive or inline tap mode deployment, the traffic from an FTP data session and its control session may not be load-balanced to the same internal resource.
- If the total number of bytes for all file names for files in a POP3, POP, SMTP, or IMAP session exceeds 1024, file events from the session may not reflect the correct file names for files that were detected after the file name buffer filled.
- When transmitting text-based files over SMTP, some mail clients convert newlines to the CRLF newline character standard. Since Mac-based hosts use the carriage return (CR) character and Unix/Linux-based hosts use the line feed (LF) character, newline conversion by the mail client can modify the size of the file. Note that some mail clients default to newline conversion when processing an unrecognizable file type.
- To detect ISO files, set the "Limit the number of bytes inspected when doing file type detection" option to a value greater than 36870, as described in [File and Malware Inspection Performance and Storage Options](#).
- .Exe files inside some .rar archives cannot be detected, including possibly rar5.

File Blocking Best Practices

Consider the following notes and limitations for file blocking:

- If an end-of-file marker is not detected for a file, regardless of transfer protocol, the file will not be blocked by a **Block Malware** rule or the custom detection list. The system waits to block the file until

the entire file has been received, as indicated by the end-of-file marker, and blocks the file after the marker is detected.

- If the end-of-file marker for an FTP file transfer is transmitted separately from the final data segment, the marker will be blocked and the FTP client will indicate that the file transfer failed, but the file will actually completely transfer to disk.
- File rules with **Block Files** and **Block Malware** actions block automatic resumption of file download via HTTP by blocking new sessions with the same file, URL, server, and client application detected for 24 hours after the initial file transfer attempt occurs.
- In rare cases, if traffic from an HTTP upload session is out of order, the system cannot reassemble the traffic correctly and therefore will not block it or generate a file event.
- If you transfer a file over NetBIOS-ssn (such as an SMB file transfer) that is blocked with a **Block Files** rule, you may see a file on the destination host. However, the file is unusable because it is blocked after the download starts, resulting in an incomplete file transfer.
- If you create file rules to detect or block files transferred over NetBIOS-ssn (such as an SMB file transfer), the system does not inspect files transferred in an established TCP or SMB session started before you deploy an access control policy invoking the file policy so those files will not be detected or blocked.
- If you configure Firepower Threat Defense high availability, and failover occurs while the original active device is identifying the file, the file type is not synced. Even if your file policy blocks that file type, the new active device downloads the file.

File Policy Best Practices

Note the following general guidelines and limitations when configuring file policies.

- You can associate a single file policy with an access control rule whose action is **Allow**, **Interactive Block**, or **Interactive Block with reset**.
- You **cannot** use a file policy to inspect traffic handled by the access control default action.
- For a new policy, the web interface indicates that the policy is not in use. If you are editing an in-use file policy, the web interface tells you how many access control policies use the file policy. In either case, you can click the text to jump to the Access Control Policies page.
- For file blocking to work, the NAP policy you apply to the access control policy must be operating in Protection mode, also known as Inline mode.
- Based on your configuration, you can either inspect a file the first time the system detects it, and wait for a cloud lookup result, or pass the file on this first detection without waiting for the cloud lookup result.
- By default, file inspection of encrypted payloads is disabled. This helps reduce false positives and improve performance when an encrypted connection matches an access control rule that has file inspection configured.

How to Configure Malware Protection

This topic summarizes the steps you must take to set up your Firepower system to protect your network from malicious software.

Procedure

- Step 1** [Plan and Prepare for Malware Protection, on page 6](#)
- Step 2** [Configure File Policies, on page 7](#)
- Step 3** [Add File Policies to Your Access Control Configuration, on page 8](#)
- Step 4** Configure network discovery policies to associate file and malware events with hosts on your network.
(Do not simply turn on network discovery; you must configure it to discover hosts on your network to build a network map of your organization.)
See [Network Discovery Policies](#) and subtopics.
- Step 5** Deploy policies to managed devices.
See [Deploy Configuration Changes](#).
- Step 6** Test your system to be sure it is processing malicious files as you expect it to.
- Step 7** [Set Up Maintenance and Monitoring of Malware Protection, on page 10](#)
-

What to do next

- (Optional) To further enhance detection of malware in your network, deploy and integrate Cisco's AMP for Endpoints product. See [\(Optional\) Malware Protection with AMP for Endpoints, on page 34](#) and subtopics.
- Understand how to investigate file and malware events.
See [File/Malware Events and Network File Trajectory](#).

Plan and Prepare for Malware Protection

This procedure is the first set of steps in the complete process for configuring your system to provide malware protection.

Procedure

- Step 1** Purchase and install licenses.
See [License Requirements for File and Malware Policies, on page 3](#) and [Licensing the Firepower System](#).
- Step 2** Understand how file policies and malware protection fit into your access control plan.
See the chapter [Understanding Access Control](#).

- Step 3** Understand the file analysis and malware protection tools.
See [File Rule Actions, on page 26](#) and subtopics.
Consider also [Advanced and Archive File Inspection Options, on page 20](#).
- Step 4** Determine whether you will use public clouds or private (on-premises) clouds for malware protection (file analysis and dynamic analysis.)
See [Cloud Connections for Malware Protection, on page 10](#) and subtopics.
- Step 5** If you will use private (on-premises) clouds for malware protection: Purchase, deploy, and test those products.
For information, contact your Cisco sales representative or authorized reseller.
- Step 6** Configure your firewall to allow communications with your chosen clouds.
See [Security, Internet Access, and Communication Ports](#).
- Step 7** Configure connections between Firepower and the malware protection clouds (public or private).
- For the AMP cloud, see [Change AMP Options, on page 15](#).
 - If you deployed an on-premises Cisco Threat Grid appliance, see [Connect to an On-Premises Dynamic Analysis Appliance, on page 17](#). (Access to the public Threat Grid cloud does not require configuration.)
-

What to do next

Continue with the next step in the malware protection workflow:

See [How to Configure Malware Protection, on page 6](#).

Configure File Policies

Before you begin

Complete the tasks up to this point in the malware protection workflow:

See [How to Configure Malware Protection, on page 6](#).

Procedure

- Step 1** Review file policy and file rule restrictions.
See [Best Practices for File Policies and Malware Detection , on page 3](#) and subtopics.
- Step 2** Create a file policy.
See [Create or Edit a File Policy, on page 19](#).
- Step 3** Create rules within your file policy.
See [File Rules, on page 24](#) and subtopics.
- Step 4** Configure advanced options.

See [Advanced and Archive File Inspection Options, on page 20](#).

What to do next

Continue with the next step in the malware protection workflow:

See [How to Configure Malware Protection, on page 6](#).

Add File Policies to Your Access Control Configuration

An access control policy can have multiple access control rules associated with file policies. You can configure file inspection for any Allow or Interactive Block access control rule, which permits you to match different file and malware inspection profiles against different types of traffic on your network before it reaches its final destination.

Before you begin

Complete the tasks up to this point in the malware protection workflow:

See [How to Configure Malware Protection, on page 6](#).

Procedure

- Step 1** Review guidelines for file policies in access control policies. (These are different from the file rule and file policy guidelines that you looked at previously.)
Review [File and Intrusion Inspection Order](#).
- Step 2** Associate the file policy with an access control policy.
See [Configuring an Access Control Rule to Perform Malware Protection, on page 9](#)
- Step 3** Assign the access control policy to managed devices.
See [Setting Target Devices for an Access Control Policy](#).
-

What to do next

Continue with the next step in the malware protection workflow:

See [How to Configure Malware Protection, on page 6](#).

Configuring an Access Control Rule to Perform Malware Protection

**Caution**

Selecting **Detect Files** or **Block Files**, enabling or disabling **Store files** in a **Detect Files** or **Block Files** rule, or adding the first or removing the last file rule that combines the **Malware Cloud Lookup** or **Block Malware** file rule action with an analysis option (**Spero Analysis** or **MSEXE**, **Dynamic Analysis**, or **Local Malware Analysis**) or a store files option (**Malware**, **Unknown**, **Clean**, or **Custom**), restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See [Snort® Restart Traffic Behavior](#) for more information.

**Note**

Inline normalization is enabled automatically when a file policy is included in an access control rule. For more information, see [The Inline Normalization Preprocessor](#).

Before you begin

- Adaptive profiling **must** be enabled (its default state) as described in [Configuring Adaptive Profiles](#) for access control rules to perform file control, including AMP.
- You must be an Admin, Access Admin, or Network Admin user to perform this task.

Procedure

- Step 1** In the access control rule editor (from **Policies > Access Control**), choose an **Action** of **Allow**, **Interactive Block**, or **Interactive Block with reset**.
- Step 2** Click **Inspection**.
- Step 3** Choose a **File Policy** to inspect traffic that matches the access control rule, or choose **None** to disable file inspection for matching traffic.
- Step 4** (Optional) Disable logging of file or malware events for matching connections by clicking **Logging** and unchecking **Log Files**.
Note Cisco recommends that you leave file and malware event logging enabled.
- Step 5** Save the rule.
- Step 6** Click **Save** to save the policy.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Related Topics

[Create or Edit a File Policy](#), on page 19
[Snort® Restart Scenarios](#)

Set Up Maintenance and Monitoring of Malware Protection

Ongoing maintenance is essential for protecting your network.

Before you begin

Configure your system to protect your network from malware.

See [How to Configure Malware Protection, on page 6](#) and referenced procedures.

Procedure

- Step 1** Ensure that your system always has the most current and effective protection.
See [Maintain Your System: Update File Types Eligible for Dynamic Analysis, on page 19](#).
- Step 2** Configure alerts for malware-related events and health monitoring.
See [Configuring AMP for Networks Alerting](#) and information in [Health Monitoring](#) about the following modules:
- Local Malware Analysis
 - Security Intelligence
 - Intrusion and File Event Rate
 - AMP for Firepower Status
 - AMP for Endpoints Status
-

What to do next

Review "What to do next items" in the malware protection workflow:

See [How to Configure Malware Protection, on page 6](#).

Cloud Connections for Malware Protection

Connections to public or private clouds are required in order to protect your network from malware.

AMP Clouds

The Advanced Malware Protection (AMP) cloud is a Cisco-hosted server that uses big data analytics and continuous analysis to provide intelligence that the system uses to detect and block malware on your network.

The AMP cloud provides dispositions for possible malware detected in network traffic by managed devices, as well as data updates for local malware analysis and file pre-classification.

If your organization has deployed AMP for Endpoints and configured Firepower to import its data, the system imports this data from the AMP cloud, including scan records, malware detections, quarantines, and indications of compromise (IOC).

Cisco offers the following options for obtaining data from the Cisco cloud about known malware threats:

- **AMP public cloud**

Your Firepower Management Center communicates directly with the public Cisco cloud.

- **An AMP private cloud**

An AMP private cloud is deployed on your network and acts as a compressed, on-premises AMP cloud, as well as an anonymized proxy to connect to the public AMP cloud. For details, see [Cisco AMP Private Cloud, on page 13](#).

If you integrate with AMP for Endpoints, the AMP private cloud has some limitations. See [AMP for Endpoints and AMP Private Cloud, on page 36](#).

Dynamic Analysis Cloud

- **Cisco Threat Grid cloud**

Public cloud that processes eligible files that you send for dynamic analysis, and provides threat scores and dynamic analysis reports. Firepower supports 200 samples/day for Cisco Threat Grid analysis.

- **On-premises Cisco Threat Grid appliance**

If your organization's security policy does not allow the Firepower System to send files outside of your network, you can deploy an on-premises appliance. This appliance does not contact the public Cisco Threat Grid cloud.

For more information, see [Dynamic Analysis On-Premises Appliance \(Cisco Threat Grid\) , on page 17](#).

Configure Connections to AMP and Threat Grid Clouds

- [AMP Cloud Connection Configurations, on page 11](#)
- [Dynamic Analysis Connections, on page 16](#)

AMP Cloud Connection Configurations

The following topics describe AMP cloud connection configurations for different scenarios:

- [Choose an AMP Cloud, on page 12](#)
- [Connecting to an AMP Private Cloud, on page 13](#)
- [Integrate Firepower and AMP for Endpoints, on page 37](#)

The following topics are also relevant:

- [Cisco AMP Private Cloud, on page 13](#)
- [Requirements and Best Practices for AMP Cloud Connections, on page 12](#)
- [Managing Connections to the AMP Cloud \(Public or Private\) , on page 14](#)

Requirements and Best Practices for AMP Cloud Connections

Requirements for AMP Cloud Connections

You must be an Admin user to set up the AMP cloud.

To ensure your FMC can communicate with the AMP cloud, see the topics under [Security, Internet Access, and Communication Ports](#).

To use the legacy port for AMP communications, see [Communication Port Requirements](#).

AMP and High Availability

Although they share file policies and related configurations, Firepower Management Centers in a high availability pair share neither cloud connections nor captured files, file events, and malware events. To ensure continuity of operations, and to ensure that detected files' malware dispositions are the same on both Firepower Management Centers, both Active and Standby Firepower Management Centers must have access to the cloud.

In high availability configurations, you must configure AMP cloud connections independently on the Active and Standby instances of the Firepower Management Center; these configurations are not synchronized.

These requirements apply to both public and private AMP clouds.

AMP Cloud Connections and Multitenancy

In a multidomain deployment, you configure the AMP for Networks connection at the Global level only. Each Firepower Management Center can have only one AMP for Networks connection.

Choose an AMP Cloud

By default, a connection to the United States (US) AMP public cloud is configured and enabled for your Firepower system. (This connection appears in the web interface as AMP for Networks and sometimes AMP for Firepower.) You cannot delete or disable an AMP for Networks cloud connection, but you can switch between different geographical AMP clouds, or configure an AMP private cloud connection.

Before you begin

- If you will use an AMP private cloud, see [Connecting to an AMP Private Cloud, on page 13](#) instead of this topic.
- Unless Firepower is integrated with AMP for Endpoints, you can configure only one AMP cloud connection. This connection is labeled **AMP for Networks** or **AMP for Firepower**.
- If you have deployed AMP for Endpoints and you want to add one or more AMP clouds to integrate that application with Firepower, see [Integrate Firepower and AMP for Endpoints, on page 37](#).
- See [Requirements and Best Practices for AMP Cloud Connections, on page 12](#).

Procedure

- Step 1** Choose **AMP > AMP Management**.
- Step 2** Click pencil to edit the existing cloud connection.

- Step 3** From the **Cloud Name** drop-down list, choose the regional cloud nearest to your Firepower Management Center.
- Step 4** Click **Save**.

What to do next

- If your deployment is a high-availability configuration, see [Requirements and Best Practices for AMP Cloud Connections](#), on page 12.
- (Optional) [Change AMP Options](#), on page 15.

Cisco AMP Private Cloud

The Firepower Management Center must connect to the AMP cloud for disposition queries for files detected in network traffic and receipt of retrospective malware events. This cloud can be public or private.

Your organization may have privacy or security concerns that make frequent or direct connections between your monitored network and the AMP cloud difficult or impossible. In these situations, you can set up a Cisco AMP Private Cloud, a proprietary Cisco product that acts as a compressed, on-premises version of the AMP cloud, as well as a secure mediator between your network and the AMP cloud. Connecting a Firepower Management Center to an AMP private cloud disables existing direct connections to the public AMP cloud.

All connections to the AMP cloud funnel through the AMP private cloud, which acts as an anonymized proxy to ensure the security and privacy of your monitored network. This includes disposition queries for files detected in network traffic, receiving of retrospective malware events, and so on. The AMP private cloud does not share any of your endpoint data over an external connection.



Note The AMP private cloud does **not** perform dynamic analysis, nor does it support anonymized retrieval of threat intelligence for other features that rely on Cisco Collective Security Intelligence (CSI), such as URL and Security Intelligence filtering.

For information about AMP private cloud (sometimes referred to as "AMPv"), see <https://www.cisco.com/c/en/us/products/security/fireamp-private-cloud-virtual-appliance/index.html>.

Connecting to an AMP Private Cloud

Before you begin

- Configure your Cisco AMP private cloud or clouds according to the directions in the documentation for that product. During configuration, note the private cloud host name. You will need this host name in order to to configure the connection on the Firepower Management Center.
- Make sure the Firepower Management Center can communicate with the AMP private cloud, and confirm that the private cloud has internet access so it can communicate with the public AMP cloud. See the topics under [Security, Internet Access, and Communication Ports](#).
- Unless your deployment is integrated with AMP for Endpoints, each Firepower Management Center can have only one AMP cloud connection. This connection is labeled **AMP for Networks** or **AMP for Firepower**.

If you integrate with AMP for Endpoints, you can configure multiple AMP for Endpoints cloud connections.

Procedure

-
- Step 1** Choose **AMP > AMP Management**.
- Step 2** Click **Add AMP Cloud Connection**.
- Step 3** From the **Cloud Name** drop-down list, choose **Private Cloud**.
- Step 4** Enter a **Name**.
- This information appears in malware events that are generated or transmitted by AMP private cloud.
- Step 5** In the **Host** field, enter the private cloud host name that you configured when you set up the private cloud.
- Step 6** Click **Browse** next to the **Certificate Upload Path** field to browse to the location of a valid TLS or SSL encryption certificate for the private cloud. For more information, see the AMP private cloud documentation.
- Step 7** If you want to use this private cloud for both AMP for Networks and AMP for Endpoints, select the **Use for AMP for Firepower** check box.
- If you configured a different private cloud to handle AMP for Networks communications, you can clear this check box; if this is your only AMP private cloud connection, you cannot.
- In a multidomain deployment, this check box appears only in the Global domain. Each Firepower Management Center can have only one AMP for Networks connection.
- Step 8** To communicate with the AMP private cloud using a proxy, check the **Use Proxy for Connection** check box.
- Step 9** Click **Register**, confirm that you want to disable existing direct connections to the AMP cloud, and finally confirm that you want to continue to the AMP private cloud management console to complete registration.
- Step 10** Log into the management console and complete the registration process. For further instructions, see the AMP private cloud documentation.
-

What to do next

In high availability configurations, you must configure AMP cloud connections independently on the Active and Standby instances of the Firepower Management Center; these configurations are not synchronized.

Managing Connections to the AMP Cloud (Public or Private)

Use the Firepower Management Center to manage connections to public and private AMP clouds used for AMP for Networks or AMP for Endpoints or both.

You can delete a connection to a public or private AMP cloud if you no longer want to receive malware-related information from the cloud. Note that deregistering a connection using the AMP for Endpoints or AMP private cloud management console does not remove the connection from the system. Deregistered connections display a failed state on the Firepower Management Center web interface.

You can also temporarily disable a connection. When you reenable a cloud connection, the cloud resumes sending data to the system, including queued data from the disabled period.

**Caution**


For disabled connections, the public or private AMP cloud can store malware events, indications of compromise, and so on until you re-enable the connection. In rare cases—for example, with a very high event rate or a long-term disabled connection—the cloud may not be able to store all information generated while the connection is disabled.

In a multidomain deployment, the system displays connections created in the current domain, which you can manage. It also displays connections created in ancestor domains, which you cannot manage. To manage connections in a lower domain, switch to that domain. Each Firepower Management Center can have only one AMP for Networks connection, which belongs to the Global domain.

Procedure

Step 1 Select **AMP > AMP Management**.

Step 2 Manage your AMP cloud connections:

- Delete — Click **Delete** () , then confirm your choice.
- Enable or Disable — Click the slider, then confirm your choice.

What to do next

In high availability configurations, you must configure AMP cloud connections independently on the Active and Standby instances of the Firepower Management Center; these configurations are not synchronized.

Change AMP Options

Procedure

Step 1 Choose **System > Integration**.

Step 2 Click **Cisco CSI**.

Step 3 Select options:

Table 1: AMP for Networks Options

Option	Description
Enable Automatic Local Malware Detection Updates	The local malware detection engine statically analyzes and preclassifies files using signatures provided by Cisco. If you enable this option, the Firepower Management Center checks for signature updates once every 30 minutes.

Option	Description
Share URI from Malware Events with Cisco	The system can send information about the files detected in network traffic to the AMP cloud. This information includes URI information associated with detected files and their SHA-256 hash values. Although sharing is opt-in, transmitting this information to Cisco helps future efforts to identify and track malware.
Use Legacy Port 32137 for AMP for Networks	<p>By default, Firepower uses port 443/HTTPS to communicate with the AMP public or private cloud to obtain file disposition data. This option allows the system to use port 32137.</p> <p>If you updated from a previous version of the system, this option may be enabled.</p> <p>This option will be greyed out if the FMC is configured with Proxy settings.</p>

Step 4 Click **Save**.

Dynamic Analysis Connections

Requirements for Dynamic Analysis

You must be an Admin, Access Admin, or Network Admin user, and be in the global domain, to use dynamic analysis.

With the appropriate license, the Firepower system automatically has access to the Cisco Threat Grid public cloud.

Dynamic analysis requires that managed devices have direct or proxied access to the Cisco Threat Grid public cloud or an on-premises Cisco Threat Grid appliance on port 443.

See also [Which Files Are Eligible for Dynamic Analysis?](#), on page 30.

If you will connect to an on-premises Threat Grid appliance, see also the prerequisites in [Connect to an On-Premises Dynamic Analysis Appliance](#), on page 17.

Viewing the Default Dynamic Analysis Connection


By default, the Firepower Management Center can connect to the public Cisco Threat Grid cloud for file submission and report retrieval. You can neither configure nor delete this connection.

Procedure

Step 1 Choose **AMP > Dynamic Analysis Connections**.

Step 2 Click **Edit** ().

Note

For information about **Associate** () **Associate** () on the **AMP > Dynamic Analysis Connections** page, see [Enabling Access to Dynamic Analysis Results in the Public Cloud](#), on page 18.

Dynamic Analysis On-Premises Appliance (Cisco Threat Grid)

If your organization has privacy or security concerns around submitting files to the public Cisco Threat Grid cloud, you can deploy an on-premises Cisco Threat Grid appliance. Like the public cloud, the on-premises appliance runs eligible files in a sandbox environment, and returns a threat score and dynamic analysis report to the Firepower System. However, the on-premises appliance does not communicate with the public cloud, or any other system external to your network.

For more information about on-premises Cisco Threat Grid appliances, see <https://www.cisco.com/c/en/us/products/security/threat-grid/index.html>.

Connect to an On-Premises Dynamic Analysis Appliance

If you install an on-premises Cisco Threat Grid appliance on your network, you can configure a dynamic analysis connection to submit files and retrieve reports from the appliance. When configuring the on-premises appliance dynamic analysis connection, you register the Firepower Management Center to the on-premises appliance.

Before you begin

- Set up your on-premises Cisco Threat Grid appliance; see the *Cisco Threat Grid Appliance Setup and Configuration Guide*.

Documentation for this appliance is available from <https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/tsd-products-support-series-home.html>.

- If your Cisco Threat Grid appliance uses a self-signed public-key certificate, download the certificate from the Threat Grid appliance; see the *Cisco Threat Grid Appliance Administrator's Guide* for information.

If you use a certificate signed by a Certificate Authority (CA), the certificate must meet the following requirements:

- The server key and signed certificate must be installed on the Threat Grid appliance. Follow the upload instructions in the *Threat Grid Administrator's Guide*.
- If there is a multi-level signing chain of CAs, all required intermediate certificates and the root certificate must be contained in a single file that will be uploaded to the FMC.
- All certificates must be PEM-encoded.
- The file's newlines must be UNIX, not DOS.
- If you want to connect to the on-premises appliance using a proxy, configure the proxy; see [Modify FMC Management Interfaces](#).
- Managed devices must have direct or proxied access to the Cisco Threat Grid appliance on port 443.

Procedure

- Step 1** Choose **AMP > Dynamic Analysis Connections**.
- Step 2** Click **Add New Connection**.
- Step 3** Enter a **Name**.
- Step 4** Enter a **Host**.
- Step 5** Next to **Certificate Upload**, click **Browse** to upload the certificate for the on-premises appliance.
- If the Threat Grid appliance will present a self-signed certificate, upload the certificate you downloaded from that appliance.
- If the Threat Grid appliance will present a CA-signed certificate, upload the file containing the certificate signing chain.
- Step 6** If you want to use a configured proxy to establish the connection, select **Use Proxy When Available**.
- Step 7** Click **Register**.
- Step 8** Click **Yes** to display the on-premises Cisco Threat Grid appliance login page.
- Step 9** Enter your username and password to the on-premises Cisco Threat Grid appliance.
- Step 10** Click **Sign in**.
- Step 11** You have the following options:
- If you previously registered the Firepower Management Center to the on-premises appliance, click **Return**.
 - If you did not register the Firepower Management Center, click **Activate**.
-


Enabling Access to Dynamic Analysis Results in the Public Cloud

Cisco Threat Grid offers more detailed reporting on analyzed files than is available in the Firepower Management Center. If your organization has an account in the Cisco Threat Grid public cloud, you can access the Cisco Threat Grid portal directly to view additional details about files sent for analysis from your managed devices. However, for privacy reasons, file analysis details are available only to the organization that submitted the files. Therefore, before you can view this information, you must associate your Firepower Management Center with the files submitted by its managed devices.

Before you begin

You must have an account on the Cisco Threat Grid public cloud, and have your account credentials ready.

Procedure

- Step 1** Select **AMP > Dynamic Analysis Connections**.
- Step 2** Click **Associate** () in the table row corresponding to the Cisco Threat Grid public cloud.
- A Cisco Threat Grid portal window opens.
- Step 3** Sign in to the Cisco Threat Grid public cloud.
- Step 4** Click **Submit Query**.

Note Do not change the default value in the **Devices** field.

If you have difficulties with this process, contact your Cisco Threat Grid representative at Cisco TAC. It may take up to 24 hours for this change to take effect.

What to do next

After the association is activated, see [Viewing Dynamic Analysis Results in the Cisco Threat Grid Public Cloud](#).

Maintain Your System: Update File Types Eligible for Dynamic Analysis

The list of file types eligible for Dynamic Analysis is determined by the vulnerability database (VDB), which is updated periodically (but no more than once per day.) If you are an Admin user, you can update file types eligible for dynamic analysis.

To ensure that your system has the current list:

Procedure

- Step 1** Do one of the following:
- (Recommended) See [Vulnerability Database Update Automation](#)
 - Regularly check for new VDB updates, and [Manually Update the VDB](#) when needed.
- If you choose this option, we recommend that you schedule regular reminders to do this.
- Step 2** If your file policies specify individual file types instead of the **Dynamic Analysis Capable** file type category, update your file policies to use the newly supported file types.
- Step 3** If the list of eligible file types changes, deploy to managed devices.
-

File Policies and File Rules

Create or Edit a File Policy

Before you begin

If you are configuring policies for malware protection, see all required procedures in [Configure File Policies, on page 7](#).

Procedure

- Step 1** Select **Policies > Access Control > Malware & File** .

Step 2 Create a new policy, or edit an existing policy.

If you are editing an existing policy: If **View** (🔍) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Tip To make a copy of an existing file policy, click **Copy** (📋), then type a unique name for the new policy in the dialog box that appears. You can then modify the copy.

Step 3 Add one or more rules to the file policy as described in [Creating File Rules, on page 33](#).

Step 4 Optionally, select Advanced and configure advanced options as described in [Advanced and Archive File Inspection Options, on page 20](#).

Step 5 Save the file policy.

What to do next

- If you are configuring policies for malware protection, see other required procedures in [Configure File Policies, on page 7](#).
- Otherwise:
 - Add the file policy to an access control rule as described in [Add File Policies to Your Access Control Configuration, on page 8](#).
 - Deploy configuration changes; see [Deploy Configuration Changes](#).

Advanced and Archive File Inspection Options

The Advanced Settings in the file policy editor has the following general options:

- **First Time File Analysis**—Select this option to analyze first-seen files while AMP cloud disposition is pending. The file must match a rule configured to perform a malware cloud lookup and Spero, local malware, or dynamic analysis. If you deselect this option, files detected for the first time are marked with an Unknown disposition
- **Enable Custom Detection List**—Block files on the custom detection list.
- **Enable Clean List**—If enabled, this policy will allow files that are on the clean list.
- **Override AMP Cloud Disposition Based upon Threat Score**—Select an option:
 - If you select **Disabled**, the system will not override the disposition provided by the AMP Cloud.
 - If you set a threshold threat score, files with an AMP cloud verdict of Unknown are considered malware if their Dynamic Analysis score is equal to or worse than the threshold.
 - If you select a lower threshold value, you increase the number of files treated as malware. Depending on the action selected in your file policy, this can result in an increase of blocked files.
 - For numeric threat score ranges, see [Threat Scores and Dynamic Analysis Summary Reports](#).

The Advanced Settings in the file policy editor has the following archive file inspection options:

- **Inspect Archives**—Enables inspection of the contents of archive files, for archive files as large as the **Maximum file size to store** advanced access control setting.



Caution Enabling or disabling **Inspect Archives** restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See [Snort® Restart Traffic Behavior](#) for more information.

- **Block Encrypted Archives**—Blocks archive files that have encrypted contents.
- **Block Uninspectable Archives**—Blocks archive files with contents that the system is unable to inspect for reasons other than encryption. This usually applies to corrupted files, or those that exceed your specified maximum archive depth.
- **Max Archive Depth**—Blocks nested archive files that exceed the specified depth. The top-level archive file is not considered in this count; depth begins at 1 with the first nested file .

Archive Files

Archive files are files that contain other files, such as .zip or .rar files.

If any individual file in an archive matches a file rule with a block action, the system blocks the entire archive, not just the individual file.

For details about options for archive file inspection, see [Advanced and Archive File Inspection Options, on page 20](#).

Archive Files That Can Be Inspected

- **File types**

A complete list of inspectable archive file types appears in the FMC web interface on the file rule configuration page. To view that page, see [Creating File Rules, on page 33](#).

Contained files that can be inspected appears in the same page.

- **File size**

You can inspect archive files as large as the **Maximum file size to store** file policy advanced access control setting.

- **Nested archives**

Archive files can contain other archive files, which can in turn contain archive files. The level at which a file is nested is its *archive file depth*. Note that the top-level archive file is not included in the depth count; depth begins at 1 with the first nested file.

The system can inspect up to three levels of nested files beneath the outermost archive file (level 0). You can configure your file policy to block archive files that exceed that depth (or a lower maximum depth that you specify).

If you choose not to block files that exceed the maximum archive file depth of 3, when archive files that contain some extractable contents and some contents nested at a depth of 3 or greater appear in monitored traffic, the system examines and reports data only for the files it was able to inspect.

All features applicable to uncompressed files (such as dynamic analysis and file storage) are available for nested files inside archive files.

- **Encrypted files**

You can configure the system to block archives whose contents are encrypted or otherwise cannot be inspected.

- **Archives that are not inspected**

If traffic that contains an archive file is on a Security Intelligence Block list or Do Not Block list, or if the top-level archive file's SHA-256 value is on the custom detection list, the system does not inspect the contents of the archive file.

If a nested file is blocked, the entire archive is blocked; however, if a nested file is allowed, the archive is not automatically passed (depending on any other nested files and characteristics).

.Exe files inside some .rar archives cannot be detected, including possibly rar5.

Archive File Dispositions

Archive file dispositions are based on the dispositions assigned to the files inside the archive. **All** archives that contain identified malware files receive a disposition of `Malware`. Archives without identified malware files receive a disposition of `Unknown` if they contain any unknown files, and a disposition of `Clean` if they contain only clean files.

Table 2: Archive File Disposition by Contents

Archive File Disposition	Number of Unknown Files	Number of Clean Files	Number of Malware Files
Unknown	1 or more	Any	0
Clean	0	1 or more	0
Malware	Any	Any	1 or more

Archive files, like other files, may have dispositions of `Custom Detection` or `Unavailable` if the conditions for those dispositions apply.

Viewing Archive Contents and Details

If your file policy is configured to inspect archive file contents, you can use the context menu in a table on pages under the Analysis > Files menu, and the network file trajectory viewer to view information about the files inside an archive when the archive file appears in a file event, malware event, or as a captured file.

All file contents of the archive are listed in table form, with a short summary of their relevant information: name, SHA-256 hash value, type, category, and archive depth. A network file trajectory icon appears by each file, which you can click to view further information about that specific file.

Override File Disposition Using Custom Lists

If a file has a disposition in the AMP cloud that you know to be incorrect, you can add the file's SHA-256 value to a file list that overrides the disposition from the cloud:

- To treat a file as if the AMP cloud assigned a clean disposition, add the file to the *clean list*.

- To treat a file as if the AMP cloud assigned a malware disposition, add the file to the *custom detection list*.

On subsequent detection, the device either allows or blocks the file without reevaluating the file's disposition. You can use the clean list or custom detection list per file policy.



Note To calculate a file's SHA-256 value, you must configure a rule in the file policy to either perform a malware cloud lookup or block malware on matching files.

For complete information about using file lists in Firepower, see [File Lists](#).

Alternatively, if applicable, use [Centralized File Lists from AMP for Endpoints, on page 23](#).

Centralized File Lists from AMP for Endpoints

If your organization has deployed AMP for Endpoints, Firepower can use Block and Allow lists created in AMP for Endpoints when it queries the AMP cloud for file dispositions.

Requirements:

- Your organization must be using the AMP public cloud.
- Your organization has deployed AMP for Endpoints.
- You have registered your Firepower system to AMP for Endpoints using the procedure in [Integrate Firepower and AMP for Endpoints, on page 37](#).

To create and deploy these lists, see the documentation or online help for AMP for Endpoints.



Note File lists created in Firepower override file lists created in AMP for Endpoints.

Managing File Policies

The File Policies page displays a list of existing file policies along with their last-modified dates. You can use this page to manage your file policies.

In a multidomain deployment, the system displays policies created in the current domain, which you can edit. It also displays policies created in ancestor domains, which you cannot edit. To view and edit policies created in a lower domain, switch to that domain.








Note The system checks for updates to the list of file types eligible for dynamic analysis (no more than once a day). If the list of eligible file types changes, this constitutes a change in the file policy; any access control policy using the file policy is marked out-of-date if deployed to any devices. You must deploy policies before the updated file policy can take effect on the device. See [Maintain Your System: Update File Types Eligible for Dynamic Analysis, on page 19](#).

Procedure

Step 1 Select **Policies > Access Control > Malware & File**.

Step 2 Manage your file policies:

- Compare—Click **Compare Policies**; see [Comparing Policies](#).
- Create — To create a file policy, click **New File Policy** and proceed as described in [Create or Edit a File Policy, on page 19](#).
- Copy — To copy a file policy, click **Copy** ().
If **View** () appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
- Delete — If you want to delete a file policy, click **Delete** () , then click **Yes** and **OK** as prompted.
If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
- Deploy—Click **Deploy**; see [Deploy Configuration Changes](#).
- Edit — If you want to modify an existing file policy, click **Edit** ().
- Report—Click **Report** (); see [Generating Current Policy Reports](#).

File Rules

A file policy, like its parent access control policy, contains rules that determine how the system handles files that match the conditions of each rule. You can configure separate file rules to take different actions for different file types, application protocols, or directions of transfer.

For example, when a file matches a rule, the rule can:

- allow or block files based on simple file type matching
- block files based on disposition (whether or not evaluation indicates that it is malicious)
- store files to the device (For information, see [Captured Files and File Storage, on page 31](#))
- submit stored (captured) files for local malware, Spero, or dynamic analysis

In addition, the file policy can:

- automatically treat a file as if it is clean or malware based on entries in the clean list or custom detection list
- treat a file as if it is malware if the file's threat score exceeds a configurable threshold
- inspect the contents of archive files (such as .zip or .rar)

- block archive files whose contents are encrypted, nested beyond a specified maximum archive depth, or otherwise uninspectable

File Rule Components

Table 3: File Rule Components

File Rule Component	Description
application protocol	The system can detect and inspect files transmitted via FTP, HTTP, SMTP, IMAP, POP3, and NetBIOS-ssn (SMB). Any , the default, detects files in HTTP, SMTP, IMAP, POP3, FTP, and NetBIOS-ssn (SMB) traffic. To improve performance, you can restrict file detection to only one of those application protocols on a per-file rule basis.
direction of transfer	<p>You can inspect incoming FTP, HTTP, IMAP, POP3, and NetBIOS-ssn (SMB) traffic for downloaded files; you can inspect outgoing FTP, HTTP, SMTP, and NetBIOS-ssn (SMB) traffic for uploaded files.</p> <p>Tip Use Any to detect files over multiple application protocols, regardless of whether users are sending or receiving.</p>
file categories and types	<p>The system can detect various types of files. These file types are grouped into basic categories, including multimedia (swf, mp3), executables (exe, torrent), and PDFs. You can configure file rules that detect individual file types, or on entire categories of file types.</p> <p>For example, you could block all multimedia files, or just ShockWave Flash (swf) files. Or, you could configure the system to alert you when a user downloads a BitTorrent (torrent) file.</p> <p>Note that executables include file types that can run macros and scripts, since these can contain malware.</p> <p>For a list of file types the system can inspect, select Policies > Access Control > Malware & File, create a temporary new file policy, then click Add Rule. Select a file type category and the file types that the system can inspect appear in the File Types list.</p> <p>Note Frequently triggered file rules can affect system performance. For example, detecting multimedia files in HTTP traffic (YouTube, for example, transmits significant Flash content) could generate an overwhelming number of events.</p>

File Rule Component	Description
file rule action	<p>A file rule's action determines how the system handles traffic that matches the conditions of the rule.</p> <p>Depending on the selected action, you can configure whether the system stores the file or performs Spero, local malware, or dynamic analysis on a file. If you select a Block action, you can also configure whether the system also resets the blocked connection.</p> <p>For descriptions of these actions and options, see File Rule Actions, on page 26.</p> <p>File rules are evaluated in rule-action, not numerical, order. For details, see File Rule Actions: Evaluation Order, on page 32.</p>

File Rule Actions

File rules give you granular control over which file types you want to log, block, or scan for malware. Each file rule has an associated action that determines how the system handles traffic that matches the conditions of the rule. To be effective, a file policy must contain one or more rules. You can use separate rules within a file policy to take different actions for different file types, application protocols, or directions of transfer.

File Rule Actions

- *Detect Files* rules allow you to log the detection of specific file types to the database, while still allowing their transmission.
- *Block Files* rules allow you to block specific file types. You can configure options to reset the connection when a file transfer is blocked, and store captured files to the managed device.
- *Malware Cloud Lookup* rules allow you to obtain and log the disposition of files traversing your network, while still allowing their transmission.
- *Block Malware* rules allow you to calculate the SHA-256 hash value of specific file types, query the AMP cloud to determine if files traversing your network contain malware, then block files that represent threats.

File Rule Action Options

Depending on the action you select, you have different options:

File Rule Action Option	Block Files capable?	Block Malware capable?	Detect Files capable?	Malware Cloud Lookup capable?
Spero Analysis* for MSEX	no	yes, you can submit executable files	no	yes, you can submit executable files
Dynamic Analysis*	no	yes, you can submit executable files with Unknown file dispositions	no	yes, you can submit executable files with Unknown file dispositions
Capacity Handling	no	yes	no	yes

File Rule Action Option	Block Files capable?	Block Malware capable?	Detect Files capable?	Malware Cloud Lookup capable?
Local Malware Analysis*	no	yes	no	yes
Reset Connection	yes (recommended)	yes (recommended)	no	no
Store files	yes, you can store all matching file types	yes, you can store file types matching the file dispositions you select	yes, you can store all matching file types	yes, you can store file types matching the file dispositions you select

* For complete information about these options, see [Malware Protection Options \(in File Rule Actions\)](#), on [page 27](#) and its subtopics.



Caution

Selecting **Detect Files** or **Block Files**, enabling or disabling **Store files** in a **Detect Files** or **Block Files** rule, or adding the first or removing the last file rule that combines the **Malware Cloud Lookup** or **Block Malware** file rule action with an analysis option (**Spero Analysis** or **MSEXE**, **Dynamic Analysis**, or **Local Malware Analysis**) or a store files option (**Malware**, **Unknown**, **Clean**, or **Custom**), restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See [Snort® Restart Traffic Behavior](#) for more information.

Malware Protection Options (in File Rule Actions)

The Firepower system applies several methods of file inspection and analysis to determine whether a file contains malware.

Depending on the options you enable in a file rule, the system inspects files using the following tools, in order:

1. [Spero Analysis](#), on [page 29](#) and [AMP Cloud Lookup](#), on [page 29](#)
2. [Local Malware Analysis](#), on [page 29](#)
3. [Dynamic Analysis](#), on [page 30](#)

For a comparison of these tools, see [Comparison of Malware Protection Options](#), on [page 27](#).

(You can also, if you choose, block all files based on their file type. For more information, see [Block All Files by Type](#), on [page 32](#).)

See also information about Cisco's AMP for Endpoints product at [\(Optional\) Malware Protection with AMP for Endpoints](#), on [page 34](#) and subtopics.

Comparison of Malware Protection Options

The following table details the benefits and drawbacks of each type of file analysis, as well as the way each malware protection method determines a file's disposition.

Analysis Type	Benefit	Limitations	Malware Identification
Spero analysis	Structural analysis of executable files, submits Spero signature to the AMP Cloud for analysis	Less thorough than local malware analysis or dynamic analysis, only for executable files	Disposition changes from Unknown to Malware only on positive identification of malware.
Local malware analysis	Consumes fewer resources than dynamic analysis, and returns results more quickly, especially if the detected malware is common	Less thorough results than dynamic analysis	Disposition changes from Unknown to Malware only on positive identification of malware.
Dynamic analysis	Thorough analysis of unknown files using Cisco Threat Grid	Eligible files are uploaded to the public cloud or an on-premises appliance. It takes some time to complete analysis	Threat score determines maliciousness of a file. Disposition can be based on the threat score threshold configured in the file policy.
Spero analysis and local malware analysis	Consumes fewer resources than configuring local malware analysis and dynamic analysis, while still using AMP cloud resources to identify malware	Less thorough than dynamic analysis, Spero analysis only for executable files	Disposition changes from Unknown to Malware only on positive identification of malware.
Spero analysis and dynamic analysis	Uses full capabilities of AMP cloud in submitting files and Spero signatures	Results obtained less quickly than if using local malware analysis	Threat score changes based on dynamic analysis results for files preclassified as possible malware. Disposition changes based on configured threat score threshold in the file policy, and from Unknown to Malware if the Spero analysis identifies malware.
Local malware analysis and dynamic analysis	Thorough results in using both types of file analysis	Consumes more resources than either alone	Threat score changes based on dynamic analysis results for files preclassified as possible malware. Disposition changes from Unknown to Malware if local malware analysis identifies malware, or based on configured threat score threshold in the file policy.

Analysis Type	Benefit	Limitations	Malware Identification
Spero analysis, local malware analysis and dynamic analysis	Most thorough results	Consumes most resources in running all three types of file analysis	Threat score changes based on dynamic analysis results for files preclassified as possible malware. Disposition changes from Unknown to Malware if Spero analysis or local malware analysis identifies malware, or based on configured threat score threshold in the file policy.
(Block transmission of all files of a specified file type)	Does not require a Malware license (This option is not technically a malware protection option.)	Legitimate files will also be blocked	(No analysis is performed.)



Note Preclassification does not itself determine a file's disposition; it is merely one of the factors that determine whether a file is eligible for Dynamic Analysis.

Spero Analysis

Spero analysis examines structural characteristics such as metadata and header information in executable files. After generating a Spero signature based on this information, if the file is an eligible executable file, the device submits it to the Spero heuristic engine in the AMP cloud. Based on the Spero signature, the Spero engine determines whether the file is malware. You can also configure rules to submit files for Spero analysis without also submitting them to the AMP cloud.

Note that you cannot manually submit files for Spero analysis.

AMP Cloud Lookup

For files that are eligible for assessment using Advanced Malware Protection, the Firepower Management Center performs a *malware cloud lookup*, querying the AMP cloud for the file's disposition based on its SHA-256 hash value.

To improve performance, the system caches dispositions returned by the cloud and uses the cached disposition for known files rather than querying the AMP cloud. For more information about this cache, see [Cached Disposition Longevity](#), on page 30.

Local Malware Analysis

Local malware analysis allows a managed device to locally inspect executables, PDFs, office documents, and other types of files for the most common types of malware, using a detection rule set provided by the Cisco Talos Intelligence Group (Talos). Because local analysis does not query the AMP cloud, and does not run the file, local malware analysis saves time and system resources.

If the system identifies malware through local malware analysis, it updates the existing file disposition from Unknown to Malware. The system then generates a new malware event. If the system does not identify malware, it does not update the file disposition from Unknown to Clean. After the system runs local malware

analysis, it caches file information such as SHA-256 hash value, timestamp, and disposition, so that if detected again within a certain period of time, the system can identify malware without additional analysis. For more information about the cache, see [Cached Disposition Longevity, on page 30](#).

Local malware analysis does not require establishing communications with the Cisco Threat Grid cloud. However, you must configure communications with the cloud to submit files for dynamic analysis, and to download updates to the local malware analysis ruleset.

Cached Disposition Longevity

Dispositions returned from an AMP cloud query, associated threat scores, and dispositions assigned by local malware analysis, have a time-to-live (TTL) value. After a disposition has been held for the duration specified in the TTL value without update, the system purges the cached information. Dispositions and associated threat scores have the following TTL values:

- Clean — 4 hours
- Unknown — 1 hour
- Malware — 1 hour

If a query against the cache identifies a cached disposition that timed out, the system re-queries the local malware analysis database and the AMP cloud for a new disposition.

Dynamic Analysis

You can configure your file policy to automatically submit files for dynamic analysis using Cisco Threat Grid (formerly AMP Threat Grid), Cisco's file analysis and threat intelligence platform.

Devices submit eligible files to Cisco Threat Grid (either the public cloud or to an on-premises appliance, whichever you have specified) regardless of whether the device stores the file.

Cisco Threat Grid runs the file in a sandbox environment, analyzes the file's behavior to determine whether the file is malicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threat score, you can view a dynamic analysis summary report with the reasons for the assigned threat score. You can also look in Cisco Threat Grid to view detailed reports for files that your organization submitted, as well as scrubbed reports with limited data for files that your organization did not submit.

For more information about Cisco Threat Grid, see <https://www.cisco.com/c/en/us/products/security/threat-grid/index.html>

To configure your system to perform dynamic analysis, see the topics under [Dynamic Analysis Connections, on page 16](#).

Which Files Are Eligible for Dynamic Analysis?

A file's eligibility for dynamic analysis depends on:

- the file type
- the file size
- the file rule's action

Additionally:

- The system submits only files that match the file rules you configure.

- The file must have a malware cloud lookup disposition of Unknown or Unavailable at the time the file is sent for analysis.
- The system must preclassify the file as potential malware.

Dynamic Analysis and Capacity Handling

Capacity handling allows you to temporarily store files that are otherwise eligible for dynamic analysis if the system is temporarily unable to submit files to the cloud, either because the device cannot communicate with the cloud or because the maximum number of submissions has been reached. The system submits the stored files when the hindering condition has passed.

Some devices can store files on the device hard drive or in a malware storage pack. See also [Malware Storage Pack, on page 32](#).

Captured Files and File Storage

The file storage feature allows you to capture selected files detected in traffic, and automatically store a copy of the file temporarily to a device's hard drive, or, if installed, to the malware storage pack.

After your device captures the files, you can:

- Store captured files on the device's hard drive for later analysis.
- Download the stored file to a local computer for further manual analysis or archival purposes.
- Manually submit eligible captured files for AMP cloud lookup or dynamic analysis.

Note that once a device stores a file, it will not re-capture it if the file is detected in the future and the device still has that file stored.

**Note**

When a file is detected for the first time on your network, you can generate a file event that represents the file's detection. However, if your file rule performs a malware cloud lookup, the system requires additional time to query the AMP cloud and return a disposition. Due to this delay, the system cannot store this file until the second time it is seen on your network, and the system can immediately determine the file's disposition.

Whether the system captures or stores a file, you can:

- Review information about the captured file from Analysis > Files > Captured Files, including whether the file was stored or submitted for dynamic analysis, file disposition, and threat score, allowing you to quickly review possible malware threats detected on your network.
- View the file's trajectory to determine how it traversed your network and which hosts have a copy.
- Add the file to the clean list or custom detection list to always treat the file as if it had a clean or malware disposition on future detection.

You configure file rules in a file policy to capture and store files of a specific type, or with a particular file disposition, if available. After you associate the file policy with an access control policy and deploy it to your devices, matching files in traffic are captured and stored. You can also limit the minimum and maximum file sizes to store.

Stored files are not included in system backups.

You can view captured file information under Analysis > Files > Captured Files, and download a copy for offline analysis.

Malware Storage Pack

Based on your file policy configuration, your device may store a substantial amount of file data to the hard drive. You can install a malware storage pack in the device; the system stores files to the malware storage pack, allowing more room on the primary hard drive to store events and configuration files. The system periodically deletes older files. If the device's primary hard drive does not have enough available space, and does not have an installed malware storage pack, you cannot store files.



Caution Do not attempt to install a hard drive that was not supplied by Cisco in your device. Installing an unsupported hard drive may damage the device. Malware storage pack kits are available for purchase **only** from Cisco, and are for use **only** with 8000 Series devices. Contact Support if you require assistance with the malware storage pack. See the *Firepower System Malware Storage Pack Guide* for more information.

Without a malware storage pack installed, when you configure a device to store files, it allocates a set portion of the primary hard drive's space to captured file storage. If you configure capacity handling to temporarily store files for dynamic analysis, the system uses the same hard drive allocation to store these files until it can resubmit them to the cloud.

When you install a malware storage pack in a device and configure file storage or capacity handling, the device allocates the entire malware storage pack for storing these files. The device cannot store any other information on the malware storage pack.

When the allocated space for captured file storage fills to capacity, the system deletes the oldest stored files until the allocated space reaches a system-defined threshold. Based on the number of files stored, you may see a substantial drop in disk usage after the system deletes files.

If a device has already stored files when you install a malware storage pack, the next time you restart the device, any captured files or capacity handling files stored on the primary hard drive are moved to the malware storage pack. Any future files the device stores are stored to the malware storage pack.

Block All Files by Type

If your organization wants to block not only the transmission of malware files, but all files of a specific type, regardless of whether the files contain malware, you can do so.

File control is supported for all file types where the system can detect malware, plus many additional file types. These file types are grouped into basic categories, such as multimedia (swf, mp3), executables (exe, torrent), and PDFs.

Blocking all files based on their type is not technically a malware protection feature; it does not require a Malware license and does not query the AMP cloud.

File Rule Actions: Evaluation Order

A file policy will likely contain multiple rules with different actions for different situations. If more than one rule can apply to a particular situation, the evaluation order described in this topic applies. In general, simple blocking takes precedence over malware inspection and blocking, which takes precedence over simple detection and logging.

The order of precedence of file-rule actions is:

- *Block Files*

- *Block Malware*
- *Malware Cloud Lookup*
- *Detect Files*

Creating File Rules



Caution Selecting **Detect Files** or **Block Files**, enabling or disabling **Store files** in a **Detect Files** or **Block Files** rule, or adding the first or removing the last file rule that combines the **Malware Cloud Lookup** or **Block Malware** file rule action with an analysis option (**Spero Analysis** or **MSEXE**, **Dynamic Analysis**, or **Local Malware Analysis**) or a store files option (**Malware**, **Unknown**, **Clean**, or **Custom**), restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See [Snort® Restart Traffic Behavior](#) for more information.

Before you begin

If you are configuring rules for malware protection, see [Configure File Policies, on page 7](#).

Procedure

- Step 1** In the file policy editor, click **Add File Rule**.
- Step 2** Select an **Application Protocol** and **Direction of Transfer** as described in [File Rule Components, on page 25](#).
- Step 3** Select one or more **File Types**.
The file types you see depend on the selected application protocol, direction of transfer, and action.
You can filter the list of file types in the following ways:
 - Select one or more **File Type Categories**, then click **All types in selected Categories**.
 - Search for a file type by its name or description. For example, type **windows** in the **Search name and description** field to display a list of Microsoft Windows-specific files.
- Tip** Hover your pointer over a file type to view its description.
- Step 4** Select a file rule **Action** as described in [File Rule Actions, on page 26](#), with consideration for [File Rule Actions: Evaluation Order, on page 32](#).
The actions available to you depend on the licenses you have installed. See [License Requirements for File and Malware Policies, on page 3](#).
- Step 5** Depending on the action you selected, configure options:
 - reset the connection after blocking the file
 - store files that match the rule
 - enable Spero analysis*

- enable local malware analysis*
- enable dynamic analysis* and capacity handling

* For information about these options, see [File Rule Actions, on page 26](#) and [Malware Protection Options \(in File Rule Actions\), on page 27](#) and its subtopics.

Step 6 Click **Add**.

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

What to do next

- If you are configuring policies for malware protection, return to [Configure File Policies, on page 7](#).
- Deploy configuration changes; see [Deploy Configuration Changes](#).

Access Control Rule Logging for Malware Protection

When the system detects a prohibited file (including malware) according to the settings in the file policy, it automatically logs an event to the Firepower Management Center database. If you do not want to log file or malware events, you can disable this logging on a per-access-control-rule basis.

The system also logs the end of the associated connection to the Firepower Management Center database, regardless of the logging configuration of the invoking access control rule.

Retrospective Disposition Changes

File dispositions can change. For example, as new information is discovered, the AMP cloud can determine that a file that was previously thought to be clean is now identified as malware, or the reverse—that a malware-identified file is actually clean. When the disposition changes for a file you queried in the past week, the AMP cloud notifies the system so it can automatically take action the next time it detects that file being transmitted. A changed disposition is called a *retrospective* disposition.

(Optional) Malware Protection with AMP for Endpoints

Cisco's AMP for Endpoints is a separate malware-protection product that can supplement malware protection provided by the Firepower system and be integrated with your Firepower deployment.

AMP for Endpoints is Cisco's enterprise-class Advanced Malware Protection solution that runs as a lightweight connector on individual users' *endpoints* (computers and mobile devices) to discover, understand, and block advanced malware outbreaks, advanced persistent threats, and targeted attacks.

Benefits of AMP for Endpoints include:

- configure custom malware detection policies and profiles for your entire organization, as well as perform flash and full scans on all your users' files
- perform malware analysis, including view heat maps, detailed file information, network file trajectory, and threat root causes

- configure multiple aspects of outbreak control, including automatic quarantines, application blocking to stop non-quarantined executables from running, and exclusion lists
- create custom protections, block execution of certain applications based on group policy, and create custom Allowed Applications lists
- use the AMP for Endpoints management console to help you mitigate the effect of malware. The management console provides a robust, flexible web interface where you control all aspects of your AMP for Endpoints deployment and manage all phases of an outbreak.

For detailed information about AMP for Endpoints, see:

- <https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html>.
- Online help in the AMP for Endpoints management console.
- AMP for Endpoints documentation available from: <http://docs.amp.cisco.com>.

Comparison of Malware Protection: Firepower vs. AMP for Endpoints

Table 4: Advanced Malware Protection Differences by Detecting Product

Feature	Firepower Malware Protection (AMP for Networks)	AMP for Endpoints
File type detection and blocking method (file control)	In network traffic, using access control and file policies	Not supported
Malware detection and blocking method	In network traffic, using access control and file policies	On individual endpoints (end-user computers and mobile devices), using a connector that communicates with the AMP cloud
Network traffic inspected	Traffic passing through a managed device	None; connectors installed on endpoints directly inspect files
Malware intelligence data source	AMP cloud (public or private)	AMP cloud (public or private)
Malware detection robustness	Limited file types	All file types
Malware analysis choices	FMC-based, plus analysis in the AMP cloud	FMC-based, plus additional options on the AMP for Endpoints management console
Malware mitigation	Malware blocking in network traffic, FMC-initiated remediations	AMP for Endpoints-based quarantine and outbreak control options, FMC-initiated remediations
Events generated	File events, captured files, malware events, and retrospective malware events	Malware events
Information in malware events	Basic malware event information, plus connection data (IP address, port, and application protocol)	In-depth malware event information; no connection data

Feature	Firepower Malware Protection (AMP for Networks)	AMP for Endpoints
Network file trajectory	FMC-based	FMC and the AMP for Endpoints management console each have a network file trajectory. Both are useful.
Required licenses or subscriptions	Licenses required to perform file control and AMP for Networks	AMP for Endpoints subscription. No license is required to bring AMP for Endpoints data into FMC.

About Integrating Firepower with AMP for Endpoints

If your organization has deployed AMP for Endpoints, you can optionally integrate that product with your Firepower deployment.

Integration with AMP for Endpoints does not require a dedicated Firepower license.

Benefits of Integrating Firepower and AMP for Endpoints

Integrating your AMP for Endpoints deployment with your Firepower system offers the following benefits:

- Centralized Blocked Applications and Allowed Applications lists configured in AMP for Endpoints can determine verdicts for file SHAs sent from Firepower to the AMP cloud for disposition.

See [Centralized File Lists from AMP for Endpoints, on page 23](#).

- The system can import malware events detected by AMP for Endpoints into Firepower Management Center so you can manage these events along with malware events generated by the Firepower system. Imported data for these events includes scans, malware detections, quarantines, blocked executions, and cloud recalls, as well as indications of compromise (IOCs) that FMC displays for hosts that it monitors.

For more information, see [Malware Event Analysis with AMP for Endpoints](#).

- You can view file trajectory and other details in the AMP for Endpoints console.

For details, see [Work with Event Data in the AMP for Endpoints Console](#).



Important If you use a Cisco AMP Private Cloud, see limitations at [AMP for Endpoints and AMP Private Cloud, on page 36](#).

AMP for Endpoints and AMP Private Cloud

If you configure a Cisco AMP private cloud to collect AMP endpoint data on your network, all AMP for Endpoints connectors send data to the private cloud, which forwards that data to the Firepower Management Center. The private cloud does not share any of your endpoint data over an external connection.

If your organization has deployed an AMP private cloud, all connections to the AMP cloud funnel through the private cloud, which acts as an anonymized proxy to ensure the security and privacy of your monitored network. This includes importing AMP for Endpoints data. The private cloud does not share any of your endpoint data over an external connection.

The following integration features are not available if you use an AMP private cloud:

- Use of Blocked Applications and Allowed Applications lists configured in AMP for Endpoints. (These lists are used to block or allow files.)
- Visibility in AMP for Endpoints of malware events generated from Firepower.

You can configure multiple private clouds to support the capacity you require.

Integrate Firepower and AMP for Endpoints

If your organization has deployed Cisco's AMP for Endpoints product, you can integrate that application with Firepower to achieve the benefits described in [Benefits of Integrating Firepower and AMP for Endpoints, on page 36](#).

When you integrate with AMP for Endpoints, you must configure an AMP for Endpoints connection even if you already have an AMP for Networks (AMP for Firepower) connection configured. You can configure multiple AMP for Endpoints cloud connections.



Caution

In a multidomain deployment, configure AMP for Endpoints connections at the leaf level only, especially if your leaf domains have overlapping IP space. If multiple subdomains have hosts with the same IP-MAC address pair, the system could save malware events that are generated by AMP for Endpoints to the wrong leaf domain, or associate IOCs with the wrong hosts.

However, you can configure AMP for Endpoints connections at any domain level, provided you use a separate AMP for Endpoints account for each connection. For example, each client of an MSSP might have its own AMP for Endpoints deployment.



Note

An AMP for Endpoints connection that has not registered successfully does not affect AMP for Networks.

Before you begin

- You must be an Admin user to perform this task.
- If your deployment uses Cisco AMP Private Cloud, see limitations at [AMP for Endpoints and AMP Private Cloud, on page 36](#).
- AMP for Endpoints must be set up and working properly on your network.
- The Firepower Management Center must have direct access to the Internet.
- Make sure your FMC and AMP for Endpoints can communicate with each other. See the topics under [Security, Internet Access, and Communication Ports](#).
- If you are connecting to the AMP cloud after either restoring your Firepower Management Center to factory defaults or reverting to a previous version, use the AMP for Endpoints management console to remove the previous connection.
- You will need your AMP for Endpoints credentials to log in to the AMP for Endpoints console during this procedure.

Procedure

- Step 1** Choose **AMP > AMP Management**.
- Step 2** Click **Add AMP Cloud Connection**.
- Step 3** From the **Cloud Name** drop-down list, choose the cloud you want to use:
- The AMP cloud closest to the geographical location of your Firepower Management Center.
 - For AMP private cloud (AMPv), choose **Private Cloud** and proceed as described in [Cisco AMP Private Cloud, on page 13](#).
- Step 4** If you want to use this cloud for both AMP for Networks and AMP for Endpoints, select the **Use for AMP for Firepower** check box.
- If you configured a different cloud to handle AMP for Networks (AMP for Firepower) communications, you can clear this check box; if this is your only AMP cloud connection, you cannot.
- In a multidomain deployment, this check box appears only in the Global domain. Each Firepower Management Center can have only one AMP for Networks connection.
- Step 5** Click **Register**.
- A spinning state icon indicates that a connection is pending, for example, after you configure a connection on the Firepower Management Center, but before you authorize it using the AMP for Endpoints management console. A **Denied** (🚫) indicates that the cloud denied the connection or the connection failed for another reason.
- Step 6** Confirm that you want to continue to the AMP for Endpoints management console, then log into the management console.
- Step 7** Using the management console, authorize the AMP cloud to send AMP for Endpoints data to the Firepower Management Center.
- Step 8** If you want to restrict the data that the FMC receives, select specific groups within your organization for which you want to receive information.
- By default, the AMP cloud sends data for all groups. To manage groups, choose **Management > Groups** on the AMP for Endpoints management console. For detailed information, see the management console online help.
- Step 9** Click **Allow** to enable the connection and start the transfer of data.
- Clicking **Deny** returns you to the Firepower Management Center, where the connection is marked as denied. If you navigate away from the Applications page on the AMP for Endpoints management console, and neither deny nor allow the connection, the connection is marked as pending on the Firepower Management Center's web interface. The health monitor does **not** alert you of a failed connection in either of these situations. If you want to connect to the AMP cloud later, delete the failed or pending connection, then recreate it.
- Incomplete registration of an AMP for Endpoints connection does not disable the AMP for Networks connection.
- Step 10** To verify that the connection is correctly configured:
- a) On the **AMP > AMP Management** page, click the Cloud Name that includes **AMP for Endpoints** in the **Cisco AMP Solution Type** column.
 - b) In the AMP for Endpoints console window that displays, choose **Accounts > Applications**.
 - c) Verify that your Firepower Management Center is on the list.

- d) In the AMP for Endpoints console window, choose **Manage > Computers**.
- e) Verify that your Firepower Management Center is on the list.

What to do next

- In the AMP for Endpoints console window, configure settings as needed. For example, define group membership for your management center and assign policies. For information, see the AMP for Endpoints online help or other documentation.
- In high availability configurations, you must configure AMP cloud connections independently on the Active and Standby instances of the Firepower Management Center; these configurations are not synchronized.
- The default health policy warns you if the Firepower Management Center cannot connect to the AMP for Endpoints portal after an initial successful connection, or if the connection is deregistered using the AMP portal.

Verify that the **AMP for Endpoints Status** monitor is enabled under **System > Health > Policy**.

History for File Policies and Malware Protection

Feature	Version	Details
Chapter restructure	any version that is republished	Restructured this chapter's content to reduce confusion. Some content was moved to or from the chapter for File/Malware Events and Network File Trajectory .
Moved URL Filtering information to the new URL Filtering chapter	6.3	Moved information about configuring cloud communications for URL Filtering to the new URL Filtering chapter. Made related changes to the structure of the Cisco CSI topics in the chapter.

