Network Security

This topic contains the following sections:

Configuring Security Services

This topic contains the following sections:

Overview of Configuring Security Services

The Secure Web Appliance uses security components to protect end users from a range of malware threats. You can configure anti-malware and web reputation settings for each policy group. When you configure

Access Policies, you can also have AsyncOS for Web choose a combination of anti-malware scanning and web reputation scoring to use when determining what content to block.

To protect end users from malware, you enable these features on the appliance, and then configure anti-malware and web reputation settings per policy.

Option	Description	Link
Anti-malware scanning	Works with multiple anti-malware scanning engines integrated on the appliance to block malware threats	Overview of Anti-Malware Scanning , on page 4
Web Reputation Filters	Analyzes web server behavior and determines whether the URL contains URL-based malware	Overview of Web Reputation Filters , on page 2
Secure Endpoint	Protects from threats in downloaded files by evaluating file reputation and by analyzing file characteristics.	Overview of File Reputation Filtering and File Analysis , on page 18

Related Topics

- Enabling Anti-Malware and Reputation Filters, on page 7
- Understanding Adaptive Scanning, on page 7

Overview of Web Reputation Filters

Web Reputation Filters assigns a web-based reputation score (WBRS) to a URL to determine the likelihood that it contains URL-based malware. The Secure Web Appliance uses web reputation scores to identify and stop malware attacks before they occur. You can use Web Reputation Filters with Access, Decryption, and Cisco Data Security Policies.

Web Reputation Scores

Web Reputation Filters use data to assess the reliability of Internet domains and score the reputation of URLs. The web reputation calculation associates a URL with network parameters to determine the probability that malware exists. The aggregate probability that malware exists is then mapped to a Web Reputation Score between -10 and +10, with +10 being the least likely to contain malware.

Example parameters include the following:

- URL categorization data
- Presence of downloadable code
- Presence of long, obfuscated End-User License Agreements (EULAs)
- Global volume and changes in volume
- Network owner information
- History of a URL
- Age of a URL
- Presence on any block lists
- Presence on any allow lists
- URL typos of popular domains

- Domain registrar information
- IP address information

Note Cisco does not collect identifiable information such as user names, passphrases, or client IP addresses.

Understanding How Web Reputation Filtering Works

Web Reputation Scores are associated with an action to take on a URL request. You can configure each policy group to correlate an action to a particular Web Reputation Score. The available actions depend on the policy group type that is assigned to the URL request:

Policy Type	Action
Access Policies	You can choose to block, scan, or allow
Decryption Policies	You can choose to drop, decrypt, or pass through
Cisco Data Security Policies	You can choose to block or monitor

Web Reputation in Access Policies

When you configure web reputation settings in Access Policies, you can choose to configure the settings manually, or let AsyncOS for Web choose the best options using Adaptive Scanning. When Adaptive Scanning is enabled, you can enable or disable web reputation filtering in each Access Policy, but you cannot edit the Web Reputation Scores.

Score	Action	Description	Example
-10 to -6.0	Block	Bad site. The request is blocked, and no further malware scanning occurs.	• URL downloads information without user permission. • Sudden spike in URL volume. • URL is a typo of a popular domain.
-5.9 to 5.9	Scan	Undetermined site. Request is passed to the DVS engine for further malware scanning. The DVS engine scans the request and server response content.	• Recently created URL that has a dynamic IP address and contains downloadable content. • Network owner IP address that has a positive Web Reputation Score.
6.0 to 10.0	Allow	Good site. Request is allowed. No malware scanning required.	• URL contains no downloadable content. • Reputable, high-volume domain with long history. • Domain present on several allow lists. • No links to URLs with poor reputations.

By default, URLs in an HTTP request that are assigned a Web Reputation Score of +7 are allowed and require no further scanning. However, a weaker score for an HTTP request, such as +3, is automatically forwarded

to the Cisco DVS engine where it is scanned for malware. Any URL in an HTTP request that has a poor reputation is blocked.

Related Topics

- Understanding Adaptive Scanning, on page 7

Web Reputation in Decryption Policies

Score	Action	Description
-10 to -9.0	Drop	Bad site. The request is dropped with no notice sent to the end user. Use this setting with caution.
-8.9 to 5.9	Decrypt	Undetermined site. Request is allowed, but the connection is decrypted and Access Policies are applied to the decrypted traffic.
6.0 to 10.0	Pass through	Good site. Request is passed through with no inspection or decryption.

Web Reputation in Cisco Data Security Policies

Score	Action	Description
-10 to -6.0	Block	Bad site. The transaction is blocked, and no further scanning occurs.
-5.9 to 0.0	Monitor	The transaction will not be blocked based on Web Reputation, and will proceed to content checks (file type and size). **Note** Sites with no score are monitored.

Overview of Anti-Malware Scanning

The Secure Web Appliance anti-malware feature uses the Cisco DVS™ engine in combination with anti-malware scanning engines to stop web-based malware threats. The DVS engine works with the Webroot™, McAfee, and Sophos anti-malware scanning engines.

The scanning engines inspect transactions to determine a malware scanning verdict to pass to the DVS engine. The DVS engine determines whether to monitor or block the request based on the malware scanning verdicts. To use the anti-malware component of the appliance, you must enable anti-malware scanning and configure global settings, and then apply specific settings to different policies.

Related Topics

- Enabling Anti-Malware and Reputation Filters, on page 7
- Understanding Adaptive Scanning, on page 7
- McAfee Scanning, on page 6

Understanding How the DVS Engine Works

The DVS engine performs anti-malware scanning on URL transactions that are forwarded from the Web Reputation Filters. Web Reputation Filters calculate the probability that a particular URL contains malware, and assign a URL score that is associated with an action to block, scan, or allow the transaction.

When the assigned web reputation score indicates to scan the transaction, the DVS engine receives the URL request and server response content. The DVS engine, in combination with the Webroot and/or Sophos or McAfee scanning engines, returns a malware scanning verdict. The DVS engine uses information from the malware scanning verdicts and Access Policy settings to determine whether to block or deliver the content to the client.

Working with Multiple Malware Verdicts

The DVS engine might determine multiple malware verdicts for a single URL. Multiple verdicts can come from one or both enabled scanning engines:

- **Different verdicts from different scanning engines.** When you enable both Webroot and either Sophos or McAfee, each scanning engine might return different malware verdicts for the same object. When a URL causes multiple verdicts from both enabled scanning engines, the appliance performs the most restrictive action. For example, if one scanning engine returns a block verdict and the other a monitor verdict, the DVS engine always blocks the request.
- **Different verdicts from the same scanning engine.** A scanning engine might return multiple verdicts for a single object when the object contains multiple infections. When a URL causes multiple verdicts from the same scanning engine, the appliance takes action according to the verdict with the highest priority. The following text lists the possible malware scanning verdicts from the highest to the lowest priority.
- Virus
- Trojan Downloader
- Trojan Horse
- Trojan Phisher
- Hijacker
- System monitor
- Commercial System Monitor
- Dialer
- Worm
- Browser Helper Object
- Phishing URL
- Adware
- Encrypted file
- Unscannable
- Other Malware

Webroot Scanning

The Webroot scanning engine inspects objects to determine the malware scanning verdict to send to the DVS engine. The Webroot scanning engine inspects the following objects:

- **URL request.** Webroot evaluates a URL request to determine if the URL is a malware suspect. If Webroot suspects the response from this URL might contain malware, the appliance monitors or blocks the request,

depending on how the appliance is configured. If Webroot evaluation clears the request, the appliance retrieves the URL and scans the server response.

- **Server response.** When the appliance retrieves a URL, Webroot scans the server response content and compares it to the Webroot signature database.

McAfee Scanning

The McAfee scanning engine inspects objects downloaded from a web server in HTTP responses. After inspecting the object, it passes a malware scanning verdict to the DVS engine so the DVS engine can determine whether to monitor or block the request.

The McAfee scanning engine uses the following methods to determine the malware scanning verdict:

- Matching virus signature patterns
- Heuristic analysis

Matching Virus Signature Patterns

McAfee uses virus definitions in its database with the scanning engine to detect particular viruses, types of viruses, or other potentially unwanted software. It searches for virus signatures in files. When you enable McAfee, the McAfee scanning engine uses this method to scan server response content.

Heuristic Analysis

Heuristic analysis is a technique that uses general rules, rather than specific rules, to detect new viruses and malware. When the McAfee scanning engine uses heuristic analysis, it looks at the code of an object, applies generic rules, and determines how likely the object is to be virus-like.

Using heuristic analysis increases the possibility of reporting false positives (clean content designated as a virus) and might impact appliance performance.When you enable McAfee, you can choose whether or not to also enable heuristic analysis when scanning objects.

McAfee Categories

McAfee Verdict	Malware Scanning Verdict Category
Known Virus	Virus
Trojan	Trojan Horse
Joke File	Adware
Test File	Virus
Wannabe	Virus
Killed	Virus
Commercial Application	Commercial System Monitor
Potentially Unwanted Object	Adware
Potentially Unwanted Software Package	Adware
Encrypted File	Encrypted File

Sophos Scanning

The Sophos scanning engine inspects objects downloaded from a web server in HTTP responses. After inspecting the object, it passes a malware scanning verdict to the DVS engine so the DVS engine can determine whether to monitor or block the request. You might want to enable the Sophos scanning engine instead of the McAfee scanning engine if McAfee anti-malware software is installed.

Understanding Adaptive Scanning

Adaptive Scanning decides which anti-malware scanning engine (including Secure Endpoint scanning for downloaded files) will process the web request.

Adaptive Scanning applies the 'Outbreak Heuristics' anti-malware category to transactions it identifies as malware prior to running any scanning engines. You can choose whether or not to block these transactions when you configure anti-malware settings on the appliance.

Adaptive Scanning and Access Policies

When Adaptive Scanning is enabled, some anti-malware and reputation settings that you can configure in Access Policies are slightly different:

- You can enable or disable web reputation filtering in each Access Policy, but you cannot edit the Web Reputation Scores.
- You can enable anti-malware scanning in each Access Policy, but you cannot choose which anti-malware scanning engine to enable. Adaptive Scanning chooses the most appropriate engine for each web request.

Note If Adaptive Scanning is not enabled and an Access Policy has particular web reputation and anti-malware settings configured, and then Adaptive Scanning is enabled, any existing web reputation and anti-malware settings are overridden.

Per-policy Secure Endpoint settings are the same whether or not Adaptive Scanning is enabled.

Enabling Anti-Malware and Reputation Filters

Before you begin

Check the Web Reputation Filters, DVS engine, and the Webroot, McAfee, and Sophos scanning engines are enabled. By default these should be enabled during system setup.

Procedure

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

Step 2 Click **Edit Global Settings**.

Step 3 Configure settings as necessary.

Setting	Description
Web Reputation Filtering	Choose whether or not to enable Web Reputation Filtering.
Adaptive Scanning	Choose whether or not to enable Adaptive Scanning. You can only enable Adaptive Scanning when Web Reputation Filtering is enabled.
File Reputation Filtering and File Analysis	See Enabling and Configuring File Reputation and Analysis Services , on page 26.
AMP for Endpoints Console Integration (**Advanced** > **Advanced Settings for File Reputation**)	Click **Register the Appliance with** AMP for Endpoints to integrate your appliance with AMP for Endpoints console. For detailed instructions, see Integrating the Appliance with AMP for Endpoints Console, on page 13.
DVS Engine Object Scanning Limits	Specify a maximum object size for scanning. The Maximum Object Size value you specify applies to the entire size of requests and responses that might be scanned by all anti-malware and anti-virus scanning engines and bySecure Endpoint features. It also specifies the maximum size of an inspectable archive for Archive inspection; see Access Policies: Blocking Objects for more about Archive inspection. When an upload or download size exceeds this size, the security component may abort the scan in progress and may not provide a scanning verdict to the Web Proxy. If an inspectable archive exceeds this size, it is marked “Not Scanned.”
Sophos	Choose whether or not to enable the Sophos scanning engine.
McAfee	Choose whether or not to enable the McAfee scanning engine. When you enable the McAfee scanning engine, you can choose whether or not to enable heuristic scanning. **Note** Heuristic analysis increases security protection, but can result in false positives and decreased performance.
Webroot	Choose whether or not to enable the Webroot scanning engine. When you enable the Webroot scanning engine, you can configure the Threat Risk Threshold (TRT). The TRT assigns a numerical value to the probability that malware exists. Proprietary algorithms evaluate the result of a URL matching sequence and assign a Threat Risk Rating (TRR). This value is associated with the threat risk threshold setting. If the TRR value is greater than or equal to the TRT, the URL is considered malware and is passed on for further processing. **Note** Setting the Threat Risk Threshold to a value lower than 90 dramatically increases the rate of URL blocking and denies legitimate requests. Cisco strongly recommends maintaining the TRT default value of 90. The minimum value for a TRT setting is 51.

Step 4 Submit and Commit Changes.

What to do next

- Understanding Adaptive Scanning, on page 7
- McAfee Scanning, on page 6

Clearing the Secure Endpoint Services Cache

Secure Endpoint clear cache functionality clears file reputation dispositions for clean, malicious, and unknown files.

Note Secure Endpoint cache is used to increase performance. By using **Clear Cache** command, you might observe a temporary performance degradation while the cache is repopulated.

Procedure

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

Step 2 In the Secure Endpoint Services section, click **Clear Cache** and confirm your action.

Configuring Anti-Malware and Reputation in Policies

When Anti-Malware and Reputation Filters are enabled on the appliance, you can configure different settings in policy groups. You can enable monitoring or blocking for malware categories based on malware scanning verdicts.

You can configure anti-malware settings in the following policy groups:

Policy Type	Link to Task
Access Policies	Anti-Malware and Reputation Settings in Access Policies, on page 10
Outbound Malware Scanning Policies	Controlling Upload Requests Using Outbound Malware Scanning Policies

You can configure web reputation settings in the following policy groups:

Policy Type	Link to Task
Access Policies	Anti-Malware and Reputation Settings in Access Policies, on page 10
Decryption Policies	Configuring Web Reputation Filter Settings for Decryption Policy Groups, on page 13
Cisco Data Security Policies	Configuring Web Reputation Filter Settings for Decryption Policy Groups, on page 13

You can configure Secure Endpoint settings only in Access Policies. See Configuring File Reputation and Analysis Features, on page 22

Anti-Malware and Reputation Settings in Access Policies

When Adaptive Scanning is enabled, the web reputation and anti-malware settings you can configure for Access Policies are slightly different than when Adaptive Scanning is turned off.

Note If your deployment includes a Security Management appliance, and you are configuring this feature in a Primary Configuration, options on this page depend on whether Adaptive Security is enabled for the relevant primary configuration. Check the setting on the Security Management appliance, on the **Web > Utilities > Security Services Display** page.

- Understanding Adaptive Scanning, on page 7

Configuring Anti-Malware and Reputation Settings with Adaptive Scanning Enabled

Procedure

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

Step 2 Click the **Anti-Malware and Reputation** link for the Access Policy you want to configure.

Step 3 Under the **Web Reputation and Anti-Malware Settings** section, choose **Define Web Reputation and Anti-Malware Custom Settings**.

This allows you to configure web reputation and anti-malware settings for this Access Policy that differ from the global policy.

Step 4 In the **Web Reputation Settings** section, choose whether or not to enable Web Reputation Filtering. Adaptive Scanning chooses the most appropriate web reputation score thresholds for each web request.

Step 5 Configure the settings in the Secure Endpoint **Settings** section.

Step 6 Scroll down to the Cisco DVS Anti-Malware Settings section.

Step 7 Configure the anti-malware settings for the policy as necessary.

Enable Suspect User Agent Scanning	Choose whether or not to scan traffic based on the user-agent field specified in the HTTP request header. When you select this checkbox, you can choose to monitor or block suspect user agents in the Additional Scanning section at the bottom of the page. **Note** Chrome browsers do not include a user-agent string in FTP-over-HTTP requests; therefore, Chrome cannot be detected as the user agent in those requests.
Enable Anti-Malware Scanning	Choose whether or not to use the DVS engine to scan traffic for malware. Adaptive Scanning chooses the most appropriate engine for each web request.
Malware Categories	Choose whether to monitor or block the various malware categories based on a malware scanning verdict.

Other Categories	Choose whether to monitor or block the types of objects and responses listed in this section. **Note** The category Outbreak Heuristics applies to transactions which are identified as malware by Adaptive Scanning prior to running any scanning engines. **Note** URL transactions are categorized as unscannable when the configured maximum time setting is reached or when the system experiences a transient error condition. For example, transactions might be categorized as unscannable during scanning engine updates or AsyncOS upgrades. The malware scanning verdicts SV_TIMEOUT and SV_ERROR, are considered unscannable transactions.

Step 8 Submit and Commit Changes.

What to do next

- Understanding Adaptive Scanning, on page 7

Configuring Anti-Malware and Reputation Settings with Adaptive Scanning Disabled

Procedure

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

Step 2 Click the **Anti-Malware and Reputation** link for the Access Policy you want to configure.

Step 3 Under the **Web Reputation and Anti-Malware Settings** section, choose **Define Web Reputation and Anti-Malware Custom Settings**.

This allows you to configure web reputation and anti-malware settings for this Access Policy that differ from the global policy.

Step 4 Configure the settings in the **Web Reputation Settings** section.

Step 5 Configure the settings in the Secure Endpoint **Settings** section.

Step 6 Scroll down to the Cisco DVS Anti-Malware Settings section.

Step 7 Configure the anti-malware settings for the policy as necessary.

Note
When you enable Webroot, Sophos or McAfee scanning, you can choose to monitor or block some additional categories in the Malware categories on this page

Setting	Description
Enable Suspect User Agent Scanning	Choose whether or not to enable the appliance to scan traffic based on the user-agent field specified in the HTTP request header. When you select this checkbox, you can choose to monitor or block suspect user agents in the Additional Scanning section at the bottom of the page. **Note** Chrome browsers do not include a user-agent string in FTP-over-HTTP requests; therefore, Chrome cannot be detected as the user agent in those requests.

Setting	Description
Enable Webroot	Choose whether or not to enable the appliance to use the Webroot scanning engine when scanning traffic.
Enable Sophos or McAfee	Choose whether or not to enable the appliance to use either the Sophos or McAfee scanning engine when scanning traffic.
Malware Categories	Choose whether to monitor or block the various malware categories based on a malware scanning verdict. The categories listed in this section depend on which scanning engines you enable above.
Other Categories	Choose whether to monitor or block the types of objects and responses listed in this section. **Note** URL transactions are categorized as unscannable when the configured maximum time setting is reached or when the system experiences a transient error condition. For example, transactions might be categorized as unscannable during scanning engine updates or AsyncOS upgrades. The malware scanning verdicts SV_TIMEOUT and SV_ERROR, are considered unscannable transactions.

Step 8 Submit and Commit Changes.

What to do next

- Configuring Web Reputation Score Thresholds for Access Policies, on page 12
- Malware Category Descriptions, on page 17

Configuring Web Reputation Scores

When you install and set up the Secure Web Appliance, it has default settings for Web Reputation Scores. However, you can modify threshold settings for web reputation scoring to fit your organization's needs.You configure the web reputation filter settings for each policy group.

Configuring Web Reputation Score Thresholds for Access Policies

Procedure

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

Step 2 Click the link under the **Anti-Malware and Reputation** column for the Access Policy group you want to edit.

Step 3 Under the **Web Reputation and Anti-Malware Settings** section, choose **Define Web Reputation and Anti-Malware Custom Settings**.

This allows you to configure web reputation and anti-malware settings for this Access Policy that differ from the global policy.

Step 4 Verify the **Enable Web Reputation Filtering** field is enabled.

Step 5 Move the markers to change the range for URL block, scan, and allow actions.

Step 6 Submit and Commit Changes.

Note
You can edit the web reputation score thresholds in Access Policies when Adaptive Scanning is disabled

Configuring Web Reputation Filter Settings for Decryption Policy Groups

Procedure

Step 1 Choose **Web Security Manager > Decryption Policies**.

Step 2 Click the link under the Web Reputation column for the Decryption Policy group you want to edit.

Step 3 Under the **Web Reputation Settings** section, choose **Define Web Reputation Custom Settings**. This allows you to override the web reputation settings from the Global Policy Group.

Step 4 Verify the **Enable Web Reputation Filtering** field is checked.

Step 5 Move the markers to change the range for URL drop, decrypt, and pass through actions.

Step 6 In the **Sites with No Score** field, choose the action to take on request for sites that have no assigned Web Reputation Score.

Step 7 Submit and Commit Changes.

Configuring Web Reputation Filter Settings for Data Security Policy Groups

Procedure

Step 1 Choose **Web Security Manager > Cisco Data Security**.

Step 2 Click the link under the Web Reputation column for the Data Security Policy group you want to edit.

Step 3 Under the **Web Reputation Settings** section, choose **Define Web Reputation Custom Settings**.

This allows you to override the web reputation settings from the Global Policy Group.

Step 4 Move the marker to change the range for URL block and monitor actions.

Step 5 Submit and Commit Changes.

Note
Only negative and zero values can be configured for web reputation threshold settings for Cisco Data Security Policies. By definition, all positive scores are monitored

Integrating the Appliance with AMP for Endpoints Console

You can integrate your appliance with AMP for Endpoints console, and perform the following actions in AMP for Endpoints console:

- Create a simple custom detection list.
- Add new malicious file SHAs to the simple custom detection list.

- Create an application allowed list.
- Add new file SHAs to the application allowed list.
- Create a custom policy.
- Attach the simple custom detection list and the application allowed list to the custom policy.
- Create a custom group.
- Attach the custom policy to the custom group.
- Move your registered appliance from the default group to the custom group.
- View the file trajectory details of a particular file SHA.

To integrate your appliance with AMP for Endpoints console, you need to register your appliance with the console.

After the integration, when a file SHA is sent to the File Reputation server, the verdict obtained for the file SHA from the File Reputation Server is overridden by the verdict already available for the same file SHA in the AMP for Endpoints console.

If a file SHA is already marked as malicious globally, and if the same file SHA is added to the blocked list in AMP for Endpoints console, the file disposition is malicious.

The Secure Endpoint report page includes a new section - **Incoming Malware Files by Category** to view the percentage of block listed file SHAs received from the AMP for Endpoints console that are displayed as **Custom Detection**. The threat name of a block listed file SHA 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 of a block listed file SHA in the AMP for Endpoints console.

The Secure Endpoint report page includes a new section - **Incoming Malicious Files by Category** to view the percentage of file SHAs on the blocked list received from the AMP for Endpoints console that are displayed as **Custom Detection**. The threat name of a file SHA on the blocked list is displayed as **Custom Detection** in the Malicious Threat Files section of the report. To view the file trajectory details about a file SHA on the blocked list in the AMP for Endpoints console, see #unique_652.

Before you begin

Make sure you have a user account in AMP for Endpoints console with admin access rights. For more details on how to create an AMP for Endpoints console user account, contact Cisco TAC.

[For clustered configuration] In a clustered configuration, you can only register your logged-in appliance with AMP for Endpoints console. If you have already registered your appliance with AMP for Endpoints console in the standalone mode, make sure to deregister the appliance manually before you join it to a cluster.

Make sure you have enabled and configured File Reputation Filtering. See Enabling and Configuring File Reputation and Analysis Services , on page 26 to know how to enable and configure File Reputation Filtering.

Procedure

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

Step 2 Click **Edit Global Settings**.

Step 3 Click **Register Appliance with** AMP for Endpoints in the Advanced Settings panel for File Reputation in the File Reputation and File Analysis page of the web interface.

Once you click Register Appliance with AMP for Endpoints, the AMP for Endpoints console login page appears.

Step 4 Click **Register Appliance with** AMP for Endpoints in the Advanced Settings panel for File Reputation in the Anti-Malware Reputation page of the web interface.

Once you click Register Appliance with AMP for Endpoints, the AMP for Endpoints console login page appears.

Note
To integrate your appliance with AMP for Endpoints console, you must register your appliance with the console. We recommend you to limit registering your appliance to the console once in an hour.

Note
You must enable and configure File Reputation Filtering before you register the appliance with AMP for Endpoints. See Enabling and Configuring File Reputation and Analysis Services , on page 26 to know how to enbale and configure File Reputaion Filtering.

Step 5 Log in to the AMP for Endpoints console with your user credentials.

Step 6 Click **Allow** in the AMP for Endpoints authorization page to register your appliance.

Once you click Allow, the registration is complete, and it redirects you to the Anti-Malware Reputation page of your appliance. Your appliance name is displayed in the AMP for Endpoints Console Integration field. You can use the appliance name to customize your appliance settings in the AMP for Endpoints console page.

What to do next

Next Steps:

- You can go to Accounts > Applications section of the AMP for Endpoints console page, to verify whether your appliance is registered with AMP for Endpoints console. Your appliance name is displayed in the Applications section of the AMP for Endpoints console page.
- After registration, your appliance is added to the default group (Audit Group) which has a default policy (Network Policy) attached to it. The default policy contains file SHAs that are added to the blocked list or the allowed list. If you want to customize the AMP for Endpoints settings for your appliance, and add your own file SHAs that are added to the blocked list or the allowed list, see the AMP for Endpoints user documentation at https://console.amp.cisco.com/docs.
- To deregister your appliance connection from AMP for Endpoints console, you can click **Deregister** in the Advanced Settings for File Reputation section in your appliance, or you need to go to the AMP for Endpoints console page at https://console.amp.cisco.com/. For more information, see the AMP for Endpoints user documentation at https://console.amp.cisco.com/docs.

Note When you change your File Reputation server to a different data center, your appliance is automatically deregistered from the AMP for Endpoints console. You must re-register your appliance with AMP for Endpoints console with the same data center selected for the File Reputation server.

Note If a malicious file SHA gets a clean verdict, then verify whether the same file SHA is added to the allowed list in AMP for Endpoints console.

Maintaining the Database Tables

The web reputation, Webroot, Sophos, and McAfee databases periodically receive updates from the Cisco update server. Server updates are automated and the update interval is set by the server.

The Web Reputation Database

The Secure Web Appliance maintains a filtering database that contains statistics and information about how different types of requests are handled. The appliance can also be configured to send web reputation statistics to a Cisco SensorBase Network server. SensorBase server information is leveraged with data feeds from the SensorBase Network and the information is used to produce a Web Reputation Score.

Logging of Web Reputation Filtering Activity and DVS Scanning

The access log file records the information returned by the Web Reputation Filters and the DVS engine for each transaction. The scanning verdict information section in the access logs includes many fields to help understand the cause for the action applied to a transaction. For example, some fields display the web reputation score or the malware scanning verdict Sophos passed to the DVS engine.

Logging Adaptive Scanning

Custom Field in Access Logs	Custom Field in W3C Logs	Description
%X6	x-as-malware-threat-name	The anti-malware name returned by Adaptive Scanning. If the transaction is not blocked, this field returns a hyphen ("-"). This variable is included in the scanning verdict information (in the angled brackets at the end of each access log entry).

Transactions blocked and monitored by the adaptive scanning engine use the ACL decision tags:

- BLOCK_AMW_RESP
- MONITOR_AMW_RESP

Caching

The following guidelines explain how AsyncOS uses the cache while scanning for malware:

- AsyncOS only caches objects if the entire object downloads. If malware is blocked during scanning, the whole object is not downloaded and therefore is not cached.
- AsyncOS scans content whether it is retrieved from the server or from the web cache.

- The length of time that content is cached varies with many factors - there is no default.
- AsyncOS rescans content when signatures are updated.

Malware Category Descriptions

Malware Type	Description
Adware	Adware encompasses all software executables and plug-ins that direct users towards products for sale. These programs may also change security settings making it impossible for users to make changes to their system settings.
Browser Helper Object	A browser helper object is a browser plug-in that may perform a variety of functions related to serving advertisements or hijacking user settings.
Commercial System Monitor	A commercial system monitor is a piece of software with system monitor characteristics that can be obtained with a legitimate license through legal means.
Dialer	A dialer is a program that utilizes your modem or another type of Internet access to connect you to a phone line or a site that causes you to accrue long distance charges to which you did not provide your full consent.
Generic Spyware	Spyware is a type of malware installed on computers that collects small pieces of information about users without their knowledge.
Hijacker	A hijacker modifies system settings or any unwanted changes to a user's system that may direct them to a website or run a program without a users consent.
Known Malicious and High-Risk Files	These are files that were identified as threats by the Secure Endpoint file reputation service.
Other Malware	This category is used to catch all other malware and suspicious behavior that does not exactly fit in one of the other defined categories.
Phishing URL	A phishing URL is displayed in the browser address bar. In some cases, it involves the use of domain names and resembles those of legitimate domains.
PUA	Potentially Unwanted Application. A PUA is an application that is not malicious, but may be considered to be undesirable.
System Monitor	A system monitor encompasses any software that performs one of the following: • Overtly or covertly records system processes and/or user action. • Makes those records available for retrieval and review at a later time.
Trojan Downloader	A trojan downloader is a Trojan that, after installation, contacts a remote host/site and installs packages or affiliates from the remote host.
Trojan Horse	A trojan horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves.

Malware Type	Description
Trojan Phisher	A trojan phisher may sit on an infected computer waiting for a specific web page to be visited or may scan the infected machine looking for user names and passphrases.
Virus	A virus is a program or piece of code that is loaded onto your computer without your knowledge.
Worm	A worm is program or algorithm that replicates itself over a computer network and performs malicious actions.

File Reputation Filtering and File Analysis

This topic contains the following sections:

Overview of File Reputation Filtering and File Analysis

Secure Endpoint 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 Secure Endpoint Virtual Private Cloud appliance, operating in either “proxy” or “air-gap” (on-premises) mode. See Configuring an On-premises File Reputation Server, on page 24.
- The private-cloud file analysis service is provided by an on-premises Cisco Secure Endpoint Malware Analytics appliance. See Configuring an On-Premises File Analysis Server , on page 25.

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 Secure Endpoint 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 21.

Related Topics

- File Reputation and File Analysis Reporting and Tracking , on page 32
- Taking Action When File Threat Verdicts Change , on page 35

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 server will send the file for analysis (if the file meets the criteria for analysis) irrespective of the analysis score..

  If the Secure Endpoint cloud disposition is MALICIOUS, regardless of file analysis score, the files are blocked.

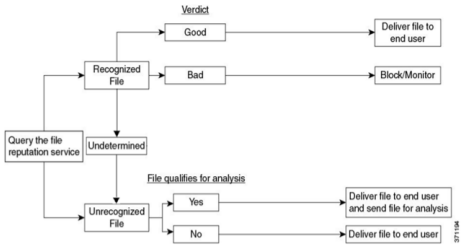
- If the reputation service has no information about the file, and the file does not meet the criteria for analysis (see Supported Files for File Reputation and Analysis Services , on page 21), the file is considered clean and the file is released to the end user .
- If you have enabled the cloud-based 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 21), 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: Secure Endpoint 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.

Note

- If the File Reputation server returns a verdict of `unknown`, `File_unknow`, `unscannable`, the analysis score will no longer be checked. This is in compliance with the behavioural change introduced in AsyncOS 15.2.4 for unknown or unscannable files to let Secure Endpoint take actions based on Secure Endpoint cloud disposition regardless of score.
- In cases where the verdict is `unknown`, `File_unknow`, `unscannable`, the file is send for further analysis. Then the file is delivered to the client as it is and the result from the TG server is stored in SWA cache and shown in reporting .

For information about verdict updates, see File Threat Verdict Updates , on page 18.

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://www.cisco.com/c/en/us/about/help/login-account-help.html.

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 Secure Endpoint.

Note A file 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 26
- Ensuring That You Receive Alerts About Secure Endpoint Issues, on page 31
- Archive or Compressed File Processing, on page 21

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 21.

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 compressed or archive 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 Secure Web Appliance sends the entire archive file to Cisco Secure Malware Analytics if one or more constituent files qualify for File Analysis. The entire archive file is marked malware if any constituent files are found malicious.

If the Secure Web Appliance fails to extract a compressed or archive file, it will be uploaded to Secure Malware Analytics for analysis.

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

- Enabling and Configuring File Reputation and Analysis Services , on page 26
- (Public Cloud File Analysis Services Only) Configuring Appliance Groups , on page 29
- Configuring File Reputation and Analysis Service Action Per Access Policy , on page 31
- Ensuring That You Receive Alerts About Secure Endpoint Issues, on page 31
- Configuring Centralized Reporting for Secure Endpoint Features , on page 32

Requirements for Communication with File Reputation and Analysis Services

- All Secure Web Appliance 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 23.
- Using of a combination of public cloud servers and private/on-premis for file reputation and file analysis is not supported. If you are using an on-premis device, then both file analysis and reputation must have an on-premis cloud server. If you are using a public cloud server, then both file reputation and file analysis must have a public cloud server.
- 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 port must be open:

Firewall Ports	Description	Protocol	In/Out	Hostname	Appliance Interface
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.	Management, unless a static route is configured to route this traffic through a data port.

- 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 , on page 26

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
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 Secure Endpoint Virtual Private Cloud appliance as a private-cloud file analysis server:

- You can obtain the Cisco Secure Endpoint 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 Secure Endpoint Virtual Private Cloud appliance.

- Set up and configure the Cisco Secure Endpoint Virtual Private Cloud appliance in either "proxy" or "air-gap" (on-premises) mode.

- Ensure the Cisco Secure Endpoint Virtual Private Cloud appliance software version is 2.2, which enables integration with Cisco Secure Web Appliance.
- Download the Secure Endpoint Virtual Private Cloud certificate and keys on that appliance for upload to this Secure Web Appliance

Note After you have set up the on-premises file-reputation server, you will configure connection to it from this Secure Web Appliance; see Step 6 of Enabling and Configuring File Reputation and Analysis Services , on page 26.

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 https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-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 Secure Web Appliance.
- 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 Secure Web Appliance.

  See the Secure Endpoint 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 Secure Web Appliance 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 Secure Web Appliance. 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 Secure Web Appliance 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 , on page 26. 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 Secure Web Appliance; see Step 7 of Enabling and Configuring File Reputation and Analysis Services , on page 26.

Enabling and Configuring File Reputation and Analysis Services

Before you begin

- Meet the Requirements for Communication with File Reputation and Analysis Services , on page 23.
- 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 Secure Endpoint Virtual Private Cloud Appliance as a private cloud file reputation server, see Configuring an On-premises File Reputation Server, on page 24.
- 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 25.

Procedure

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 21

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.

Option	Description

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:
	• **Console Hostname** – The Console Hostname of the Secure Endpoint Private Cloud appliance.
	• **Activation Code** – The Activation Code of the Secure Endpoint Private Cloud appliance.
	• **Certificate Authority** – Choose the certificate authority from the drop-down list.
	  • **Use Cisco Default Certificate Authority**: Choose this option to use the default certificate authority for your server.
	  • **Use Uploaded Certificate Authority**: Choose this option to use a custom certificate authority for your server.
	For more information on how to obtain the Console hostname and activation code, see the Secure Endpoint Private Cloud documentation.
	Note
	To perform SSL Communication for File Reputation, you must add the AMP on-premises reputation server CA certificate to the certificate store on this appliance, using either the CLI command certconfig > CERTAUTHORITY > CUSTOM, or Network > Certificates (Custom Certificate Authorities) in the web interface. Obtain this certificate from the Secure Endpoint Private Cloud appliance (Integrations > Secure Web Appliance> Version 15.2.4 and above > SSL Configuration > download).

AMP for Endpoints Console Integration	Click **Register the Appliance with AMP for Endpoints** to integrate your appliance with AMP for Endpoints console. For detailed instructions, see Integrating the Appliance with AMP for Endpoints Console, on page 13.
Proxy Settings for File Reputation	If you want to configure a upstream proxy, enter the appropriate **Server**, **Port**, **Username**, and **Passphrase** information.
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	If you want to configure a different upstream proxy, 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**.
- From AsyncOS 15.2.4 release, the **Threshold Settings** panel is disabled. Hence, you will not be able to configure Secure Endpoint threshold settings. See File Processing Overview , on page 19 for more details.

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 Secure Web Appliance.
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 Secure Endpoint 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 Secure Endpoint Malware Analytics documentation from https://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.

Procedure

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?

Procedure

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.
Secure Web 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

Procedure

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 **Secure Endpoint 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 Secure Endpoint Issues

Ensure that the appliance is configured to send you alerts related to Secure Endpoint.

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)	
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.	Secure Endpoint	Error

Related Topics

- Several Alerts About Failure to Connect to File Reputation or File Analysis Servers , on page 36
- Taking Action When File Threat Verdicts Change , on page 35

Configuring Centralized Reporting for Secure Endpoint Features

If you will centralize reporting on a Security Management appliance, see important configuration requirements in the Secure Endpoint 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 , on page 33
- File Reputation and File Analysis Report Pages, on page 33
- Viewing File Reputation Filtering Data in Other Reports , on page 34
- About Web Tracking and Secure Endpoint Features , on page 34

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 > Secure Endpoint and click an SHA-256 link in the table. The details page shows associated filenames.

File Reputation and File Analysis Report Pages

Report	Description
Secure Endpoint	Shows file-based threats that were identified by the file reputation service. For files with changed verdicts, see the Secure Endpoint Verdict updates report. Those verdicts are not reflected in the Secure Endpoint 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 Secure Endpoint 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 Secure Endpoint section of the report.

Report	Description
Secure Endpoint 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.
Secure Endpoint Reputation	Because Secure Endpoint is focused on targeted and zero-day threats, threat verdicts can change as aggregated data provides more information. The Secure Endpoint 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 18. 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 Secure Endpoint" 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 Secure Endpoint tab.

About Web Tracking and Secure Endpoint 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 Secure Endpoint 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.

Note From AsyncOS 15.2.4, the threshold settings under **Security Services** > **Anti Malware and Reputation Settings** > **File Analysis** > **Advanced** is disabled. The appliance will no longer compare the Secure Endpoint threat score with the threshold score (configured on the **Security Services** > **Anti-Malware and Reputation** page) to determine what action to take. Refer to File Processing Overview , on page 19 for detailed information.

- Verdict updates are available only in the Secure Endpoint 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

Procedure

Step 1 View the Secure Endpoint 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 18

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 Secure Endpoint including File Analysis is logged in Access Logs or in Secure Endpoint 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 23.
- 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 Secure Endpoint **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 Secure Web Appliance is unable to connect to the Secure Endpoint Malware Analytics server to upload files for analysis.

Solution

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

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

Related Topics

- Enabling and Configuring File Reputation and Analysis Services , on page 26

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 Secure Endpoint 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 Secure Web Appliances 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 29. 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.

Managing Access to Web Applications

This topic contains the following sections:

Overview of Managing Access to Web Applications

The Application Visibility and Control (AVC) or Application Discovery and Control (ADC) engine lets you create policies to control application activity on the network without having to fully understand the underlying technology of each application. You can configure application control settings in Access Policy groups. You can block or allow applications individually or according to application type. You can also apply controls to particular application types.

Using Access Policies you can:

- Control application behaviors or activity or fine gain control.

  ADC has the Fine Gain Control (FGC) or behavior configuration. You can configure FGC for multiple applications.

- Control the amount of bandwidth used for particular application types

Note This is applicable for AVC only.

- Notify end-users when they are blocked
- Assign controls to Instant Messaging, Blogging and Social Media applications
- Specify Range Request settings

Note This is applicable for AVC only.

To control applications using the AVC or ADC engine, perform the following tasks:

Task	Link to Task
Enable the AVC or ADC engine	Enabling the AVC or ADC Engine, on page 39
Set Controls in an Access Policy Group	Configuring Application Control Settings in an Access Policy Group, on page 43
Limit bandwidth consumed by some application types to control congestion **Note** This is applicable for AVC only.	Controlling Bandwidth, on page 43
Allow instant messaging traffic, but disallow file sharing using instant messenger	Controlling Instant Messaging Traffic, on page 46

Enabling the AVC or ADC Engine

Enable the AVC or ADC engine when you enable the Acceptable Use Controls.

Note You can view the AVC or ADC engine scanning activity in the Application Visibility report on the Reporting > Application Visibility page.

What to do next

Related Topics

- Application Engine and Default Actions , on page 40
- User Experience When Requests Are Blocked by the AVC or ADC Engine, on page 40

Application Engine and Default Actions

AsyncOS periodically queries the update servers for new updates to all security service components, including the AVC engine. AVC engine updates can include support for new application types and applications, as well as updated support for existing applications if any application behaviors change. By updating the AVC engine between AsyncOS version updates, the Secure Web Appliance remains flexible without requiring a server upgrade.

AsyncOS for Web assigns the following default actions for the Global Access Policy:

- New Application Types default to **Monitor**.
- New application behaviors, such as block file transfer within a particular application; defaults to **Monitor**.
- New applications for an existing application type default to the Application Type's default.

Note In the Global Access Policy, you can set the default action for each Application Type, so new applications introduced in an AVC or ADC engine update automatically inherit the specified default action. See Configuring Application Control Settings in an Access Policy Group, on page 43.

User Experience When Requests Are Blocked by the AVC or ADC Engine

When the AVC or ADC engine blocks a transaction, the Web Proxy sends a block page to the end user. However, not all Websites display the block page to the end user; many Websites display dynamic content using JavaScript instead of a static Web page and are not likely to display the block page. Users are still properly blocked from downloading malicious data, but they may not always be informed of this by the Website.

Note When the HTTPS proxy is disabled and Webroot is:

- Enabled - The AVC or ADC engine may or may not be launched and return the verdict. The transaction will be processed according to scanner's verdict.
- Disabled - The AVC or ADC engine will be launched and return the verdict. The transaction will be processed according to AVC or ADC's verdict.

Policy Application Control Settings

Controlling applications involves configuring the following elements:

Option	Description
Application Types	A category that contains one or more applications.
Applications	Particular applications within an Application Type.
Application behaviors	Particular actions or behaviors that users can do within an application that administrators can control. Not all applications include behaviors you can configure.

You can configure application control settings in Access Policy groups. On the **Web Security Manager** > **Access Policies** page, click the **Applications** link for the policy group you want to configure. When configuring applications, you can choose the following actions:

Option	Description
Block	This action is a final action. Users are prevented from viewing a webpage and instead an end-user notification page displays **Note** When an application is configured to be blocked under ADC/AVC, every sub-category under the application will also be blocked. A specific sub-category can be blocked using fine and gain control feature, however this feature is limited to certain apps like smugmug, facebook, linkedin, etc.
Monitor	This action is an intermediary action. The Web Proxy continues comparing the transaction to the other control settings to determine which final action to apply
Restrict	This action indicates that an application behavior is blocked. For example, when you block file transfers for a particular instant messaging application, the action for that application is Restrict.
Bandwidth Limit	For certain applications, such as Media and Facebook, you can limit the bandwidth available for Web traffic. You can limit bandwidth for the application itself, and for its users.

Related Topics

- Range Request Settings, on page 41
- Rules and Guidelines for Configuring Application Control , on page 42

Range Request Settings

When HTTP range requests are disabled and a large file is downloaded over multiple streams, the consolidated package is scanned. This disables the performance advantages of download-management utilities and applications that are used to download large objects.

Alternatively, when Range Request Forwarding is enabled (see Configuring Web Proxy Settings), you can control how incoming range requests are handled on a per-policy basis. This process is known as “byte serving” and is a means of bandwidth optimization when requesting large files.

However, enabling range request forwarding can interfere with policy-based Application Visibility and Control (AVC) efficiency, and can compromise security. Please exercise caution and enable HTTP Range Request Forwarding only if the advantages outweigh the security implications.

Note The Range Request Settings are available only when Range Request Forwarding is enabled, and at least one application is set to Block, Restrict, or Throttle.

Range Request Settings for Policy

Range Request Settings	• **Do not forward range requests**—The client sends a request for a particular range. But, the Secure Web Appliance removes the range header from the request before sending it to the target server. The Secure Web Appliance then scans the entire file and sends the range of bytes to the client. **Note** When the client sends the range request for the first time, Secure Web Appliance, expecting subsequent range requests from the client, sends the entire file. For any successive request from the same or another client, Secure Web Appliance delivers only the partial content to the client. • **Forward range requests**—The client sends a request for a particular range. The Secure Web Appliance sends the same request to the target server and receives a partial content which is then returned to the client. The Secure Web Appliance scans only the partial content for which the scan results may not be accurate.
Exception list	You can specify traffic destinations which are exempt from the current forwarding selection. That is, when **Do not forward range requests** is selected, you can specify destinations for which requests are forwarded. Similarly, when **Forward range requests** is selected, you can specify destinations for which requests are not forwarded.

Rules and Guidelines for Configuring Application Control

Consider the following rules and guidelines when configuring application control settings:

- The supported Application Types, applications, and application behaviors may change between AsyncOS for Web upgrades, or after AVC or ADC engine updates.
- If you enable Safe Search or Site Content Rating, the AVC Engine is tasked with identifying applications for safe browsing. As one of the criteria, the AVC engine will scan the response body to detect a search application. As a result, the appliance will not forward range headers.
- In Application Type listings, the summary for each Application Type lists the final actions for its applications, but does not indicate whether these actions are inherited from the global policy or configured in the current Access Policy. To learn more about the action for a particular application, expand the application type.
- In the Global Access Policy, you can set the default action for each Application Type, so new applications introduced in an AVC or ADC engine update automatically inherit the default action.
- You can quickly configure the same action for all applications in an application type by clicking the “edit all” link for the Application Type in Browse view. However, you can only configure the application action, not application behavior actions. To configure application behaviors, you must edit the application individually.
- In Search view, when you sort the table by the action column, the sort order is by the final action. For example, “Use Global (Block)” comes after “Block” in the sort order.
- Decryption may cause some applications to fail unless the root certificate for signing is installed on the client.

Related Topics

- Configuring Application Control Settings in an Access Policy Group, on page 43
- Configuring Overall Bandwidth Limits, on page 44
- Viewing AVC or ADC Activity, on page 46

Configuring Application Control Settings in an Access Policy Group

Procedure

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

Step 2 Click the link in the Policies table under the Applications column for the policy group you want to edit.

Step 3 When configuring the Global Access Policy:

a) Define the default action for each Application Type in the **Default Actions for Application Types** section.

b) You can edit the default actions for each Application Type's individual members, as a group or individually, in the **Edit Applications Settings** section of the page. Editing the default action for individual applications is described in the following steps.

Step 4 When configuring a user defined Access Policy, choose **Define Applications Custom Settings** in the **Edit Applications Settings** section.

Step 5 In the Application Settings area, choose **Browse view** or **Search view** from the drop-down menu:

- **Browse view.** You can browse Application Types. You can use Browse view to configure all applications of a particular type at the same time. When an Application Type is collapsed in Browse view, the summary for the Application Type lists the final actions for its applications; however it does not indicate whether the actions are inherited from the global policy, or configured in the current Access Policy.
- **Search view.** You can search for applications by name. You might use Search view when the total list of applications is long and you need to quickly find and configure a particular application.

Step 6 Configure the action for each application and application behavior.

Step 7 Configure the bandwidth controls for each applicable application.

Step 8 Submit and Commit Changes.

What to do next

Related Topics

- Controlling Bandwidth, on page 43

Controlling Bandwidth

When both the overall limit and user limit applies to a transaction, the most restrictive option applies. You can define bandwidth limits for particular URL categories by defining an Identity group for a URL category and using it in an Access Policy that restricts the bandwidth.

You can define the following bandwidth limits:

Bandwidth limit	Description	Link to Task
Overall	Define an overall limit for all users on the network for the supported application types. The overall bandwidth limit affects the traffic between the Secure Web Appliance and application servers. It does not limit traffic served from the web cache.	Configuring Overall Bandwidth Limits, on page 44
User	Define a limit for particular users on the network per application type. User bandwidth limits traffic from web servers as well as traffic served from the web cache.	Configuring User Bandwidth Limits, on page 44

Note Defining bandwidth limits only throttles the data going to users. It does not block data based on reaching a quota. The Web Proxy introduces latency into each application transaction to mimic a slower link to the server.

Configuring Overall Bandwidth Limits

Procedure

Step 1 Choose **Web Security Manager** > **Overall Bandwidth Limits**

Step 2 Click **Edit Settings**.

Step 3 Select the **Limit to** option.

Step 4 Enter the amount of traffic to limit in either Megabits per second (Mbps) or kilobits per second (kbps).

Step 5 Submit and Commit Changes.

Configuring User Bandwidth Limits

You can define user bandwidth limits by configuring bandwidth control settings on the Applications Visibility and Control page of Access Policies. You can define the following types of bandwidth controls for users in Access Policies:

Option	Description	Link to task
Default bandwidth limit for an application type	In the Global Access Policy, you can define the default bandwidth limit for all applications of an application type.	Configuring the Default Bandwidth Limit for an Application Type, on page 45
Bandwidth limit for an application type	In a user defined Access Policy, you can override the default bandwidth limit for the application type defined in the Global Access Policy.	Overriding the Default Bandwidth Limit for an Application Type, on page 45

Option	Description	Link to task
Bandwidth limit for an application	In a user defined or Global Access Policy, you can choose to apply the application type bandwidth limit or no limit (exempt the application type limit).	Configuring Bandwidth Controls for an Application, on page 46

Configuring the Default Bandwidth Limit for an Application Type

Procedure

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

Step 2 Click the link in the policies table under the Applications column for the Global Access Policy.

Step 3 In the **Default Actions for Application Types** section, click the link next to "Bandwidth Limit" for the application type you want to edit.

Step 4 Select **Set Bandwidth Limit** and enter the amount of traffic to limit in either Megabits per second (Mbps) or kilobits per second (kbps).

Step 5 Click **Apply**.

Step 6 Submit and Commit Changes.

Overriding the Default Bandwidth Limit for an Application Type

You can override the default bandwidth limit defined at the Global Access Policy group in the user defined Access Policies. You can only do this in Browse view.

Procedure

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

Step 2 Click the link in the policies table under the Applications column for the user defined policy group you want to edit.

Step 3 Choose **Define Applications Custom Settings** in the **Edit Applications Settings** section.

Step 4 Click the link next to "Bandwidth Limit" for the application type you want to edit.

Step 5 To choose a different bandwidth limit value, select **Set Bandwidth Limit** and enter the amount of traffic to limit in either Megabits per second (Mbps) or kilobits per second (kbps). To specify no bandwidth limit, select **No Bandwidth Limit for Application Type**.

Step 6 Click **Apply**.

Step 7 Submit and Commit Changes.

Configuring Bandwidth Controls for an Application

Procedure

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

Step 2 Click the link in the policies table under the Applications column for the policy group you want to edit.

Step 3 Expand the application type that contains the application you want to define.

Step 4 Click the link for the application you want to configure.

Step 5 Select **Monitor**, and then choose to use either the bandwidth limit defined for the application type or no limit.

Note
The bandwidth limit setting is not applicable when the application is blocked or when no bandwidth limit is defined for the application type.

Step 6 Click **Done**.

Step 7 Submit and Commit Changes.

Controlling Instant Messaging Traffic

You can block or monitor the IM traffic, and depending on the IM service, you can block particular activities (also known as application behaviors) in an IM session.

Procedure

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

Step 2 Click the link in the policies table under the Applications column for the policy group you want to edit.

Step 3 Click **Define Applications Custom Setting**.

Step 4 Expand the Instant Messaging application type.

Step 5 Click the link next to the IM application you want to configure.

Step 6 To block all traffic for this IM application, select **Block**.

Step 7 To monitor the IM application, but block particular activities within the application, select **Monitor**, and then select the application behavior to **Block**.

Step 8 Click **Done**.

Step 9 Submit and Commit Changes.

Viewing AVC or ADC Activity

The **Reporting > Application Visibility** page displays information about the top applications and application types used. It also displays the top applications and application types blocked.

AVC or ADC Information in Access Log File

The access log file records the information returned by the AVC or ADC engine for each transaction. The scanning verdict information section in the access logs includes the fields listed below:

Description	Custom Field in Access Logs	Custom Field in W3C Logs
Application name	%XO	x-app
Application type	%Xu	x-type
Application behavior	%Xb	x-avc-behavior

Note If you configure the ADC Application behavior for a particular application, then only it can be searched. Otherwise the custom behavior will be "Unknown".

Prevent Loss of Sensitive Data

This topic contains the following sections:

Overview of Prevent Loss of Sensitive Data

The Secure Web Appliance secures your data by providing the following capabilities:

Option	Description
Cisco Data Security filters	The Cisco Data Security filters on the Secure Web Appliance evaluate data leaving the network over HTTP, HTTPS and FTP.
Third-party data loss prevention (DLP) integration	The Secure Web Appliance integrates with leading third party content-aware DLP systems that identify and protect sensitive data. The Web Proxy uses the Internet Content Adaptation Protocol (ICAP) which allows proxy servers to offload content scanning to external systems

When the Web Proxy receives an upload request, it compares the request to the Data Security and External DLP Policy groups to determine which policy group to apply. If both types of policies are configured, it compares the request to Cisco Data Security policies before external DLP policies. After it assigns the request to a policy group, it compares the request to the policy group's configured control settings to determine what to do with the request. How you configure the appliance to handle upload requests depends on the policy group type.

Note Upload requests that try to upload files with a size of zero (0) bytes are not evaluated against Cisco Data Security or External DLP policies.

To restrict and control data that is leaving the network, you can perform the following tasks:

Task	Link to Task
Create Cisco Data Security policies	Managing Upload Requests, on page 49
Create External DLP policies	Managing Upload Requests on an External DLP System, on page 50
Create Data Security and External DLP policies	Creating Data Security and External DLP Policies, on page 51
Control Upload Requests using Cisco Data Security policies	Managing Settings for Upload Requests, on page 53
Control Upload Requests Using External DLP policies	Controlling Upload Requests Using External DLP Policies, on page 57

Bypassing Upload Requests Below a Minimum Size

To help reduce the number of upload requests recorded in the log files, you can define a minimum request body size, below which upload requests are not scanned by the Cisco Data Security Filters or the external DLP server.

To do this, use the following CLI commands:

- `datasecurityconfig`. Applies to the Cisco Data Security filters.
- `externaldlpconfig`. Applies to the configured external DLP servers.

The default minimum request body size is 4 KB (4096 bytes) for both CLI commands. Valid values are 1 to 64 KB. The size you specify applies to the entire size of the upload request body.

Note All chunk encoded uploads and all native FTP transactions are scanned by the Cisco Data Security filters or external DLP servers when enabled. However, they can still be bypassed based on a custom URL category.

User Experience When Requests Are Blocked As Sensitive Data

When the Cisco Data Security filters or an external DLP server blocks an upload request, it provides a block page that the Web Proxy sends to the end user. Not all websites display the block page to the end user. For example, some Web 2.0 websites display dynamic content using javascript instead of a static Web page and

are not likely to display the block page. Users are still properly blocked from performing data security violations, but they may not always be informed of this by the website.

Managing Upload Requests

Before you begin

Go to **Security Services** > **Data Security Filters** to enable the Cisco Data Security filters.

Procedure

Create and configure Data Security Policy groups.

Cisco Data Security policies use URL filtering, Web reputation, and upload content information when evaluating the upload request. You configure each of these security components to determine whether or not to block the upload request.

When the Web Proxy compares an upload request to the control settings, it evaluates the settings in order. Each control setting can be configured to perform one of the following actions for Cisco Data Security policies:

Action	Description
Block	The Web Proxy does not permit the connection and instead displays an end user notification page explaining the reason for the block.
Allow	The Web Proxy bypasses the rest of the Data Security Policy security service scanning and then evaluates the request against the Access Policies before taking a final action. For Cisco Data Security policies, Allow bypasses the rest of data security scanning, but does not bypass External DLP or Access Policy scanning. The final action the Web Proxy takes on the request is determined by the applicable Access Policy (or an applicable external DLP Policy that may block the request).
Monitor	The Web Proxy continues comparing the transaction to the other Data Security Policy group control settings to determine whether to block the transaction or evaluate it against the Access Policies.

For Cisco Data Security policies, only the Block action is a final action that the Web Proxy takes on a client request. The Monitor and Allow actions are intermediary actions. In both cases, the Web Proxy evaluates the transaction against the External DLP Policies (if configured) and Access Policies. The Web Proxy determines which final action to apply based on the Access Policy group control settings (or an applicable external DLP Policy that may block the request).

What to do next

Related Topics

- Managing Upload Requests on an External DLP System, on page 50
- Managing Settings for Upload Requests, on page 53

Managing Upload Requests on an External DLP System

To configure the Secure Web Appliance to handle upload requests on an external DLP system, perform the following tasks:

Procedure

Step 1 Choose **Network > External DLP Servers.** Define an external DLP system. To pass an upload request to an external DLP system for scanning, you must define at least one ICAP-compliant DLP system on the Secure Web Appliance.

Step 2 **Create and configure External DLP Policy groups.** After an external DLP system is defined, you create and configure External DLP Policy groups to determine which upload requests to send to the DLP system for scanning.

Step 3 When an upload request matches an External DLP Policy, the Web Proxy sends the upload request to the DLP system using the Internet Content Adaptation Protocol (ICAP) for scanning. The DLP system scans the request body content and returns a block or allow verdict to the Web Proxy. The allow verdict is similar to the Allow action for Cisco Data Security policies in that the upload request will be compared to the Access Policies. The final action the Web Proxy takes on the request is determined by the applicable Access Policy.

What to do next

Related Topics

- Controlling Upload Requests Using External DLP Policies, on page 57
- Defining External DLP Systems, on page 54

Evaluating Data Security and External DLP Policy Group Membership

Each client request is assigned to an Identity and then is evaluated against the other policy types to determine which policy group it belongs for each type. The Web Proxy evaluates *upload requests* against the Data Security and External DLP policies. The Web Proxy applies the configured policy control settings to a client request based on the client request's policy group membership.

Matching Client Requests to Data Security and External DLP Policy Groups

To determine the policy group that a client request matches, the Web Proxy follows a specific process for matching the group membership criteria. It considers the following factors for group membership:

- **Identity.** Each client request either matches an Identification Profile, fails authentication and is granted guest access, or fails authentication and gets terminated.
- **Authorized users.** If the assigned Identification Profile requires authentication, the user must be in the list of authorized users in the Data Security or External DLP Policy group to match the policy group. The list of authorized users can be any of the specified groups or users or can be guest users if the Identification Profile allows guest access.
- **Advanced options.** You can configure several advanced options for Data Security and External DLP Policy group membership. Some options (such as proxy port and URL category) can also be defined within the Identity. When an advanced option is configured in the Identity, it is not configurable in the Data Security or External DLP Policy group level.

The information in this section gives an overview of how the Web Proxy matches upload requests to both Data Security and External DLP Policy groups.

The Web Proxy sequentially reads through each policy group in the policies table. It compares the upload request status to the membership criteria of the first policy group. If they match, the Web Proxy applies the policy settings of that policy group.

If they do not match, the Web Proxy compares the upload request to the next policy group. It continues this process until it matches the upload request to a user defined policy group. If it does not match a user defined policy group, it matches the global policy group. When the Web Proxy matches the upload request to a policy group or the global policy group, it applies the policy settings of that policy group.

Creating Data Security and External DLP Policies

You can create Data Security and External DLP Policy groups based on combinations of several criteria, such as one or more Identification Profiles or the URL category of the destination site. You must define at least one criterion for policy group membership. When you define multiple criteria, the upload request must meet all criteria to match the policy group. However, the upload request needs to match only one of the configured Identification Profiles.

Procedure

Step 1 Choose **Web Security Manager > Cisco Data Security** (for Defining Data Security Policy group membership) or **Web Security Manager > External Data Loss Prevention** (for Defining External DLP Policy group membership).

Step 2 Click **Add Policy**.

Step 3 In the **Policy Name** field, enter a name for the policy group, and in the Description field (optional) add a description.

Note
Each policy group name must be unique and only contain alphanumeric characters or the space character.

Step 4 In the **Insert Above Policy** field, choose where in the policies table to place the policy group.

When configuring multiple policy groups you must specify a logical order for each group. Order your policy groups to ensure that correct matching occurs.

Step 5 In the **Identities and Users** section, choose one or more Identification Profile groups to apply to this policy group.

Step 6 (Optional) Expand the **Advanced** section to define additional membership requirements.

Step 7 To define policy group membership by any of the advanced options, click the link for the advanced option and configure the option on the page that appears.

Advanced Option	Description
Protocols	Choose whether or not to define policy group membership by the protocol used in the client request. Select the protocols to include. "All others" means any protocol not listed above this option. **Note** When the HTTPS Proxy is enabled, only Decryption Policies apply to HTTPS transactions. You cannot define policy membership by the HTTPS protocol for Access, Routing, Outbound Malware Scanning, Data Security, or External DLP Policies.

Advanced Option	Description
Proxy Ports	Choose whether or not to define policy group membership by the proxy port used to access the Web Proxy. Enter one or more port numbers in the Proxy Ports field. Separate multiple ports with commas. For explicit forward connections, this is the port configured in the browser. For transparent connections, this is the same as the destination port. You might want to define policy group membership on the proxy port if you have one set of clients configured to explicitly forward requests on one port, and another set of clients configured to explicitly forward requests on a different port. Cisco recommends only defining policy group membership by the proxy port when the appliance is deployed in explicit forward mode, or when clients explicitly forward requests to the appliance. If you define policy group membership by the proxy port when client requests are transparently redirected to the appliance, some requests might be denied. **Note** If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.
Subnets	Choose whether or not to define policy group membership by subnet or other addresses. You can choose to use the addresses that may be defined with the associated Identification Profile, or you can enter specific addresses here. **Note** If the Identification Profile associated with this policy group defines its membership by addresses, then in this policy group you must enter addresses that are a subset of the addresses defined in the Identification Profile. Adding addresses in the policy group further narrows down the list of transactions that match this policy group.
URL Categories	Choose whether or not to define policy group membership by URL categories. Select the user defined or predefined URL categories. **Note** If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.
User Agents	Choose whether to define policy group membership by the user agents (client applications such as updaters and Web browsers) used in the client request. You can select some commonly defined user agents, or define your own using regular expressions. Specify whether membership definition includes only the selected user agents, or specifically excludes the selected user agents. **Note** If the Identification Profile associated with this policy group defines Identification Profile membership by this advanced setting, the setting is not configurable at the non-Identification Profile policy group level.
User Location	Choose whether or not to define policy group membership by user location, either remote or local. This option only appears when the Secure Mobility is enabled.

Step 8 Submit your changes.

Step 9 If you are creating a Data Security Policy group, configure its control settings to define how the Web Proxy handles upload requests.

The new Data Security Policy group automatically inherits global policy group settings until you configure options for each control setting.

If you are creating an External DLP Policy group, configure its control settings to define how the Web Proxy handles upload requests.

The new External DLP Policy group automatically inherits global policy group settings until you configure custom settings.

Step 10 Submit and Commit Changes.

What to do next

Related Topics

- Evaluating Data Security and External DLP Policy Group Membership, on page 50
- Matching Client Requests to Data Security and External DLP Policy Groups, on page 50
- Managing Settings for Upload Requests, on page 53
- Controlling Upload Requests Using External DLP Policies, on page 57

Managing Settings for Upload Requests

Each upload request is assigned to a Data Security Policy group and inherits the control settings of that policy group. The control settings of the Data Security Policy group determine whether the appliance blocks the connection or evaluates it against the Access Polices.

Configure control settings for Data Security Policy groups on the Web Security Manager > Cisco Data Security page.

You can configure the following settings to determine what action to take on upload requests:

Option	Link
URL Categories	URL Categories, on page 53
Web Reputation	Web Reputation, on page 54
Content	Content Blocking, on page 54

After a Data Security Policy group is assigned to an upload request, the control settings for the policy group are evaluated to determine whether to block the request or evaluate it against the Access Policies.

URL Categories

AsyncOS for Web allows you to configure how the appliance handles a transaction based on the URL category of a particular request. Using a predefined category list, you can choose to monitor or block content by category. You can also create custom URL categories and choose to allow, monitor, or block traffic for a website in the custom category.

Web Reputation

The Web Reputation setting inherits the global setting. To customize web reputation filtering for a particular policy group, you can use the Web Reputation Settings pull-down menu to customize web reputation score thresholds.

Only negative and zero values can be configured for web reputation threshold settings for Cisco Data Security policies. By definition, all positive scores are monitored.

Content Blocking

You can use the settings on the Cisco Data Security > Content page to configure the Web Proxy to block data uploads based on the following file characteristics:

- **File size.** You can specify the maximum *upload* size allowed. All uploads with sizes equal to or greater than the specified maximum are blocked. You can specify different maximum file sizes for HTTP/HTTPS and native FTP requests.

  When the upload request size is greater than both the maximum upload size and the maximum scan size (configured in the "DVS Engine Object Scanning Limits" field on Security Services > Anti-Malware page), the upload request is still blocked, but the entry in the data security logs does not record the file name and content type. The entry in the access logs is unchanged.

- **File type.** You can block predefined file types or custom MIME types you enter. When you block a predefined file type, you can block all files of that type or files greater than a specified size. When you block a file type by size, the maximum file size you can specify is the same as the value for the "DVS Engine Object Scanning Limits" field on Security Services > Anti-Malware page. By default, that value is 32 MB.

  Cisco Data Security filters do not inspect the contents of archived files when blocking by file type. Archived files can be blocked by its file type or file name, not according to its contents.

Note For some groups of MIME types, blocking one type blocks all MIME types in the group. For example, blocking application/x-java-applet blocks all java MIME types, such as application/java and application/javascript.

- **File name.** You can block files with specified names. You can use text as a literal string or a regular expression for specifying file names to block.

Note Only enter file names with 8-bit ASCII characters. The Web Proxy only matches file names with 8-bit ASCII characters.

Defining External DLP Systems

The Secure Web Appliance can integrate with multiple external DLP servers from the same vendor by defining multiple DLP servers in the appliance. You can define the load-balancing technique the Web Proxy uses when contacting the DLP systems. This is useful when you define multiple DLP systems. See SSL Configurationfor information about specifying the protocols used to secure communications with external DLP servers.

Note Verify the external DLP server does not send the Web Proxy modified content. AsyncOS for Web only supports the ability to block or allow upload requests. It does not support uploading content modified by an external DLP server.

Configuring External DLP Servers

Procedure

Step 1 Choose **Network > External DLP Servers**.

Step 2 Click **Edit Settings**.

Setting	Description
Protocol for External DLP Servers	Choose either: • **ICAP** – DLP client/server ICAP communications are not encrypted. • **Secure ICAP** – DLP client/server ICAP communications are via an encrypted tunnel. Additional related options appear.
External DLP Servers	Enter the following information to access an ICAP compliant DLP system: • **Server address** and **Port** – The hostname or IP address and TCP port for accessing the DLP system. • **Reconnection attempts** – The number of times the Web Proxy tries to connect to the DLP system before failing. • **Service URL** – The ICAP query URL specific to the particular DLP server. The Web Proxy includes what you enter here in the ICAP request it sends to the external DLP server. The URL must start with the ICAP protocol: icap:// • Certificate (optional) – The certificate provided to secure each External DLP Server connection can be Certificate Authority (CA)-signed or self-signed. Obtain the certificate from the specified server, and then upload it to the appliance: • Browse to and select the certificate file, and then click **Upload File**. **Note** This single file must contain both the client certificate and private key in unencrypted form. • **Use this certificate for all DLP servers using Secure ICAP** – Check this box to use the same certificate for all External DLP Servers you define here. Leave the option unchecked to enter a different certificate for each server. • Start Test – You can test the connection between the Secure Web Appliance and the defined external DLP server(s) by clicking **Start Test**.

Setting	Description
Load Balancing	If multiple DLP servers are defined, select which load-balancing technique the Web Proxy uses to distribute upload requests to different DLP servers. You can choose the following load balancing techniques: • **None (failover).** The Web Proxy directs upload requests to one DLP server. It tries to connect to the DLP servers in the order they are listed. If one DLP server cannot be reached, the Web Proxy attempts to connect to the next one in the list. • **Fewest connections.** The Web Proxy keeps track of how many active requests are with the different DLP servers and it directs the upload request to the DLP server currently servicing the fewest number of connections. • **Hash based.** The Web Proxy uses a hash function to distribute requests to the DLP servers. The hash function uses the proxy ID and URL as inputs so that requests for the same URL are always directed to the same DLP server. • **Round robin.** The Web Proxy cycles upload requests equally among all DLP servers in the listed order.
Service Request Timeout	Enter how long the Web Proxy waits for a response from the DLP server. When this time is exceeded, the ICAP request has failed and the upload request is either blocked or allowed, depending on the Failure Handling setting. Default is 60 seconds.
Maximum Simultaneous Connections	Specifies the maximum number of simultaneous ICAP request connections from the Secure Web Appliance to each configured external DLP server. The Failure Handling setting on this page applies to any request which exceeds this limit. Default is 25.
Failure Handling	Choose whether upload requests are blocked or allowed (passed to Access Policies for evaluation) when the DLP server fails to provide a timely response. Default is allow ("Permit all data transfers to proceed without scanning").
Trusted Root Certificate	Browse to and select the trusted-root certificate for the certificate(s) provided with the External DLP Servers, and then click Upload File. See Certificate Managementfor additional information.
Invalid Certificate Options	Specify how various invalid certificates are handled: **Drop** or **Monitor**.
Server Certificates	This section displays all DLP server certificates currently available on the appliance.

Step 3 (Optional) You can add another DLP server by clicking **Add Row** and entering the DLP Server information in the new fields provided.

Step 4 Submit and Commit Changes.

Controlling Upload Requests Using External DLP Policies

Once the Web Proxy receives the upload request headers, it has the information necessary to decide if the request should go to the external DLP system for scanning. The DLP system scans the request and returns a verdict to the Web Proxy, either block or monitor (evaluate the request against the Access Policies).

Procedure

Step 1 Choose **Web Security Manager > External Data Loss Prevention**.

Step 2 Click the link under the Destinations column for the policy group you want to configure.

Step 3 Under the **Edit Destination Settings** section, choose "**Define Destinations Scanning Custom Settings**."

Step 4 In the **Destination to scan** section, choose one of the following options:

- **Do not scan any uploads.** No upload requests are sent to the configured DLP system(s) for scanning. All upload requests are evaluated against the Access Policies.
- **Scan all uploads.** All upload requests are sent to the configured DLP system(s) for scanning. The upload request is blocked or evaluated against the Access Policies depending on the DLP system scanning verdict.
- **Scan uploads except to specified custom and external URL categories.** Upload requests that fall in specific custom URL categories are excluded from DLP scanning policies. Click **Edit custom categories list** to select the URL categories to scan.

Step 5 Submit and Commit Changes.

Logging of Data Loss Prevention Scanning

The access logs indicate whether or not an upload request was scanned by either the Cisco Data Security filters or an external DLP server. The access log entries include a field for the Cisco Data Security scan verdict and another field for the External DLP scan verdict based.

In addition to the access logs, the Secure Web Appliance provides the following log file types to troubleshoot Cisco Data Security and External DLP Policies:

- **Data Security Logs.** Records client history for upload requests that are evaluated by the Cisco Data Security filters.
- **Data Security Module Logs.** Records messages related to the Cisco Data Security filters.
- **Default Proxy Logs.** In addition recording errors related to the Web Proxy, the default proxy logs include messages related to connecting to external DLP servers. This allows you to troubleshoot connectivity or integration problems with external DLP servers.

The following text illustrates a sample Data Security Log entry:

```
Mon Mar 30 03:02:13 2009 Info: 303 10.1.1.1 - -
<<bar,text/plain,5120><foo,text/plain,5120>>
BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting ns server.com nc
```

Field Value	Description
`Mon Mar 30 03:02:13 2009 Info:`	Timestamp and trace level
`303`	Transaction ID
`10.1.1.1`	Source IP address
`-`	User name
`-`	Authorized group names
`<<bar,text/plain,5120><foo,text/plain,5120>>`	File name, file type, file size for each file uploaded at once **Note** This field does not include text/plain files that are less than the configured minimum request body size, the default of which is 4096 bytes.
`BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting`	Cisco Data Security policy and action
`ns`	Web reputation score
`server.com`	Outgoing URL
`nc`	URL category

Note To learn when data transfer, such as a POST request, to a site was blocked by the external DLP server, search for the IP address or hostname of the DLP server in the access logs.

Notify End-Users of Proxy Actions

This topic contains the following sections:

- Custom Messages on Notification Pages, on page 68
- Editing Notification Page HTML Files Directly , on page 69
- Notification Page Types, on page 73

End-User Notifications Overview

You can configure the following types of notifications for end users:

Option	Description	Further information
End-user acknowledgement page	Informs end users that their web activity is being filtered and monitored. An end-user acknowledgment page is displayed when a user first accesses a browser after a certain period of time.	End-User Acknowledgment Page, on page 60
End-user notification pages	Page shown to end users when access to a particular page is blocked, specific to the reason for blocking it.	End-User Notification Pages , on page 63
End-user URL filtering warning page	Warns end users that a site they are accessing does not meet your organization's acceptable use policies, and allows them to continue if they choose.	Configuring the End-User URL Filtering Warning Page, on page 67
FTP notification messages	Gives end users the reason a native FTP transaction was blocked.	Configuring FTP Notification Messages, on page 67.
Time and Volume Quotas Expiry Warning Page	Notifies end users when their access is blocked because they have reached the configured data volume or time limit.	Configure these settings on the Security Services > End User Notification page, Time and Volume Quotas Expiry Warning Page section. See also Time Ranges and Quotas.

Configuring General Settings for Notification Pages

Specify display languages and logo for notification pages. Restrictions are described in this procedure.

Procedure

Step 1 Select **Security Services > End-User Notification**.

Step 2 Click **Edit Settings**.

Step 3 In the General Settings section, select the language the Web Proxy should use when displaying notification pages.

- The HTTP language setting applies to all HTTP notification pages (acknowledgment, on-box end-user, customized end-user, and end-user URL filtering warning).

- The FTP language applies to all FTP notification messages.

Step 4 Choose whether or not to use a logo on each notification page. You can specify the Cisco logo or any graphic file referenced at the URL you enter in the Use Custom Logo field.

This setting applies to all HTTP notification pages served over IPv4. AsyncOS does not support images over IPv6.

Step 5 Submit and Commit Changes.

What to do next

Related Topics

- Caveats for URLs and Logos in Notification Pages , on page 69

End-User Acknowledgment Page

You can configure the Secure Web Appliance to inform users that it is filtering and monitoring their web activity. When configured, the appliance displays an end-user acknowledgment page for every user accessing the web using HTTP or HTTPS. It displays the end-user acknowledgment page when a user tries to access a website for the first time, or after a configured time interval.

The Web Proxy tracks users by username if authentication has made a username available. If no user name is available, you can choose how to track users, either by IP address or web browser session cookie.

Note Native FTP transactions are exempt from the end-user acknowledgment page.

- Access HTTPS and FTP Sites with the End-User Acknowledgment Page, on page 60
- About the End-user Acknowledgment Page, on page 61
- Configuring the End-User Acknowledgment Page, on page 61

Access HTTPS and FTP Sites with the End-User Acknowledgment Page

The end-user acknowledgment page works because it displays an HTML page to the end user that forces them to click an acceptable use policy agreement. After users click the link, the Web Proxy redirects clients to the originally requested website. It keeps track of when users accepted the end-user acknowledgment page using a surrogate (either by IP address or web browser session cookie) if no username is available for the user.

- **HTTPS.** The Web Proxy tracks whether the user has acknowledged the end-user acknowledgment page with a cookie, but it cannot obtain the cookie unless it decrypts the transaction. You can choose to either bypass (pass through) or drop HTTPS requests when the end-user acknowledgment page is enabled and tracks users using session cookies. Do this using the advancedproxyconfig > EUN CLI command, and choose bypass for the “Action to be taken for HTTPS requests with Session based EUA (“bypass” or “drop”).” command.
- **FTP over HTTP.** Web browsers never send cookies for FTP over HTTP transactions, so the Web Proxy cannot obtain the cookie. To work around this, you can exempt FTP over HTTP transactions from requiring the end-user acknowledgment page. Do this by creating a custom URL category using “ftp://”

as the regular expression (without the quotes) and defining and Identity policy that exempts users from the end-user acknowledgment page for this custom URL category.

About the End-user Acknowledgment Page

- When a user is tracked by IP address, the appliance uses the shortest value for maximum time interval and maximum IP address idle timeout to determine when to display the end-user acknowledgment page again.
- When a user is tracked using a session cookie, the Web Proxy displays the end-user acknowledgment page again if the user closes and then reopens their web browser or opens a second web browser application.
- Using a session cookie to track users when the client accesses HTTPS sites or FTP servers using FTP over HTTP does not work.
- When the appliance is deployed in explicit forward mode and a user goes to an HTTPS site, the end-user acknowledgment page includes only the domain name in the link that redirects the user to the originally requested URL. If the originally requested URL contains text after the domain name, that text is truncated.
- When the end-user acknowledgment page is displayed to a user, the access log entry for that transaction shows OTHER as the ACL decision tag. This is because the originally requested URL was blocked, and instead the user was shown the end-user acknowledgment page.

Configuring the End-User Acknowledgment Page

Before you begin

- To configure the display language and customize the displayed logo, see Configuring General Settings for Notification Pages, on page 59.
- If you will customize the message shown to end users, see Custom Messages on Notification Pages, on page 68. If you require more customization than the Custom Message box allows, see Editing Notification Page HTML Files Directly , on page 69.

You can enable and configure the end-user acknowledgment page in the web interface or the command line interface. When you configure the end-user acknowledgment page in the web interface, you can include a custom message that appears on each page.

In the CLI, use `advancedproxyconfig > eun`.

Procedure

Step 1 Choose **Security Services > End-User Notification**.

Step 2 Click **Edit Settings**.

Step 3 Enable the "**Require end-user to click through acknowledgment page**" field.

Step 4 Enter options:

Setting	Description
Time Between Acknowledgements	The Time Between Acknowledgments determines how often the Web Proxy displays the end-user acknowledgment page for each user. This setting applies to users tracked by username and users tracked by IP address or session cookie. You can specify any value from 30 to 2678400 seconds (one month). Default is one day (86400 seconds). When the Time Between Acknowledgments changes and is committed, the Web Proxy uses the new value even for users who have already acknowledged the Web Proxy.
Inactivity Timeout	The Inactivity Timeout determines how long a user tracked and acknowledged by IP address or session cookie (unauthenticated users only) can be idle before the user is no longer considered to have agreed to the acceptable use policy. You can specify any value from 30 to 2678400 seconds (one month). Default is four hours (14400 seconds).
Surrogate Type	Determines which method the Web Proxy uses to track the user: • **IP Address.** The Web Proxy allows the user at that IP address to use any web browser or non-browser HTTP process to access the web once the user clicks the link on the end-user acknowledgment page. Tracking the user by IP address allows the user to access the web until the Web Proxy displays a new end-user acknowledgment page due to inactivity or the configured time interval for new acknowledgments. Unlike tracking by a session cookie, tracking by IP address allows the user to open up multiple web browser applications and not have to agree to the end-user acknowledgment unless the configured time interval has expired. **Note** When IP address is configured and the user is authenticated, the Web Proxy tracks users by username instead of IP address. • **Session Cookie.** The Web Proxy sends the user's web browser a cookie when the user clicks the link on the end-user acknowledgment page and uses the cookie to track their session. Users can continue to access the web using their web browser until the Time Between Acknowledgments value expires, they have been inactive longer than the allotted time, or they close their web browser. If the user using a non-browser HTTP client application, they must be able to click the link on the end-user acknowledgment page to access the web. If the user opens a second web browser application, the user must go through the end-user acknowledgment process again in order for the Web Proxy to send a session cookie to the second web browser. **Note** Using a session cookie to track users when the client accesses HTTPS sites or FTP servers using FTP over HTTP is not supported.
Custom message	Customize the text that appears on every end-user acknowledgment page. You can include some simple HTML tags to format the text. **Note** You can only include a custom message when you configure the end-user acknowledgment page in the web interface, versus the CLI. See also Custom Messages on Notification Pages, on page 68.

Step 5 (Optional) Click **Preview Acknowledgment Page Customization** to view the current end-user acknowledgment page in a separate browser window.

Note
If the notification HTML files have been edited, this preview functionality is not available.

Step 6 Submit and Commit Changes.

End-User Notification Pages

When a policy blocks a user from a website, you can configure the appliance to notify the user why it blocked the URL request. There are several ways to achieve this:

To	See
Display predefined, customizable pages that are hosted on the Secure Web Appliance.	Configuring On-Box End-User Notification Pages, on page 63
Redirect the user to HTTP end-user notification pages at a specific URL.	Off-Box End-User Notification Pages , on page 64

Configuring On-Box End-User Notification Pages

Before you begin

- To configure the display language and customize the displayed logo, see Configuring General Settings for Notification Pages, on page 59.
- If you will customize the message displayed using on-box notifications, review the topics under Custom Messages on Notification Pages, on page 68. If you require more customization than the Custom Message box allows, see Editing Notification Page HTML Files Directly , on page 69.

On-box pages are predefined, customizable notification pages residing on the appliance.

Procedure

Step 1 **Security Services > End-User Notification**.

Step 2 Click **Edit Settings**.

Step 3 From the Notification Type field, choose **Use On Box End User Notification**.

Step 4 Configure the on-box end-user notification page settings.

Setting	Description
Custom Message	Include any additional text required on each notification page. When you enter a custom message, AsyncOS places the message before the last sentence on the notification page which includes the contact information.

Setting	Description
Contact Information	Customize the contact information listed on each notification page. AsyncOS displays the contact information sentence as the last sentence on a page, before providing notification codes that users can provide to the network administrator.
End-User Misclassification Reporting	If enabled, the misclassification request is sent over HTTPS if HTTPS proxy is enabled or else it is sent over HTTP. You will not receive any security alert notification. When enabled, users can report misclassified URLs to Cisco. An additional button appears on the on-box end-user notification pages for sites blocked due to suspected malware or URL filters. This button allows the user to report when they believe the page has been misclassified. It does not appear for pages blocked due to other policy settings. **Note** • You must enable SensorBase Network Participation. See Enabling Participation in The Cisco SensorBase Network for more information. • You must have a valid Cisco account linked to the serial number/s of your appliance/s. • Reporting of misclassified URLs does not work on virtual Secure Web Appliance.

Step 5 (Optional) Click **Preview Notification Page Customization** link to view the current end-user notification page in a separate browser window.

Note
If the notification HTML files have been edited, this preview functionality is not available.

Step 6 Submit and Commit Changes.

Off-Box End-User Notification Pages

The Web Proxy can be configured to redirect all HTTP end-user notification pages to a specific URL that you specify.

Displaying the Correct Off-Box Page Based on the Reason for Blocking Access

By default, AsyncOS redirects all blocked websites to the URL regardless of the reason why it blocked the original page. However, AsyncOS also passes parameters as a query string appended to the redirect URL so you can ensure that the user sees a unique page explaining the reason for the block. For more information on the included parameters, see Off-Box End-User Notification Page Parameters, on page 65.

When you want the user to view a different page for each reason for a blocked website, construct a CGI script on the web server that can parse the query string in the redirect URL. Then the server can perform a second redirect to an appropriate page.

URL Criteria for Off-Box Notification Pages

- You can use any HTTP or HTTPS URL.
- The URL may specify a specific port number.
- The URL may not have any arguments after the question mark.
- The URL must contain a well-formed hostname.

For example, if you have the following URL entered in the Redirect to Custom URL field:

```
http://www.example.com/eun.policy.html
```

And you have the following access log entry:

```
1182468145.492 1 172.17.0.8 TCP_DENIED/403 3146 GET http://www.espn.com/index.html HTTP/1.1
 - NONE/- - BLOCK_WEBCAT-DefaultGroup-DefaultGroup-NONE-NONE-DefaultRouting
<IW_sprt,-,-,-,-,-,-,-,-,-,-,-,-,-,IW_sprt,-> -
```

Then AsyncOS creates the following redirected URL:

```
http://www.example.com/eun.policy.html?Time=21/Jun/
2007:23:22:25%20%2B0000&ID=0000000004&Client_IP=172.17.0.8&User=-
&Site=www.espn.com&URI=index.html&Status_Code=403&Decision_Tag=
BLOCK_WEBCAT-DefaultGroup-DefaultGroup-NONE-NONE-DefaultRouting
&URL_Cat=Sports%20and%20Recreation&WBRS=-&DVS_Verdict=-&
DVS_ThreatName=-&Reauth_URL=-
```

Off-Box End-User Notification Page Parameters

AsyncOS passes the parameters to the web server as standard URL Parameters in the HTTP GET request. It uses the following format:

```
<notification_page_url>?param1=value1&param2=value2
```

The table describes the parameters AsyncOS includes in the query string.

Parameter Name	Description
Time	Date and time of the transaction.
ID	Transaction ID.
Client_IP	IP address of the client.
User	Username of the client making the request, if available.
Site	Hostname of the destination in the HTTP request.
URI	URL path specified in the HTTP request.
Status_Code	HTTP status code for the request.
Decision_Tag	ACL decision tag as defined in the Access log entry that indicates how the DVS engine handled the transaction.

Parameter Name	Description
URL_Cat	URL category that the URL filtering engine assigned to the transaction request. **Note:** AsyncOS for Web sends the entire URL category name for both predefined and user defined URL categories. It performs URL encoding on the category name, so spaces are written as "%20".
WBRS	WBRS score that the Web Reputation Filters assigned to the URL in the request.
DVS_Verdict	Malware category that the DVS engine assigns to the transaction.
DVS_ThreatName	The name of the malware found by the DVS engine.
Reauth_URL	A URL that users can click to authenticate again if the user is blocked from a website due to a restrictive URL filtering policy. Use this parameter when the "Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction" global authentication setting is enabled and the user is blocked from a website due to a blocked URL category. To use this parameter, make sure the CGI script performs the following steps: 1. Get the value of `Reauth_Url` parameter. 2. URL-decode the value. 3. Base64 decode the value and get the actual re-authentication URL. 4. Include the decoded URL on the end-user notification page in some way, either as a link or button, along with instructions for users informing them they can click the link and enter new authentication credentials that allow greater access.

Note AsyncOS always includes all parameters in each redirected URL. If no value exists for a particular parameter, AsyncOS passes a hyphen (-).

Redirecting End-User Notification Pages to a Custom URL (Off-Box)

Procedure

Step 1 **Security Services > End-User Notification**.

Step 2 Click **Edit Settings**.

Step 3 In the **End-User Notification Pages** section, choose **Redirect to Custom URL**.

Step 4 In the **Notification Page URL** field, enter the URL to which you want to redirect blocked websites.

Step 5 (Optional) Click **Preview Custom URL** link.

Step 6 Submit and Commit Changes.

Configuring the End-User URL Filtering Warning Page

Before you begin

- If you will customize the message displayed using on-box notifications, review the topics under Custom Messages on Notification Pages, on page 68. If you require more customization than the Custom Message box allows, see Editing Notification Page HTML Files Directly , on page 69.

An end-user URL filtering warning page is displayed when a user first accesses a website in a particular URL category after a certain period of time. You can also configure the warning page when a user accesses adult content when the site content ratings feature is enabled.

Procedure

Step 1 **Security Services > End-User Notification**.

Step 2 Click **Edit Settings**.

Step 3 Scroll down to the End-User URL Filtering Warning Page section.

Step 4 In the Time Between Warning field, enter the time interval the Web Proxy uses between displaying the end-user URL filtering warning page for each URL category per user.

You can specify any value from 30 to 2678400 seconds (one month). Default is 1 hour (3600 seconds). You can enter the value in seconds, minutes, or days. Use ‘s’ for seconds, ‘m’ for minutes, and ‘d’ for days.

Step 5 In the Custom Message field, enter text you want to appear on every end-user URL filtering warning page.

Step 6 (Optional) Click **Preview URL Category Warning Page Customization** to view the current end-user URL filtering warning page in a separate browser window.

Note
If the notification HTML files have been edited, this preview functionality is not available.

Step 7 Submit and Commit Changes.

Configuring FTP Notification Messages

Before you begin

If you will customize the message displayed using on-box notifications, review the topics under Custom Messages on Notification Pages, on page 68. If you require more customization than the Custom Message box allows, see Editing Notification Page HTML Files Directly , on page 69.

The FTP Proxy displays a predefined, customizable notification message to native FTP clients when the FTP Proxy cannot establish a connection with the FTP server for any reason, such as an error with FTP Proxy authentication or a bad reputation for the server domain name. The notification is specific to the reason the connection was blocked.

Procedure

Step 1 **Security Services > End-User Notification**.

Step 2 Click **Edit Settings**.

Step 3 Scroll down to the Native FTP section.

Step 4 In the **Language** field, select the language to use when displaying native FTP notification messages.

Step 5 In the **Custom Message** field, enter the text you want to display in every native FTP notification message.

Step 6 Submit and Commit Changes.

Custom Messages on Notification Pages

The following sections apply to text entered into the "Custom Message" box for any notification type configured on the Edit End User Notification page.

- Supported HTML Tags in Custom Messages on Notification Pages, on page 68
- Caveats for URLs and Logos in Notification Pages , on page 69

Supported HTML Tags in Custom Messages on Notification Pages

You can use HTML tags to format the text in any notification on the Edit End User Notification page that offers a "Custom Message" box. Tags must be in lower case and follow standard HTML syntax (closing tags, etc.)

You can use the following HTML tags.

- <a>
-
-
- <big></big>
-
- <code></code>
-
-
- <small></small>
-

For example, you can make some text italic:

```
Please acknowledge the following statements <i>before</i> accessing the Internet.
```

With the tag, you can use any CSS style to format text. For example, you can make some text red:

```
 <span style="color: red">Warning:</span> You must acknowledge the following statements
<i>before</i> accessing the Internet.
```

Note If you need greater flexibility or wish to add JavaScript to your notification pages, you must edit the HTML notification files directly. JavaScript entered into the Custom Message box for notifications in the web user interface will be stripped out. See Editing Notification Page HTML Files Directly , on page 69.

Caveats for URLs and Logos in Notification Pages

This section applies if you will make any of the following customizations:

- Enter text into the "Custom Message" box for any notification on the Edit End User Notification page
- Directly edit HTML files for on-box notifications
- Use a custom logo

All combinations of URL paths and domain names in embedded links within custom text, and the custom logo, are exempted from the following for on-box notifications:

- User authentication
- End-user acknowledgment
- All scanning, such as malware scanning and web reputation scoring

For example, if the following URLs are embedded in custom text:

```
http://www.example.com/index.html
```

```
http://www.mycompany.com/logo.jpg
```

Then all of the following URLs will also be treated as exempt from all scanning:

```
http://www.example.com/index.html
```

```
http://www.mycompany.com/logo.jpg
```

```
http://www.example.com/logo.jpg
```

```
http://www.mycompany.com/index.html
```

Also, where an embedded URL is of the form: `<protocol>://<domain-name>/<directory path>/` then all sub-files and sub-directories under that directory path on the host will also be exempted from all scanning.

For example, if the following URL is embedded: `http://www.example.com/gallery2/` URLs such as `http://www.example.com/gallery2/main.php` will also be treated as exempt.

This allows you to create a more sophisticated page with embedded content so long as the embedded content is relative to the initial URL. However, you should also take care when deciding which paths to include as links and custom logos.

Editing Notification Page HTML Files Directly

Each notification page is stored on the Secure Web Appliance as an HTML file. If you require more customization than the "Custom Message" box in the web-based interface allows, you can directly edit these HTML files. For example, you can include standard JavaScript or edit the overall look and feel of each page.

Information in the following sections applies to any type of end-user notification HTML file on the appliance, including End-User Acknowledgment pages.

- Requirements for Editing Notification HTML Files Directly , on page 70

Requirements for Editing Notification HTML Files Directly

- Each notification page file must be a valid HTML file. For a list of HTML tags you can include, see Supported HTML Tags in Custom Messages on Notification Pages, on page 68.
- The customized notification page file names must exactly match the file names shipped with the Secure Web Appliance.

  If the `configuration\eun` directory does not contain a particular file with the required name, then the appliance displays the standard on-box end-user notification page.
- Do not include any links to URLs in the HTML files. Any link included in the notification pages are subject to the access control rules defined in the Access Policies and users might end up in a recursive loop.
- Test your HTML files in supported client browsers to ensure that they behave as expected, especially if they include JavaScript.
- For your customized pages to take effect, you must enable the customized files using the `advancedproxyconfig > EUN > Refresh EUN Pages` CLI command.

Editing Notification HTML Files Directly

Before you begin

- Understand the requirements in Requirements for Editing Notification HTML Files Directly , on page 70.
- See Variables for Customizing Notification HTML Files , on page 71 and Using Variables in Notification HTML Files , on page 71.

Procedure

Step 1 Use an FTP client to connect to the Secure Web Appliance.

Step 2 Navigate to the `configuration\eun` directory.

Step 3 Download the language directory files for the notification pages you want to edit.

Step 4 On your local machine, use a text or HTML editor to edit the HTML files.

Step 5 Use the FTP client to upload the customized HTML files to the same directory from which you downloaded them in step 3.

Step 6 Open an SSH client and connect to the Secure Web Appliance.

Step 7 Run the `advancedproxyconfig > EUN` CLI command.

Step 8 Type **2** to use the custom end-user notification pages.

Step 9 If the custom end-user notification pages option is currently enabled when you update the HTML files, type **1** to refresh the custom end-user notification pages.

If you do not do this, the new files do not take effect until the Web Proxy restarts.

Step 10 Commit your change.

Step 11 Close the SSH client.

Using Variables in Notification HTML Files

When editing notification HTML files, you can include conditional variables to create if-then statements to take different actions depending on the current state.

The table describes the different conditional variable formats.

Conditional Variable Format	Description
%?*V*	This conditional variable evaluates to TRUE if the output of variable %*V* is not empty.
%!*V*	Represents the following condition: `else` Use this with the %?*V* conditional variable.
%#*V*	Represents the following condition: `endif` Use this with the %?*V* conditional variable.

For example, the following text is some HTML code that uses %R as a conditional variable to check if re-authentication is offered, and uses %r as a regular variable to provide the re-authentication URL.

```
%?R
<div align="left">
  <form name="ReauthInput" action="%r" method="GET">
    <input name="Reauth" type="button" OnClick="document.location='%r'"
id="Reauth" value="Login as different user...">
  </form>
</div>
%#R
```

Any variable included in Variables for Customizing Notification HTML Files , on page 71 can be used as a conditional variable. However, the best variables to use in conditional statements are the ones that relate to the *client request* instead of the server response, and the variables that may or may not evaluate to TRUE instead of the variables that always evaluate to TRUE.

Variables for Customizing Notification HTML Files

You can use variables in the notification HTML files to display specific information to the user. You can also turn each variable into a conditional variable to create if-then statements. For more information, see Using Variables in Notification HTML Files , on page 71.

Variable	Description	Always Evaluates to TRUE if Used as Conditional Variable
%a	Authentication realm for FTP	No
%A	ARP address	Yes
%b	User-agent name	No
%B	Blocking reason, such as BLOCK-SRC or BLOCK-TYPE	No
%c	Error page contact person	Yes
%C	Entire Set-Cookie: header line, or empty string	No
%d	Client IP address	Yes
%D	User name	No
%e	Error page email address	Yes
%E	The error page logo URL	No
%f	User feedback section	No
%F	The URL for user feedback	No
%g	The web category name, if available	Yes
%G	Maximum file size allowed in MB	No
%h	The hostname of the proxy	Yes
%H	The server name of the URL	Yes
%i	Transaction ID as a hexadecimal number	Yes
%I	Management IP Address	Yes
%j	URL category warning page custom text	No
%k	Redirection link for the end-user acknowledgment page and end-user URL filtering warning page	No
%K	Response file type	No
%l	WWW-Authenticate: header line	No
%L	Proxy-Authenticate: header line	No
%M	The Method of the request, such as “GET” or “POST”	Yes
%n	Malware category name, if available	No
%N	Malware threat name, if available	No
%o	Web reputation threat type, if available	No

Variable	Description	Always Evaluates to TRUE if Used as Conditional Variable
%O	Web reputation threat reason, if available	No
%p	String for the Proxy-Connection HTTP header	Yes
%P	Protocol	Yes
%q	Identity policy group name	Yes
%Q	Policy group name for non-Identity polices	Yes
%r	Redirect URL	No
%R	Re-authentication is offered. This variable outputs an empty string when false and a space when true, so it is not useful to use it alone. Instead, use it as condition variable.	No
%S	The signature of the proxy	No, always evaluates to FALSE
%t	Timestamp in Unix seconds plus milliseconds	Yes
%T	The date	Yes
%u	The URI part of the URL (the URL excluding the server name)	Yes
%U	The full URL of the request	Yes
%v	HTTP protocol version	Yes
%W	Management WebUI port	Yes
%X	Extended blocking code. This is a 16-byte base64 value that encodes the most of the web reputation and anti-malware information logged in the access log, such as the ACL decision tag and WBRS score.	Yes
%Y	Administrator custom text string, if set, else empty	No
%y	End-user acknowledgment page custom text	Yes
%z	Web reputation score	Yes
%Z	DLP meta data	Yes
%%	Prints the percent symbol (%) in the notification page	N/A

Notification Page Types

By default, the Web Proxy displays a notification page informing users they were blocked and the reason for the block.

Most notification pages display a different set of codes that may help administrators or Cisco Customer Support troubleshoot any potential problem. Some codes are for Cisco internal use only. The different codes that might

appear in the notification pages are the same as the variables you can include in customized notification pages, as shown in Variables for Customizing Notification HTML Files , on page 71.

The table describes the different notification pages users might encounter.

File Name and Notification Title	Notification Description	Notification Text
ERR_ACCEPTED Feedback Accepted, Thank You	Notification page that is displayed after the users uses the “Report Misclassification” option.	The misclassification report has been sent. Thank you for your feedback.
ERR_ADAPTIVE_SECURITY Policy: General	Block page that is displayed when the user is blocked due to the Adaptive Scanning feature.	Based on your organization’s security policies, this web site <*URL* > has been blocked because its content has been determined to be a security risk.
ERR_ADULT_CONTENT Policy Acknowledgment	The warning page that is displayed when the end-user accesses a page that is classified as adult content. Users can click an acknowledgment link to continue to the originally requested site.	You are trying to visit a web page whose content are rated as explicit or adult. By clicking the link below, you acknowledge that you have read and agree with the organization's policies that govern the usage of the Internet for this type of content. Data about your browsing behavior may be monitored and recorded. You will be periodically asked to acknowledge this statement for continued access to this kind of web page. Click here to accept this statement and access the Internet.
ERR_AVC Policy: Application Controls	Block page that is displayed when the user is blocked due to the Application Visibility and Control engine.	Based on your organization’s access policies, access to application %1 of type %2 has been blocked.
ERR_BAD_REQUEST Bad Request	Error page that results from an invalid transaction request.	The system cannot process this request. A non-standard browser may have generated an invalid HTTP request. If you are using a standard browser, please retry the request.
ERR_BLOCK_DEST Policy: Destination	Block page that is displayed when the user tries to access a blocked website address.	Based on your organization’s Access Policies, access to this web site <*URL* > has been blocked.

File Name and Notification Title	Notification Description	Notification Text
ERR_BROWSER Security: Browser	Block page that is displayed when the transaction request comes from an application that has been identified to be compromised by malware or spyware.	Based on your organization's Access Policies, requests from your computer have been blocked because it has been determined to be a security threat to the organization's network. Your browser may have been compromised by a malware/spyware agent identified as "<*malware name* >". Please contact <*contact name* > <*email address* > and provide the codes shown below. If you are using a non-standard browser and believe it has been misclassified, use the button below to report this misclassification.
ERR_BROWSER_CUSTOM Policy: Browser	Block page that is displayed when the transaction request comes from a blocked user agent.	Based on your organization's Access Policies, requests from your browser have been blocked. This browser "<*browser type* >" is not permitted due to potential security risks.
ERR_CERT_INVALID Invalid Certificate	Block page that is displayed when the requested HTTPS site uses an invalid certificate.	A secure session cannot be established because the site <*hostname* > provided an invalid certificate.
ERR_CONTINUE_ UNACKNOWLEDGED Policy Acknowledgment	Warning page that is displayed when the user requests a site that is in a custom URL category that is assigned the Warn action. Users can click an acknowledgment link to continue to the originally requested site.	You are trying to visit a web page that falls under the URL Category <*URL category* >. By clicking the link below, you acknowledge that you have read and agree with the organization's policies that govern the usage of the Internet for this type of content. Data about your browsing behavior may be monitored and recorded. You will be periodically asked to acknowledge this statement for continued access to this kind of web page. Click here to accept this statement and access the Internet.

File Name and Notification Title	Notification Description	Notification Text
ERR_DNS_FAIL DNS Failure	Error page that is displayed when the requested URL contains an invalid domain name.	The hostname resolution (DNS lookup) for this hostname <*hostname* > has failed. The Internet address may be misspelled or obsolete, the host <*hostname* > may be temporarily unavailable, or the DNS server may be unresponsive. Please check the spelling of the Internet address entered. If it is correct, try this request later.
ERR_EXPECTATION_ FAILED Expectation Failed	Error page that is displayed when the transaction request triggers the HTTP 417 “Expectation Failed” response.	The system cannot process the request for this site <*URL* >. A non-standard browser may have generated an invalid HTTP request. If using a standard browser, please retry the request.
ERR_FILE_SIZE Policy: File Size	Block page that is displayed when the requested file is larger than the allowed maximum file size.	Based on your organization’s Access Policies, access to this web site or download <*URL* > has been blocked because the download size exceeds the allowed limit.
ERR_FILE_TYPE Policy: File Type	Block page that is displayed when the requested file is a blocked file type.	Based on your organization’s Access Policies, access to this web site or download <*URL* > has been blocked because the file type “<*file type* >” is not allowed.
ERR_FILTER_FAILURE Filter Failure	Error page that is displayed when the URL filtering engine is temporarily unable to deliver a URL filtering response and the “Default Action for Unreachable Service” option is set to Block.	The request for page <*URL* > has been denied because an internal server is currently unreachable or overloaded. Please retry the request later.
ERR_FOUND Found	Internal redirection page for some errors.	The page <*URL* > is being redirected to <*redirected URL* >.
ERR_FTP_ABORTED FTP Aborted	Error page that is displayed when the FTP over HTTP transaction request triggers the HTTP 416 “Requested Range Not Satisfiable” response.	The request for the file <*URL* > did not succeed. The FTP server <*hostname* > unexpectedly terminated the connection. Please retry the request later.

File Name and Notification Title	Notification Description	Notification Text
ERR_FTP_AUTH_REQUIRED FTP Authorization Required	Error page that is displayed when the FTP over HTTP transaction request triggers the FTP 530 “Not Logged In” response.	Authentication is required by the FTP server <*hostname* >. A valid user ID and passphrase must be entered when prompted. In some cases, the FTP server may limit the number of anonymous connections. If you usually connect to this server as an anonymous user, please try again later.
ERR_FTP_CONNECTION_FAILED FTP Connection Failed	Error page that is displayed when the FTP over HTTP transaction request triggers the FTP 425 “Can’t open data connection” response.	The system cannot communicate with the FTP server <*hostname* >. The FTP server may be temporarily or permanently down, or may be unreachable because of network problems. Please check the spelling of the address entered. If it is correct, try this request later.
ERR_FTP_FORBIDDEN FTP Forbidden	Error page that is displayed when the FTP over HTTP transaction request is for an object the user is not allowed to access.	Access was denied by the FTP server <*hostname* >. Your user ID does not have permission to access this document.
ERR_FTP_NOT_FOUND FTP Not Found	Error page that is displayed when the FTP over HTTP transaction request is for an object that does not exist on the server.	The file <*URL* > could not be found. The address is either incorrect or obsolete.
ERR_FTP_SERVER_ERR FTP Server Error	Error page that is displayed for FTP over HTTP transactions that try to access a server that does support FTP. The server usually returns the HTTP 501 “Not Implemented” response.	The system cannot communicate with the FTP server <*hostname* >. The FTP server may be temporarily or permanently down, or may not provide this service. Please confirm that this is a valid address. If it is correct, try this request later.
ERR_FTP_SERVICE_UNAVAIL FTP Service Unavailable	Error page that is displayed for FTP over HTTP transactions that try to access an FTP server that is unavailable.	The system cannot communicate with the FTP server <*hostname* >. The FTP server may be busy, may be permanently down, or may not provide this service. Please confirm that this is a valid address. If it is correct, try this request later.

File Name and Notification Title	Notification Description	Notification Text
ERR_GATEWAY_TIMEOUT Gateway Timeout	Error page that is displayed when the requested server has not responded in a timely manner.	The system cannot communicate with the external server <*hostname* >. The Internet server may be busy, may be permanently down, or may be unreachable because of network problems. Please check the spelling of the Internet address entered. If it is correct, try this request later.
ERR_IDS_ACCESS_FORBIDDEN IDS Access Forbidden	Block page that is displayed when the user tries to upload a file that is blocked due to a configured Cisco Data Security Policy.	Based on your organization's data transfer policies, your upload request has been blocked. File details: <*file details* >
ERR_INTERNAL_ERROR Internal Error	Error page that is displayed when there is an internal error.	Internal system error when processing the request for the page <*URL* >. Please retry this request. If this condition persists, please contact <*contact name* > <*email address* > and provide the code shown below.
ERR_MALWARE_SPECIFIC Security: Malware Detected	Block page that is displayed when malware is detected when downloading a file.	Based on your organization's Access Policies, this web site <*URL* > has been blocked because it has been determined to be a security threat to your computer or the organization's network. Malware <*malware name* > in the category <*malware category* > has been found on this site.
ERR_MALWARE_SPECIFIC_OUTGOING Security: Malware Detected	Block page that is displayed when malware is detected when uploading a file.	Based on your organization's policy, the upload of the file to URL (<*URL* >) has been blocked because the file was detected to contain malware that will be harmful to the receiving end's network security. Malware Name: <*malware name* > Malware Category: <*malware category* >
ERR_NATIVE_FTP_DENIED	Block message displayed in native FTP clients when the native FTP transaction is blocked.	530 Login denied

File Name and Notification Title	Notification Description	Notification Text
ERR_NO_MORE_ FORWARDS No More Forwards	Error page that is displayed when the appliance has detected a forward loop between the Web Proxy and another proxy server on the network. The Web Proxy breaks the loop and displays this message to the client.	The request for the page <*URL* > failed. The server address <*hostname* > may be invalid, or you may need to specify a port number to access this server.
ERR_POLICY Policy: General	Block page that is displayed when the request is blocked by any policy setting.	Based on your organization's Access Policies, access to this web site <*URL* > has been blocked.
ERR_PROTOCOL Policy: Protocol	Block page that is displayed when the request is blocked based on the protocol used.	Based on your organization's Access Policies, this request has been blocked because the data transfer protocol "<*protocol type* >" is not allowed.
ERR_PROXY_AUTH_ REQUIRED Proxy Authorization Required	Notification page that is displayed when users must enter their authentication credentials to continue. This is used for explicit transaction requests.	Authentication is required to access the Internet using this system. A valid user ID and passphrase must be entered when prompted.
ERR_PROXY_PREVENT_ MULTIPLE_LOGIN Already Logged In From Another Machine	Block page that is displayed when someone tries to access the web using the same username that is already authenticated with the Web Proxy on a different machine. This is used when the User Session Restrictions global authentication option is enabled.	Based on your organization's policies, the request to access the Internet was denied because this user ID has an active session from another IP address. If you want to login as a different user, click on the button below and enter a different a user name and passphrase.
ERR_PROXY_REDIRECT Redirect	Redirection page.	This request is being redirected. If this page does not automatically redirect, click here to proceed.

File Name and Notification Title	Notification Description	Notification Text
ERR_PROXY_UNACKNOWLEDGED Policy Acknowledgment	End-user acknowledgment page. For more information, see End-User Notification Pages , on page 63.	Please acknowledge the following statements before accessing the Internet. Your web transactions will be automatically monitored and processed to detect dangerous content and to enforce organization's policies. By clicking the link below, you acknowledge this monitoring and accept that data about the sites you visit may be recorded. You will be periodically asked to acknowledge the presence of the monitoring system. You are responsible for following organization's polices on Internet access. Click here to accept this statement and access the Internet.
ERR_PROXY_UNLICENSED Proxy Not Licensed	Block page that is displayed when there is no valid license key for the Secure Web Appliance Web Proxy.	Internet access is not available without proper licensing of the security device. Please contact <*contact name*> <*email address*> and provide the code shown below. **Note** To access the management interface of the security device, enter the configured IP address with port.
ERR_RANGE_NOT_SATISFIABLE Range Not Satisfiable	Error page that is displayed when the requested range of bytes cannot be satisfied by the web server.	The system cannot process this request. A non-standard browser may have generated an invalid HTTP request. If you are using a standard browser, please retry the request.
ERR_REDIRECT_PERMANENT Redirect Permanent	Internal redirection page.	The page <*URL*> is being redirected to <*redirected URL*>.
ERR_REDIRECT_REPEAT_REQUEST Redirect	Internal redirection page.	Please repeat your request.

File Name and Notification Title	Notification Description	Notification Text
ERR_SAAS_AUTHENTICATION Policy: Access Denied	Notification page that is displayed when users must enter their authentication credentials to continue. This is used for accessing applications.	Based on your organization's policy, the request to access <*URL* > was redirected to a page where you must enter the login credentials. You will be allowed to access the application if authentication succeeds and you have the proper privileges.
ERR_SAAS_AUTHORIZATION Policy: Access Denied	Block page that is displayed when users try to access a application that they have no privilege to access.	Based on your organization's policy, the access to the application <*URL* > is blocked because you are not an authorized user. If you want to login as a different user, enter a different username and passphrase for a user that is authorized to access this application.
ERR_SAML_PROCESSING Policy: Access Denied	Error page that is displayed when an internal process fails trying to process the single sign-on URL for accessing a application.	The request to access <*user name* > did not go through because errors were found during the process of the single sign on request.
ERR_SERVER_NAME_EXPANSION Server Name Expansion	Internal redirection page that automatically expands the URL and redirects users to the updated URL.	The server name <*hostname* > appears to be an abbreviation, and is being redirected to <*redirected URL* >.
ERR_URI_TOO_LONG URI Too Long	Block page that is displayed when the URL length is too long.	The requested URL was too long and could not be processed. This may represent an attack on your network. Please contact <*contact name* > <*email address* > and provide the code shown below.
ERR_WBRS Security: Malware Risk	Block page that is displayed when the Web Reputation Filters block the site due to a low web reputation score.	Based on your organization's access policies, this web site <*URL* > has been blocked because it has been determined by Web Reputation Filters to be a security threat to your computer or the organization's network. This web site has been associated with malware/spyware. Threat Type: %o Threat Reason: %O

File Name and Notification Title	Notification Description	Notification Text
ERR_WEBCAT Policy: URL Filtering	Block page that is displayed when users try to access a website in a blocked URL category.	Based on your organization's Access Policies, access to this web site <*URL* > has been blocked because the web category "<*category type* >" is not allowed.
ERR_WWW_AUTH_ REQUIRED WWW Authorization Required	Notification page that is displayed when the requested server requires users to enter their credentials to continue.	Authentication is required to access the requested web site <*hostname* >. A valid user ID and passphrase must be entered when prompted.

Detecting Rogue Traffic on Non-Standard Ports

This topic contains the following sections:

Overview of Detecting Rogue Traffic

The Secure Web Appliance has an integrated Layer-4 Traffic Monitor that detects rogue traffic across all network ports and stops malware attempts to bypass port 80. When internal clients are infected with malware and attempt to phone-home across non-standard ports and protocols, the L4 Traffic Monitor prevents phone-home activity from going outside the corporate network. By default, the L4 Traffic Monitor is enabled and set to monitor traffic on all ports. This includes DNS and other services.

The L4 Traffic Monitor uses and maintains its own internal database. This database is continuously updated with matched results for IP addresses and domain names.

Configuring the L4 Traffic Monitor

Procedure

Step 1 Configure the L4 Traffic Monitor inside the firewall.

Step 2 Ensure the L4 Traffic Monitor is "logically" connected after the proxy ports and before any device that performs network address translation (NAT) on client IP addresses.

Step 3 Configure the Global Settings

See Configuring L4 Traffic Monitor Global Settings, on page 83.

Step 4 Create L4 TrafficMonitor Policies

See Creating a Policy to Detect Rogue Traffic, on page 84.

List of Known Sites

Address	Description
Known allowed	Any IP address or hostname listed in the Allow List property. These addresses appear in the log files as "allowed list" addresses.
Unlisted	Any IP address that is not known to be a malware site nor is a known allowed address. They are not listed on the Allow List, Additional Suspected Malware Addresses properties, or in the L4 Traffic Monitor Database. These addresses do not appear in the log files.
Ambiguous	These appear in the log files as "greylist" addresses and include: • Any *IP address* that is associated with both an unlisted *hostname* and a known malware *hostname* . • Any *IP address* that is associated with both an unlisted *hostname* and a *hostname* from the Additional Suspected Malware Addresses property
Known malware	These appear in the log files as "blocked list" addresses and include: • Any IP address or hostname that the L4 Traffic Monitor Database determines to be a known malware site and *not* listed in the Allow List. • Any *IP address* that is listed in the Additional Suspected Malware Addresses property, *not* listed in the Allow List and is *not* ambiguous

Configuring L4 Traffic Monitor Global Settings

Procedure

Step 1 Choose **Security Services > L4 Traffic Monitor**.

Step 2 Click **Edit Global Settings**.

Step 3 Choose whether or not to enable the L4 Traffic Monitor.

Step 4 When you enable the L4 Traffic Monitor, choose which ports it should monitor:

- **All ports.** Monitors all 65535 TCP ports for rogue activity.
- **All ports except proxy ports.** Monitors all TCP ports except the following ports for rogue activity.

- Ports configured in the "HTTP Ports to Proxy" property on the Security Services > Web Proxy page (usually port 80).
- Ports configured in the "Transparent HTTPS Ports to Proxy" property on the Security Services > HTTPS Proxy page (usually port 443).

Step 5 Submit and Commit Changes.

Updating L4 Traffic Monitor Anti-Malware Rules

Procedure

Step 1 Choose **Security Services > L4 Traffic Monitor**.

Step 2 Click **Update Now**.

Creating a Policy to Detect Rogue Traffic

The actions the L4 Traffic Monitor takes depends on the L4 Traffic Monitor policies you configure :

Procedure

Step 1 Choose **Web Security Manager > L4 Traffic Monitor**.

Step 2 Click **Edit Settings**.

Step 3 On the **Edit L4 Traffic Monitor Policies** page, configure the L4 Traffic Monitor policies:

a) **Define** the **Allow List**

b) Add known good sites to the **Allow List**

Note
Do not include the Secure Web Appliance IP address or hostname to the Allow List otherwise the L4 Traffic Monitor does not block any traffic.

c) Determine which action to perform for **Suspected Malware Addresses**:

Action	Description
Allow	It always allows traffic to and from known allowed and unlisted addresses
Monitor	It monitors traffic under the following circumstances: • When the Action for Suspected Malware Addresses option is set to Monitor, it always monitors all traffic that is not to or from a known allowed address. • When the Action for Suspected Malware Addresses option is set to Block, it monitors traffic to and from ambiguous addresses

Action	Description
Block	When the Action for Suspected Malware Addresses option is set to Block, it blocks traffic to and from known malware addresses

Note
- When you choose to block suspected malware traffic, you can also choose whether or not to always block ambiguous addresses. By default, ambiguous addresses are monitored.

- If the L4 Traffic Monitor is configured to block, the L4 Traffic Monitor and the Web Proxy must be configured on the same network. Use the **Network > Routes** page to confirm that all clients are accessible on routes that are configured for data traffic.

- In a VM setup, the requests in transparent mode are duplicated while passing through the P1 and T1 interfaces at an intermittent time difference. Hence, some IPs even after blocking them may pass through the appliance.

d) Define the **Additional Suspected Malware Addresses** properties

Note
Adding internal IP addresses to the Additional Suspected Malware Addresses list causes legitimate destination URLs to show up as malware in L4 Traffic Monitor reports. To avoid this do not enter internal IP addresses in the "**Additional Suspected Malware Addresses**" field on the **Web Security Manager > L4 Traffic Monitor Policies** page.

Step 4 Submit and Commit Changes.

What to do next

Related Topics

- Overview of Detecting Rogue Traffic, on page 82
- Valid Formats, on page 85.

Valid Formats

When you add addresses to the Allow List or Additional Suspected Malware Addresses properties, separate multiple entries with whitespace or commas. You can enter addresses in any of the following formats:

- **IPv4 IP address.** Example: IPv4 format: 10.1.1.0. IPv6 format: 2002:4559:1FE2::4559:1FE2
- **CIDR address.** Example: 10.1.1.0/24.
- **Domain name.** Example: example.com.
- **Hostname.** Example: crm.example.com.

Viewing L4 Traffic Monitor Activity

The S-Series appliance supports several options for generating feature specific reports and interactive displays of summary statistics.

Monitoring Activity and Viewing Summary Statistics

The **Reporting > L4 Traffic Monitor** page provides statistical summaries of monitoring activity. You can use the following displays and reporting tools to view the results of L4 Traffic Monitor activity:

To view...	See...
Client statistics	Reporting > Client Activity
Malware statistics Port statistics	Reporting > L4 Traffic Monitor
L4 Traffic Monitor log files	System Administration > Log Subscriptions • trafmon_errlogs • trafmonlogs

Note If the Web Proxy is configured as a forward proxy and L4 Traffic Monitor is set to monitor all ports, the IP address of the proxy's data port is recorded and displayed as a client IP address in the client activity report on the **Reporting > Client Activity** page. If the Web Proxy is configured as a transparent proxy, enable IP spoofing to correctly record and display the client IP addresses.

L4 Traffic Monitor Log File Entries

The L4 Traffic Monitor log file provides a detailed record of monitoring activity.