Configuring Security Services

This topic contains the following sections:

- Overview of Configuring Security Services , on page 1
- Overview of Web Reputation Filters , on page 2
- Overview of Anti-Malware Scanning , on page 4
- Understanding Adaptive Scanning, on page 7
- Enabling Anti-Malware and Reputation Filters, on page 7
- Configuring Anti-Malware and Reputation in Policies, on page 9
- Integrating the Appliance with AMP for Endpoints Console, on page 14
- Maintaining the Database Tables, on page 16
- Logging of Web Reputation Filtering Activity and DVS Scanning , on page 16
- Caching, on page 17
- Malware Category Descriptions, on page 17

Overview of Configuring Security Services

The Web Security 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
Advanced Malware Protection	Protects from threats in downloaded files by evaluating file reputation and by analyzing file characteristics.	Overview of File Reputation Filtering and File Analysis

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 Web Security 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

Policy Type	Action
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.

Score	Action	Description
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 Web Security 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 5

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 Advanced Malware Protection 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 Advanced Malware Protection 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.

Setting	Description
File Reputation Filtering and File Analysis	See Enabling and Configuring File Reputation and Analysis Services.
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 14.
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 by Advanced Malware Protection 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 5

Clearing the Advanced Malware Protection Services Cache

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

Note AMP 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 Advanced Malware Protection 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 Advanced Malware Protection settings only in Access Policies. See Configuring File Reputation and Analysis Features

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 Advanced Malware Protection **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 Advanced Malware Protection **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.
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 Web Security 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 Advanced Malware Protection 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 Advanced Malware Protection 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_452.

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 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
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 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 Web Security 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 Advanced Malware Protection 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.

Malware Type	Description
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.
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.