File Reputation Filtering and File Analysis

This chapter contains the following sections:

Overview of File Reputation Filtering and File Analysis

Advanced Malware Protection protects against zero-day and targeted file-based threatsby:

- Obtaining the reputation of known files.
- Analyzing behavior of certain files that are not yet known to the reputation service.
- Continuously evaluating emerging threats as new information becomes available, and notifying you about files that are determined to be threats after they have entered your network.

This feature is available for file downloads. Uploaded files.

The file reputation and file analysis services have options for either public- or private-cloud (on-premesis).

- The private-cloud file reputation service is provided by Cisco AMP Virtual Private Cloud appliance, operating in either “proxy” or “air-gap” (on-premises) mode. See Configuring an On-premises File Reputation Server, on page 7.
- The private-cloud file analysis service is provided by an on-premises Cisco AMP Malware Analytics appliance. See Configuring an On-Premises File Analysis Server , on page 7.

File Threat Verdict Updates

Threat verdicts can change as new information emerges. A file may initially be evaluated as unknown or clean, and the user may thus be allowed to access the file. If the threat verdict changes as new information becomes available, you will be alerted, and the file and its new verdict appear in the AMP Verdict Updates report. You can investigate the point-of-entry transaction as a starting point to remediating any impacts of the threat.

Verdicts can also change from malicious to clean.

When the appliance processes subsequent instances of the same file, the updated verdict is immediately applied.

Information about the timing of verdict updates is included in the file-criteria document referenced in Supported Files for File Reputation and Analysis Services , on page 3.

Related Topics

- File Reputation and File Analysis Reporting and Tracking , on page 15
- Taking Action When File Threat Verdicts Change , on page 18

File Processing Overview

First, the website from which the file is downloaded is evaluated against the Web Based Reputation Service (WBRS).

If the web reputation score of the site is in the range configured to "Scan," the appliance simultaneously scans the transaction for malware and queries the cloud-based service for the reputation of the file. (If the site's reputation score is in the "Block" range, the transaction is handled accordingly and there is no need to process the file further.) If malware is found during scanning, the transaction is blocked regardless of the reputation of the file.

If Adaptive Scanning is also enabled, file reputation evaluation and file analysis are included in Adaptive Scanning.

Communications between the appliance and the file reputation service are encrypted and protected from tampering.

After a file's reputation is evaluated:

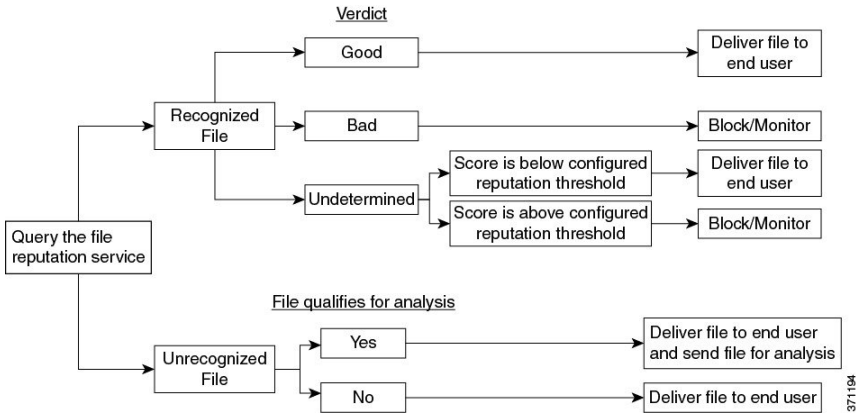
- If the file is known to the file reputation service and is determined to be clean, the file is released to the end user .
- If the file reputation service returns a verdict of malicious, then the appliance applies the action that you have specified for such files.
- If the file is known to the reputation service but there is insufficient information for a definitive verdict, the reputation service returns a threat score based on characteristics of the file such as threat fingerprint and behavioral analysis. If this score meets or exceeds the configured reputation threshold, the appliance applies the action that you have configured in the access policy for malicious or high-risk files.
- If the reputation service has no information about the file, and the file does not meet the criteria for analysis (see Supported Files for File Reputation and Analysis Services , on page 3), the file is considered clean and the file is released to the end user .
- If you have enabled the cloud-based File Analysis service, and the reputation service has no information about the file, and the file meets the criteria for files that can be analyzed (see Supported Files for File Reputation and Analysis Services , on page 3), then the file is considered clean and is optionally sent for analysis.
- For deployments with on-premises file analysis, the reputation evaluation and file analysis occur simultaneously. If the reputation service returns a verdict, that verdict is used, as the reputation service includes inputs from a wider range of sources. If the file is unknown to the reputation service, the file is released to the user but the file analysis result is updated in the local cache and is used to evaluate future instances of the file .

- If the file reputation verdict information is unavailable because the connection with the server timed out, the file is considered as Unscannable and the actions configured are applied.

Low Risk Files

When a file is initially evaluated as unknown, and has no dynamic content, the appliance sends it to the pre-classification engine, where it is designated as low risk. This file is not uploaded for analysis. If the same file is accessed within the cache expiry, it is evaluated again as low risk, and is not uploaded for analysis. After the cache timeout, if the same file is accessed again, it is evaluated as unknown and low risk sequentially. This process is repeated for low risk files. Since these low risk files are not uploaded, they will not be a part of file analysis reports.

Figure 1: Advanced Malware Protection Workflow for Cloud File Analysis Deployments



If the file is sent for analysis:

- If the file is sent to the cloud for analysis: Files are sent over HTTPS.
- Analysis normally takes minutes, but may take longer.
- A file that is flagged as malicious after File Analysis may not be identified as malicious by the reputation service. File reputation is determined by a variety of factors over time, not necessarily by a single file analysis verdict.
- Results for files analyzed using an on premises Cisco Secure Endpoint Malware Analytics appliance are cached locally.

For information about verdict updates, see File Threat Verdict Updates , on page 1.

Supported Files for File Reputation and Analysis Services

The reputation service evaluates most file types. File type identification is determined by file content and is not dependent on the filename extension.

Some files with unknown reputation can be analyzed for threat characteristics. When you configure the file analysis feature, you choose which file types are analyzed. New types can be added dynamically; you will receive an alert when the list of uploadable file types changes, and can select added file types to upload.

Details about what files are supported by the reputation and analysis services are available only to registered Cisco customers. For information about which files are evaluated and analyzed, see *File Criteria for Advanced Malware Protection Services for Cisco Content Security Products*, available from

http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html. The criteria for evaluating a file's reputation and for sending files for analysis may change at any time.

In order to access this document, you must have a Cisco customer account with a support contract. To register, visit https://tools.cisco.com/RPF/register/register.do.

Your setting for **DVS Engine Object Scanning Limits** on the **Security Services > Anti-Malware and Reputation** page also determines the maximum file size for file reputation and analysis.

You should configure policies to block download of files that are not addressed by Advanced Malware Protection.

Note A file (either in incoming mail or outgoing mail) that has already been uploaded for analysis from any source will not be uploaded again. To view analysis results for such a file, search for the SHA-256 from the File Analysis reporting page.

Related Topics

- Enabling and Configuring File Reputation and Analysis Services , on page 8
- Ensuring That You Receive Alerts About Advanced Malware Protection Issues, on page 14
- Archive or Compressed File Processing, on page 4

Archive or Compressed File Processing

If the file is compressed or archived,

- Reputation of the compressed or archive file is evaluated.
- In case of some selective file types, the compressed or archive file is decompressed and reputations of all the extracted files are evaluated.

For information about which archived and compressed files are examined, including file formats, see the information linked from Supported Files for File Reputation and Analysis Services , on page 3.

In this scenario,

- If one of the extracted files is malicious, the file reputation service returns a verdict of Malicious for the compressed or the archive file.
- If the compressed or archive file is malicious and all the extracted files are clean, the file reputation service returns a verdict of Malicious for the compressed or the archive file.
- If the verdict of any of the extracted files is unknown, the extracted files are optionally (if configured and the file type is supported for file analysis) sent for file analysis.
- If the extraction of a file fails while decompressing a compressed or an archive file, the file reputation service returns a verdict of Unscannable for the compressed or the archive file. Keep in mind that, in this scenario, if one of the extracted files is malicious, the file reputation service returns a verdict of Malicious for the compressed or the archive file (Malicious verdict takes precedence over Unscannable verdict).
- An archive or compressed file is treated as unscannable in the following scenarios:
  - The data compression ratio is more than 20.
  - The archive file contains more than five levels of nesting.
  - The archive file contains more than 200 child files.

- The archive file size is more than 50 MB.
- The archive file is password protected or unreadable.

Note Reputation of the extracted files with safe MIME types, for example, text/plain, are not evaluated.

Privacy of Information Sent to the Cloud

- Only the SHA that uniquely identifies a file is sent to the reputation service in the cloud. The file itself is not sent.
- If you are using the file analysis service in the cloud and a file qualifies for analysis, the file itself is sent to the cloud.
- Information about every file that is sent to the cloud for analysis and has a verdict of "malicious" is added to the reputation database. This information is used along with other data to determine a reputation score.

  Information about files analyzed by an on premises Cisco Secure Endpoint Malware Analytics appliance is not shared with the reputation service.

Configuring File Reputation and Analysis Features

Requirements for Communication with File Reputation and Analysis Services

- All that use these services must be able to connect to them directly over the internet (excluding File Analysis services configured to use an on-premises Cisco Secure Endpoint Malware Analytics Appliance.)
- By default, communication with file reputation and analysis services is routed through the Management port (M1) on the appliance. If your appliance does not route data through the management port, see Routing Traffic to File Reputation and File Analysis Servers Through a Data Interface , on page 6.
- By default, communication with file reputation and cloud-based analysis services is routed through the interface that is associated with the default gateway. To route this traffic through a different interface,

create a static route for each address in the Advanced section of the Security Services > File Reputation and Analysis page.

- The following firewall ports must be open:

Firewall Ports	Description	Protocol	In/Out	Hostname	Appliance Interface
32137 (default) or 443	Access to cloud services for obtaining file reputation.	TCP	Out	As configured in Security Services > Anti-Malware and Reputation, Advanced section: Advanced Settings for File Reputation, Cloud Server Pool parameter.	Management, unless a static route is configured to route this traffic through a data port.
443	Access to cloud services for file analysis.	TCP	Out	As configured in Security Services > Anti-Malware and Reputation, Advanced section: Advanced Settings for File Analysis.	

- When you configure the file reputation feature, choose whether to use SSL over port 443.

Related Topics

- Enabling and Configuring File Reputation and Analysis Services

Routing Traffic to File Reputation and File Analysis Servers Through a Data Interface

If the appliance is configured to restrict the management port to appliance management services only (on the **Network > Interfaces** page), configure the appliance to route file reputation and analysis traffic through the data port instead.

Add routes for data traffic on the Network > Routes page. For general requirements and instructions, see Configuring TCP/IP Traffic Routes

For Connection To	Destination Network	Gateway
The file reputation service	In Security Services > Anti-Malware and Reputation, Advanced section > Advanced Settings for File Reputation section, provide the name (URL) of the **File Reputation Server**, and the cloud server pool's **Cloud Domain** name. If you choose Private Cloud for File Reputation Server, enter the host name or IP address of the Server, and provide a valid Public Key. This must be the same key used by the private cloud appliance. Host name of the Cloud Server Pool, as configured in Security Services ; Anti-Malware and Reputation, Advanced section: Advanced Settings for File Reputation.	IP address of the gateway for the data port

For Connection To	Destination Network	Gateway
The file analysis service	• In Security Services > Anti-Malware and Reputation, Advanced section > Advanced Settings for File Analysis section, provide the name (URL) of the **File Analysis Server**. If you choose Private Cloud for the File Analysis Server, enter the Server URL, and provide a valid Certificate Authority. • The File Analysis Client ID is client ID for this appliance on the File Analysis server (read-only). Host name of the File Analysis Server, as configured in Security Services; Anti-Malware and Reputation, Advanced section: Advanced Settings for File Analysis.	IP address of the gateway for the data port

Related Topics

- Configuring TCP/IP Traffic Routes

Configuring an On-premises File Reputation Server

If you will use a Cisco AMP Virtual Private Cloud appliance as a private-cloud file analysis server:

- You can obtain the Cisco Advanced Malware Protection Virtual Private Cloud Appliance documentation, including the Installation and Configuration of FireAMP Private Cloud guide, from http://www.cisco.com/c/en/us/support/security/fireamp-private-cloud-virtual-appliance/tsd-products-support-series-home.html

  Use that documentation to perform the tasks described in this topic.

  Additional documentation is available using the Help link in the AMP Virtual Private Cloud appliance.
- Set up and configure the Cisco AMP Virtual Private Cloud appliance in either “proxy” or “air-gap” (on-premises) mode.
- Ensure the Cisco AMP Virtual Private Cloud appliance software version is 2.2, which enables integration with Cisco .
- Download the AMP Virtual Private Cloud certificate and keys on that appliance for upload to this

Note After you have set up the on-premises file-reputation server, you will configure connection to it from this ; see Step 6 of Enabling and Configuring File Reputation and Analysis Services , on page 8

Configuring an On-Premises File Analysis Server

If you will use a Cisco Secure Endpoint Malware Analytics Appliance as a private-cloud file analysis server:

- Obtain the Cisco Secure Endpoint Malware Analytics Appliance Setup and Configuration Guide and the Cisco Secure Endpoint Malware Analytics Appliance Administration Guide. Cisco Secure Endpoint Malware Analytics Appliance documentation is available from http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides%20-list.html.

  Use this documentation to perform the tasks described in this topic.

  Additional documentation is available from the Help link in the Cisco Secure Endpoint Malware Analytics appliance.

  In the Administration Guide, search for information about all of the following: integrations with other Cisco appliances, CSA, Cisco Sandbox API .

- Set up and configure the Cisco Secure Endpoint Malware Analytics Appliance.
- If necessary, update your Cisco Secure Endpoint Malware Analytics Appliance software to version 1.2.1, which supports integration with Cisco.

  See the AMP Malware Analytics documentation for instructions for determining the version number and for performing the update.

- Ensure that your appliances can communicate with each other over your network. Cisco must be able to connect to the CLEAN interface of the Cisco Secure Endpoint Malware Analytics appliance.
- If you will deploy a self-signed certificate: Generate a self-signed SSL certificate from the Cisco Secure Endpoint Malware Analytics appliance to be used on your . See instructions for downloading SSL certificates and keys in the administrator's guide for your Cisco Secure Endpoint Malware Analytics appliance. Be sure to generate a certificate that has the hostname of your Cisco Secure Endpoint Malware Analytics appliance as CN. The default certificate from the Cisco Secure Endpoint Malware Analytics appliance does NOT work.
- Registration of your with your Malware Analytics appliance occurs automatically when you submit the configuration for File Analysis, as described in Enabling and Configuring File Reputation and Analysis Services . However, you must activate the registration as described in the same procedure.

Note After you have set up the on-premises file-analysis server, you will configure connection to it from this ; see Step 7 of Enabling and Configuring File Reputation and Analysis Services

Enabling and Configuring File Reputation and Analysis Services

Before you begin

- Acquire feature keys for the file reputation service and the file analysis service and transfer them to this appliance. See Working with Feature Keys for more information about adding feature keys to the appliance.
- Meet the Requirements for Communication with File Reputation and Analysis Services , on page 5.
- Ensure that a Data network interface is enabled on the appliance if you want to use a Data network interface for File Reputation and Analysis services. See Enabling or Changing Network Interfaces
- Verify connectivity to the update servers configured in Configuring Upgrade and Service Update Settings.

- If you will use a Cisco AMP Virtual Private Cloud Appliance as a private cloud file reputation server, see Configuring an On-premises File Reputation Server, on page 7.
- If you will use a Cisco Secure Endpoint Malware Analytics Appliance as a private cloud file analysis server, see Configuring an On-Premises File Analysis Server , on page 7.

Step 1 Select **Security Services > Anti-Malware and Reputation**.

Step 2 Click **Edit Global Settings**.

Step 3 Click **Enable File Reputation Filtering** and optionally **Enable File Analysis**.

- If **Enable File Reputation Filtering** is checked, you must configure the section **File Reputation Server** (in **Step 6**), by either choosing the URL of an external public-reputation cloud server, or by providing the Private reputation cloud server connection information.
- Similarly, if **Enable File Analysis** is checked, you must configure the section **File Analysis Server URL** (in **Step 7**), providing either the URL of an external cloud server, or the Private analysis cloud connection information.

Note New file types may be added after an upgrade and are not enabled by default. If you have enabled file analysis, and require the new file types to be included in analysis, you must enable them.

Step 4 Accept the license agreement if presented.

Step 5 In the **File Analysis** section, select the required file types from the appropriate file groups (for example, "Microsoft Documents") to send for file analysis.

For information about supported file types, see the document described in Supported Files for File Reputation and Analysis Services , on page 3

Step 6 Expand the **Advanced Settings for File Reputation** panel and adjust the following options as needed:

Option	Description
Cloud Domain	The name of the domain to be used for file reputation queries.
File Reputation Server	Choose either: the host name of the public reputation cloud server, or Private reputation cloud. If you choose Private reputation cloud, provide the following: • **Server** – The host name or IP address of the Cisco AMP Virtual Private Cloud appliance. • **Public Key** – Provide a valid public key for encrypted communications between this appliance and your private cloud appliance. This must be the same key used by the private cloud server: locate the key file on this appliance, and then click **Upload File**. **Note** You must have already downloaded the key file from the server to this appliance.
Routing Table	The routing table (associated with an appliance network interface type, either Management or Data) to be used for Advanced Malware Protection services. If the appliance has both the Management interface and one or more Data interfaces enabled, you can select Management or Data.

Option	Description
SSL Communication for File Reputation	Check **Use SSL (Port 443)** to communicate on port 443 instead of the default port, 32137. Refer to the Cisco AMP Virtual Private Cloud Appliance user guide for information about enabling SSH access to the server. **Note** SSL communication over port 32137 may require you to open that port in your firewall. This option also allows you to configure an upstream proxy for communication with the file reputation service. If checked, provide the appropriate **Server**, **Username** and **Passphrase** information. When **Use SSL (Port 443)** is selected, you can also check **Relax Certificate Validation** to skip standard certificate validation if the tunnel proxy server's certificate is not signed by a trusted root authority. For instance, select this option if using a self-signed certificate on a trusted internal tunnel proxy server. **Note** If you checked **Use SSL (Port 443)** in the SSL Communication for File Reputation section of the Advanced Settings for File Reputation, you must add the AMP on-premises reputation server CA certificate to the certificate store on this appliance, using Network > Certificates (Custom Certificate Authorities) in the Web interface. Obtain this certificate from the server (Configuration > SSL > Cloud server > download).
Heartbeat Interval	The frequency, in minutes, with which to ping for retrospective events.
Query Timeout	The number of elapsed seconds before the reputation query times out.
File Reputation Client ID	The client ID for this appliance on the File Reputation server (read-only).

Note Do not change any other settings in this section without guidance from Cisco support.

Step 7 If you will use the cloud service for file analysis, expand the Advanced Settings for File Analysis panel and adjust the following options as needed:

Option	Description
File Analysis Server URL	Choose either: the name (URL) of an external cloud server, or **Private analysis cloud**. If specifying an external cloud server, choose the server that is physically nearest to your appliance. Newly available servers will be added to this list periodically using standard update processes. Choose Private analysis cloud to use an on-premises Cisco Secure Endpoint Malware Analytics appliance for file analysis, and provide the following: • **TG Servers** – Enter the IPv4 address or hostname of the standalone or clustered Cisco Secure Endpoint Malware Analytics appliances. You can add a maximum of seven Cisco Secure Endpoint Malware Analytics appliances. **Note** The Serial Number indicates the order in which you add the standalone or clustered Cisco Secure Endpoint Malware Analytics appliances. It does not denote the priority of the appliances. **Note** You cannot add standalone and cluster servers in one instance. It must be either standalone or cluster. You can add only one standalone server in an instance. If it is a cluster mode, you can add multiple servers upto seven and all the servers must belong to the same cluster. You cannot add multiple clusters. • **Certificate Authority** – Choose either **Use Cisco Default Certificate Authority**, or **Use Uploaded Certificate Authority**. If you choose Use **Uploaded Certificate Authority**, click **Browse** to upload a valid certificate file for encrypted communications between this appliance and your private cloud appliance. This must be the same certificate used by the private cloud server. **Note** If you have configured the Cisco Secure Endpoint Malware Analytics portal on your appliance for file analysis, you can access the Cisco Secure Endpoint Malware Analytics portal (for example, https://panacea.threatgrid.eu) to view and track the files submitted for file analysis. For more information on how to access the Cisco Secure Endpoint Malware Analytics portal, contact Cisco TAC.
Proxy Settings	Check **Use File Reputation Proxy** checkbox to use the same File Reputation tunnel proxy that you have already configured, as an upstream proxy for file analysis. If you want to configure a different upstream proxy, uncheck the **Use File Reputation Proxy** checkbox and enter the appropriate **Server**, **Port**, **Username**, and **Passphrase** information.
File Analysis Client ID	The client ID for this appliance on the File Analysis server (read-only).

Step 8 (Optional) Expand the Cache Settings panel, if you want to configure the cache expiry period for File Reputation disposition values.

Step 9 Expand the Threshold Settings panel, if you want to set the upper limit for the acceptable file analysis score. The score above this threshold indicates that the file is infected. Choose any one of the following options:

- Use value from Cloud Service (95)
- Enter Custom Value – defaults to 95

Note The **Threshold Settings** option are now categorized as **File Analysis Threshold** instead of **Reputation Threshold**.

Step 10 Submit and commit your changes.

Step 11 If you are using an on-premises Cisco Secure Endpoint Malware Analytics appliance, activate the account for this appliance on the Cisco Secure Endpoint Malware Analytics appliance.

Complete instructions for activating the "user" account are available in the Cisco Secure Endpoint Malware Analytics documentation.

a) Note the File Analysis Client ID that appears at the bottom of the page section. This identifies the "user" that you will activate.
b) Sign in to the Cisco Secure Endpoint Malware Analytics appliance.
c) Select **Welcome... > Manage Users** and navigate to User Details.
d) Locate the "user" account based on the File Analysis Client ID of your .
e) Activate this "user" account for your appliance.

Important! Changes Needed in File Analysis Setting

If you plan to use a new public cloud File Analysis service, make sure you read the following instructions to maintain datacenter isolation:

- The existing appliance grouping information is not preserved in the new File Analysis server. You must regroup your appliances on the new File Analysis server.
- Messages that are quarantined to the File Analysis Quarantine are retained until the retention period. After the quarantine retention period, the messages are released from the File Analysis Quarantine, and re-scanned by the AMP engine. The file is then uploaded to the new File Analysis server for analysis but the message is not sent to the File Analysis Quarantine again.

For more details, refer to the Cisco AMP Malware Analytics documentation from http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html.

(Public Cloud File Analysis Services Only) Configuring Appliance Groups

To allow all content security appliances in your organization to view file analysis result details in the cloud for files sent for analysis from any appliance in your organization, you need to join all appliances to the same appliance group.

Note You can configure appliance groups at the machine level. The appliance groups cannot be configured at the cluster level.

Step 1 Select **Security Services > Anti-Malware and Reputation** .

Step 2 [Applicable if Smart Licensing is disabled on your email gateway] Enter the group ID manually in the **Appliance ID/Name** field and click **Group Now**.

Or

[Applicable if Smart Licensing is enabled on your email gateway] The system automatically registers the Smart Account ID as group ID and displays it in the **Appliance Group ID/Name** field.

Notes:

- An appliance can belong to only one group.
- You can add a machine to a group at any time.
- You can configure appliance groups at the machine and the cluster levels.
- If this is the first appliance being added to the group, provide a useful identifier for the group. This ID is case-sensitive and cannot contain spaces.
- The appliance group ID you provide must be identical on all appliances that will share data about files that are uploaded for analysis. However, the ID is not validated on subsequent appliances in the group.
- If you update the appliance group ID, the change takes effect immediately, and it does not require a Commit.
- You must configure all appliances in a group to use the same File Analysis server in the cloud.
- If Smart Licensing is enabled, the appliances are grouped using the Smart Account ID.

Step 3 In the Appliance Grouping for File Analysis Cloud Reporting section, enter the File Analysis Cloud Reporting Group ID.

- If this is the first appliance being added to the group, provide a useful identifier for the group.
- This ID is case-sensitive, and cannot contain spaces.
- The ID you provide must be identical on all appliances that will share data about files that are uploaded for analysis. However, the ID is not validated on subsequent group appliances.
- If you enter the Group ID incorrectly or need to change it for any other reason, you must open a case with Cisco TAC.
- This change takes effect immediately; it does not require a Commit.
- All appliances in the group must be configured to use the same File Analysis server in the cloud.
- An appliance can belong to only one group.
- You can add a machine to a group at any time, but you can do it only once.

Step 4 Click **Add Appliance to Group**.

Which Appliances Are In the Analysis Group?

Step 1 Select **Security Services> Anti-Malware and Reputation** .

Step 2 In the Appliance Grouping for File Analysis Cloud Reporting section, click **View Appliances in Group**.

Step 3 To view the **File Analysis Client ID** of a particular appliance, look in the following location:

Appliance	Location of File Analysis Client ID
Email Security appliance	Advanced Settings for File Analysis section on the **Security Services > File Reputation and Analysis** page.
Web Security Appliance	Advanced Settings for File Analysis section on the **Security Services > Anti-Malware and Reputation** page.
Security Management appliance	At the bottom of the **Management Appliance > Centralized Services > Security Appliances** page.

Configuring File Reputation and Analysis Service Action Per Access Policy

Step 1 Select **Web Security Manager > Access Policies**.

Step 2 Click the link in the **Anti-Malware and Reputation** column for a policy in the table.

Step 3 In the **Advanced Malware Protection Settings** section, select **Enable File Reputation Filtering and File Analysis**.

If File Analysis is not enabled globally, only File Reputation Filtering is offered.

Step 4 Select an action for **Known Malicious and High-Risk Files**: **Monitor** or **Block**.

The default is Monitor.

Step 5 Submit and commit your changes.

Ensuring That You Receive Alerts About Advanced Malware Protection Issues

Ensure that the appliance is configured to send you alerts related to Advanced Malware Protection.

You will receive alerts when:

Alert Description	Type	Severity
You are setting up a connection to an on-premises (private cloud) Cisco Secure Endpoint Malware Analytics appliance and you need to activate the account as described in Enabling and Configuring File Reputation and Analysis Services .	Anti-Malware	Warning
Feature keys expire	(As is standard for all features)	

Alert Description	Type	Severity
The file reputation or file analysis service is unreachable.	Anti-Malware	Warning
Communication with cloud services is established.	Anti-Malware	Info
		Info
A file reputation verdict changes.	Anti-Malware	Info
File types that can be sent for analysis have changed. You may want to enable upload of new file types.	Anti-Malware	Info
Analysis of some file types is temporarily unavailable.	Anti-Malware	Warning
Analysis of all supported file types is restored after a temporary outage.	Anti-Malware	Info
Invalid File Analysis service key. You need to contact Cisco TAC with the file analysis id details to fix this error.	AMP	Error

Related Topics

- Several Alerts About Failure to Connect to File Reputation or File Analysis Servers , on page 19
- Taking Action When File Threat Verdicts Change , on page 18

Configuring Centralized Reporting for Advanced Malware Protection Features

If you will centralize reporting on a Security Management appliance, see important configuration requirements in the Advanced Malware Protection sections in the web reporting topic of the online help or user guide for your management appliance.

File Reputation and File Analysis Reporting and Tracking

Identifying Files by SHA-256 Hash

Because filenames can easily be changed, the appliance generates an identifier for each file using a Secure Hash Algorithm (SHA-256). If an appliance processes the same file with different names, all instances are recognized as the same SHA-256. If multiple appliances process the same file, all instances of the file have the same SHA-256 identifier.

In most reports, files are listed by their SHA-256 value (in an abbreviated format). To identify the filenames associated with a malware instance in your organization, select Reporting > Advanced Malware Protection and click an SHA-256 link in the table. The details page shows associated filenames.

File Reputation and File Analysis Report Pages

Report	Description
Advanced Malware Protection	Shows file-based threats that were identified by the file reputation service. For files with changed verdicts, see the AMP Verdict updates report. Those verdicts are not reflected in the Advanced Malware Protection report. If a file extracted from a compressed or archived file is malicious, only the SHA value of the compressed or archived file is included in the Advanced Malware Protection report. The **Incoming Malware Files by Category** section shows the percentage of file SHAs on the blocked list received from the AMP for Endpoints console that are categorised as **Custom Detection**. The threat name of file SHA on the blocked list obtained from AMP for Endpoints console is displayed as **Simple Custom Detection** in the Incoming Malware Threat Files section of the report. You can click the link in the More Details section of the report to view the file trajectory details about file SHA on the blocked list in the AMP for Endpoints console. You can view the **Low Risk** verdict details in the Incoming Files Handed by AMP section of the report.
Advanced Malware Protection File Analysis	Displays the time and verdict (or interim verdict) for each file sent for analysis. The appliance checks for analysis results every 30 minutes. To view more than 1000 File Analysis results, export the data as a .csv file. Drill down to view detailed analysis results, including the threat characteristics for each file. You can also search for additional information about an SHA, or click the link at the bottom of the file analysis details page to view additional details on the server that analyzed the file. **Note** If extracted files from a compressed or an archive file are sent for file analysis, only SHA values of these extracted files are included in the File Analysis report.

Report	Description
Advanced Malware Protection Reputation	Because Advanced Malware Protection is focused on targeted and zero-day threats, threat verdicts can change as aggregated data provides more information. The AMP Reputation report lists the files processed by this appliance for which the verdict has changed since the message was received. For more information about this situation, see File Threat Verdict Updates , on page 1. To view more than 1000 verdict updates, export the data as a .csv file. In the case of multiple verdict changes for a single SHA-256, this report shows only the latest verdict, not the verdict history. To view all affected messages for a particular SHA-256 within the maximum available time range (regardless of the time range selected for the report) click a SHA-256 link.

Viewing File Reputation Filtering Data in Other Reports

Data for file reputation and analysis is available in other reports where relevant. A ;Blocked by Advanced Malware Protection" column may be hidden by default in applicable reports. To display additional columns, click the Columns link below the table.

The Report by User Location includes an Advanced Malware Protection tab.

About Web Tracking and Advanced Malware Protection Features

When searching for file threat information in Web Tracking, keep the following points in mind:

- To search for malicious files found by the file reputation service, select **Known Malicious and High-Risk Files** for the **Filter by Malware Category** option in the Malware Threat area in the Advanced section in Web Message Tracking.
- Web Tracking includes only information about file reputation processing and the original file reputation verdicts returned at the time a transaction message was processed. For example, if a file was initially found to be clean, then a verdict update found the file to be malicious, only the clean verdict appears in Tracking results.

  No information is provided for clean or unscannable attachments.

  “Block – AMP” in search results means the transaction was blocked because of the file's reputation verdict.

  In Tracking details, the “AMP Threat Score” is the best-effort score that the cloud reputation service provides when it cannot determine a clear verdict for the file. In this situation, the score is between 1 and 100. (Ignore the AMP Threat Score if an AMP Verdict is returned or if the score is zero .) The appliance compares this score to the threshold score (configured on the Security Services > Anti-Malware and Reputation page) to determine what action to take. By default, files with scores between 60 and 100 are considered malicious. Cisco does not recommend changing the default threshold score. The WBRS score

is the reputation of the site from which the file was downloaded; this score is not related to the file reputation.

- Verdict updates are available only in the AMP Verdict Updates report. The original transaction details in Web Tracking are not updated with verdict changes. To see transactions involving a particular file , click a SHA-256 in the verdict updates report.
- Information about File Analysis, including analysis results and whether or not a file was sent for analysis, are available only in the File Analysis report.

  Additional information about an analyzed file may be available from the cloud or on-premises File Analysis server. To view any available File Analysis information for a file, select **Reporting > File Analysis** and enter the SHA-256 to search for the file , or click the SHA-256 link in Web Tracking details. If the File Analysis service has analyzed the file from any source, you can see the details. Results are displayed only for files that have been analyzed.

  If the appliance processed a subsequent instance of a file that was sent for analysis, those instances will appear in Web Tracking search results.

Taking Action When File Threat Verdicts Change

Step 1 View the AMP Verdict Updates report.

Step 2 Click the relevant SHA-256 link to view web tracking data for all transactions involving that file that end users were allowed to access.

Step 3 Using the tracking data, identify the users that may have been compromised, as well as information such as the file names involved in the breach and the web site from which the file was downloaded.

Step 4 Check the File Analysis report to see if this SHA-256 was sent for analysis, to understand the threat behavior of the file in more detail.

What to do next

Related Topics

File Threat Verdict Updates , on page 1

Troubleshooting File Reputation and Analysis

Log Files

In logs:

- `AMP` and `amp` refer to the file reputation service or engine.
- `Retrospective` refers to verdict updates.
- `VRT` and `sandboxing` refer to the file analysis service.

Information about Advanced Malware Protection including File Analysis is logged in Access Logs or in AMP Engine Logs. For more information, see the topic on monitoring system activity through logs.

In the log message "Response received for file reputation query" possible values for "upload action" are:

- 1: SEND. In this case, you must send the file for File Analysis.
- 2: DON'T SEND. In this case, you do not send the file for File Analysis.
- 3: SEND ONLY METADATA. In this case, you send only the metadata and not the entire file for File Analysis.
- 0: NO ACTION. In this case, no other action is required.

Several Alerts About Failure to Connect to File Reputation or File Analysis Servers

Problem

You receive several alerts about failures to connect to the file reputation or analysis services in the cloud. (A single alert may indicate only a transient issue.)

Solution

- Ensure that you have met the requirements in Requirements for Communication with File Reputation and Analysis Services , on page 5.
- Check for network issues that may prevent the appliance from communicating with the cloud services.
- Increase the Query Timeout value:

  Select **Security Services > Anti-Malware and Reputation**. The Query Timeout value is in the Advanced settings area of the Advanced Malware Protection **Services** section.

API Key Error (On-Premises File Analysis)

Problem

You receive an API key alert when attempting to view File Analysis report details, or the is unable to connect to the AMP Malware Analytics server to upload files for analysis.

Solution

This error can occur if you change the hostname of the AMP Malware Analytics server and you are using a self-signed certificate from the AMP Malware Analytics server, as well as possibly under other circumstances. To resolve the issue:

- Generate a new certificate from the AMP Malware Analytics appliance that has the new hostname.
- Upload the new certificate to the .
- Reset the API key on the AMP Malware Analytics appliance. For instructions, see the online help on the AMP Malware Analytics appliance.

Related Topics

- Enabling and Configuring File Reputation and Analysis Services

Files are Not Uploaded As Expected

Problem

Files are not evaluated or analyzed as expected. There is no alert or obvious error.

Solution

Consider the following:

- The file may have been sent for analysis by another appliance and thus already be present on the File Analysis server or in the cache of the appliance that is processing the file.
- Check the maximum file size limit configured for the **DVS Engine Object Scanning Limits** on the **Security Services > Anti-Malware and Reputation** page. This limit applies to Advanced Malware Protection features.

File Analysis Details in the Cloud Are Incomplete

Problem

Complete file analysis results in the public cloud are not available for files uploaded from other Web Security Appliance s in my organization.

Solution

Be sure to group all appliances that will share file analysis result data. See (Public Cloud File Analysis Services Only) Configuring Appliance Groups , on page 12. This configuration must be done on each appliance in the group.

Alerts about File Types That Can Be Sent for Analysis

Problem

You receive alerts of severity Info about file types that can be sent for file analysis.

Solution

This alert is sent when supported file types change, or when the appliance checks to see what file types are supported. This can occur when:

- You or another administrator changes the file types selected for analysis.

- Supported file types change temporarily based on availability in the cloud service. In this case, support for the file types selected on the appliance will be restored as soon as possible. Both processes are dynamic and do not require any action from you.
- The appliance restarts, for example as part of an AsyncOS upgrade.