

File/Malware Events and Network File Trajectory

The following topics provide an overview of file and malware events, local malware analysis, dynamic analysis, captured files, and network file trajectories.

- File and malware events and network file trajectory, on page 1
- File and malware events, on page 2
- View details about analyzed files, on page 22
- Using captured file workflows, on page 24
- Submit files for analysis manually, on page 28
- Network file trajectory, on page 29
- History for file and malware events and network file trajectory, on page 36

File and malware events and network file trajectory

File and malware events are security data logs that

- are automatically generated and logged when matched traffic triggers a file policy,
- trigger automatic logging of the associated connection to the Secure Firewall Management Center database when generated, and
- provide analysis data to address negative impacts and block future attacks.

File analysis and network file trajectory features

Based on file analysis results, you can review captured files and generated malware and file events using tables on pages available under the **Events & Logs** > **+ Show more** > **Files** > **File Events**. These include details such as file composition, disposition, threat score, and dynamic analysis summary reports.

To further target your analysis, you can use a malware file's *network file trajectory* (a map of how the file traversed your network, passing among hosts, as well as various file properties) to track the spread of an individual threat across hosts over time, allowing you to concentrate outbreak control and prevention efforts where most useful.

If you configure local malware analysis or dynamic analysis in a file rule, the system preclassifies files matching the rule and generates a file composition report.

If your organization has deployed *Secure Endpoint* and integrated that deployment with your Secure Firewall Management Center, you can also import records of scans, malware detections, and quarantines, as well as

indications of compromise (IOC) identified by that product. This data is displayed alongside event data gathered by Secure Firewall for a more complete picture of malware on your network.

The Context Explorer, dashboards, and reporting features can also aid a deeper understanding of the files and malware detected, captured, and blocked. You can also use events to trigger correlation policy violations, or alert you via email, SMTP, or syslog.



Note To configure your system to detect malware and generate file and malware events, refer to *Network Malware Protection and File Policies* in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

File and malware events

File and malware events are logging records that

- represent files and malware detected by the Secure Firewall Management Center
- provide different information depending on how and why they were generated, and
- include file events, malware events, and retrospective malware events with varying field availability.

Event types

The system generates different types of file and malware events:

- *File events*: Events that represent files, including malware, detected by the system (malware defense). File events do not contain Secure Endpoint-related fields.
- *Malware events*: Events that represent malware detected by either malware defense or Secure Endpoint. Malware events can also record data other than threats from your Secure Endpoint deployment, such as scans and quarantines.
- *Retrospective malware events*: Events that represent files detected by malware defense whose dispositions (whether the files are malware) have changed.



Note

- Files identified as malware by malware defense generate both a file event and a malware event. Malware events generated by Secure Endpoint do not have corresponding file events.
- Files that are not identified as malware (clean and neutral files) generate file events. A single file event is created for each file, regardless of how many times the file is downloaded. However, connection events are generated for each instance of the file being downloaded.
- File events generated by inspecting NetBIOS-ssn (SMB) traffic do not immediately generate connection events because the client and server establish a persistent connection. The system generates connection events after the client or server ends the session.
- The system supports the display and input of file names that use Unicode (UTF-8) characters. However, Unicode file names appear in PDF reports in transliterated form. Additionally, the SMB protocol replaces unprintable characters in file names with periods.

File and malware event types

File and malware event types are security classifications that identify and categorize different kinds of file-related activities and malicious software incidents detected within network traffic for analysis and threat response.

File events

The system logs the file events generated when a managed device detects or blocks a file in network traffic, according to the rules in currently deployed file policies.

When the system generates a file event, it also logs the end of the associated connection to the Secure Firewall Management Center database, regardless of the logging configuration of the invoking access control rule.

Malware events

The system (specifically the malware defense feature) generates malware events when it detects malware in network traffic as part of your overall access control configuration. Malware events contain the disposition of the resulting event and contextual data about how, where, and when the malware was detected.

Table 1: Malware event generation scenarios

When the system detects a file and...	Disposition
successfully queries the AMP cloud (performs a malware cloud lookup) for the file's disposition	Malware, Clean, or Unknown
queries the AMP cloud but cannot establish a connection or the cloud is otherwise unavailable	Unavailable You may see a small percentage of events with this disposition; this is expected behavior.
the threat score associated with a file exceeds the malware threshold threat score defined in the file policy that detected the file, or local malware analysis identifies malware	Malware
it is on the custom detection list (manually marked as malware)	Custom Detection
it is on the on the clean list (manually marked as clean),	Clean

File rule actions and file disposition in malware events

Each file rule defines an action that determines how the system manages traffic matching the conditions of the rule. If you select *Block Malware* or *Malware Cloud Lookup* as file rule action, the system queries the AMP cloud to assess if files traversing the network contain malware, and blocks files identified as threats. A cloud lookup allows the system to retrieve and log the file's disposition based on its SHA-256 hash value.

The table maps file rule actions to file disposition and the resulting action in malware events.

Table 2: File disposition and file action in malware events

File Rule Action Selected	File Disposition	File Action in the Malware Event
• Block Malware • Malware Cloud Lookup	Malware	Block
	• Clean • Unknown • Unavailable • NA	Cloud Lookup **Note** Under the file policy editor Advanced Settings, you can set a threshold threat score for **If AMP Cloud disposition is Unknown, override disposition based upon threat score** option. 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.

Retrospective malware events

A retrospective malware event is a security event that

- represents a disposition change for files detected in the last week that have the same SHA-256 hash value,
- contains limited information including the date and time of notification, the new disposition, the SHA-256 hash value, and the threat name, and
- does not contain IP addresses or other contextual information.

Retrospective malware event processing

For malware detected in network traffic, dispositions can change. For example, 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 last week, the AMP cloud notifies the system. Then, two things happen:

- The Secure Firewall Management Center generates a new retrospective malware event.

  This new retrospective malware event represents a disposition change for all files detected in the last week that have the same SHA-256 hash value. For that reason, these events contain limited information: the date and time the Secure Firewall Management Center was notified of the disposition change, the new disposition, the SHA-256 hash value of the file, and the threat name. They do not contain IP addresses or other contextual information.

- The Secure Firewall Management Center changes the file disposition for previously detected files with the retrospective event's associated SHA-256 hash value.

  If a file's disposition changes to Malware, the Secure Firewall Management Center logs a new malware event to its database. Except for the new disposition, the information in this new malware event is identical to that in the file event generated when the file was initially detected.

  If a file's disposition changes to Clean, the Secure Firewall Management Center does not delete the malware event. Instead, the event reflects the change in disposition. This means that files with clean dispositions can appear in the malware table, but only if they were originally thought to be malware. Files that were never identified as malware appear only in the files table.

Malware events generated by Secure Endpoint

A malware event generated by Secure Endpoint is a security event that

- occurs when lightweight connectors on endpoints inspect files and communicate with the AMP cloud to determine if files contain malware,
- includes threat identifications, scans, quarantines, blocked executions, and cloud recalls sent from the AMP cloud to the Secure Firewall Management Center, and
- is logged by the Secure Firewall Management Center when files are positively identified as malware.

Endpoint connector functionality

Organizations using Secure Endpoint install lightweight connectors on *endpoints*: computers and mobile devices. Connectors can inspect files upon upload, download, execution, open, copy, move, and so on. These connectors communicate with the AMP cloud to determine if inspected files contain malware.

When a file is positively identified as malware, the AMP cloud sends the threat identification to the Secure Firewall Management Center. The AMP cloud can also send other kinds of information to the Secure Firewall Management Center, including data on scans, quarantines, blocked executions, and cloud recalls. The Secure Firewall Management Center logs this information as malware events.



Note The IP addresses reported in malware events generated by Secure Endpoint may not be in your network map—and may not even be in your monitored network at all. Depending on your deployment, level of compliance, and other factors, endpoints in your organization monitored by Secure Endpoint may not be the same hosts as those monitored by malware defense.

Malware event analysis with Secure Endpoint

Malware event analysis with Secure Endpoint is a security feature that

- displays malware events detected by Secure Endpoint on Firewall Management Center event pages alongside events detected by Malware Defense,
- enables viewing of file trajectory and other information about a particular SHA in Secure Endpoint when using the Cisco public cloud, and
- provides integrated malware detection capabilities across endpoint and network security solutions.

If your organization has deployed Cisco Secure Endpoint:

- You can configure the system to display malware events detected by Secure Endpoint on Firewall Management Center event pages, alongside events detected by Malware Defense.
- If you are using the AMP public cloud, you can view file trajectory and other information about a particular SHA in Secure Endpoint. Simply right-click a file's SHA hash in a table on an event page.

To configure this functionality, refer to *Integrate DeviceUUID (Syslog Only)Secure Firewall and Secure Endpoint* in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Event data from Secure Endpoint

Event data from Secure Endpoint is file and malware detection information that

- provides in-depth malware event information with endpoint context such as file path and invoking client application,
- differs from network-based detection in timing and data type, as malware detection occurs at the endpoint during download or execution, and
- integrates with Firewall Management Center to provide comprehensive malware protection data.

Data differences between detection methods

Malware events detected by Secure Endpoint contain different information than malware events detected by managed devices in network traffic.

Because Secure Endpoint malware detection is performed at the endpoint at download or execution time, while managed devices detect malware in network traffic, the information in the two types of malware events is different. For example, malware events detected by Secure Endpoint ("endpoint-based malware") contain information on file path, invoking client application, and so on, while malware detections in network traffic contain port, application protocol, and originating IP address information about the connection used to transmit the file.

As another example, for malware events detected by Malware Defense ("network-based malware events"), user information represents the user most recently logged into the host where the malware was destined, as determined by network discovery. But Secure Endpoint-reported users represent the user currently logged into the endpoint where the malware was detected.



Note Depending on your deployment, endpoints monitored by Secure Endpoint may not be the same hosts as those monitored by malware defense. For this reason, malware events generated by Secure Endpoint do not add hosts to the network map. However, the system uses IP and MAC address data to tag monitored hosts with indications of compromise obtained from your Secure Endpoint deployment. If two different hosts monitored by different malware solutions have the same IP and MAC address, the system can incorrectly tag monitored hosts with Secure Endpoint IOCs.

This table summarizes the differences between the event data generated by Firepower when using a Malware Defense license, and event data generated by Secure Endpoint.

Table 3: Summary of data differences between AMP products

Feature	malware defense	Secure Endpoint
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	Firewall Management Center-based	Firewall Management Center and the Secure Endpoint management console each have a network file trajectory. Both are useful.

Related topics

Integrate Firepower and Secure Endpoint in the *Cisco Secure Firewall Management Center Device Configuration Guide*

Using file and malware event workflows

This procedure allows you to view file and malware events in a table format and manipulate the event view to display information relevant to your analysis.

The page you see when you access events differs depending on the workflow, which is simply a series of pages you can use to evaluate events by moving from a broad to a more focused view. You can also create a custom workflow that displays only the information that matches your specific needs.

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

You must be an Admin or Security Analyst user to perform this task.

Procedure

Choose one of the following:

- **Events & Logs** > **+ Show more** > **Files** > **File Events**
- **Events & Logs** > **+ Show more** > **Files** > **Malware Events**

Tip In the table view of events, several fields are hidden by default. To show a hidden field in an event view, expand the search constraints, then click the field name under **Disabled Columns**.

Tip To quickly view the connections where specific files were detected, choose the files using the check boxes in the table, then choose **Connections Events** from the **Jump to** drop-down list.

Tip Right-click an item in the table to see options. (Not every column offers options.)

Related Topics

File and malware event fields, on page 8
Predefined file workflows
Predefined malware workflows
Configure event view settings

File and malware event fields

File and malware events, which you can view and search using workflows, contain the fields listed in this section. Keep in mind that the information available for any individual event can vary depending on how and why it was generated.



Note Files identified as malware by malware defense generate both a file event and a malware event. Malware events generated by Secure Endpoint do not have corresponding file events, and file events do not have Secure Endpoint-related fields.

Syslog messages are populated with initial values and do not update, even if the equivalent field in the Firewall Management Center web interface is updated, for example with a retrospective verdict.

Action (Syslog: FileAction)

The action associated with file policy rule that detected the file, and any associated file rule action options.

AMP Cloud

The name of the AMP cloud where the AMP for Endpoints event originated.

Application File Name

The client application accessing the malware file when AMP for Endpoints detection occurred. These applications are **not** tied to network discovery or application control.

Application File SHA256

The SHA-256 hash value of the parent file accessing the AMP for Endpoints-detected or quarantined file when detection occurred.

In the unified event viewer, this field appears as **Application File SHA-256**.

Application Protocol (Syslog: ApplicationProtocol)

The application protocol used by the traffic in which a managed device detected the file.

Application Protocol Category or Tag

The criteria that characterize the application to help you understand the application's function.

Application Risk

The risk associated with the application traffic detected in the connection: Very High, High, Medium, Low, or Very Low. Each type of application detected in the connection has an associated risk; this field displays the highest of those.

Archive Depth (Syslog: ArchiveDepth)

The level (if any) at which the file was nested in an archive file.

Archive Name (Syslog: ArchiveFileName)

The name of the archive file (if any) which contained the malware file.

To view the contents of an archive file, go to any table under **Events & Logs** > **+ Show more** > **Files** > **File Events** that lists the archive file, right-click the archive file's table row to open the context menu, then click **View Archive Contents**.

Archive SHA256 (Syslog: ArchiveSHA256)

The SHA-256 hash value of the archive file (if any) which contains the malware file.

To view the contents of an archive file, go to any table under **Events & Logs** > **+ Show more** > **Files** > **File Events** that lists the archive file, right-click that archive file's table row to open the context menu, then click **View Archive Contents**.

ArchiveFileStatus (Syslog Only)

The status of an archive being inspected. Can have the following values:

- Pending — Archive is being inspected
- Extracted — Successfully inspected without any problems
- Failed — Failed to inspect, insufficient system resources
- Depth Exceeded — Successful, but archive exceeded the nested inspection depth
- Encrypted — Partially successful, archive was or contains an archive that is encrypted
- Not Inspectable — Partially successful, file is possibly malformed or corrupt

Business Relevance

The business relevance associated with the application traffic detected in the connection: Very High, High, Medium, Low, or Very Low. Each type of application detected in the connection has an associated business relevance; this field displays the lowest (least relevant) of those.

Category / File Type Category

The general categories of file type, for example: Office Documents, Archive, Multimedia, Executables, PDF files, Encoded, Graphics, or System Files.

Client (Syslog: Client)

The client application that runs on one host and relies on a server to send a file.

Client Category or Tag

The criteria that characterize the application to help you understand the application's function.

Connection Counter (Syslog Only)

A counter that distinguishes one connection from another simultaneous connection. This field has no significance on its own.

The following fields collectively uniquely identify the connection event associated with a particular file or malware event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

Connection Instance ID (Syslog Only)

The Snort instance that processed the connection event. This field has no significance on its own.

The following fields collectively uniquely identify the connection event associated with a particular file or malware event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

Count

After you apply a constraint that creates two or more identical rows, the number of events that match the information in each row.

Detection Name

The name of the detected malware.



Note Malware events involving archive files occur when malware is detected inside archive files, such as ZIP or other compressed files. The top-level archive event may not show a detection name because the archive itself is not malicious. Detection names are assigned only to the infected child files within the archive. Use the archive's SHA-256 hash or the archive file name to map and correlate the parent archive event with its infected child files.

Detector

The AMP for Endpoints detector that identified the malware, such as ClamAV, Spero, or SHA.

Device

For file events and for malware events generated by firewall devices, the name of the device that detected the file.

For malware events generated by AMP for Endpoints and for retrospective malware events generated by the AMP cloud, the name of the Firewall Management Center.

DeviceUUID (Syslog Only)

The unique identifier of the firewall device that generated an event.

The following fields collectively uniquely identify the connection event associated with a particular file or malware event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

Disposition / File Disposition (Syslog: SHA_Disposition)

The file's disposition:

Malware

Indicates that the AMP cloud categorized the file as malware, local malware analysis identified malware, or the file's threat score exceeded the malware threshold defined in the file policy.

Clean

Indicates that the AMP cloud categorized the file as clean, or that a user added the file to the clean list. Clean files appear in the malware table only if they were changed to clean.

Unknown

Indicates that the system queried the AMP cloud, but the file has not been assigned a disposition; in other words, the AMP cloud has not categorized the file.

Custom Detection

Indicates that a user added the file to the custom detection list.

Unavailable

Indicates that the system could not query the AMP cloud. You may see a small percentage of events with this disposition; this is expected behavior.

N/A

Indicates a Detect Files or Block Files rule handled the file and the Secure Firewall Management Center did not query the AMP cloud.

File dispositions appear only for files for which the system queried the AMP cloud.

Syslog fields reflect only the initial disposition; they do not update to reflect retrospective verdicts.

Domain

For file events and for malware events generated by firewall devices, the domain of the device that detected the file. For malware events generated by AMP for Endpoints and for retrospective malware events generated by the AMP cloud, the domain associated with the AMP cloud connection that reported the event.

This field is only present if you have ever configured the Firewall Management Center for multitenancy.

DstIP (Syslog Only)

The IP address of the host that responded to the connection. This may be the IP address of the sender or the recipient of the file, depending on the value in the FileDirection field:

If FileDirection is `Upload`, then this is the IP address of the file recipient.

If FileDirection is `Download`, then this is the IP address of the file sender.

See also **SrcIP**.

See also Initiator and responder, source and destination, and sender and receiver fields.

DstPort (Syslog Only)

The port used in the connection described under **DstIP**.

Egress Virtual Router

In networks using virtual routing, the name of the virtual router through which traffic exited the network.

Event Subtype

The AMP for Endpoints action that led to malware detection, for example, Create, Execute, Move, or Scan.

Event Type

The sub-type of malware event.

File Name (Syslog: FileName)

The name of the file.

File Path

The file path of the malware file detected by AMP for Endpoints, not including the file name.

File Policy (Syslog: FilePolicy)

The file policy that detected the file.

File Storage / Stored (Syslog: FileStorageStatus)

The storage status of the file associated with the event:

Stored

Returns all events where the associated file is currently stored.

Stored in connection

Returns all events where the system captured and stored the associated file, regardless of whether the associated file is currently stored.

Failed

Returns all events where the system failed to store the associated file.

Syslog fields contain only the initial status; they do not update to reflect changed status.

File Timestamp

The time and date that AMP for Endpoints detected the malware file was created.

FileDirection (Syslog Only)

Whether the file was downloaded or uploaded during the connection. Possible values are:

- Download — the file was transferred from the DstIP to the SrcIP.
- Upload — the file was transferred from the SrcIP to the DstIP.

FileSandboxStatus (Syslog Only)

Indicates whether the file was sent for dynamic analysis and if so, the status.

First Packet Time (Syslog Only)

The time the system encountered the first packet.

The following fields collectively uniquely identify the connection event associated with a particular file or malware event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

FirstPacketSecond (Syslog Only)

The time at which the file download or upload flow started.

The time the event occurred is captured in the message header timestamp.

HTTP Response Code

The HTTP status code sent in response to a client's HTTP request when a file is transferred.

Ingress Virtual Router

In networks using virtual routing, the name of the virtual router through which traffic entered the network.

IOC

Whether the malware event triggered an indication of compromise (IOC) against a host involved in the connection. When AMP for Endpoints data triggers an IOC rule, a full malware event is generated, with the type AMP IOC.

Message

Additional information associated with a malware event. For file events and for malware events generated by firewall devices, this field is populated only for files whose disposition has changed, that is, that have an associated retrospective event.

MITRE

A count of techniques that you can click to bring up a modal, which shows the full list of MITRE tactics and techniques within that hierarchy.

Protocol (Syslog Only)

The protocol used for the connection, for example TCP or UDP.

Receiving Continent

The continent of the host receiving the file.

Receiving Country

The country of the host receiving the file.

Receiving IP

In the Firewall Management Center web interface, for file events and for malware events generated by firewall devices, the IP address of the host receiving the file. See also Initiator and responder, source and destination, and sender and receiver fields.

For malware events generated by AMP for Endpoints, the IP address of the endpoint whose connector reported the event.

For syslog equivalents (events generated by firewall devices only), see **DstIP** and **SrcIP**.

Receiving Port

In the Firewall Management Center web interface, the destination port used by the traffic where the file was detected.

For syslog equivalents, see **DstIP** and **SrcIP** and **DstPort** and **SrcPort**.

Sending Continent

The continent of the host sending the file.

Sending Country

The country of the host sending the file.

Sending IP

In the Firewall Management Center web interface, the IP address of the host sending the file. See also Initiator and responder, source and destination, and sender and receiver fields.

For syslog equivalents, see **DstIP** and **SrcIP**.

Sending Port

In the Firewall Management Center web interface, the source port used by the traffic where the file was detected.

For syslog equivalents, see **DstIP** and **SrcIP** and **DstPort** and **SrcPort**.

SHA256 / File SHA256 (Syslog: FileSHA256)

The SHA-256 hash value of the file.

To have a SHA256 value, the file must have been handled by one of:

- a Detect Files file rule with **Store files** enabled
- a Block Files file rule with **Store files** enabled
- a Malware Cloud Lookup file rule
- a Block Malware file rule
- AMP for Endpoints

This column also displays a network file trajectory icon that represents the most recently detected file event and file disposition, and that links to the network file trajectory.

Size (KB) / File Size (KB) (Syslog: FileSize)

In the Firewall Management Center web interface, the size of the file, in kilobytes.

In syslog messages: The size of the file, in bytes.

Note that if the system determines the file type of a file before the file is fully received, the file size may not be calculated. In this case, this field is blank.

SperoDisposition (Syslog Only)

Indicates whether the SPERO signature was used in file analysis. Possible values:

- Spero detection performed on file
- Spero detection not performed on file

SrcIP (Syslog Only)

The IP address of the host that initiated the connection. This may be the IP address of the sender or the recipient of the file, depending on the value in the FileDirection field:

If FileDirection is `Upload`, this is the IP address of the file sender.

If FileDirection is `Download`, this is the IP address of the file recipient.

See also **DstIP**.

See also Initiator and responder, source and destination, and sender and receiver fields.

SrcPort (Syslog Only)

The port used in the connection described under **SrcIP**.

SSL Actual Action (Syslog: SSLActualAction)

The action the system applied to encrypted traffic:

Block or Block with reset

Represents blocked encrypted connections.

Decrypt (Resign)

Represents an outgoing connection decrypted using a re-signed server certificate.

Decrypt (Replace Key)

Represents an outgoing connection decrypted using a self-signed server certificate with a substituted public key.

Decrypt (Known Key)

Represents an incoming connection decrypted using a known private key.

Default Action

Indicates the connection was handled by the default action.

Do not Decrypt

Represents a connection the system did not decrypt.

Field values are displayed in the **SSL Status** field on the search workflow pages.

SSL Certificate Information

The information stored on the public key certificate used to encrypt traffic, including:

- Subject/Issuer Common Name
- Subject/Issuer Organization

- Subject/Issuer Organization Unit
- Not Valid Before/After
- Serial Number, Certificate Fingerprint
- Public Key Fingerprint

For syslog, see **SSLCertificate**.

SSL Failure Reason (Syslog: SSLFlowStatus)

The reason the system failed to decrypt encrypted traffic:

- Unknown
- No Match
- Success
- Uncached Session
- Unknown Cipher Suite
- Unsupported Cipher Suite
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- Internal Error
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable

- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- Invalid Action

Field values are displayed in the **SSL Status** field on the search workflow pages.

SSL Status

The action associated with the **SSL Actual Action** (Decryption rule, default action, or undecryptable traffic action) that logged the encrypted connection. The **Lock icon** links to TLS/SSL certificate details. If the certificate is unavailable (for example, for connections blocked due to TLS/SSL handshake error), the lock icon is grayed out.

If the system fails to decrypt an encrypted connection, it displays the **SSL Actual Action** (undecryptable traffic action) taken, as well as the **SSL Failure Reason**. For example, if the system detects traffic encrypted with an unknown cipher suite and allows it without further inspection, this field displays `Do Not Decrypt (Unknown Cipher Suite)`.

When searching this field, type one or more of the **SSL Actual Action** and **SSL Failure Reason** values to view encrypted traffic the system handled or failed to decrypt.

SSL Subject/Issuer Country

The two-character ISO 3166-1 alpha-2 country code for the subject or issuer country associated with the encryption certificate.

SSLCertificate (Syslog Only)

The certificate fingerprint of the TLS/SSL server.

Threat Name (Syslog: ThreatName)

The name of the detected malware.

Threat Score (Syslog: ThreatScore)

The threat score most recently associated with this file. This is a value from 0 to 100 based on the potentially malicious behaviors observed during dynamic analysis.

The threat score icon links to the Dynamic Analysis Summary report.

Time

The date and time the event was generated. This field is not searchable.

In syslog messages, see **FirstPacketSecond**.

Type / File Type (Syslog: FileType)

The type of file, for example, HTML or MSEXE.

URI / File URI (Syslog: URI)

The URI of the connection associated with the file transaction, for example, the URL from which a user downloaded the file.

User (Syslog: User)

The username associated with the IP address that initiated the connection. If this IP address is external to your network, the associated username is typically unknown.

If applicable, the username is preceded by `<realm>\`.

For file events and for malware events generated by firewall devices, this field displays the username that was determined by an identity policy or authoritative logins. In absence of an identity policy, it displays No Authentication Required.

For malware events generated by AMP for Endpoints, AMP for Endpoints determines user names. These users *cannot* be tied to user discovery or control. They do not appear in the Users table, nor can you view details for these users.

Web Application (Syslog: WebApplication)

The application that represents the content or requested URL for HTTP traffic detected in the connection.

Web Application Category or Tag

Criteria that characterize the application to help you understand the application's function.

Malware event sub-types

The table lists the malware event subtypes, whether a malware event generated by Malware Defense (a "network-based malware event") or Secure Endpoint (an "endpoint-based malware event") can have that subtype, and whether the system uses that subtype to build network file trajectories.

Table 4: Malware event types

Malware Event Subtype/Search Value	malware defense	Secure Endpoint	File Trajectory
Threat Detected in Network File Transfer	yes	no	yes
Threat Detected in Network File Transfer (retrospective)	yes	no	yes
Threat Detected	no	yes	yes
Threat Detected in Exclusion	no	yes	yes
Threat Quarantined	no	yes	yes
AMP IOC (Indications of compromise)	no	yes	no
Blocked Execution	no	yes	no
Cloud Recall Quarantine	no	yes	no
Cloud Recall Quarantine Attempt Failed	no	yes	no

Malware Event Subtype/Search Value	malware defense	Secure Endpoint	File Trajectory
Cloud Recall Quarantine Started	no	yes	no
Cloud Recall Restore from Quarantine	no	yes	no
Cloud Recall Restore from Quarantine Failed	no	yes	no
Cloud Recall Restore from Quarantine Started	no	yes	no
Quarantine Failure	no	yes	no
Quarantined Item Restored	no	yes	no
Quarantine Restore Failed	no	yes	no
Quarantine Restore Started	no	yes	no
Scan Completed, No Detections	no	yes	no
Scan Completed With Detections	no	yes	no
Scan Failed	no	yes	no
Scan Started	no	yes	no

Information available in file and malware event fields

Lists the information available in file and malware event fields for system displays and integrations.

If your organization has deployed Secure Endpoint and integrated that product with your Secure Firewall deployment:

- Malware events and indications of compromise (IOCs) imported from your Secure Endpoint deployment do not contain contextual connection information, but they do include information obtained at download or execution time, such as file path, invoking client application, and so on.
- File event table views do not display Secure Endpoint-related fields.

The table shows which fields are available for various types of file and malware events.

Table 5: Information available in file and malware event fields

Field	File Event	Malware Events Detected by the System	Retrospective Events Detected by the System	Malware Events Detected by Secure Endpoint
Action	yes	yes	yes	no
AMP Cloud	no	no	no	yes
Application File Name	no	no	no	yes

Field	File Event	Malware Events Detected by the System	Retrospective Events Detected by the System	Malware Events Detected by Secure Endpoint
Application File SHA256	no	no	no	yes
Application Protocol	yes	yes	no	no
Application Protocol Category or Tag	yes	yes	yes	no
Application Risk	yes	yes	yes	no
Archive Depth	yes	yes	no	yes
Archive Name	yes	yes	no	yes
Archive SHA256	yes	yes	no	yes
Business Relevance	yes	yes	yes	no
Category / File Type Category	yes	yes	no	yes
Client	yes	yes	yes	no
Client Category or Tag	yes	yes	yes	no
Count	yes	yes	yes	yes
Detection Name	no	yes	no	no
Detector	no	no	no	yes
Device	yes	yes	yes	yes
Disposition / File Disposition	yes	yes	yes	no
Domain	yes	yes	yes	yes
Event Subtype	no	no	no	yes
Event Type	no	yes	yes	yes
File Name	yes	yes	no	yes
File Path	no	no	no	yes
File Policy	yes	no	no	no
File Timestamp	no	no	no	yes
HTTP Response Code	yes	yes	no	no
IOC (Indication of Compromise)	no	yes	yes	yes
Message	yes	yes	no	yes
Receiving Continent	yes	yes	yes	no

Field	File Event	Malware Events Detected by the System	Retrospective Events Detected by the System	Malware Events Detected by Secure Endpoint
Receiving Country	yes	yes	no	no
Receiving IP	yes	yes	no	yes
Receiving Port	yes	yes	no	no
Security Context	yes	yes	yes	yes
Sending Continent	yes	yes	yes	no
Sending Country	yes	yes	no	no
Sending IP	yes	yes	no	no
Sending Port	yes	yes	no	no
SHA256 / File SHA256	yes	yes	yes	yes
Size (KB) / File Size (KB)	yes	yes	no	yes
SSL Actual Action (search only)	yes	yes	no	no
SSL Certificate Information (search only)	yes	yes	no	no
SSL Failure Reason (search only)	yes	yes	no	no
SSL Status	yes	yes	no	no
SSL Subject/Issuer Country (search only)	yes	yes	no	no
File Storage / Stored (search only)	yes	yes	no	no
Threat Name	no	yes	yes	yes
Threat Score	yes	yes	no	no
Time	yes	yes	yes	yes
Type / File Type	yes	yes	no	yes
URI / File URI	yes	yes	no	no
User	yes	yes	no	yes
Web Application	yes	yes	yes	no
Web Application Category or Tag	yes	yes	yes	no

View details about analyzed files

To see additional options, right-click a file SHA in a table on an event page. For more information, refer to Event investigation using web-based resources.

File composition reports

A file composition report is an analysis document that

- helps identify potentially embedded malware within analyzed files,
- lists file properties and any detected viruses, and
- is pruned when the system prunes stored files.

File composition report access

If you configure local malware analysis or dynamic analysis, the system generates a file composition report after analyzing a file. The report may also list additional information specific to that file type.

To view file composition information, refer to Using a network file trajectory, on page 33.

View file details in AMP private cloud

If you have deployed an AMP private cloud, you can view additional details about analyzed files in your private cloud.

For more information, refer to the documentation for your private cloud.

Procedure

Sign in directly to your AMP private cloud console.

Threat scores and dynamic analysis summary reports

The Secure Firewall Management Center caches a file's threat score for the same amount of time as the file's disposition. If the system later detects these files, it displays the cached threat scores instead of re-querying the Secure Malware Analytics Cloud or Secure Malware Analytics Appliance. You can automatically assign a malware file disposition to any file with a threat score that exceeds the defined malware threshold threat score.

Threat scores

Table 6: Threat score ratings

Threat Score	Numeric Score	Icon
`Low`	1-25	**Low**
`Medium`	26-50	**Medium**
`High`	51-75	**High**
`Very High`	76-100	**Very High**

The Secure Firewall Management Center caches a file's threat score for the same amount of time as the file's disposition. If the system later detects these files, it displays the cached threat scores instead of re-querying the Secure Malware Analytics Cloud or Secure Malware Analytics Appliance. You can automatically assign a malware file disposition to any file with a threat score that exceeds the defined malware threshold threat score.

Dynamic analysis summary

If a dynamic analysis summary is available, you can click the threat score icon to view it. If multiple reports exist, this summary is based on the most recent report matching the exact threat score. If none match the exact threat score, the report with the highest threat score is displayed. If more than one report exists, you can select a threat score to view each separate report.

The summary lists each component threat comprising the threat score. Each component threat is expandable to list the AMP cloud findings, as well as any processes related to this component threat.

The process tree shows the processes that started when the Secure Malware Analytics Cloud attempted to run the file. This can help identify whether a file that contains malware is attempting to access processes and system resources beyond what is expected (for example, running a Word document opens Microsoft Word, then starts Internet Explorer, then runs the Java Runtime Environment).

Each listed process contains a process identifier you can use to verify the actual process. Child nodes in the process tree represent processes started as a result of parent processes.

From the dynamic analysis summary, you can click **View Full Report** to view the full Analysis Report, detailing the AMP cloud's full analysis, including general file information, a more in-depth review of all detected processes, a breakdown of the file analysis, and other relevant information.

View Dynamic Analysis Results in the Cisco Secure Malware Analytics Cloud

Access more detailed reporting on analyzed files than is available in the Firewall Management Center by viewing additional details about files sent for analysis from your managed devices through the Secure Malware Analytics portal.

Secure Malware Analytics offers more detailed reporting on analyzed files than is available in the 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.

Before you begin

- Associate your Firewall Management Center with your Secure Malware Analytics Cloud account. See *Enabling Access to Dynamic Analysis Results in the Public Cloud* in the *Cisco Secure Firewall Management Center Device Configuration Guide*.
- License requirement: Malware
- You must be in the global domain for this task.
- You must have one of these user roles: Admin, Access Admin, Network Admin

Follow these steps to view dynamic analysis results in the Cisco Secure Malware Analytics Cloud:

Procedure

Step 1 Access the Secure Malware Analytics Cloud portal at the address provided in your Secure Malware Analytics documentation.

Step 2 Sign in with the account credentials that you used to create the association in the prerequisites to this task.

Step 3 View files submitted by your organization, or search for a particular file using its SHA.

If you have questions, refer to Secure Malware Analytics documentation.

Using captured file workflows

This task allows you to view a list of captured files in a table and manipulate the event view depending on the information relevant to your analysis. The page you see when you access captured files differs depending on the workflow, which is simply a series of pages you can use to evaluate events by moving from a broad to a more focused view. You can also create a custom workflow that displays only the information that matches your specific needs.

When a managed device captures a file detected in network traffic, it logs an event.

Note If a device captures a file containing malware, the device generates two events: a file event when it detects the file, and a malware event when it identifies malware.

If the system recaptures a file after a configuration change, such as an updated file policy, it updates existing information for that file.

For example, if you configure a file policy to capture files with a **Malware Cloud Lookup** action, the system stores the file disposition and threat score along with the file. Then, if you update your file policy, and the system recaptures the same file due to a new **Detect Files** action, the system updates the file's **Last Changed** value. However, the system does not remove the existing disposition and threat score, even though you did not perform another malware cloud lookup.

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

Before you begin

You must be an Admin or Security Analyst user to perform this task.

Procedure

Choose **Events & Logs** > **+ Show more** > **Files** > **Captured Files**.

Tip In the table view of events, several fields are hidden by default. To show a hidden field in an event view, expand the search constraints, then click the field name under **Disabled Columns**.

Related Topics

Captured file fields, on page 25
Predefined captured file workflows
Configure event view settings

Captured file fields

The table view of captured files, which is the final page in predefined captured file workflows, and which you can add to custom workflows, includes a column for each field in the captured files table.

When searching this table keep in mind that your search results depend on the available data in the events you are searching; depending on the available data, your search constraints may not apply. For example, if a file has never been submitted for dynamic analysis, it may not have an associated threat score.

Table 7: Captured file fields

Field	Description
Archive Inspection Status	For archive files, the status of archive inspection: • Pending indicates that the system is still inspecting the archive file and its contents. If the file passes through your system again, complete information becomes available. • Extracted indicates that the system was able to extract and inspect the archive's contents. • Failed may, in rare cases, occur if the system is unable to process an extraction. • Depth Exceeded indicates that the archive contains further nested archive files beyond the maximum allowed depth. • Encrypted indicates that the archive file's contents are encrypted and could not be inspected. • Not Inspectable indicates that the system did not extract and inspect the archive's contents. Policy rule actions, policy configuration, and corrupted files are three major reasons for this status. To view the contents of an archive file, right-click its row in the table to bring up the context menu, then choose **View Archive Contents**.

Field	Description
Category	The general categories of file type, for example: Office Documents, Archive, Multimedia, Executables, PDF files, Encoded, Graphics, or System Files.
Detection Name	The name of the detected malware.
Disposition	The file's malware defense disposition: • Malware indicates that local malware analysis identified malware, the AMP cloud categorized the file as malware, or that the file's threat score exceeded the malware threshold defined in the file policy. • Clean indicates that the AMP cloud categorized the file as clean, or that a user added the file to the clean list. • Unknown indicates that the system queried the AMP cloud, but the file has not been assigned a disposition; in other words, the AMP cloud has not categorized the file. • Custom Detection indicates that a user added the file to the custom detection list. • Unavailable indicates that the system could not query the AMP cloud. You may see a small percentage of events with this disposition; this is expected behavior. • N/A indicates a Detect Files or Block Files rule handled the file and the Secure Firewall Management Center did not query the AMP cloud.
Domain	The domain where the captured file was detected. This field is only present if you have ever configured the Firewall Management Center for multitenancy.

Field	Description
Dynamic Analysis Status	One or more values indicating whether the file was submitted for dynamic analysis: • Analysis Complete: file submitted for dynamic analysis that received a threat score and dynamic analysis summary report. • Capacity Handled: file stored because it could not be submitted currently. • Capacity Handled (Network Issue): file stored because it could not be submitted due to a network connectivity issue. • Capacity Handled (Rate Limit): file stored because it could not be submitted due to the maximum number of submissions reached. • Device Not Activated: file not submitted because the device is not activated on the on-premises Secure Malware Analytics Appliance. If you see this status, contact Support. • Failure (Analysis Timeout): file submitted for which the AMP cloud has yet to return a result. • Failure (Cannot Run File): file submitted that the AMP cloud could not run in the test environment. • Failure (Network Issue): file that did not get submitted due to a network connectivity failure. • Failed to send: file could not be submitted for dynamic analysis due to an internal submission failure before reaching the Secure Malware Analytics cloud. • Not Sent for Analysis: file not submitted. • Not Suspicious (Not Sent For Analysis): file pre-classified as non-malware. • Previously Analyzed: file with a cached threat score, indicating that it has been previously sent. • Rejected for Analysis: based on static analysis, the file is unlikely to pose a risk, for example because it includes no dynamic elements. • Sent for Analysis: file pre-classified as malware and queued for dynamic analysis.
Dynamic Analysis Status Changed	The last time the file's dynamic analysis status changed.
File Name	The most recently detected file name associated with the file's SHA-256 hash value.
Last Changed	The last time the information associated with this file was updated.
Last Sent	The time the file was most recently submitted to the AMP cloud for dynamic analysis.
Local Malware Analysis Status	One of these values indicating whether the system performed local malware analysis on a file: • Analysis Complete: the system inspected the file using local malware analysis and pre-classified the file • Analysis Failed: the system attempted to inspect the file using local malware analysis and failed • Manual Request Submitted: a user submitted a file for local malware analysis • Not Analyzed: the system did not inspect the file with local malware analysis

Field	Description
SHA256	The SHA-256 hash value of the file, as well as a network file trajectory icon representing the most recently detected file event and file disposition. To view the network file trajectory, click the trajectory icon.
Storage Status	Indicates whether the file is stored on a managed device: • File Stored • Not Stored (Disposition Was Pending)
Threat Score	The threat score most recently associated with this file. To view the Dynamic Analysis Summary report, click the threat score icon.
Type	The type of file; for example, HTML or MSEXE.

Stored files download

Stored files download is a security feature that

- enables downloading files from devices to a local host for long-term storage and analysis,
- archives files in a `.zip` package with disposition, file type, and SHA-256 hash value information, and
- requires confirmation by default due to potential malware risks.

Download process details

Once a device stores a file, as long as the Secure Firewall Management Center can communicate with that device and it has not deleted the file, you can download the file to a local host for long-term storage and analysis, and manually analyze the file. You can download a file from any associated file event, malware event, captured file view, or the file's trajectory.

Because malware is harmful, by default, you must confirm every file download. However, you can disable the confirmation in your User Preferences.

Because files with a disposition of Unknown may contain malware, when you download a file, the system first archives the file in a `.zip` package. The `.zip` file name contains the file disposition and file type, if available, and SHA-256 hash value. You can password-protect the `.zip` file to prevent accidental unpacking. You can edit or remove the default `.zip` file password in your User Preferences.



Caution Cisco strongly recommends you do **not** download malware, as it can cause adverse consequences. Exercise caution when downloading any file, as it may contain malware. Ensure you have taken any necessary precautions to secure the download destination before downloading files.

Submit files for analysis manually

You can manually submit captured files for analysis to help identify threats and gain faster insights.

When files are submitted manually, the system performs local analysis first. Then it submits them to the cloud for dynamic analysis. If local analysis is not enabled in a file policy, files are sent only for cloud-based dynamic analysis.

Manual submission allows you to analyze a range of file types (including those not eligible for automatic submission, such as .swf, .jar, and others), helping you quickly pinpoint causes of incidents.

Note The system checks the AMP cloud for updates (no more than once a day) to the list of file types eligible for dynamic analysis. It also checks for the minimum and maximum file sizes you can submit.

Before you begin

- Ensure at least one file rule is configured to store captured files.
- For more information, refer to the *Network Malware Protection and File Policies* chapter in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Depending on the situation, you can submit files for analysis in two ways.

Procedure

Step 1 To submit a single file for analysis:

a) Select one of these options:

- **Events & Logs** > **+ Show more** > **Files** > **File Events**
- **Events & Logs** > **+ Show more** > **Files** > **Malware Events**
- **Events & Logs** > **+ Show more** > **Files** > **Captured Files**

b) Click **Table View of <Event type or files>**.

c) Right-click a file in the table and select **Analyze File**.

Step 2 To submit multiple captured files for analysis (up to 25 at a time):

a) Select **Events & Logs** > **+ Show more** > **Files** > **Captured Files**

b) Select the checkbox beside each file to analyze.

c) Click **Analyze**.

Network file trajectory

A network file trajectory is a security feature that

- maps how hosts transferred files, including malware files, across your network,
- charts file transfer data, the disposition of the file, and if a file transfer was blocked or the file was quarantined, and

- enables determination of which hosts and users may have transferred malware, which hosts are at risk, and observation of file transfer trends.

File tracking capabilities

You can track the transmission of any file with an AMP cloud-assigned disposition. The system can use information related to detecting and blocking malware from both malware defense and Secure Endpoint to build a trajectory.

Recently detected malware and analyzed trajectories

Recently detected malware and analyzed trajectories are network security information displays that

- show the malware most recently detected on your network,
- display the files whose trajectory maps you have most recently viewed, and
- provide detailed information about each file including SHA-256 hash values, names, types, and current file dispositions.

Network file trajectory list page information

The Network File Trajectory List page displays the malware most recently detected on your network, as well as the files whose trajectory maps you have most recently viewed. From these lists, you can view when each file was most recently seen on the network, the file's SHA-256 hash value, name, type, current file disposition, contents (for archive files), and the number of events associated with the file.

The page also contains a search box that lets you locate files, either based on SHA-256 hash value or file name, or by the IP address of the host that transferred or received a file. After you locate a file, you can click the **File SHA256** value to view the detailed trajectory map.

Network file trajectory

A network file trajectory is a file analysis detail that

- tracks a file's movement across the network by searching for its SHA-256 value or by clicking a **File SHA 256** link,
- provides summary information about the file's identity, activity, and disposition, and
- shows related events, hosts, and users associated with the file.

Network file trajectory detailed view components

The network file trajectory details page comprises three main parts:

- Summary Information: A file's trajectory page displays summary information about the file, including file identification information; when the file was first seen and most recently seen on the network, and by what user; the number of related events and hosts associated with the file; and the file's current disposition. From this section, if the managed device stored the file, you can download it locally, submit the file for dynamic analysis, or add the file to a file list.

- Trajectory Map: A file's trajectory map visually tracks a file from the first detection on your network to the most recent. The map shows when hosts transferred or received the file, how often they transferred the file, and when the file was blocked or quarantined. Vertical lines between data points represent file transfers between hosts. Horizontal lines connecting the data points show a host's file activity over time.

  The map also shows how often file events occurred for the file and when the system assigned the file a disposition or retrospective disposition. You can select a data point in the map and highlight a path that traces back to the first instance the host transferred that file; this path also intersects with every occurrence involving the host as either sender or receiver of the file, and identifies the user involved.

- Related Events: The Events table lists event information for each data point in the map. Using the table and the map, you can pinpoint specific file events, hosts and users on the network that transferred or received this file, related events in the map, and other related events in a table constrained on selected values.

Network file trajectory summary information

The summary information appears at the top of the details page for a file that appears in the network file trajectory list.



Tip To view related file events, click a field value link. The first page in the File Events default workflow opens in a new window, displaying all file events that also contain the selected value.

Table 8: Network file trajectory summary information fields

Name	Description
Archive Contents	For inspected archive files, the number of files the archive contains.
Current Disposition	One of the malware defense file dispositions: • **Malware** indicates that the AMP cloud categorized the file as malware, local malware analysis identified malware, or the file's threat score exceeded the malware threshold defined in the file policy. • **Clean** indicates that the AMP cloud categorized the file as clean, or that a user added the file to the clean list. • **Unknown** indicates that the system queried the AMP cloud, but the file has not been assigned a disposition; in other words, the AMP cloud has not categorized the file. • **Custom Detection** indicates that a user added the file to the custom detection list. • **Unavailable** indicates that the system could not query the AMP cloud. You may see a small percentage of events with this disposition; this is expected behavior. • **N/A** indicates a Detect Files or Block Files rule handled the file and the Secure Firewall Management Center did not query the AMP cloud.
Detection Name	Name of the malware detected by local malware analysis.

Name	Description
Event Count	The number of events seen on the network associated with the file, and the number of events displayed in the map if there are more than 250 detected events.
File Category	The general categories of file type, for example, **Office Documents** or **System Files**.
File Names	The names of the file associated with the event, as seen on the network. If multiple file names are associated with a SHA-256 hash value, the most recent detected file name is listed. You can expand this to view the remaining file names by clicking **more**.
File SHA256	The SHA-256 hash value of the file. The hash is displayed by default in a condensed format. To view the full hash value, hover your pointer over it. If multiple SHA-256 hash values are associated with a file name, hover your pointer over the link to view all of the hash values.
File Size (KB)	The size of the file, in kilobytes.
File Type	The file type of the file, for example, **HTML** or **MSEXE**.
First Seen	The first time malware defense or Secure Endpoint detected the file, as well as the IP address of the host that first uploaded the file and identifying information for the user involved.
Last Seen	The most recent time malware defense or Secure Endpoint detected the file, as well as the IP address of the host that last downloaded the file and identifying information for the user involved.
Parent Application	The client application accessing the malware file when detection occurred by Secure Endpoint. These applications are **not** tied to network discovery or application control.
Seen On	The number of hosts that either sent or received the file. Because one host can upload and download a file at different times, the total number of hosts may not match the total number of senders plus the total number of receivers in the **Seen On Breakdown** field.
Seen On Breakdown	The number of hosts that sent the file, followed by the number of hosts that received the file.
Threat Name	Name of the threat associated with the detected malware by Secure Endpoint.
Threat Score	The file's threat score.

Network file trajectory maps and related events lists

A network file trajectory map is a visual representation that

- displays file movement across network hosts using IP addresses on the y-axis and timestamps on the x-axis,
- shows up to 250 events associated with a file SHA-256 hash in chronological order, and
- combines file events, file transfers, and retrospective events with disposition information in a single interface.

Map layout and event display

The file trajectory map's y-axis contains a list of all host IP addresses that have interacted with the file. The IP addresses are listed in descending order based on when the system first detected the file on that host. Each row contains all events associated with that IP address, whether a single file event, file transfer, or retrospective event. The x-axis contains the date and time the system detected each event. The timestamps are listed in chronological order. If multiple events occurred within a minute, all are listed within the same column. You can scroll the map horizontally and vertically to view additional events and IP addresses.

The map displays up to 250 events associated with the file SHA-256 hash. If there are more than 250 events, the map displays the first 10, then truncates extra events with an **Arrow**. The map then displays the remaining 240 events.

The first page of the File Events default workflow appears in a new window with all the extra events constrained based on the file type. If malware events generated by Secure Endpoint are not displayed, you must switch to the Malware Events table to view these.

Each data point represents an event plus the file disposition, as described in the legend below the map. For example, a Malware Block event icon combines the Malicious Disposition icon and the Block Event icon.

Malware events generated by Secure Endpoint ("endpoint-based malware events") include one icon. A retrospective event displays an icon in the column for each host on which the file is detected. File transfer events always include two icons, one file send icon and one file receive icon, connected by a vertical line. Arrows indicate the file transfer direction from sender to receiver.

To track a file's progress through the network, you can click any data point to highlight a path that includes all data points related to the selected data point. This includes data points associated with these types of events:

- any file transfers in which the associated IP address was either sender or receiver
- any malware events generated by Secure Endpoint ("endpoint-based malware events") involving the associated IP address
- if another IP address was involved, all file transfers in which that associated IP address was either sender or receiver
- if another IP address was involved, any malware events generated by Secure Endpoint ("endpoint-based malware events") involving the other IP address

All IP addresses and timestamps associated with any highlighted data point are also highlighted. The corresponding event in the Events table is also highlighted. If a path includes truncated events, the path itself is highlighted with a dotted line. Truncated events might intersect the path, but are not displayed in the map.

Using a network file trajectory

Use network file trajectory to track files as they move through your network, analyze their behavior, and identify potential security threats by examining file events and associated metadata.

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

Tip If your organization has deployed Secure Endpoint, that product also has a network file trajectory feature. To pivot from Firewall Management Center to Secure Endpoint, refer to Work with Event Data in the Secure Endpoint Console, on page 35. For details about the file trajectory feature in Secure Endpoint, refer to Secure Endpoint documentation.

Before you begin

If you are using malware defense, you need the Malware Defense license.

You must be an Admin or Security Analyst user to perform this task.

Follow these steps to use a network file trajectory.

Procedure

Step 1 Choose **Events & Logs** > **+ Show more** > **Files** > **Network File Trajectory**.

Tip You can also access a file's trajectory from the Context Explorer, dashboard, or event views with file information.

Step 2 Click a **File SHA 256** link in the list.

Step 3 Optionally, enter a complete SHA-256 hash value, the host IP address, or the name of a file you want to track into the search field, and press Enter.

Tip If only one result matches, the Network File Trajectory page for that file appears.

Step 4 In the Summary Information section, you can:

- Add a file to a file list: To add a file or remove a file from the clean list or custom detection list, click **Edit** ( ).
- Download a file: To download a file, click **Download** ( ), and if prompted, confirm you want to download the file. If the file is unavailable for download, this download file is dimmed.
- Report: Click threat score to view the Dynamic Analysis Summary report.
- Submit for dynamic analysis: Click **AMP Cloud** to submit the file for dynamic analysis. If the file is unavailable for submission or you cannot connect to the AMP cloud, this AMP cloud is dimmed.
- View archive contents: To view information about an archive file's contents, click **View** ( ).
- View file composition: To view a file's composition, click **File List**. If the system has not generated a file composition report, this file list is dimmed.
- View captured files with same threat score: Click the threat score link to view all captured files with that threat score.

Note Cisco strongly recommends you do **not** download malware, as it can cause adverse consequences. Exercise caution when downloading any file, as it may contain malware. Ensure you have taken any necessary precautions to secure the download destination before downloading files.

Step 5 On the trajectory map, you can:

- Locate the first instance: Click an IP address to locate the first time a file event occurred involving an IP address. This highlights a path to that data point, as well as any intervening file events and IP addresses related to the first file event. The corresponding event in the Events table is also highlighted. The map scrolls to that data point if not currently visible.
- Track: Click any data point to highlight a path that includes all data points related to the selected data point, tracking a file's progress through the network.
- View hidden events: Click the arrow to view all events not displayed in the File Summary event view.
- View matching file events: Hover your pointer over the **Matching File Event** to view summary information for the event. If you click any event summary information link, the first page of the File Events default workflow appears in a new window with all the extra events constrained based on the file type. The File Summary event view opens in a new window, displaying all file events that match on the criteria value you clicked.

Step 6 In the Events table, you can:

- Highlight: Choose a table row to highlight a data point in the map. The map scrolls to display the selected file event if not currently visible.
- Sort: Click the column headers to sort events in ascending or descending order.

Work with Event Data in the Secure Endpoint Console

This task allows you to access the Secure Endpoint console to view malware event data and use the global network file trajectory tool.

If your organization has deployed Secure Endpoint, you can view malware event data in the Secure Endpoint console, and use that application's global network file trajectory tool.

Tip For information about using Secure Endpoint and its console, refer to the online help in the console or other documentation available from https://www.cisco.com/c/en/us/support/security/fireamp-endpoints/tsd-products-support-series-home.html.

Before you begin

- The connection to Secure Endpoint must be configured (see *Integrate Secure Firewall and Secure Endpoint* in the *Cisco Secure Firewall Management Center Device Configuration Guide*) and Secure Firewall Management Center must be able to connect to the AMP cloud.

- You will need your Secure Endpoint credentials.
- You must be an Admin user to perform this task.
- If you want to pivot from a malware event in Firewall Management Center, ensure that the Secure Endpoint contextual cross-launch options are properly enabled. Refer to the topics under Event investigation using web-based resources.

Follow these steps to access the Secure Endpoint console from the Secure Firewall Management Center:

Procedure

Step 1 Method 1:

a) Choose **Integrations** > **+ Show more** > **AMP** > **AMP Management**.
b) Click the cloud name in the table.

Step 2 Method 2:

a) Navigate to a malware event in a table under **Events & Logs** > **+ Show more** > **Files** > **Captured Files**.
b) Right-click a file SHA and choose the Secure Endpoint option.

History for file and malware events and network file trajectory

This reference tracks the chronological development and enhancement of file and malware events and network file trajectory features across different software versions, documenting when specific capabilities were introduced and their implementation details.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
MITRE information in file and malware events.	7.4	7.4	The system now includes MITRE information (from local malware analysis) in file and malware events. You can view MITRE information in both the classic and unified events views. Note that the MITRE column is hidden by default in both event views.
Improved preclassification of files for dynamic analysis.	6.7	Any	Additional assessment avoids unnecessary sending of files for dynamic analysis. The new Dynamic Analysis Status for files not sent to the cloud based on this assessment is **Rejected for Analysis**. New/modified screens: **Analysis** > **Captured Files** > **Table View of Captured Files**.
Unique identifier for connection events in syslogs.	6.4.0.4	Any	These syslog fields collectively uniquely identify a connection event and appear in syslogs for file and malware events: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Send file and malware events via syslog.	6.4	Any	Field descriptions in this chapter specify the fields included in syslog messages. For configuration information, refer to Configuration locations for syslogs for file and malware events.