

File Policies for Network 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.

- Network malware protection and file policies, on page 1
- 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
- Configure malware protection, on page 7
- Cloud connections for malware protection, on page 12
- File policies and file rules, on page 15
- Retrospective disposition changes, on page 31
- File and malware inspection performance and storage options, on page 32
- Tune file and malware inspection performance and storage, on page 33
- (Optional) Malware protection with Secure Endpoint, on page 34

Network malware protection and file policies

Advanced Malware Protection (AMP) for Firepower can detect, capture, track, analyze, log, and optionally block the transmission of malware in network traffic. In the Cloud-Delivered Firewall Management Center web interface, this feature is called malware defense, 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.

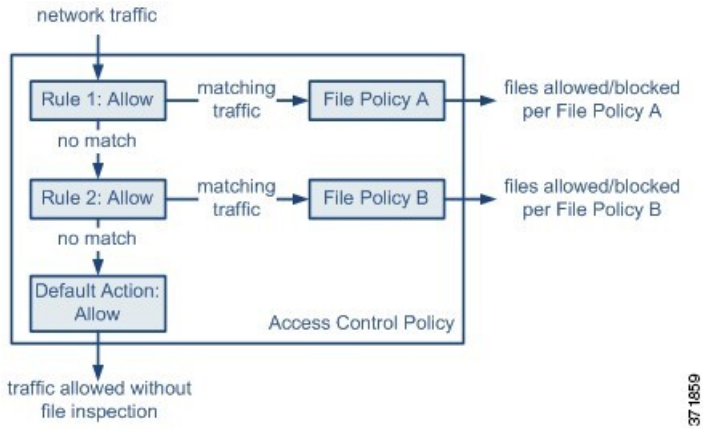
When the system detects malware on your network, it generates file and malware events. To analyze file and malware event data, see the *File/Malware Events and Network File Trajectory* chapter in the *Cisco Secure Firewall Management Center Administration Guide* .

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.

File policy traffic flow

Consider this diagram of a simple access control policy in an inline deployment.



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.

Prerequisites for file policies

This reference lists the prerequisites necessary for implementing file policies in your network security deployment.

Model support

Any

Secure Firewall 200 supports Malware Analysis through AMP Cloud Lookup only. It does not support the storing of files or the submission of files for analysis. This includes Spero, Local Malware Analysis, File Capture, and Clam AV. Any unsupported feature configured in a policy is automatically turned off when deployed to the device.

Supported domains

Any

User roles

- Administrator
- Access Admin

License requirements for file and malware policies

This reference provides the specific license requirements needed to implement various file rule actions and malware detection capabilities in 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)	IPS (for Firewall Threat Defense 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	IPS (for Firewall Threat Defense devices) Protection (for Classic devices) Malware Defense	Malware Cloud Lookup, Block Malware
Store files	IPS (for Firewall Threat Defense devices) Protection (for Classic devices) Malware Defense	Any file rule action with **Store Files** selected

For details about Malware Defense licenses, refer to:

- *Malware Defense Licenses* in the *Cisco Secure Firewall Management Center Administration Guide*

Best practices for file policies and malware detection

In addition to the items described below, follow the steps in Configure malware protection, on page 7 and referenced topics.

File rule best practices

Consider these guidelines and limitations when configuring file rules:

Prerequisites

- 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.
- If a file rule is configured with a **Malware Cloud Lookup** or **Block Malware** action and the Cloud-Delivered Firewall Management Center cannot establish connectivity with the AMP cloud, the system cannot perform any configured rule action options until connectivity is restored.

General file rule best practices

- 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.
- 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.

Dynamic Analysis

- 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 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.

File detection best practices

Consider these notes and limitations when implementing file detection:

Prerequisite

If adaptive profiling is not enabled, access control rules cannot perform file control, including AMP.

General file detection best practices

- 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.
- 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, on page 32.
- .Exe files inside some .rar archives cannot be detected, including possibly rar5.

- If the file disposition is Neutral, it is an unknown disposition.

FTP-Specific considerations

- 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.

Email protocols considerations

- 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.

File blocking best practices

Consider these notes and limitations for file blocking:

HTTP transfers

- 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.

End-of-File detection

- 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.

SMB or NetBIOS-ssn transfers

- 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 the ongoing file transfers. However, the system inspects the new files that are transferred after you deploy an access control policy invoking the file policy.
- SMB has a functionality called multi-channel which creates multiple parallel sessions with the same IP address and different ports. For a given transaction over multi-channel, the file download is multiplexed across these sessions which is not inspected by the system as a single file.
- Files transferred concurrently in a single TCP or SMB session are not inspected.
- In a cluster environment, if an existing SMB session is moved to a new device due to a cluster role change or a device failure, then the files in any ongoing file transfers may not be inspected.
- Some SMB file transfers between Microsoft Windows systems use very high TCP window size for quick file transfers. To detect or block such file transfers, it is recommended that you increase the value of **Maximum Queued Bytes** and **Maximum Queued Segments** under **Network Analysis Policy** > **TCP Stream Configuration** > **Troubleshooting Options**.

High availability

If you configure Firewall 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

Follow these best practices for file policy configuration to ensure proper functionality and optimal performance.

Prerequisites

- 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.
- 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.

Encrypted traffic

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.



Attention The File Inpsect preprocessor with the following generator IDs (GIDs) are enabled by default for file/malware policy: GID: 146 and GID: 147.

General file policy best practices

- 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.

- 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.
- If you enable an access control policy with a file policy that uses either a Malware action or a Store Files option, the computing power and system performance of the device is reduced.
- NEW_OFFICE file type in file policy configuration identifies Microsoft files: DOCX, XLSX, and PPTX. When you apply a policy action to NEW_OFFICE, the action applies uniformly to all three file types—DOCX, XLSX, and PPTX.

  If your security requirements need differentiated handling of Office file formats, such as blocking DOCX documents while permitting XLSX spreadsheets, do not use the NEW_OFFICE aggregate file type. Instead, perform these steps:

  1. Select individual file types (DOCX, XLSX, PPTX) separately in your file policy rule.
  2. Create separate rules with distinct actions for each format you need to control granularly.
  3. Test your policy to ensure each Office format is handled according to your security intent.

  This approach ensures that your file policy aligns with your organization's security posture and prevents unintended blocking of legitimate business traffic.

Configure malware protection

You need to set up your system to protect your network from malicious software by following a series of configuration steps.

Procedure

Step 1 Plan and prepare for malware protection, on page 8

Step 2 Configure file policies, on page 9

Step 3 Add file policies to your access control configuration, on page 9

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 Verify and monitor malware protection, on page 11

What to do next

- (Optional) To further enhance detection of malware in your network, deploy and integrate Cisco's Secure Endpoint product. Refer to (Optional) Malware protection with Secure Endpoint, on page 34 and subtopics.

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.

Refer to License requirements for file and malware policies, on page 3 and *Licenses* in the *Cisco Secure Firewall Management Center Administration Guide*.

Step 2 Understand how file policies and malware protection fit into your access control plan.

Refer to the chapter Access Control Policies.

Step 3 Understand the file analysis and malware protection tools.

Refer to File rule actions, on page 22 and subtopics.

Consider also Advanced and archive file inspection options, on page 16.

Step 4 Determine whether you will use public clouds or private (on-premises) clouds for malware protection (file analysis and dynamic analysis.)

Refer to Cloud connections for malware protection, on page 12 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.

Refer to *Security, Internet Access, and Communication Ports* in the *Cisco Secure Firewall Management Center Administration Guide*.

Step 7 Configure connections between Firepower and the malware protection clouds (public or private, as applicable).

What to do next

Continue with the next step in the malware protection workflow:

Refer to Configure malware protection, on page 7.

Configure file policies

File policies are a critical component of the malware protection workflow that allow you to define specific rules and advanced options for file inspection and handling.

Before you begin

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

Refer to Configure malware protection, on page 7.

Procedure

Step 1 Review file policy and file rule restrictions.

Refer to Best practices for file policies and malware detection, on page 3 and subtopics.

Step 2 Create a file policy.

Refer to Create or edit a file policy, on page 15.

Step 3 Create rules within your file policy.

Refer to File rules, on page 20 and subtopics.

Step 4 Configure advanced options.

Refer to Advanced and archive file inspection options, on page 16.

What to do next

Continue with the next step in the malware protection workflow:

Refer to Configure malware protection, on page 7.

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 Configure malware protection, on page 7.

Procedure

Step 1 Review guidelines for file policies in access control policies. (These are different from the file rule and file policy guidelines.)

Review File and intrusion inspection order.

Step 2 Associate the file policy with an access control policy.

Refer to Configure an access control rule to perform malware protection, on page 10

Step 3 Assign the access control policy to managed devices.

See Assign access control policy to devices.

What to do next

Continue with the next step in the malware protection workflow:

Refer to Configure malware protection, on page 7.

Configure an access control rule to perform malware protection

Access control rules with file policies provide comprehensive malware protection by inspecting traffic flows and applying security analysis to files traversing your network.

Caution 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 assigned device handles traffic. Refer to Snort restart traffic behavior.

Note Inline normalization is enabled automatically when a file policy is included in an access control rule. For more information, refer to The Inline Normalization Preprocessor.

Before you begin

- Adaptive profiling **must** be enabled (its default state) 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 Choose a **File Policy** to inspect traffic that matches the access control rule, or choose **None** to disable file inspection for matching traffic.

Step 3 (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 4 Save the rule.

Step 5 Click **Save** to save the policy.

What to do next

- Deploy configuration changes.

Verify and monitor malware protection

Ongoing maintenance is essential for protecting your network.

Before you begin

Configure your system to protect your network from malware.

Refer to Configure malware protection, on page 7 and referenced procedures.

Procedure

Step 1 Ensure that your system always has the most current and effective protection.

Refer to Maintain your system: file types eligible for dynamic analysis, on page 15.

Step 2 Configure alerts for malware-related events and health monitoring.

See the *Cisco Secure Firewall Management Center Administration Guide* for information on *Configuring malware defense Alerting* and for information about the following modules:

- Local Malware Analysis
- Security Intelligence
- Threat Data Updates on Devices
- Intrusion and File Event Rate

- AMP for Firepower Status
- Secure Endpoint Status

What to do next

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

Refer to Configure malware protection, on page 7.

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 Secure Endpoint 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 these options for obtaining data from the Cisco cloud about known malware threats:

- **AMP public cloud**: Your Cloud-Delivered Firewall Management Center communicates directly with the public Cisco cloud. There are three public AMP clouds, in the United States, Europe, and Asia.

Dynamic analysis cloud

Dynamic analysis cloud options include:

- Secure Malware Analytics 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 Secure Malware Analytics analysis.

AMP cloud connection configurations

Change AMP options

Use this procedure to modify AMP (Advanced Malware Protection) for Networks configuration settings that control automatic signature updates and data sharing with the Cisco cloud.

Procedure

Step 1 Choose **Integrations** > **Cloud Services**.

Step 2 Configure these parameters:

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 Cloud-Delivered Firewall Management Center checks for signature updates once every 30 minutes.
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.

Step 3 Click **Save**.

Dynamic analysis connections

Dynamic analysis connections are network connections that enable real-time security analysis and threat detection capabilities.

Prerequisites for dynamic analysis

This topic lists the prerequisites to use 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 system automatically has access to the Secure Malware Analytics Cloud.
- Dynamic analysis requires that managed devices have direct or proxied access to the Secure Malware Analytics Cloud or an on-premises Secure Malware Analytics Appliance on port 443.
- See also Files eligible for dynamic analysis, on page 27.
-

View the default dynamic analysis connection

By default, the Cloud-Delivered Firewall Management Center can connect to the public Secure Malware Analytics Cloud for file submission and report retrieval. You can neither configure nor delete this connection.

Procedure

Step 1 Choose **Integrations** > **+ Show more** > **AMP** > **AMP Management**.

Step 2 You can view the cloud in use on the default dynamic analysis connection. To associate the device, click **Associate** ( ). For more information, refer to Enable access to dynamic analysis results in the public cloud, on page 14.

Enable access to dynamic analysis results in the public cloud

Secure Malware Analytics offers more detailed reporting on analyzed files than is available in the Cloud-Delivered Firewall Management Center. If your organization has a Secure Malware Analytics Cloud account, you can access the Secure Malware Analytics 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 Cloud-Delivered Firewall Management Center with the files submitted by its managed devices.

Before you begin

You must have a Secure Malware Analytics Cloud account, and have your account credentials ready.

Procedure

Step 1 Select **Integrations** > **+ Show more** > **AMP** > **AMP Management**.

Step 2 Click **Associate** ( ) in the table row corresponding to the Secure Malware Analytics Cloud.

A Secure Malware Analytics portal window opens.

Step 3 Sign in to the Secure Malware Analytics 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 Secure Malware Analytics 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, refer to *Viewing Dynamic Analysis Results in the Cisco Cloud* in the *Cisco Secure Firewall Management Center Administration Guide*.

Maintain your system: 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.

The supported file types for automatic submission can vary in every release. The currently supported files for automatic submission are:

- PE Executable (32-bit Only)
- EXE
- DLL
- PDF
- MSOLE2 (Microsoft Object Linking and Embedding Compound File)
- DOCX, PPTX, XLSX



Note GZ and ZIP file types are not supported for automatic submission.

Procedure

Step 1 Do one of the following:

- (Recommended) Refer to *Vulnerability Database Update Automation* as discussed in the *Cisco Secure Firewall Management Center Administration Guide*
- Regularly check for new VDB updates, and *Manually Update the VDB* as discussed in the *Cisco Secure Firewall Management Center Administration Guide* 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

File policies and file rules work together to control file handling and inspection in network traffic.

Create or edit a file policy

File policies allow you to control file transfers and provide malware protection by defining rules that specify which files can be transferred, blocked, or inspected for threats.

Before you begin

If you are configuring policies for malware protection, refer to all required procedures in Configure file policies, on page 9.

Procedure

Step 1 Select **Policies** > **Security policies** > **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 Create file rules, on page 30.

Step 4 Optionally, select Advanced and configure advanced options as described in Advanced and archive file inspection options, on page 16.

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 9.
- Otherwise:
  - Add the file policy to an access control rule as described in Add file policies to your access control configuration, on page 9.
  - Deploy configuration changes.

Advanced and archive file inspection options

The Advanced Settings in the file policy editor provides general options for file analysis and archive file inspection to enhance security policy configuration.

The Advanced Settings in the file policy editor has these 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.

- **If AMP Cloud disposition is Unknown, override 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.

The Advanced Settings in the file policy editor has these 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.
- **Block Encrypted Archives**—Blocks password-protected archives.
- **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.

Archive file inspection capabilities

The system provides various options for inspecting archive files.

- **File types**: A complete list of inspectable archive file types appears in the Cloud-Delivered Firewall Management Center web interface on the file rule configuration page. To view that page, see Create file rules, on page 30. 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.

For details about options for archive file inspection, see Advanced and archive file inspection options, on page 16.

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.

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

Override file disposition using custom lists is a security mechanism that

- allows administrators to correct incorrect file dispositions from the AMP cloud by adding SHA-256 values to specific file lists
- enables treating files as clean or malware regardless of the original cloud disposition, and
- provides per-file policy control without reevaluating the file's disposition on subsequent detection.

File list types and usage

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, refer to File lists.

Alternatively, if applicable, use Centralized file lists from Secure Endpoint, on page 19.

Centralized file lists from Secure Endpoint

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

Requirements for centralized file lists

Your deployment must meet these requirements:

- Your organization must be using the AMP public cloud.
- Your organization has deployed Secure Endpoint.
- You have registered your system to Secure Endpoint using the procedure in Integrate Firepower and Secure Endpoint, on page 36.

To create and deploy these lists, refer to the documentation or online help for Secure Endpoint.

Note File lists created in Firepower override file lists created in Secure Endpoint.

Manage 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.

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: file types eligible for dynamic analysis, on page 15.

Procedure

Step 1 Select **Policies** > **Security policies** > **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 15.
- **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—Choose **Deploy** > **Deploy**; see Deploy configuration changes.
- **Edit**— If you want to modify an existing file policy, click **Edit** ( ).
- **Report**—Click **Report**( ); Refer to Generate 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.

File rule actions

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 28)

- 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

File rules consist of several components that determine how the system detects and handles files transmitted over various application protocols. Understanding these components helps configure effective file detection and inspection policies.

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	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. **Tip** Use **Any** to detect files over multiple application protocols, regardless of whether users are sending or receiving.

File Rule Component	Description
file categories and types	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. 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. Note that executables include file types that can run macros and scripts, since these can contain malware. For a list of file types the system can inspect, select **Policies** > **Security policies** > **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. **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.
file rule action	A file rule's action determines how the system handles traffic that matches the conditions of the rule. 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. For descriptions of these actions and options, see File rule actions, on page 22. File rules are evaluated in rule-action, not numerical, order. For details, see File rule actions: evaluation order, on page 29.

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 include these types:

- *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 MSEXE	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
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, refer to Malware protection options, on page 23 and its subtopics.



Caution 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 assigned device handles traffic. Refer to Snort restart traffic behavior.

Malware protection options

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

File inspection sequence

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

1. Spero analysis, on page 25 and AMP cloud lookup, on page 26

2. Local malware analysis, on page 26
3. Dynamic analysis, on page 27

For a comparison of these tools, see Comparison of malware protection options, on page 24.

(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 29.)

Refer to information about Cisco's Secure Endpoint product at (Optional) Malware protection with Secure Endpoint, on page 34 and subtopics.

Comparison of malware protection options

This 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 Secure Malware Analytics	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.

Analysis Type	Benefit	Limitations	Malware Identification
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.
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 Defense 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 You cannot manually submit files for Spero analysis.

AMP cloud lookup

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

Performance optimization

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 26.

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 Talos Intelligence Group. Because local analysis does not query the AMP cloud, and does not run the file, local malware analysis saves time and system resources.

Local malware analysis behavior

When the system identifies malware through local malware analysis, it updates the existing file disposition from Unknown to Malware and 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 26.

Local malware analysis does not require establishing communications with the Secure Malware Analytics 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:

TTL values for dispositions and threat scores

Dispositions and associated threat scores have these 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

Dynamic analysis is a security analysis method that

- automatically submits files for behavioral analysis using Secure Malware Analytics (formerly Threat Grid), Cisco's file analysis and threat intelligence platform,
- runs files in a sandbox environment to analyze behavior and determine maliciousness, and
- returns a threat score indicating the likelihood that a file contains malware.

Dynamic analysis process and capabilities

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

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

Secure Malware Analytics 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 Secure Malware Analytics 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 Secure Malware Analytics, refer to 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 13.

Files eligible for dynamic analysis

A file's eligibility for dynamic analysis depends on the file type, the file size, and the file rule's action.

Additional requirements:

- 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 is a system feature that temporarily stores 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.

Storage options

Some devices can store files on the device hard drive or in a malware storage pack. Refer Malware storage packs, on page 28.

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.

File capture and storage capabilities

After your device captures 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 **Events & Logs** > **Analysis** > **Unified Events**, 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.

Malware storage packs

A malware storage pack

- provides additional storage capacity for file data when installed in security devices
- allows the primary hard drive to store events and configuration files by dedicating the entire storage pack to captured files, and

- automatically receives stored files from the primary hard drive when installed on devices that already contain file data.

Storage allocation and file management

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. Contact Support if you require assistance with the malware storage pack.

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.

For more information on using MSP on the Firepower devices, see the Firepower Hardware Installation Guide for your device.

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 type categories and licensing

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 Defense 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*

Create file rules

Use this procedure when you need to add file rules to an existing file policy to control file handling and security actions.



Caution 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 assigned device handles traffic. Refer to Snort restart traffic behavior.

Before you begin

If you are configuring rules for malware protection, refer to Configure file policies, on page 9.

Procedure

Step 1 Select **Policies** > **Security policies** > **Malware & File** .

Step 2 Click the edit icon to modify an existing file policy.

Step 3 In the file policy editor, click **Add Rule**.

Step 4 Select an **Application Protocol** and **Direction of Transfer** as described in File rule components, on page 21.

Step 5 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 these 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 6 Select a file rule **Action** as described in File rule actions, on page 22, with consideration for File rule actions: evaluation order, on page 29.

The actions available to you depend on the licenses you have installed. Refer to License requirements for file and malware policies, on page 3.

Step 7 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, refer to File rule actions, on page 22 and Malware protection options, on page 23 and its subtopics.

Step 8 Click **Add.**

Step 9 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 9.
- 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 Cloud-Delivered Firewall 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 Cloud-Delivered Firewall 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.

File and malware inspection performance and storage options

Increasing the file sizes can affect the performance of the system.

Table 4: Advanced access control file and malware defense options

Field	Description	Guidelines and Restrictions
Limit the number of bytes inspected when doing file type detection	Specifies the number of bytes inspected when performing file type detection.	0 - 4294967295 (4GB) 0 removes the restriction. The default value is the maximum segment size of a TCP packet (1460 bytes). In most cases, the system can identify common file types using the first packet. To detect ISO files, enter a value greater than 36870.
Allow file if cloud lookup for Block Malware takes longer than (seconds)	Specifies how long the system will hold the last byte of a file that matches a **Block Malware** rule and that does not have a cached disposition, while malware cloud lookup occurs. If the time elapses without the system obtaining a disposition, the file passes. Dispositions of Unavailable are not cached.	0 - 30 seconds Do *not* set this option to 0 without contacting Support. Cisco recommends that you use the default value to avoid blocking traffic because of connection failures.
Do not calculate SHA-256 hash values for files larger than (in bytes)	Prevents the system from storing files larger than a certain size, performing a malware cloud lookup on the files, or blocking the files if added to the custom detection list.	0 - 4294967295 (4GB) 0 removes the restriction. This value must be greater than or equal to **Maximum file size to store (bytes)** and **Maximum file size for dynamic analysis testing (bytes)**.

Maximum file size for advanced file inspection and storage (bytes)	These settings specify:
	• The file size that the system can inspect using these detectors:
	  • Spero analysis
	  • Sandboxing and preclassification
	  • Local malware analysis/ClamAV
	  • Archive inspection
	• The file size that the system can store using a file rule.
		0 - 10485760 (10MB)
		0 disables file storage.
		Must be less than or equal to **Maximum file size to store (bytes)** and **Do not calculate SHA-256 hash values for files larger than (in bytes)**.

Minimum file size for advanced file inspection and storage (bytes)		0 - 10485760 (10MB) 0 disables file storage. Must be greater than or equal to **Minimum file size to store (bytes)**, and less than or equal to **Do not calculate SHA-256 hash values for files larger than (in bytes)**.

Field	Description	Guidelines and Restrictions
Maximum file size for dynamic analysis testing (bytes)	Specifies the minimum file size the system can submit to the AMP cloud for dynamic analysis.	0 -10485760 (10MB) Must be less than or equal to **Maximum file size for dynamic analysis testing (bytes)** and **Do not calculate SHA-256 hash values for files larger than (in bytes)**. The file size for dynamic analysis must be within the limits defined by the minimum and maximum settings for file analysis. The system checks the AMP cloud for updates to the minimum file size you can submit (no more than once a day). If the new minimum size is larger than your current value, your current value is updated to the new minimum, and your policy is marked out-of-date.
Minimum file size for dynamic analysis testing (bytes)	Specifies the maximum file size the system can submit to the AMP cloud for dynamic analysis.	0 -10485760 (10MB) Must be greater than or equal to **Minimum file size for dynamic analysis testing (bytes)**, and less than or equal to **Do not calculate SHA-256 hash values for files larger than (in bytes)**. The file size for dynamic analysis must be within the limits defined by the minimum and maximum settings for file analysis. The system checks the AMP cloud for updates to the maximum file size you can submit (no more than once a day). If the new maximum size is smaller than your current value, your current value is updated to the new maximum, and your policy is marked out-of-date.

Tune file and malware inspection performance and storage

File and malware inspection can impact system performance and storage utilization. Tuning these settings helps ensure optimal security posture while maintaining acceptable system performance.

Before you begin

You must be an Admin, Access Admin, or Network Admin user to perform this task.

Procedure

Step 1 In the access control policy editor, click **Advanced Settings**.

Step 2 Click **Edit** (✎) next to **Files and Malware Settings**.

If **View** (👁) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Step 3 Set any of the options described in File and malware inspection performance and storage options, on page 32.

Step 4 Click **OK**.

Step 5 Click **Save** to save the policy.

(Optional) Malware protection with Secure Endpoint

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

Secure Endpoint 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 Secure Endpoint

- 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 Secure Endpoint 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 Secure Endpoint deployment and manage all phases of an outbreak.

For detailed information about Secure Endpoint, refer to:

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

Comparison of malware protection: Firepower vs. Secure Endpoint

This table compares the advanced malware protection differences between Firepower malware protection and Secure Endpoint across various features including detection methods, network traffic inspection, malware analysis, mitigation capabilities, and licensing requirements.

Table 5: Advanced malware protection differences by detecting product

Feature	Firepower Malware Protection (malware defense)	Secure Endpoint
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	Cloud-Delivered Firewall Management Center-based, plus analysis in the AMP cloud	Cloud-Delivered Firewall Management Center-based, plus additional options on the Secure Endpoint management console
Malware mitigation	Malware blocking in network traffic, Cloud-Delivered Firewall Management Center-initiated remediations	Secure Endpoint-based quarantine and outbreak control options, Cloud-Delivered Firewall Management Center-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
Network file trajectory	Cloud-Delivered Firewall Management Center-based	Cloud-Delivered Firewall Management Center and the Secure Endpoint management console each have a network file trajectory. Both are useful.
Required licenses or subscriptions	Licenses required to perform file control and malware defense	Secure Endpoint subscription. No license is required to bring Secure Endpoint data into Cloud-Delivered Firewall Management Center.

Integrate Secure Firewall with Secure Endpoint

If your organization has deployed Secure Endpoint, you can optionally integrate that product with your Secure Firewall deployment.

Integration with Secure Endpoint does not require a dedicated Secure Firewall license.

Benefits of integrating Firepower and Secure Endpoint

Integrating your Secure Endpoint deployment with your system offers these benefits:

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

  Refer to Centralized file lists from Secure Endpoint, on page 19.

- The system can import malware events detected by Secure Endpoint into Cloud-Delivered Firewall Management Center so you can manage these events along with malware events generated by the system. Imported data for these events includes scans, malware detections, quarantines, blocked executions, and cloud recalls, as well as indications of compromise (IOCs) that Cloud-Delivered Firewall Management Center displays for hosts that it monitors.
- You can view file trajectory and other details in the Secure Endpoint console.



Important If you use a Cisco AMP Private Cloud, refer to limitations at Secure Endpoint and AMP private cloud, on page 36.

Secure Endpoint and AMP private cloud

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

Private cloud functionality and limitations

The private cloud acts as an anonymized proxy to ensure the security and privacy of your monitored network. This includes importing Secure Endpoint data. The private cloud does not share any of your endpoint data over an external connection.

The integration features that are not available with an AMP private cloud are:

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

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

Integrate Firepower and Secure Endpoint

If your organization has deployed Cisco's Secure Endpoint product, you can integrate that application with Firepower to achieve the benefits described in Benefits of integrating Firepower and Secure Endpoint, on page 35.

When you integrate with Secure Endpoint, you must configure the Secure Endpoint connection even if you already have malware defense (AMP for Firepower) connections configured. You can configure multiple Secure Endpoint cloud connections.



Note Secure Endpoint connections that have not registered successfully do not affect malware defense.

Before you begin

- You must be an Admin user to perform this task.
- Secure Endpoint must be set up and working properly on your network.
- If you are connecting to the AMP cloud after either reimaging or restoring your Cloud-Delivered Firewall Management Center from backup, use the Secure Endpoint management console to remove the previous connection.
- You will need your Secure Endpoint credentials to log in to the Secure Endpoint console during this procedure.

Procedure

Step 1 Choose **Integrations** > **+ Show more** > **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.

Step 4 If you want to use this cloud for both malware defense and Secure Endpoint, select the **Use for AMP for Firepower** check box.

If you configured a different cloud to handle malware defense (AMP for Firepower) communications, you can clear this check box; if this is your only AMP cloud connection, you cannot.

Step 5 Click **Register**.

A **Spinning state** ( ) icon indicates that a connection is pending, for example, after you configure a connection on the Cloud-Delivered Firewall Management Center, but before you authorize it using the Secure Endpoint management console. A **Denied** ( ) icon indicates that the cloud denied the connection or the connection failed for another reason.

Step 6 Confirm that you want to continue to the Secure Endpoint management console, then log into the management console.

Step 7 Using the management console, authorize the AMP cloud to send Secure Endpoint data to Cloud-Delivered Firewall Management Center.

Step 8 If you want to restrict the data that the Cloud-Delivered Firewall Management Center 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 Secure Endpoint 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 Cloud-Delivered Firewall Management Center, where the connection is marked as denied. If you navigate away from the Applications page on the Secure Endpoint management console, and neither deny nor allow the connection, the connection is marked as pending on the Cloud-Delivered Firewall 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 the Secure Endpoint connection does not disable the malware defense connection.

What to do next

- In the Secure Endpoint console window, configure settings as needed. For example, define group membership for your management center and assign policies. For information, see the Secure Endpoint online help or other documentation.
- The default health policy warns you if the Cloud-Delivered Firewall Management Center cannot connect to the Secure Endpoint portal after an initial successful connection, or if the connection is deregistered using the AMP portal.

  Verify that the Secure Endpoint Status monitor is enabled under **Troubleshooting** > **+ Show more** > **Health** > **Policies**.
- To verify that the connection is correctly configured:
  1. On the **Integrations** > **+ Show more** > **AMP** > **AMP Management** page, click the Cloud Name that includes Secure Endpoint in the **Cisco AMP Solution Type** column.
  2. In the Secure Endpoint console window that displays, choose **Accounts > Applications**.
  3. Verify that your Cloud-Delivered Firewall Management Center is on the list.
  4. In the Secure Endpoint console window, choose **Manage > Computers**.
  5. Verify that your Cloud-Delivered Firewall Management Center is on the list.