

Access Control

This topic contains the following sections:

- Classify End-Users for Policy Application, on page 1
- Classify URLs for Policy Application, on page 11
- Create Decryption Policies to Control HTTPS Traffic, on page 57
- Create Policies to Control Internet Requests, on page 72
- SaaS Access Control, on page 101
- Scan Outbound Traffic for Existing Infections, on page 107

Classify End-Users for Policy Application

This topic contains the following sections:

- Overview of Classify Users and Client Software, on page 1
- Classify Users and Client Software: Best Practices, on page 2
- Identification Profile Criteria, on page 2
- Classifying Users and Client Software, on page 3
- Identification Profiles and Authentication , on page 9
- Troubleshooting Identification Profiles, on page 10
- Troubleshooting Surrogate Types in Identification Profiles, on page 11

Overview of Classify Users and Client Software

Identification Profiles let you classify users and user agents (client software) for these purposes:

- Group transaction requests for the application of policies (except SaaS)
- Specification of identification and authentication requirements

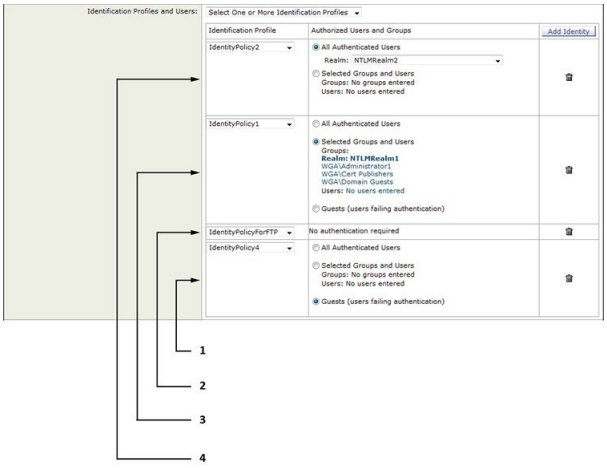
AsyncOS assigns an Identification Profile to every transaction:

- Custom Identification Profiles — AsyncOS assigns a custom profile based on that identity's criteria.
- The Global Identification Profile — AsyncOS assigns the global profile to transactions that do not meet the criteria for any custom profile. By default, the global profile does not require authentication.

AsyncOS processes Identification Profiles sequentially, beginning with the first. The global profile is the last profile.

An Identification Profile may include only one criterion. Alternately, Identification Profiles that include multiple criteria require that all the criteria are met.

One policy may call on multiple Identification Profiles:



1	This Identification Profile allows guest access and applies to users who fail authentication.
2	Authentication is not used for this Identification Profile.
3	The specified user groups in this Identification Profile are authorized for this policy.
4	This Identification Profile uses an authentication sequence and this policy applies to one realm in the sequence.

Classify Users and Client Software: Best Practices

- Create fewer, more general Identification Profiles that apply to all users or fewer, larger groups of users. Use policies, rather than profiles, for more granular management.
- Create Identification Profiles with unique criteria.
- If deployed in transparent mode, create an Identification Profile for sites that do not support authentication. See Bypassing Authentication.

Identification Profile Criteria

These transaction characteristics are available to define an Identification Profile:

Option	Description
Subnet	The client subnet must match the list of subnets in a policy.
Protocol	The protocol used in the transaction: HTTP, HTTPS, SOCKS, or native FTP.

Option	Description
Port	The proxy port of the request must be in the Identification Profile's list of ports, if any are listed. For explicit forward connections, this is the port configured in the browser. For transparent connections, this is the same as the destination port.
User Agent	The user agent (client application) making the request must be in the Identification Profile's list of user agents, if any are listed. Some user agents cannot handle authentication, therefore creating an profile that does not require authentication is necessary. User agents include programs such as updaters and browsers, such as Internet Explorer and Mozilla Firefox.
URL Category	The URL category of the request URL must be in the Identification Profile's list of URL categories, if any are listed.
Authentication requirements	If the Identification Profile requires authentication, the client authentication credentials must match the Identification Profile's authentication requirements.

Classifying Users and Client Software

Before you begin

- Create authentication realms. See How to Create an Active Directory Authentication Realm (NTLMSSP and Basic) or Creating an LDAP Authentication Realm .
- Be aware that when you commit changes to Identification Profiles, end-users must re-authenticate.
- If you are in Cloud Connector mode, be aware that an additional Identification Profile option is available: Machine ID. See Identifying Machines for Policy Application.
- (Optional) Create authentication sequences. See Creating Authentication Sequences
- (Optional) Enable Secure Mobility if the Identification Profile will include mobile users.
- (Optional) Understand authentication surrogates. See Tracking Identified Users .

Procedure

Step 1 Choose **Web Security Manager** > **Identification Profiles**.

Step 2 Click **Add Profile** to add a profile.

Step 3 Use the **Enable Identification Profile** check box to enable this profile, or to quickly disable it without deleting it.

Step 4 Assign a unique profile **Name**.

Step 5 A **Description** is optional.

Step 6 From the **Insert Above** drop-down list, choose where this profile is to appear in the table.

Note
Position Identification Profiles that do not require authentication above the first Identification Profile that requires authentication.

Step 7 In the **User Identification Method** section, choose an identification method and then supply related parameters; displayed options vary according to the method chosen.

a) Choose an identification method from the **User Identification Method** drop-down list.

Option	Description
Exempt from authentication/ identification	Users are identified primarily by IP address. No additional parameters are required.
Authenticate users	Users are identified by the authentication credentials they enter.
Transparently identify users with ISE	Available when the ISE service is enabled (Network > Identity Services Engine). For these transactions, the user name and associated Secure Group Tags will be obtained from the Identity Services Engine. In ISE-PIC deployments, ISE groups and users information is received. For more information, see Tasks for Integrating the ISE/ISE-PIC Service.
Transparently identify users with authentication realm	This option is available when one or more authentication realms are configured to support transparent identification.

Note
When at least one Identification Profile with authentication or transparent identification is configured, the policy tables will support defining policy membership using user names, directory groups, and Secure Group Tags.

Note
Context Directory Agent (CDA) is no longer supported. It is recommended to configure ISE/ISE-PIC for transparent user identification to achieve the same functionality.

Options to configure CDA will not be available in future releases.

For more information, see https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/bulletin-c25-2428601.html.

b) Supply parameters appropriate to the chosen method. Not all of the sections described in this table are visible for each choice.

Fallback to Authentication Realm or Guest Privileges	If user authentication is not available from ISE: • **Support Guest Privileges** – The transaction will be allowed to continue, and will match subsequent policies for Guest users from all Identification Profiles. • **Block Transactions** – Do not allow Internet access to users who cannot be identified by ISE. • **Support Guest privileges** – Check this box to grant guest access to users who fail authentication due to invalid credentials.

Authentication Realm	**Select a Realm or Sequence**—Choose a defined authentication realm or sequence. **Select a Scheme**—Choose an authentication scheme: • **Kerberos**—The client is transparently authenticated by means of Kerberos tickets. • **Basic** – The client always prompts users for credentials. After the user enters credentials, browsers typically offer a check box to remember the provided credentials. Each time the user opens the browser, the client either prompts for credentials or resends the previously saved credentials. Credentials are sent unsecured as clear text (Base64). A packet capture between the client and Secure Web Appliance can reveal the user name and passphrase. • **NTLMSSP**—The client transparently authenticates using its Windows login credentials. The user is not prompted for credentials. However, the client prompts the user for credentials under the following circumstances: • The Windows credentials failed. • The client does not trust the Secure Web Appliance because of browser security settings. Credentials are sent securely using a three-way handshake (digest style authentication). The passphrase is never sent across the connection. • **Header Based Authentication** —The Client and the Secure Web Appliance considers the user as authenticated and does not prompt again for authentication or user credentials. The X-Authenticated feature works when the Secure Web Appliance acts as an upstream device. After successful authentication, the downstream device sends the user name and user groups (optional) to the Secure Web Appliance through the X-Authenticated-User and X-Authenticated-Groups (optional) extended HTTP headers. The X-Authenticated-Groups header will be considered, only if you configure the **Use Groups in X-Authenticate-Groups Header/Custom Header for matching Access Policies** option in the appliance (**Network** > **Authentication** > **Edit Global Settings**). **Note** X-Authenticated headers are applicable only on Access Policies or Routing Policies. However, associating the Identification Profile that has **Header Based Authentication** enabled, to a decryption policy will not be matched. • **Support Guest privileges** – Check this box to grant guest access to users who fail authentication due to invalid credentials.
Realm for Group Authentication	• **Select a Realm or Sequence** – Choose a defined authentication realm or sequence.

Authentication Surrogates	Specify how transactions will be associated with a user after successful authentication (options vary depending on Web Proxy deployment mode): • **IP Address** – The Web Proxy tracks an authenticated user at a particular IP address. For transparent user identification, select this option. • **Persistent Cookie** – The Web Proxy tracks an authenticated user on a particular application by generating a persistent cookie for each user per application. Closing the application does not remove the cookie. • **Session Cookie** – The Web Proxy tracks an authenticated user on a particular application by generating a session cookie for each user per domain per application. (However, when a user provides different credentials for the same domain from the same application, the cookie is overwritten.) Closing the application removes the cookie. • **No Surrogate** – The Web Proxy does not use a surrogate to cache the credentials, and it tracks an authenticated user for every new TCP connection. When you choose this option, the web interface disables other settings that no longer apply. This option is available only in explicit forward mode and when you disable credential encryption on the Network > Authentication page. • **Apply same surrogate settings to explicit forward requests** – Check to apply the surrogate used for transparent requests to explicit requests; enables credential encryption automatically. This option appears only when the Web Proxy is deployed in transparent mode. **Note** • You can define a timeout valve for the authentication surrogate for all requests in Global Authentication Settings. • If you have configured the Identification Profiles to use different authentication surrogates (IP address, persistent cookie, session cookie, and so on), then the access is authenticated using the IP address surrogate even though the access matches Identification Profiles with other surrogates.

Step 8 In the **Membership Definition** section, supply membership parameters appropriate to the chosen identification method. Note that all of the options described in this table are not available to every User Identification Method.

Membership Definition	
Define Members by User Location	Configure this Identification Profile to apply to: **Local Users Only**, **Remote Users Only**, or **Both**. This selection affects the available authentication settings for this Identification Profile.
Define Members by Subnet	Enter the addresses to which this Identification Profile should apply. You can use IP addresses, CIDR blocks, and subnets. **Note** If nothing is entered, the Identification Profile applies to all IP addresses.

Define Members by Protocol	Select the protocols to which this Identification Profile should apply; select all that apply: • **HTTP/HTTPS** – Applies to all requests that use HTTP or HTTPS as the underlying protocol, including FTP over HTTP, and any other protocol tunneled using HTTP CONNECT. • **Native FTP** – Applies to native FTP requests only. • **SOCKS** – Applies to SOCKS Policies only
Define Members by Machine ID	• **Do Not Use Machine ID in This Policy** – The user is not identified by machine ID. • **Define User Authentication Policy Based on Machine ID** – The user is identified primarily by machine ID. Click the Machine Groups area to display the Authorized Machine Groups page. For each group you want to add, in the Directory Search field, start typing the name of the group to add and then click Add. You can select a group and click Remove to remove it from the list. Click Done to return to the previous page. Click the Machine IDs area to display the Authorized Machines page. In the Authorized Machines, field, enter the machine IDs to associate with the policy then click Done. **Note** Authentication using Machine ID is supported only in Connector mode and requires Active Directory.

Advanced	Expand this section to define additional membership requirements. • **Proxy Ports** – Specify one or more proxy ports used to access the Web Proxy. Enter port numbers separated by commas. For explicit forward connections, the proxy port is configured in the browser. For transparent connections, this is the same as the destination port. Defining identities by port works best when the appliance is deployed in explicit forward mode, or when clients explicitly forward requests to the appliance. Defining identities by port when client requests are transparently redirected to the appliance may result in some requests being denied. • **URL Categories** – Select user-defined or predefined URL categories. Membership for both is excluded by default, meaning the Web Proxy ignores all categories unless they are selected in the Add column. If you need to define membership by URL category, only define it in the Identity group when you need to exempt from authentication requests to that category. • **User Agents** – Defines policy group membership by the user agents found in the client request. You can select some commonly defined agents, or define your own using regular expressions. Also specify whether these user-agent specifications are inclusive or exclusive. In other words, whether membership definition includes only the selected user agents, or specifically excludes the selected user agents

Step 9 Submit and Commit Changes.

What to do next

- Overview of Acquire End-User Credentials
- Managing Web Requests Through Policies Task Overview, on page 74

Enable/Disable an Identity

Before you begin

- Be aware that disabling an Identification Profile removes it from associated policies.
- Be aware that re-enabling an Identification Profile does not re-associate it with any policies.

Procedure

Step 1 Choose **Web Security Manager** > **Identification Profiles**.

Step 2 Click a profile in the Identification Profiles table to open the Identification Profile page for that profile.

Step 3 Check or clear **Enable Identification Profile** immediately under Client/User Identification Profile Settings.

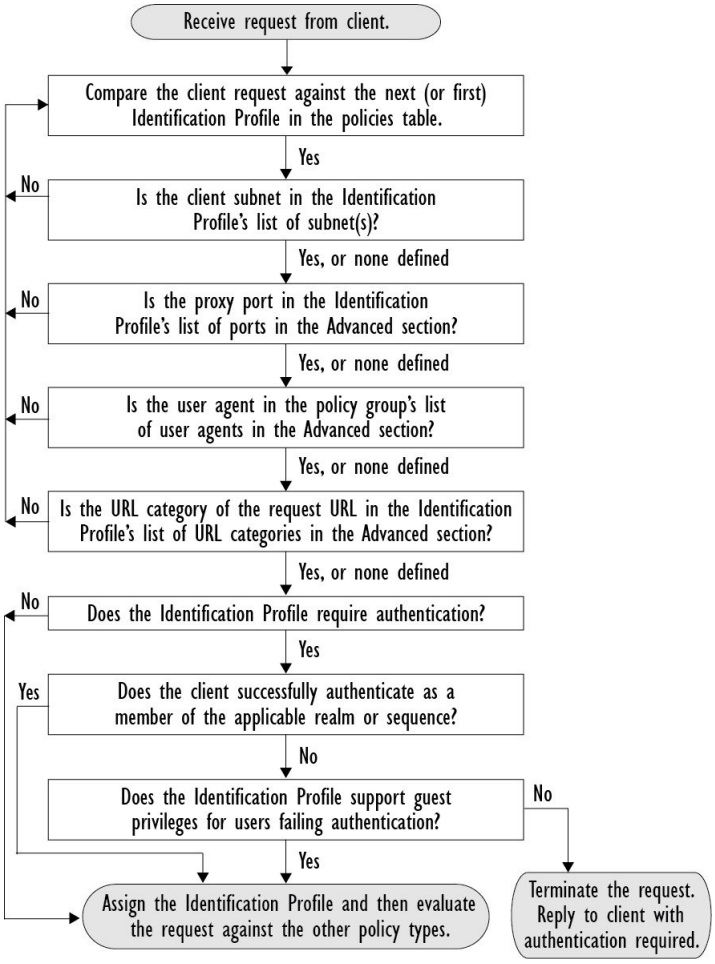
Step 4 Submit and Commit Changes.

Identification Profiles and Authentication

The following diagram shows how the Web Proxy evaluates a client request against an Identification Profile when the Identification Profiles is configured to use:

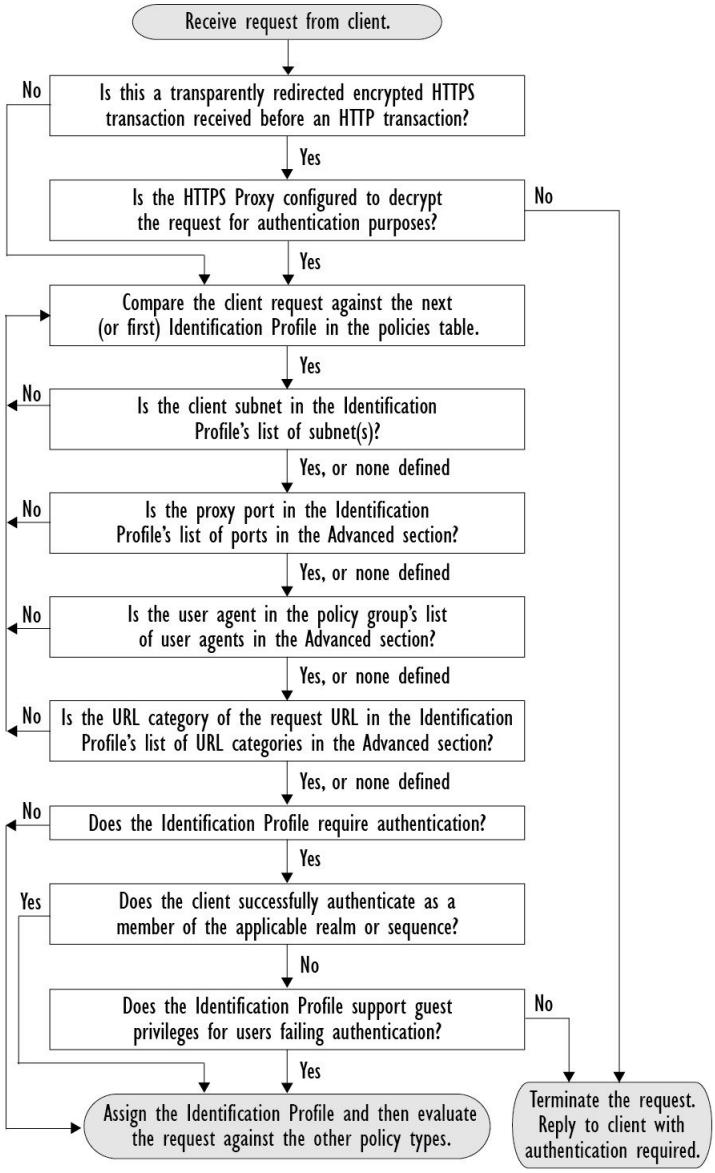
- No authentication surrogates
- IP addresses as authentication surrogates
- Cookies as authentication surrogates with transparent requests
- Cookies as authentication surrogates with explicit requests and credential encryption is enabled

Figure 1: Identification Profiles and Authentication Processing – No Surrogates and IP-based Surrogates



The following diagram shows how the Web Proxy evaluates a client request against an Identification Profile when the Identification Profile is configured to use cookies as the authentication surrogates, credential encryption is enabled, and the request is explicitly forwarded.

Figure 2: Identification Profiles and Authentication Processing – Cookie-based Surrogates



Troubleshooting Identification Profiles

- Basic Authentication Problems
- Policy Problems
- Policy is Never Applied
- Policy Troubleshooting Tool: Policy Trace
- Upstream Proxy Problems

Troubleshooting Surrogate Types in Identification Profiles

When the Web Security Appliance is configured to use both IP address and cookie-based authentication surrogates and the access from the end-user matches both Identities, then the IP address overrides cookie-based authentication surrogates.

In a network with both shared and individual computers, it is recommended to create two different identification profiles based on IP addresses and subnets, which will determine whether IP or Cookie authentication surrogates are used.

Classify URLs for Policy Application

This topic contains the following sections:

- Overview of Categorizing URL Transactions, on page 11
- Configuring the URL Filtering Engine , on page 14
- Managing Updates to the Set of URL Categories , on page 15
- Filtering Transactions Using URL Categories, on page 20
- YouTube Categorization, on page 26
- Creating and Editing Custom URL Categories, on page 28
- Filtering Adult Content, on page 34
- Redirecting Traffic in the Access Policies, on page 36
- Warning Users and Allowing Them to Continue, on page 37
- Creating Time Based URL Filters, on page 38
- Viewing URL Filtering Activity, on page 39
- Regular Expressions, on page 40
- URL Category Descriptions, on page 43

Overview of Categorizing URL Transactions

Using policy groups, you can create secure policies that control access to web sites containing questionable content. The sites that are blocked, allowed, or decrypted depend on the categories you select when setting up category blocking for each policy group. To control user access based on a URL category, you must enable Cisco Web Usage Controls. This is a multi-layered URL filtering engine that uses domain prefixes and keyword analysis to categorize URLs.

You can use URL categories when performing the following tasks:

Option	Method
Define policy group membership	Matching URLs to URL Categories, on page 13

Option	Method
Control access to HTTP, HTTPS, and FTP requests	Filtering Transactions Using URL Categories, on page 20
Create user defined custom URL categories that specify specific hostnames and IP addresses	Creating and Editing Custom URL Categories, on page 28

Categorization of Failed URL Transactions

The Dynamic Content Analysis engine categorizes URLs when controlling access to websites in Access Policies only. It does not categorize URLs when determining policy group membership or when controlling access to websites using Decryption or Cisco Data Security Policies. This is because the engine works by analyzing the response content from the destination server, so it cannot be used on decisions that must be made at request time before any response is downloaded from the server.

If the web reputation score for an uncategorized URL is within the WBRS ALLOW range, AsyncOS allows the request without performing Dynamic Content Analysis.

After the Dynamic Content Analysis engine categorizes a URL, it stores the category verdict and URL in a temporary cache. This allows future transactions to benefit from the earlier response scan and be categorized at request time instead of at response time.

Enabling the Dynamic Content Analysis engine can impact transaction performance. However, most transactions are categorized using the Cisco Web Usage Controls URL categories database, so the Dynamic Content Analysis engine is usually only called for a small percentage of transactions.

Enabling the Dynamic Content Analysis Engine

Note It is possible for an Access Policy, or an Identity used in an Access Policy, to define policy membership by a predefined URL category and for the Access Policy to perform an action on the same URL category. The URL in the request can be uncategorized when determining Identity and Access Policy group membership, but must be categorized by the Dynamic Content Analysis engine after receiving the server response. Cisco Web Usage Controls ignores the category verdict from the Dynamic Content Analysis engine and the URL retains the “uncategorized” verdict for the remainder of the transaction. Future transactions will still benefit from the new category verdict.

Procedure

Step 1 Choose **Security Services > Acceptable Use Controls**.

Step 2 Enable the Cisco Web Usage Controls.

Step 3 **Click** to enable the Dynamic Content Analysis engine.

Step 4 Submit and Commit Changes.

Uncategorized URLs

An uncategorized URL is a URL that does not match any pre-defined URL category or *included* custom URL category.

Note When determining policy group membership, a custom URL category is considered included, only when it is selected for policy group membership.

All transactions resulting in unmatched categories are reported on the Reporting > URL Categories page as "Uncategorized URLs." A large number of uncategorized URLs are generated from requests to web sites within the internal network. Cisco recommends using custom URL categories to group internal URLs and allow all requests to internal web sites. This decreases the number of web transactions reported as "Uncategorized URLs" and instead reports internal transactions as part of "URL Filtering Bypassed" statistics.

Related Topics

- Understanding Unfiltered and Uncategorized Data, on page 39.
- Creating and Editing Custom URL Categories, on page 28.

Matching URLs to URL Categories

When the URL filtering engine matches a URL category to the URL in a client request, it first evaluates the URL against the custom URL categories *included* in the policy group. If the URL in the request does not match an included custom category, the URL filtering engine compares it to the predefined URL categories. If the URL does not match any included custom or predefined URL categories, the request is uncategorized.

Note When determining policy group membership, a custom URL category is considered included only when it is selected for policy group membership.

To see what category a particular web site is assigned to, go to the URL in Reporting Uncategorized and Misclassified URLs, on page 13.

Related Topics

- Uncategorized URLs, on page 13.

Reporting Uncategorized and Misclassified URLs

You can report uncategorized and misclassified URLs to Cisco. Cisco provides a URL submission tool on its website that allows you to submit multiple URLs simultaneously:

- https://talosintelligence.com/tickets
  - To check the status of submitted URLs, click the Status on Submitted URLs tab on this page.
  - You can also use the URL submission tool to look up the assigned URL category for any URL.
- https://www.talosintelligence.com/reputation_center/support

- To submit a dispute, you must be logged into your Cisco account. Disputes can be filed for URLs, IPs, or domains.
- Use the Reputation Center Search box to look up web reputation information.

URL Categories Database

The category that a URL falls into is determined by a filtering categories database. The Secure Web Appliance collects information and maintains a separate database for each URL filtering engine. The filtering categories databases periodically receive updates from the Cisco update server.

The URL categories database includes many different factors and sources of data internal to Cisco and from the Internet. One of the factors occasionally considered, heavily modified from the original, is information from the Open Directory Project.

To see what category a particular web site is assigned to, go to the URL in Reporting Uncategorized and Misclassified URLs, on page 13.

Related Topics

- Manually Updating the URL Category Set , on page 19

Configuring the URL Filtering Engine

By default, the Cisco Web Usage Controls URL filtering engine is enabled in the System Setup Wizard.

Procedure

Step 1 Choose **Security Services > Acceptable Use Controls**.

Step 2 Click **Edit Global Settings**.

Step 3 Verify the Enable Acceptable Use Controls property is enabled.

Step 4 Choose any one of the following Cisco Web Usage Controls:

a. Enable Application Control

Note
Starting with AsyncOS 15.0, you can use either AVC or ADC engine to monitor web traffic. By default, AVC is enabled.

- Enable Application Visibility and Control (AVC)—has 300+ applications
- Enable Application Discovery and Control (ADC)—has 3000+ applications

b. Enable Dynamic Content Analysis Engine

c. Enable Multiple URL Categories

Note
The Multiple URL Categories feature is applicable only for Access Policies. You cannot apply the Multiple URL Categories feature for decryption policies and identification profiles.

Step 5 Choose the default action the Web Proxy should use when the URL filtering engine is unavailable, either Monitor or Block. Default is Monitor.

Step 6 Submit and Commit Changes.

Managing Updates to the Set of URL Categories

The set of predefined URL categories may occasionally be updated in order to accommodate new web trends and evolving usage patterns. Updates to the URL category set are distinct from the changes that add new URLs and re-map misclassified URLs. Category set updates may change configurations in your existing policies and therefore require action. URL category set updates may occur between product releases; an AsyncOS upgrade is not required.

Information is available from: http://www.cisco.com/en/US/products/ps10164/prod_release_notes_list.html.

Take the following actions:

When to Act	Method
Before updates occur (Do these tasks as part of your initial setup)	Understanding the Impacts of URL Category Set Updates , on page 15 Controlling Updates to the URL Category Set , on page 18 Default Settings for New and Changed Categories , on page 19 Receiving Alerts About Category and Policy Changes , on page 20
After updates occur	Responding to Alerts about URL Category Set Updates , on page 20

Understanding the Impacts of URL Category Set Updates

URL category set updates can have the following impacts on existing Access Policies, Decryption Policies, and Cisco Data Security policies, and on Identities:

- Effects of URL Category Set Changes on Policy Group Membership , on page 15
- Effects of URL Category Set Updates on Filtering Actions in Policies , on page 15

Effects of URL Category Set Changes on Policy Group Membership

This section applies to all policy types with membership that can be defined by URL category, and to Identities. When policy group membership is defined by URL category, changes to the category set may have the following effects:

- If the sole criterion for membership is a deleted category, the policy or identity is disabled.

If membership in any policy is defined by a URL category that changes, and if this causes ACL list changes, the web proxy will restart.

Effects of URL Category Set Updates on Filtering Actions in Policies

URL category set updates can change policy behavior in the following ways:

Change	Effect on Policies and Identities
A new category can be added	For the new URL categories now, one of the following actions will be picked from the Default Action for Update Categories option of the Policy Configuartion page: • Least Restrictive • Most Restrictive The actions are set by default for the new categories. In Access Policies, and Cisco Data Security Policies: • Most Restrictive is Block • Least Restrictive is Monitor In Web Traffic Tap (WTT) Policies: • Most Restrictive is Tap • Least Restrictive is No Tap In Decryption Policies: • Most Restrictive is Block • Least Restrictive is Pass Through
A category can be deleted	The action associated with the deleted category is deleted. If the policy depended exclusively on the deleted category, the policy is disabled. If a policy depends on an identity that depended exclusively on a deleted category, the policy will be disabled.
A category can be renamed	No change to the behavior of the existing policy.
A category can split	A single category can become multiple new categories. New category actions will be picked from the Default Action for Update Categories.

Change	Effect on Policies and Identities
Two or more existing categories can merge	If all original categories in a policy had the same action assigned, the merged category has the same action as the original categories. If all original categories were set to “Use Global Setting” then the merged category is also set to “Use Global Setting.” If the policy had different actions assigned to the original categories, the action assigned to the merged category depends on the Uncategorized URLs setting in that policy: • If Uncategorized URLs is set to Block (or “Use Global Setting” when the global setting is Block), then the most restrictive action among the original categories is applied to the merged category. • If Uncategorized URLs is set to any action other than Block (or “Use Global Setting” when the global setting is anything other than Block), then the least restrictive action among the original categories is applied to the merged category. In this case, sites that were previously blocked may now be accessible to users. If policy membership is defined by URL category, and some of the categories involved in the merge, or the Uncategorized URLs action, are not included in the policy membership definition, then the values in the Global Policy are used for the missing items. The order of restrictiveness is as follows (not all actions are available for all policy types): • Block • Drop • Decrypt • Warn • Time-based • Monitor • Pass Through **Note** Time-based policies that are based on merged categories adopt the action associated with any one of the original categories. (In time-based policies, there may be no obviously most- or least-restrictive action.)

Related Topics

• Merged Categories - Examples , on page 18.

Merged Categories - Examples

Some examples of merged categories, based on settings on the URL Filtering page for the policy:

Original Category 1	Original Category 2	Uncategorized URLs	Merged Category
Monitor	Monitor	(Not Applicable)	Monitor
Block	Block	(Not Applicable)	Block
Use Global Settings	Use Global Settings	(Not Applicable)	Use Global Settings
Warn	Block	Monitor Use the least restrictive among the original categories.	Warn
Monitor	• Block or • Use Global Settings,when Global is set to Block	• Block or • Use Global Setting, when Global is set to Block Use the most restrictive among the original categories.	Block
Block	• Monitor or • Use Global Settings, when Global is set to Monitor	• Monitor or • Use Global Setting, when Global is set to Monitor Use the least restrictive among the original categories.	Monitor
For policies in which membership is defined by URL category: Monitor	An action for this category is not specified in this policy, but the value in the Global Policy for this category is Block	An action for Uncategorized URLs is not specified in this policy, but the value in the Global Policy for Uncategorized URLs is Monitor	Monitor

Controlling Updates to the URL Category Set

By default, URL category set updates to occur automatically. These updates may change existing policy configurations, so you may prefer to disable all automatic updates.

Option	Method
If you disable updates, you will need to manually update all services listed in the Update Servers (list) section of the System Administration > Upgrade and Update Settings page	Manually Updating the URL Category Set , on page 19 and Manually Updating Security Service Components

Option	Method
Disabling all automatic updates	Configuring Upgrade and Service Update Settings.

Note If you use the CLI, disable updates by setting the update interval to zero (0)

Manually Updating the URL Category Set

Note
- Do not interrupt an update in progress.
- If you have disabled automatic updates, you can manually update the set of URL categories at your convenience.

Procedure

Step 1 Choose **Security Services > Acceptable Use Controls**.

Step 2 Determine whether an update is available:

Look at the "Cisco Web Usage Controls - Web Categorization Categories List" item in the Acceptable Use Controls Engine Updates table.

Step 3 To update, click **Update Now**.

Default Settings for New and Changed Categories

URL category set updates may change the behavior of your existing policies. You should specify default settings for certain changes when you configure your policies, so that they are ready when URL category set updates occur. When new categories are added, or existing categories merge into a new category, the default action for these categories for each policy are affected by the **Default Action for Update Categories** setting in that policy.

Verifying Existing Settings and/or Making Changes

Procedure

Step 1 Choose **Web Security Manager**.

Step 2 For each Access Policy, Decryption Policy, and Cisco Data Security policy click the **URL Filtering** link.

Step 3 Check the selected setting for Uncategorized URLs.

What to do next

Related Topics

- Effects of URL Category Set Updates on Filtering Actions in Policies , on page 15.

Receiving Alerts About Category and Policy Changes

Category set updates trigger two types of alerts:

- Alerts about category changes
- Alerts about policies that have changed or been disabled as a result of category set changes.

Procedure

Step 1 Choose **System Administration > Alerts**.

Step 2 Click **Add Recipient** and add email address (or multiple email addresses).

Step 3 Decide which **Alert Types** and **Alert Severities** to receive.

Step 4 Submit and Commit Changes.

Responding to Alerts about URL Category Set Updates

When you receive an alert about category set changes, you should do the following:

- Check policies and identities to be sure that they still meet your policy goals after category merges, additions, and deletions, and
- Consider modifying policies and identities to benefit from new categories and the added granularity of split categories.

Related Topics

- Understanding the Impacts of URL Category Set Updates , on page 15

Filtering Transactions Using URL Categories

The URL filtering engine lets you filter transactions in Access, Decryption, and Data Security Policies. When you configure URL categories for policy groups, you can configure actions for custom URL categories, if any are defined, and predefined URL categories.

The URL filtering actions you can configure depends on the type of policy group:

Option	Method
Access Policies	Configuring URL Filters for Access Policy Groups, on page 21
Decryption Policies	Configuring URL Filters for Decryption Policy Groups, on page 24
Cisco Data Security Policies	Configuring URL Filters for Data Security Policy Groups, on page 25

Related Topics

- Redirecting Traffic in the Access Policies, on page 36
- Warning Users and Allowing Them to Continue, on page 37
- Creating and Editing Custom URL Categories, on page 28
- Effects of URL Category Set Updates on Filtering Actions in Policies , on page 15

Configuring URL Filters for Access Policy Groups

You can configure URL filtering for user-defined Access Policy groups and the Global Policy Group.

Procedure

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

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

Step 3 (Optional) In the Custom URL Category Filtering section, you can add custom URL categories on which to take action in this policy:

a) Click **Select Custom Categories**.

b) Choose which custom URL categories to include in this policy and click **Apply**.

Choose which custom URL categories the URL filtering engine should compare the client request against. The URL filtering engine compares client requests against included custom URL categories, and ignores excluded custom URL categories. The URL filtering engine compares the URL in a client request to included custom URL categories before predefined URL categories.

The custom URL categories included in the policy appear in the Custom URL Category Filtering section.

Step 4 In the Custom URL Category Filtering section, choose an action for each included custom URL category.

Action	Description
Use Global Settings	Uses the action for this category in the Global Policy Group. This is the default action for user defined policy groups. Applies to user defined policy groups only. **Note** When a custom URL category is excluded in the global Access Policy, then the default action for included custom URL categories in user defined Access Policies is Monitor instead of Use Global Settings. You cannot choose Use Global Settings when a custom URL category is excluded in the global Access Policy.
Block	The Web Proxy denies transactions that match this setting.
Redirect	Redirects traffic originally destined for a URL in this category to a location you specify. When you choose this action, the Redirect To field appears. Enter a URL to which to redirect all traffic.
Allow	Always allows client requests for web sites in this category. Allowed requests bypass all further filtering and malware scanning. Only use this setting for trusted web sites. You might want to use this setting for internal sites.

Action	Description
Monitor	The Web Proxy neither allows nor blocks the request. Instead, it continues to evaluate the client request against other policy group control settings, such as web reputation filtering.
Warn	The Web Proxy initially blocks the request and displays a warning page, but allows the user to continue by clicking a hypertext link in the warning page.
Quota-Based	As a individual user approaches either the volume or time quotas you have specified, a warning is displayed. When a quota is met, a block page is displayed. See Time Ranges and Quotas, on page 93.
Time-Based	The Web Proxy blocks or monitors the request during the time ranges you specify. See Time Ranges and Quotas, on page 93.

Step 5 In the Predefined URL Category Filtering section, choose one of the following actions for each category:

- Use Global Settings
- Monitor
- Warn
- Block
- Time-Based
- Quota-Based

Step 6 In the Uncategorized URLs section, choose the action to take for client requests to web sites that do not fall into a predefined or custom URL category. This setting also determines the default action for new and merged categories resulting from URL category set updates.

Step 7 Submit and Commit Changes.

What to do next

- Exceptions to Blocking for Embedded and Referred Content, on page 22

Exceptions to Blocking for Embedded and Referred Content

A web site may embed or refer to content that is categorized as a different category, or that is considered an application. For example, a News web site could contain content categorized as Streaming Video, and that is identified as being the application Youtube. By default, embedded content is blocked or monitored based on the action selected for its own category or application, regardless of what web site it is embedded in. Use this table to set exceptions (for example, to permit all content referred from News web sites, or from a custom category representing your intranet).



Note Application Referred Content setting depends on the available Application Control Engine. Review the Application Referred Content if Application Control Engine changes.

Note Requests for embedded content usually include the address of the site from which the request originated (this is known as the "referer" field in the request's HTTP header). This header information is used to determine categorization of the referred content.

You can use this feature to define exceptions to the default actions for embedded/referred content; for example, to permit all content embedded in or referred to from *News* Websites, or from a custom category representing your intranet.

Note Referer-based exceptions are supported only in Access policies. To use this feature with HTTPS traffic, before defining exceptions in Access policies, you must configure HTTPS decryption of the URL Categories that you will select for exception. See Configuring URL Filters for Decryption Policy Groups, on page 24 for information about configuring HTTPS decryption. See Conditions and Restrictions for Exceptions to Blocking for Embedded and Referred Content for additional information about using this feature with HTTPS decryption.

Procedure

Step 1 On the URL Filtering page for a particular Access Policy (see Configuring URL Filters for Access Policy Groups, on page 21), click **Enable Exceptions** in the Exceptions to Blocking for Embedded/Referred Content section.

Step 2 Click the **Click to select categories** link in the Set Exception for Content Referred by These Categories column, opening the URL filtering category referral-exception selection page.

Step 3 From the Predefined and Custom URL Categories lists, select the categories for which you wish to define this referral exception, then click **Done** to return to the URL Filtering page for this Access Policy.

Step 4 Choose an exception type from the Set Exception for this Referred Content drop-down list:

- **All embedded/referred content** – All content embedded in and referred from sites of the specified category types is not blocked, regardless of the categorization of that content.
- **Selected embedded/referred content** – After choosing this option, select specific Categories and Applications that are not blocked when originating from the specified URL categories.
- **All embedded/referred content except** – After choosing this option, all content embedded in and referred from sites of the specified category types is not blocked, except those URL categories and applications you now specify here. In other words, these types will remain blocked.

Note
The Referrer Exception option is enabled by default for the custom URL category even when this category is not included in Access Policies.

Step 5 Submit and Commit Changes.

What to do next

You can elect to display “Permitted by Referrer” transaction data in the tables and charts provided on the following Reporting pages: URL Categories, Users and Web Sites, as well as related charts on the Overview page. See Choosing Which Data to Chart for more information about selecting chart-display options.

Configuring URL Filters for Decryption Policy Groups

You can configure URL filtering for user defined Decryption Policy groups and the global Decryption Policy group.

Procedure

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

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

Step 3 (Optional) In the Custom URL Category Filtering section, you can add custom URL categories on which to take action in this policy:

a) Click **Select Custom Categories**.

b) Choose which custom URL categories to include in this policy and click **Apply**.

Choose which custom URL categories the URL filtering engine should compare the client request against. The URL filtering engine compares client requests against included custom URL categories, and ignores excluded custom URL categories. The URL filtering engine compares the URL in a client request to included custom URL categories before predefined URL categories.

The custom URL categories included in the policy appear in the Custom URL Category Filtering section.

Step 4 Choose an action for each custom and predefined URL category.

Action	Description
Use Global Setting	Uses the action for this category in the global Decryption Policy group. This is the default action for user defined policy groups. Applies to user defined policy groups only. When a custom URL category is excluded in the global Decryption Policy, then the default action for included custom URL categories in user defined Decryption Policies is Monitor instead of Use Global Settings. You cannot choose Use Global Settings when a custom URL category is excluded in the global Decryption Policy.
Pass Through	Passes through the connection between the client and the server without inspecting the traffic content.
Monitor	The Web Proxy neither allows nor blocks the request. Instead, it continues to evaluate the client request against other policy group control settings, such as web reputation filtering.
Decrypt	Allows the connection, but inspects the traffic content. The appliance decrypts the traffic and applies Access Policies to the decrypted traffic as if it were a plain text HTTP connection. By decrypting the connection and applying Access Policies, you can scan the traffic for malware.

Action	Description
Drop	Drops the connection and does not pass the connection request to the server. The appliance does not notify the user that it dropped the connection.

Note
If you want to *block* a particular URL category for HTTPS requests, choose to decrypt that URL category in the Decryption Policy group and then choose to block the same URL category in the Access Policy group.

Step 5 In the Uncategorized URLs section, choose the action to take for client requests to web sites that do not fall into a predefined or custom URL category.

This setting also determines the default action for new and merged categories resulting from URL category set updates.

Step 6 Submit and Commit Changes.

Configuring URL Filters for Data Security Policy Groups

You can configure URL filtering for user defined Data Security Policy groups and the Global Policy Group.

Procedure

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

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

Step 3 (Optional) In the Custom URL Category Filtering section, you can add custom URL categories on which to take action in this policy:

a) Click **Select Custom Categories**.

b) Choose which custom URL categories to include in this policy and click **Apply**.

Choose which custom URL categories the URL filtering engine should compare the client request against. The URL filtering engine compares client requests against included custom URL categories, and ignores excluded custom URL categories. The URL filtering engine compares the URL in a client request to included custom URL categories before predefined URL categories.

The custom URL categories included in the policy appear in the Custom URL Category Filtering section.

Step 4 In the Custom URL Category Filtering section, choose an action for each custom URL category.

Action	Description
Use Global Setting	Uses the action for this category in the Global Policy Group. This is the default action for user defined policy groups. Applies to user defined policy groups only. When a custom URL category is excluded in the global Cisco Data Security Policy, then the default action for included custom URL categories in user defined Cisco Data Security Policies is Monitor instead of Use Global Settings. You cannot choose Use Global Settings when a custom URL category is excluded in the global Cisco Data Security Policy.

Action	Description
Allow	Always allows upload requests for web sites in this category. Applies to custom URL categories only. Allowed requests bypass all further data security scanning and the request is evaluated against Access Policies. Only use this setting for trusted web sites. You might want to use this setting for internal sites.
Monitor	The Web Proxy neither allows nor blocks the request. Instead, it continues to evaluate the upload request against other policy group control settings, such as web reputation filtering.
Block	The Web Proxy denies transactions that match this setting.

Note
If you do not disable the maximum file size limitation, Secure Web Appliance continues to validate the maximum file size when the Allow or Monitor options are selected in the URL filtering.

Step 5 In the Predefined URL Category Filtering section, choose one of the following actions for each category:

- Use Global Settings
- Monitor
- Block

Step 6 In the Uncategorized URLs section, choose the action to take for upload requests to web sites that do not fall into a predefined or custom URL category. This setting also determines the default action for new and merged categories resulting from URL category set updates.

Step 7 Submit and Commit Changes.

What to do next

Related Topics

- Effects of URL Category Set Updates on Filtering Actions in Policies , on page 15.

YouTube Categorization

The YouTube categorization feature enables you to create a custom URL category for YouTube and set policies on the YouTube custom category for secure and control access.

Note When you configure the time-based access policy rules to block specific YouTube category:

- The time-based rules that you set are not applicable to the videos that are already opened and playing at the time when you configure the access policy.
- The rules will be applicable only to the videos that are newly opened after you set the rules.

Note

- Make sure that the googleapis.com is not blocked in upstream proxy or upstream firewall. If you have configured an exception for Cisco update server and WBNP telemetry server, configure the same for googleapis.com as well.
- You cannot block the video that appears on the main page of a channel, even if the video belongs to a blocked YouTube category.

  For example, you blocked autos and vehicles under YouTube category. If you open a video under the specified category on the main page of a channel related to autos and vehicles, the video will not be blocked. If you try to open the same video in a separate tab, it will be blocked as expected.

To configure the YouToube categorization feature, perform the following tasks.

Step	Task	Links to Topics and Procedures
1.	Create custom and external URL category for YouTube with www.youtube.com and m.youtube.com.	Creating and Editing Custom URL Categories, on page 28.
2.	Add custom and external URL category for YouTube to a decryption policy.	Configuring URL Filters for Decryption Policy Groups, on page 24.
3.	Enable YouTube categorization feature.	Enabling the YouTube Categorization Feature, on page 27.
4.	Apply access policies to custom and external URL category for YouTube.	Configuring URL Filters for Access Policy Groups, on page 21. **Note** You must set the actions 'Block, Monitor, or Warn' under the YouTube Category Filtering section in the **Access Policies: URL Filtering** page.

Enabling the YouTube Categorization Feature

Before you begin

- Enable HTTPS proxy (**Security Services** > **HTTPS Proxy**).
- Enable Acceptable Use Controls (**Security Services** > **Acceptable Use Controls**).
- Configure Custom and External URL categories (**Web Security Manager** > **Custom and External URL Categories**) with www.youtube.com and m.youtube.com.
- Configure decryption policy using the Custom and External URL category for YouTube, with action as 'decrypt'.
- Generated the Google API key using Google API services for YouTube. To generate Google API key:
  1. Logon to https://console.developers.google.com/ using Google account credentials. (Recommend not to use personal Google account).

2. Create a project.
3. In the **Enable APIs and Services**, enable **YouTube Data API v3.**
4. Generate an API key using the wizard or use the **Credentials** option under **APIs & Services**.

Note If you are generating the API key using wizard, under **YouTube Data API v3**:

a. From the **Where will you be calling the API from?** drop-down list, choose **Other non-UI (e.g. cron job, daemon)** .

b. In the **What data will you be accessing** section, choose **Public data**.

c. Click **What credentials do I need?** then click **Done**.

Procedure

Step 1 Choose **Security Services** > **Acceptable Use Controls**.

Step 2 Click **Edit Global Settings**.

Step 3 Check the Enable checkbox next to YouTube categorization.

Step 4 Enter the API key generated using the Google API services.

You must generate the API key using the Google API services before you enable the YouTube Categorization feature.

Step 5 Enter the query timeout to set timeout period between the appliance and the YouTube API server.

Step 6 Choose the routing table through which the YouTube category traffic passes through:

- Data : For P1 and P2 interfaces
- Management: For M1 interface

Note
The default routing table is data. The above two options are avaialble only if you have configured two separate routing tables for data and management services (Network > Interfaces).

Step 7 Submit and commit your changes.

Creating and Editing Custom URL Categories

You can create custom and external live-feed URL categories that describe specific host names and IP addresses. In addition, you can edit and delete existing URL categories. When you include these custom URL categories in the same Access, Decryption, or Cisco Data Security Policy group and assign different actions to each category, the action of the higher included custom URL category takes precedence.

Note The number of external live feed files that can be used in these URL category definitions is limited to 30 and each file should contain no more than 5000 entries. Increasing external feed entries or having a large number of Regex entries causes performance degradation.

The Secure Web Appliance uses the first four characters of custom URL category names preceded by "c_" in the access logs. Consider the custom URL category name if you use Sawmill to parse the access logs. If the first four characters of the custom URL category include a space, Sawmill cannot properly parse the access log entry. Instead, only use supported characters in the first four characters. If you want to include the full name of a custom URL category in the access logs, add the %XF format specifier to the access logs.

Note If DNS resolves several IPs to a website, and if one of those IPs is custom blocked list, then the Secure Web Appliance blocks the website for all IPs, irrespective of they not being listed in the custom blocked list.

Before you begin

Go to **Security Services** > **Acceptable Use Controls** to enable Acceptable Use Controls.

Procedure

Step 1 Choose **Web Security Manager > Custom and External URL Categories**.

Step 2 To create a custom URL category, click **Add Category**. To edit an existing custom URL category, click the name of the URL category.

Step 3 Provide the following information.

Setting	Description
Category Name	Enter an identifier for this URL category. This name appears when you configure URL filtering for policy groups.
List Order	Specify the order of this category in the list of custom URL categories. Enter "1" for the first URL category in the list. The URL filtering engine evaluates a client request against the custom URL categories in the order specified.
Category Type	Choose **Local Custom Category** or **External Live Feed Category**.
Routing Table	Choose **Management** or **Data**. This choice is available only if "split routing" is enabled; that is, it is not available with local custom categories. See Enabling or Changing Network Interfaces for information about enabling split routing.

Setting	Description

Sites / Feed File Location	If you choose **Local Custom Category** for the **Category Type**, provide the custom **Sites**:
	• Enter one or more Site addresses for this custom category. You can enter multiple addresses separated by line breaks or commas. These addresses can be in any of the following formats:
	  • IPv4 address, such as 10.1.1.0
	  • IPv6 address, such as 2001:0db8::
	  • IPv4 CIDR address, such as 10.1.1.0/24
	  • IPv6 CIDR address, such as 2001:0db8::/32
	  • Domain name, such as example.com
	  • Hostname, such as crm.example.com
	  • Partial hostname, such as .example.com; this will also match www.example.com
	  • Regular expressions can be entered in the **Advanced** section, as described below.
	Note
	  •
	  • It is possible to use the same address in multiple custom URL categories, but the order in which the categories are listed is relevant. If you include these categories in the same policy, and define different actions for each, the action defined for the category listed highest in the custom URL categories table will be the one applied.
	• (Optional) Click **Sort URLs** to sort all addresses in the Sites field.
	Note
	Once you sort the addresses, you cannot retrieve their original order.

Excluded Sites	If you choose **External Live Feed Category** for the **Category Type**, provide the sites that you want to exclude from the existing feed file. You can enter multiple addresses separated by line breaks or commas. These addresses can be in any of the following formats: • IPv6 addresses such as 2001:0db8::/32 • IPv4 addresses such as 10.1.1.0. • CIDR IPv6 addresses such as 2001:0db8::/32 • CIDR IPv4 address such as 10.1.1.0/24 • Domain name, such as example.com • Hostname, such as crm.example.com • Partial hostname, such as .example.com; will also match www.example.com

Setting	Description
Feed Location (cont.)	If you choose **External Live Feed Category** for the **Category Type**, provide the **Feed File Location** information; that is, locate and download the file containing the addresses for this custom category: **a.** Select either **Cisco Feed Format**, or **Office 365 Feed Format**, or **Office 365 Web Service**, and provide the appropriate feed-file information. • **Cisco Feed Format**: • Choose the transport protocol to be used—either HTTPS or HTTP—and then enter the URL of the live-feed file. This file must be a comma-separated values (.csv)-formatted file. See External Feed-file Formats, on page 33 for more information about this file. • Optionally, provide **Authentication** credentials in the **Advanced** section. Provide a Username and Passphrase to be used for connection to the specified feed server. • **Office 365 Feed Format**: • Enter the **Office 365 Feed Location** (URL) of the live-feed file. This file must be an XML-formatted file; see External Feed-file Formats, on page 33 for more information about this file. • **Office 365 Web Service** Enter the web service URL. It must not contain a ClientRequestId, and have JSON as the format. The appliance automatically generates the ClientRequestId. **b.** For Cisco Feed Format and Office 365 Feed formats, click **Get File** to test the connection to the feed server, and then parse and download the feed file from the server. Progress is displayed in the text box below the **Get File** button. If an error occurs, the problem is indicated and must be rectified before trying again. Refer to Issues Downloading An External Live Feed File for additional information about possible errors. For the Office 365 Web Service, click **Start Test** to initiate the service and download URLs and IPs. **Note** You can use no more than 30 External Live Feed files in these URL category definitions, and each file should contain no more than 5000 entries. Increasing the number of external feed entries causes performance degradation. **Tip** After you save your changes to this live-feed category, you can click **View** in the **Feed Content** column for this entry on the Custom and External URL Categories page (**Web Security Manager** > **Custom and External URL Categories**) to open a window that displays the addresses contained in the Cisco Feed Format or Office 365 Feed Format feed file you downloaded here.

Setting	Description
Advanced	If you choose **Local Custom Category** for the Category Type, you can enter regular expressions in this section to specify additional sets of addresses. You can use regular expressions to specify multiple addresses that match the patterns you enter. **Note** • The URL filtering engine compares URLs with addresses entered in the Sites field first. If the URL of a transaction matches an entry in the Sites field, it is not compared to any expression entered here. • Use "%20" instead of space character while adding URL paths as regular expressions. URL paths must not contain space characters when used as regular expressions. • See Regular Expressions, on page 40 for more information about using regular expressions.
Advanced (Exclude Regular Expresions)	If you choose **External Live Feed Category** for the **Category Type**, enter the regular expressions that you want to exclude from the existing feed file. Entries must exactly match the regular expressions existing in the feed file.
Auto Update the Feed	Choose a feed update option: • **Do not auto update** • **Every *n* HH:MM**; for example, enter 00:05 for five minutes. However, note that updating frequently can affect Secure Web Appliance performance. **Note** Upon every reload and republish, the appliance downloads the available feed file and updates the downloaded time, even if the available feed file is same as the currently downloaded one.

Step 4 Submit and Commit Changes.

What to do next

Related Topics

- Regular Expressions, on page 40.
- Customizing Access Logs.
- Problems with Custom and External URL Categories

Address Formats and Feed-file Formats for Custom and External URL Categories

When Creating and Editing Custom and External URL Categories, you must provide one or more network addresses, whether for a **Local Custom Category**, or in an **External Live Feed Category** feed file. In each instance, you can enter multiple addresses separated by line breaks or commas. These addresses can be in any of the following formats:

- IPv4 address, such as 10.1.1.0

- IPv6 address, such as 2001:0db8::
- IPv4 CIDR address, such as 10.1.1.0/24
- IPv6 CIDR address, such as 2001:0db8::/32
- Domain name, such as example.com
- Hostname, such as crm.example.com
- Partial hostname, such as .example.com; this will also match www.example.com
- Regular expressions to specify multiple addresses that match the provided patterns (see Regular Expressions, on page 40 for more information about using regular expressions)



Note It is possible to use the same address in multiple custom URL categories, but the order in which the categories are listed is relevant. If you include these categories in the same policy, and define different actions for each, the action defined for the category listed highest in the custom URL categories table will be the one applied.

External Feed-file Formats

If you select **External Live Feed Category** for the **Category Type** when Creating and Editing Custom and External URL Categories, you must select the feed format (**Cisco Feed Format** or **Office 365 Feed Format**) and then provide a URL to the appropriate feed-file server.

The expected format for each feed file is as follows:

- **Cisco Feed Format** – This must be a comma-separated values (.csv) file; that is, a text file with a .csv extension. Each entry in the .csv file must be on a separate line, formatted as address/comma/addresstype (for example: `www.cisco.com,site` or `ad2.*\.com`,regex). Valid addresstypes are `site` and `regex`. Here is an excerpt from a Cisco Feed Format .csv file:

```
www.cisco.com,site

\.xyz,regex

ad2.*\.com,regex

www.trafficholder.com,site

2000:1:1:11:1:1::200,site
```



Note Do not include `http://` or `https://` as part of any `site` entry in the file, or an error will occur. In other words, `www.example.com` is parsed correctly, while `http://www.example.com` produces an error.

- **Office 365 Feed Format** – This is an XML file located on a Microsoft Office 365 server, or a local server to which you saved the file. It is provided by the Office 365 service and cannot be modified. The network addresses in the file are enclosed by XML tags, following this structure: `products` > `product` > `addresslist` > `address`. In the current implementation, an `addresslist` type can be IPv6, IPv4, or URL (which can include domains and regex patterns). Here is a snippet of an Office 365 feed file:

```
<products updated="4/15/2016">
   <product name="o365">
      <addresslist type="IPv6">
         <address>2603:1040:401::d:80</address>
         <address>2603:1040:401::a</address>
         <address>2603:1040:401::9</address>
      </addresslist>
      <addresslist type="IPv4">
         <address>13.71.145.72</address>
         <address>13.71.148.74</address>
         <address>13.71.145.114</address>
      </addresslist>
      <addresslist type="URL">
         <address>*.aadrm.com</address>
         <address>*.azurerms.com</address>
         <address>*.cloudapp.net2</address>
      </addresslist>
   </product>
   <product name="LYO">
      <addresslist type="URL">
         <address>*.broadcast.skype.com</address>
         <address>*.Lync.com</address>
      </addresslist>
   </product>
 </products>
```

Filtering Adult Content

You can configure the Secure Web Appliance to filter adult content from some web searches and websites. To enforce safe search and site content ratings, the AVC engine takes advantage of the safe mode feature implemented at a particular website by rewriting URLs and/or web cookies to force the safety mode to be on.

The following features filter adult content:

Option	Description
Enforce safe searches	You can configure the Secure Web Appliance so that outgoing search requests appear to search engines as safe search requests. This can prevent users from bypassing acceptable use policies using search engines.
Enforce site content ratings	Some content sharing sites allow users to restrict their own access to the adult content on these sites by either enforcing their own safe search feature or blocking access to adult content, or both. This classification feature is commonly called content ratings.



Note Any Access Policy that has either the safe search or site content ratings feature enabled is considered a safe browsing Access Policy.

Enforcing Safe Searches and Site Content Ratings



Note When 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.

Procedure

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

Step 2 Click the link under the URL Filtering column for an Access Policy group or the Global Policy Group.

Step 3 When editing a user-defined Access Policy, choose Define Content Filtering Custom Settings in the Content Filtering section.

Step 4 Click the **Enable Safe Search** check box to enable the safe search feature.

Step 5 Choose whether to block users from search engines that are not currently supported by the Secure Web Appliance safe search feature.

Step 6 Click the **Enable Site Content Rating** check box to enable the site content ratings feature.

Step 7 Choose whether to block all adult content from the supported content ratings websites or to display the end-user URL filtering warning page.

Note
When the URL of one of the supported search engines or supported content ratings websites is included in a custom URL category with the Allow action applied, no search results are blocked and all content is visible.

Step 8 Submit and Commit Changes.

What to do next

Related Topics

- Warning Users and Allowing Them to Continue, on page 37.

Logging Adult Content Access

By default, the access logs include a safe browsing scanning verdict inside the angled brackets of each entry. The safe browsing scanning verdict indicates whether or not either the safe search or site content ratings feature was applied to the transaction. You can also add the safe browsing scanning verdict variable to the access logs or W3C access logs:

- Access logs: %XS
- W3C access logs: x-request-rewrite

Value	Description
ensrch	The original client request was unsafe and the safe search feature was applied.
encrt	The original client request was unsafe and the site content ratings feature was applied.
unsupp	The original client request was to an unsupported search engine.
err	The original client request was unsafe, but neither the safe search nor the site content ratings feature could be applied due to an error.
-	Neither the safe search nor the site content ratings feature was applied to the client request because the features were bypassed (for example, the transaction was allowed in a custom URL category) or the request was made from an unsupported application.

Requests blocked due to either the safe search or site content rating features, use one of the following ACL decision tags in the access logs:

- BLOCK_SEARCH_UNSAFE
- BLOCK_CONTENT_UNSAFE
- BLOCK_UNSUPPORTED_SEARCH_APP
- BLOCK_CONTINUE_CONTENT_UNSAFE

Related Topics

- ACL Decision Tags.

Redirecting Traffic in the Access Policies

You can configure the Secure Web Appliance to redirect traffic originally destined for a URL in a custom URL category to a location you specify. This allows you to redirect traffic at the appliance instead of at the destination server. You can redirect traffic for a custom Access Policy group or the Global Policy Group

Before you begin

To redirect traffic you must define at least one custom URL category.

Procedure

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

Step 2 Click the link under the URL Filtering column for an Access Policy group or the Global Policy Group.

Step 3 In the Custom URL Category Filtering section, click **Select Custom Categories**.

Step 4 In the **Select Custom Categories for this Policy** dialog box, choose **Include in policy** for the custom URL category you want to redirect.

Step 5 Click **Apply**.

Step 6 Click the Redirect column for the custom category you want to redirect.

Step 7 Enter the URL to which you want to redirect traffic in the **Redirect To** field for the custom category.

Step 8 Submit and Commit Changes.

Note
Beware of infinite loops when you configure the appliance to redirect traffic.

What to do next

Related Topics

- Creating and Editing Custom URL Categories, on page 28

Logging and Reporting

When you redirect traffic, the access log entry for the originally requested website has an ACL tag that starts with REDIRECT_CUSTOMCAT. Later in the access log (typically the next line) appears the entry for the website to which the user was redirected.

The reports displayed on the Reporting tab display redirected transactions as “Allowed.”

Warning Users and Allowing Them to Continue

You can warn users that a site does not meet the organization’s acceptable use policies. Users are tracked in the access log by user name if authentication has made a user name available, and tracked by IP address if no user name is available.

You can warn and allow users to continue using one of the following methods:

- Choose the Warn action for a URL category in an Access Policy group or
- Enable the site content ratings feature and warn users that access adult content instead of blocking them.

Configuring Settings for the End-User Filtering Warning Page

Note

- The warn and continue feature only works for HTTP and decrypted HTTPS transactions. It does not work with native FTP transactions.
- When the URL filtering engine warns users for a particular request, it provides a warning page that the Web Proxy sends to the end user. However, not all websites display the warning page to the end user. When this happens, users are blocked from the URL that is assigned the Warn option without being given the chance to continue accessing the site anyway.

Procedure

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

Step 2 Click **Edit Settings**.

Step 3 Configure the following settings on the **End-User Filtering Warning** page:

Option	Method
Time Between Warning	The Time Between Warning determines how often the Web Proxy displays the end-user URL filtering warning page for each URL category per user. This setting applies to users tracked by username and users tracked by IP address. Specify any value from 30 to 2678400 seconds (one month). Default is 1 hour (3600 seconds).
Custom Message	The custom message is text you enter that appears on every end-user URL filtering warning page. Include some simple HTML tags to format the text.

Step 4 Click Submit.

What to do next

Related Topics

- Filtering Adult Content, on page 34
- Custom Messages on Notification Pages
- Configuring the End-User URL Filtering Warning Page

Creating Time Based URL Filters

You can configure how the Secure Web Appliance to handles requests for URLs in particular categories differently based on time and day.

Before you begin

Go to the **Web Security Manager > Defined Time Range** page to define at least one time range.

Procedure

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

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

Step 3 Select **Time-Based** for the custom or predefined URL category you want to configure based on time range.

Step 4 In the **In Time Range** field, choose the defined time range to use for the URL category.

Step 5 In the **Action** field, choose the action to enact on transactions in this URL category during the defined time range.

Step 6 In the **Otherwise** field, choose the action to enact on transactions in this URL category *outside* the defined time range.

Step 7 Submit and Commit Changes.

What to do next

Related Topics

- Time Ranges and Quotas, on page 93

Viewing URL Filtering Activity

The **Reporting > URL Categories** page provides a collective display of URL statistics that includes information about top URL categories matched and top URL categories blocked. This page displays category-specific data for bandwidth savings and web transactions.

Related Topics

- Generate Reports to Monitor End-user Activity

Understanding Unfiltered and Uncategorized Data

When viewing URL statistics on the Reporting > URL Categories page, it is important to understand how to interpret the following data:

Data Type	Description
URL Filtering Bypassed	Represents policy, port, and admin user agent blocking that occurs before URL filtering.
Uncategorized URL	Represents all transactions for which the URL filtering engine is queried, but no category is matched.

URL Category Logging in Access Logs

The access log file records the URL category for each transaction in the scanning verdict information section of each entry.

Related Topics

- Monitor System Activity Through Logs.
- URL Category Descriptions, on page 43.

Regular Expressions

The Secure Web Appliance uses a regular expression syntax that differs slightly from the regular expression syntax used by other Velocity pattern-matching engine implementations. Further, the appliance does not support using a backward slash to escape a forward slash. If you need to use a forward slash in a regular expression, simply type the forward slash without a backward slash.

Note Technically, AsyncOS for Web uses the Flex regular expression analyzer.

You can use regular expressions in the following locations:

- **Custom URL categories for Access Policies.** When you create a custom URL category to use with Access Policy groups, you can use regular expressions to specify multiple web servers that match the pattern you enter. The maximum number of characters that can be used in regular expressions has been set to 2048 to restrict any web security vulnerability.
- **Custom user agents to block.** When you edit the applications to block for an Access Policy group, you can use regular expressions to enter specific user agents to block.

Note Regular expressions that perform extensive character matching consume resources and can affect system performance. For this reason, regular expressions should be cautiously applied.

Related Topics

- Creating and Editing Custom URL Categories, on page 28

Forming Regular Expressions

Regular expressions are rules that typically use the word “matches” in the expressions. They can be applied to match specific URL destinations or web servers. For example, the following regular expression matches any pattern containing “`blocksite.com`”:

```
\.blocksite\.com
```

Consider the following regular expression example:

```
server[0-9]\.example\.com
```

In this example, `server[0-9]` matches `server0`, `server1`, `server2`, ..., `server9` in the domain `example.com`.

In the following example, the regular expression matches files ending in `.exe`, `.zip` and `.bin` in the downloads directory.

```
/downloads/.*\.(exe|zip|bin)
```



Note You must enclose regular expressions that contain blank spaces or non-alphanumeric characters in ASCII quotation marks.

Guidelines for Avoiding Validation Failures

Important: Regular expressions that return more that 63 characters will fail and produce an invalid-entry error. Please be sure to form regular expressions that do not have the potential to return more than 63 characters.

Follow these guidelines to minimize validation failures:

- Use literal expressions rather than wildcards and bracketed expressions whenever possible. A literal expression is essentially just straight text such as "`It's as easy as ABC123`". This is less likely to fail than using "`It's as easy as [A-C]{3}[1-3]{3}`". The latter expression results in the creation of non-deterministic finite automatons (NFA) entries, which can dramatically increase processing time.
- Avoid the use of an unescaped dot whenever possible. The dot is a special regular-expression character that means match any character except for a newline. If you want to match an actual dot, for example, as in "`url.com`", then escape the dot using the \ character, as in "`url\.com`". Escaped dots are treated as literal entries and therefore do not cause issues.
- Any unescaped dot in a pattern that will return more than 63 characters after the dot will be disabled by the pattern-matching engine, and an alert to that effect will be sent to you, and you will continue to receive an alert following each update until you correct or replace the pattern.

  Similarly, use more specific matches rather than unescaped dots wherever possible. For example, if you want to match a URL that is followed by a single digit, use "`url[0-9]`" rather than "`url.`".
- Unescaped dots in a larger regular expression can be especially problematic and should be avoided. For example, "`Four score and seven years ago our fathers brought forth on this continent, a new nation, conceived in Liberty, and dedicated to the proposition that all men are created .qual`" may cause a failure. Replacing the dot in "`.qual`" with the literal "`equal`" should resolve the problem.

  Also, an unescaped dot in a pattern that will return more than 63 characters after the dot will be disabled by the pattern-matching engine. Correct or replace the pattern.
- You cannot use "`.*`" to begin or end a regular expression. You also cannot use "`./`" in a regular expression intended to match a URL, nor can you end such an expression with a dot.
- Combinations of wildcards and bracket expressions can cause problems. Eliminate as many combinations as possible. For example, "`id:[A-F0-9]{8}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{12}\) Gecko/20100101 Firefox/9\.0\.1\$`" may cause a failure, while "`Gecko/20100101 Firefox/9\.0\.1\$`" will not. The latter expression does not include any wildcards or bracketed expressions, and both expressions use only escaped dots.

  When wildcards and bracketed expressions cannot be eliminated, try to reduce the expression's size and complexity. For example, "`[0-9a-z]{64}`" may cause a failure. Changing it to something smaller or less complex, such as "`[0-9]{64}`" or "`[0-9a-z]{40}`" may resolve the problem.

If a failure occurs, try to resolve it by applying the previous rules to the wildcard (such as *, + and .) and bracketed expressions.

Note You can use the CLI option `advancedproxyconfig > miscellaneous > Do you want to enable URL lower case conversion for velocity regex?` to enable or disable default regex conversion to lower case for case-insensitive matching. Use if you are experiencing issues with case sensitivity. See Secure Web Appliance CLI Commands for more information about this option.

Regular Expression Character Table

Meta-character	Description
.	Matches any single character, except the newline character (0x0A). For example, the regular expression r.t matches the strings rat, rut, r t, but not root. Be wary of using unescaped dots in long patterns, and especially in the middle of longer patterns. See Guidelines for Avoiding Validation Failures, on page 41 for more information.
*	Matches zero or more occurrences of the character immediately preceding. For example, the regular expression .* means match any string of characters, and [0-9]* matches any string of digits. Be wary of using this meta-character, especially in conjunction with the dot character. Any pattern containing an unescaped dot that returns more than 63 characters after the dot will be disabled. See Guidelines for Avoiding Validation Failures, on page 41 for more information.
\	The escape character; it means treat the following meta-character as an ordinary character. For example, \^ is used to match the caret character (^) rather than the beginning of a line. Similarly, the expression \. is used to match an actual dot rather than any single character.
^	Matches the beginning of a line. For example, the regular expression ^When in matches the beginning of the string “When in the course of human events” but not the string “What and when in the”.
$	Matches the end of a line or string. For example, b$\. matches any line or string that ends with “b.”
+	Matches one or more occurrences of the character or regular expression immediately preceding. For example, the regular expression 9+ matches 9, 99, and 999.
?	Matches zero or one occurrence of the preceding pattern element. For example, colou?r matches both “colour” and “color” since the “u” is optional.
( )	Treat the expression between the left and right parens as a group, limiting the scope of other meta-characters. For example, (abc)+ matches one or more occurrences of the string “abc”; such as, “abcabcabc” or “abc123” but not “abab” or “ab123”.
|	Logical OR: matches the preceding pattern or the following pattern. For example (him|her) matches the line “it belongs to him” and the line “it belongs to her” but does not match the line “it belongs to them.”

Meta-character	Description
[ ]	Matches any one of the characters between the brackets. For example, the regular expression r[aou]t matches “rat”, “rot”, and “rut”, but not “ret”. Ranges of characters are specified by a beginning character, a hyphen, and an ending character. For example, the pattern [0-9] means match any digit. Multiple ranges can be specified as well. The pattern [A-Za-z] means match any upper- or lower-case letter. To match any character except those in the range (that is, the complementary range), use a caret as the first character after the opening bracket. For example, the expression [^269A-Z] matches any characters except 2, 6, 9, and uppercase letters.
{ }	Specifies the number of times to match the previous pattern. For example: D{1,3} matches one to three occurrences of the letter D Matches a specific number {**n**} or a minimum number {**n**,} of instances of the preceding pattern. For example, the expression A[0-9]{3} matches “A” followed by exactly three digits. That is, it matches “A123” but not “A1234”. The expression [0-9]{4,} matches any sequence of four or more digits.
“...”	Literally interpret any characters enclosed within the quotation marks.

URL Category Descriptions

This section lists the URL categories for Cisco Web Usage Controls. The tables also include the abbreviated URL category names that may appear in the Web Reputation filtering and anti-malware scanning section of an access log file entry.

Note In the access logs, the URL category abbreviations for Cisco Web Usage Controls include the prefix “IW_” before each abbreviation so that the “art” category becomes “IW_art.”

URL Category	Abbreviation	Code	Description	Example URLs
Adult	adlt	1006	Directed at adults, but not necessarily pornographic. May include adult clubs (strip clubs, swingers clubs, escort services, strippers); general information about sex, non-pornographic in nature; genital piercing; adult products or greeting cards; information about sex not in the context of health or disease.	www.adultentertainmentexpo.com www.sincerelynot.com

URL Category	Abbreviation	Code	Description	Example URLs
Advertisements	adv	1027	Banner and pop-up advertisements that often accompany a web page; other advertising websites that provide advertisement content. Advertising services and sales are classified as "Business and Industry."	www.adforce.com www.doubleclick.com
Alcohol	alc	1077	Alcohol as a pleasurable activity; beer and wine making, cocktail recipes; liquor sellers, wineries, vineyards, breweries, alcohol distributors. Alcohol addiction is classified as "Health and Medicine." Bars and restaurants are classified as "Dining and Drinking."	www.samueladams.com www.whisky.com
Animals and Pets	pets	1107	Information about domestic animals, livestock, service animals, pets and their care. Veterinary services, medicines, and animal health. Pet and animal training, aquariums, zoos, and animal shows. Includes animal shelters, humane societies, animal centric charities, and sanctuaries, bee keeping, training, and animal husbandry; dinosaurs and extinct animals.	www.petmd.com www.wheatenorg.uk
Arts	art	1002	Galleries and exhibitions; artists and art; photography; literature and books; performing arts and theater; musicals; ballet; museums; design; architecture. Cinema and television are classified as "Entertainment."	www.moma.org www.nga.gov
Astrology	astr	1074	Astrology; horoscope; fortune telling; numerology; psychic advice; tarot.	www.astro.com www.astrology.com
Auctions	auct	1088	Online and offline auctions, auction houses, and classified advertisements.	www.craigslist.com www.ebay.com

URL Category	Abbreviation	Code	Description	Example URLs
Business and Industry	busi	1019	Marketing, commerce, corporations, business practices, workforce, human resources, transportation, payroll, security and venture capital; office supplies; industrial equipment (process equipment), machines and mechanical systems; heating equipment, cooling equipment; materials handling equipment; packaging equipment; manufacturing: solids handling, metal fabrication, construction and building; passenger transportation; commerce; industrial design; construction, building materials; shipping and freight (freight services, trucking, freight forwarders, truckload carriers, freight and transportation brokers, expedited services, load and freight matching, track and trace, rail shipping, ocean shipping, road feeder services, moving and storage).	www.freightcenter.com www.ge.com
Cannabis	cann	1109	Websites that focus on the recreational and medicinal consumption of cannabis. Sites may include marketing, discussions about legal and regulatory issues, growth and production, paraphernalia, research, and investment in the cannabis industry. Dispensaries, cannabinoid (CBD oil, THC, etc.) based products are also included.	www.localproduct.co www.oregonbc.com
Chat and Instant Messaging	chat	1040	Web-based instant messaging and chat rooms.	www.icq.com www.e-chat.co
Cheating and Plagiarism	plag	1051	Promoting cheating and selling written work, such as term papers, for plagiarism.	www.bestessays.com www.superiorpapers.com
Child Abuse Content	cprn	1064	Worldwide illegal child sexual abuse content.	—

URL Category	Abbreviation	Code	Description	Example URLs
Cloud and Data Centers	serv	1118	Platforms used to serve cloud infrastructure or data center hosting to support an organization's applications, services, or data processing. Due to the de-centralized nature of these domains and IP addresses, a more specific category cannot be applied based on content or ownership.	www.azurewebsites.net www.s3.amazonaws.com
Computer Security	csec	1065	Offering security products and services for corporate and home users.	www.computersecurity.com www.symantec.com
Computers and Internet	comp	1003	Information about computers and software, such as hardware, software, software support; information for software engineers, programming and networking; website design; the web and Internet in general; computer science; computer graphics and clipart. “Freeware and Shareware” is a separate category.	www.xml.com www.w3.org
Conventions, Conferences and Trade Shows	expo	1110	Seminars, trade shows, conventions and conferences themed around a particular industry, market, or common interest. May include information about acquiring tickets, registration, abstract or presentation proposal guidelines, workshops, sponsorship details, vendor or exhibitor information, and other marketing or promotional material. This category includes academic, professional, as well as pop-culture events, all of which tend to be a short-lived or annual event.	www.thesmallbusinessexpo.com www.makerfaire.com
Cryptocurrency	cryp	1111	Online brokerages and websites that enable users to trade cryptocurrencies; information regarding cryptocurrencies including analysis, commentary, advice, performance indexes, and price charts. General information about cryptomining and mining businesses are included in this category but domains and IP addresses directly involved in mining activities are categorized as Cryptomining.	www.coinbase.com www.coinsutra.com

URL Category	Abbreviation	Code	Description	Example URLs
Cryptomining	mine	1112	Hosts that are actively participating in a cryptocurrency mining pool.	www.give-me-coins.com www.slushpool.com
Dating	date	1055	Dating, online personals, matrimonial agencies.	www.eharmony.com www.match.com
Digital Postcards	card	1082	Enabling sending of digital postcards and e-cards.	www.hallmarkecards.com www.bluemountain.com
Dining and Drinking	food	1061	Eating and drinking establishments; restaurants, bars, taverns, and pubs; restaurant guides and reviews.	www.zagat.com www.experiencethepub.com
DIY Projects	diy	1097	Guidance and information to create, improve, modify, decorate and repair something without the aid of experts or professionals.	www.diy-tips.co.uk www.thisoldhouse.com
DNS-Tuneling	tunn	1122	Sites that provide DNS Tunneling as a service. These services can be for PC or mobile and create a VPN connection specifically over DNS to send traffic that may bypass corporate policies and inspection.	
DoH and DoT	doht	1113	Encrypted DNS requests using either the DNS over HTTPS (DoH) protocol or the DNS over TLS protocol. These protocols are typically used as a layer of security and privacy by end-users, but the encryption hides the destination of the request and passes it through a third-party.	www.cloudflare-dns.com www.dns.google.com
Dynamic and Residential	dyn	1091	IP addresses of broadband links that usually indicates users attempting to access their home network, for example for a remote session to a home computer.	http://109.60.192.55
Dynamic DNS Provider	ddns	1114	sers may use dynamic DNS services to make certain applications or content accessible via the web from endpoints hosted on dynamically assigned IP addresses. Access is granted through a hostname on the domain owned by the dynamic DNS service.	www.noip.com www.afraid.org

URL Category	Abbreviation	Code	Description	Example URLs
Education	edu	1001	Education-related, such as schools, colleges, universities, teaching materials, and teachers' resources; technical and vocational training; online training; education issues and policies; financial aid; school funding; standards and testing.	www.education.com www.greatschools.org
Entertainment	ent	1093	Details or discussion of films; music and bands; television; celebrities and fan websites; entertainment news; celebrity gossip; entertainment venues. Compare with the "Arts" category.	www.eonline.com www.ew.com
Extreme	extr	1075	Material of a sexually violent or criminal nature; violence and violent behavior; tasteless, often gory photographs, such as autopsy photos; photos of crime scenes, crime and accident victims; excessive obscene material; shock websites.	www.car-accidents.com www.crime-scene-photos.com
Fashion	fash	1076	Clothing and fashion; hair salons; cosmetics; accessories; jewelry; perfume; pictures and text relating to body modification; tattoos and piercing; modeling agencies. Dermatological products are classified as "Health and Medicine."	www.fashion.net www.styleseat.com
File Transfer Services	fts	1071	File transfer services with the primary purpose of providing download services and hosted file sharing	www.sharefile.com www.wetransfer.com
Filter Avoidance	filt	1025	Promoting and aiding undetectable and anonymous web usage, including cgi, php and glype anonymous proxy services.	www.bypassschoolfilter.com www.filterbypass.com
Finance	fnnc	1015	Primarily financial in nature, such as accounting practices and accountants, taxation, taxes, banking, insurance, investing, the national economy, personal finance involving insurance of all types, credit cards, retirement and estate planning, loans, mortgages. Stock and shares are classified as "Online Trading."	www.finance.yahoo.com www.bankofamerica.com

URL Category	Abbreviation	Code	Description	Example URLs
Freeware and Shareware	free	1068	Providing downloads of free and shareware software.	www.freewarehome.com www.filehippo.com
Gambling	gamb	1049	Casinos and online gambling; bookmakers and odds; gambling advice; competitive racing in a gambling context; sports booking; sports gambling; services for spread betting on stocks and shares. Websites dealing with gambling addiction are classified as "Health and Medicine." Government-run lotteries are classified as "Lotteries".	www.888.com www.gambling.com
Games	game	1007	Various card games, board games, word games, and video games; combat games; sports games; downloadable games; game reviews; cheat sheets; computer games and Internet games, such as role-playing games.	www.games.com www.shockwave.com
Government and Law	gov	1011	Government websites; foreign relations; news and information relating to government and elections; information relating to the field of law, such as attorneys, law firms, law publications, legal reference material, courts, dockets, and legal associations; legislation and court decisions; civil rights issues; immigration; patents and copyrights; information relating to law enforcement and correctional systems; crime reporting, law enforcement, and crime statistics; military, such as the armed forces, military bases, military organizations; anti-terrorism.	www.usa.gov www.law.com
Hacking	hack	1050	Discussing ways to bypass the security of websites, software, and computers.	www.hackthissite.org www.gohacking.com
Hate Speech	hate	1016	Websites promoting hatred, intolerance, or discrimination on the basis of social group, color, religion, sexual orientation, disability, class, ethnicity, nationality, age, gender, gender identity; sites promoting racism; sexism; racist theology; hate music; neo-Nazi organizations; supremacism; Holocaust denial.	www.kkk.com www.aryanunity.com

URL Category	Abbreviation	Code	Description	Example URLs
Health and Medicine	hmed	1104	Health care; diseases and disabilities; medical care; hospitals; doctors; medicinal drugs; mental health; psychiatry; pharmacology; exercise and fitness; physical disabilities; vitamins and supplements; sex in the context of health (disease and health care); tobacco use, alcohol use, drug use, and gambling in the context of health (disease and health care).	www.webmd.com www.health.com
Humor	lol	1079	Jokes, sketches, comics and other humorous content. Adult humor likely to offend is classified as "Adult."	www.pun.me www.jokes.com
Hunting	hunt	1022	Hunting and Fishing Professional or sport hunting; gun clubs and other hunting related sites.	www.bulletsafaris.com www.mfha.org
Illegal Activities	ilac	1022	Promoting crime, such as stealing, fraud, illegally accessing telephone networks; computer viruses; terrorism, bombs, and anarchy; websites depicting murder and suicide as well as explaining ways to commit them.	www.ekran.no www.pyrobin.com
Illegal Downloads	ildl	1084	Providing the ability to download software or other materials, serial numbers, key generators, and tools for bypassing software protection in violation of copyright agreements. Torrents are classified as "Peer File Transfer."	www.keygenninja.com www.rootscrack.com
Illegal Drugs	drug	1047	Information about recreational drugs, drug paraphernalia, drug purchase and manufacture.	www.shroomery.org www.hightimes.com
Infrastructure and Content Delivery Networks	infr	1018	Content delivery infrastructure and dynamically generated content; websites that cannot be classified more specifically because they are secured or otherwise difficult to classify.	www.akamai.net www.webstat.net

URL Category	Abbreviation	Code	Description	Example URLs
Internet of Things	iot	1116	Domains used to monitor the general health, activity, or aid in the configuration of Internet of Things (IoT) and other network-aware electronics. Additionally these sites may provide software or firmware updates or allow remote access to administer the device. IoT exists in both consumer and professional segments, in products such as printers, televisions, thermostats, system monitoring, automation, and smart appliances.	www.samsungotn.net www.transport.nest.com
Internet Telephony	voip	1067	Telephonic services using the Internet.	www.skype.com www.getvoca.com
Job Search	job	1004	Career advice; resume writing and interviewing skills; job placement services; job databanks; permanent and temporary employment agencies; employer websites.	www.careerbuilder.com www.monster.com
Lingerie and Swimsuits	ling	1031	Intimate apparel and swimwear, especially when modeled.	www.swimsuits.com www.victoriassecret.com
Lotteries	lotr	1034	Sweepstakes, contests and state-sponsored lotteries.	www.calottery.com www.flalottery.com
Military	mil	1099	Military, such as the armed forces; military bases; military organizations; anti-terrorism.	www.goarmy.com www.todaysmilitary.com
Mobile Phones	cell	1070	Short Message Services (SMS); ringtones and mobile phone downloads. Cellular carrier websites are included in the "Business and Industry" category.	www.cbfsms.com www.zedge.net
Museums	muse	1117	Museums and exhibits, both online and physical, dedicated to preserving information regarding subjects that could be of general interest or highly specialized. Subjects could range from art, history, science, or be of cultural importance.	www.ushmm.org www.[illegible]

URL Category	Abbreviation	Code	Description	Example URLs
Nature and Conservation	ncon	1106	Sites related to natural resources; ecology and conservation; forests; wilderness; plants; flowers; forest conservation; forest, wilderness, and forestry practices; forest management (reforestation, forest protection, conservation, harvesting, forest health, thinning, and prescribed burning); agricultural practices (agriculture, gardening, horticulture, landscaping, planting, weed control, irrigation, pruning, and harvesting); pollution issues (air quality, hazardous waste, pollution prevention, recycling, waste management, water quality, and the environmental cleanup industry).	www.nature.org www.thepottedgarden.co.uk
News	news	1058	News; headlines; newspapers; television stations; magazines; weather; ski conditions.	www.cnn.com www.news.bbc.co.uk
Non-governmental Organizations	ngo	1087	Non-governmental organizations such as clubs, lobbies, communities, non-profit organizations and labor unions.	www.panda.org www.unions.org
Non-sexual Nudity	nsn	1060	Nudism and nudity; naturism; nudist camps; artistic nudes.	www.1001fessesproject.com www.naturistsociety.com
Not Actionable	nact	1103	Sites that have been inspected but are unreachable or do not have enough content to be assigned a category.	—
Online Communities	comm	1024	Affinity groups; special interest groups; web newsgroups; message boards. Excludes websites classified as “Professional Networking” or “Social Networking.”	www.reddit.com www.stackexchange.com
Online Document Sharing and Collaboration	docs	1115	Cloud-based software used to create, convert, or edit documents. Collaboration and sharing features may be available with access permissions typically configured by the author. Documents may be stored online or available to download.	www.pastebin.com www.docs.google.com

URL Category	Abbreviation	Code	Description	Example URLs
Online Meetings	meet	1100	Online meetings; desktop sharing; remote access and other tools that facilitate multi-location collaboration	www.join.me www.teamviewer.com
Online Storage and Backup	osb	1066	Offsite and peer-to-peer storage for backup, sharing, and hosting.	www.adrive.com www.dropbox.com
Online Trading	trad	1028	Online brokerages; websites that enable the user to trade stocks online; information relating to the stock market, stocks, bonds, mutual funds, brokers, stock analysis and commentary, stock screens, stock charts, IPOs, stock splits. Services for spread betting on stocks and shares are classified as "Gambling." Other financial services are classified as "Finance."	www.tdameritrade.com www.etrade.com
Organizational Email	pem	1085	Websites used to access business email (often via Outlook Web Access).	www.mail.zoho.com www.webmail.edmc.edu
Paranormal	prnm	1101	UFOs; ghosts; cryptid; telekenesis; urban legends; and myths.	www.ghoststudy.com www.ufocasebook.com
Parked Domains	park	1092	Websites that monetize traffic from the domain using paid listings from an ad network, or are owned by "squatters" hoping to sell the domain name for a profit. These also include fake search websites which return paid ad links.	www.domainzaar.com www.cricketbuzz.com
Peer File Transfer	p2p	1056	Peer-to-peer file request websites. This does not track the file transfers themselves.	www.bittorrent.com www.torrentdownloads.me
Personal Sites	pers	1081	Websites about and from private individuals; personal homepage servers; websites with personal contents; personal blogs with no particular theme.	www.blogmaverick.com www.stallman.org
Personal VPN	pvpn	1102	Virtual private network (VPN) sites or tools that are typically for personal use, and, may or may not be approved for corporate usage.	www.openvpn.net www.torvpn.com
Photo Search and Images	img	1090	Facilitating the storing and searching for, images, photographs, and clip-art.	www.flickr.com www.photobucket.com

URL Category	Abbreviation	Code	Description	Example URLs
Politics	pol	1083	Websites of politicians; political parties; news and information on politics, elections, democracy, and voting.	www.politics.com www.gp.org
Pornography	porn	1054	Sexually explicit text or depictions. Includes explicit anime and cartoons; general explicit depictions; other fetish material; explicit chat rooms; sex simulators; strip poker; adult movies; lewd art; web-based explicit email.	www.redtube.com www.youporn.com
Private IP Addresses as Host	piah	1121	Private IP addresses which are used as the host part of a URL. Private IP addresses are meant for internal use behind border routers only, so they are not publicly routable.	
Professional Networking	pnet	1089	Social networking for the purpose of career or professional development. See also “Social Networking.”	www.linkedin.com www.europeanpwn.net
Real Estate	rest	1045	Information that would support the search for real estate; office and commercial space; real estate listings, such as rentals, apartments, and homes; house building.	www.realtor.com www.zillow.com
Recipes and Food	reci	1105	Sites dedicated to sharing or discussing information about cooking, recipes, and food or non-alcoholic beverages; cultural aspects of cuisine and food; diet descriptions and adherence tips, general nutrition information about foods. Use and instruction on cooking appliances and utensils. Food celebrity, lifestyle, and enthusiast blogs.	www.allrecipes.com www.seriouseats.com
Reference	ref	1017	City and state guides; maps, time; reference sources; dictionaries; libraries.	www.wikipedia.org www.yellowpages.com
Regional Restricted Sites (Germany)	xdeu	1125	URLs that are restricted in Germany due to content which may be unlawful as determined by the regional government.	
Regional Restricted Sites (Great Britain)	xgbr	1123	URLs that are restricted in Great Britain due to content which may be unlawful as determined by the regional government.	

URL Category	Abbreviation	Code	Description	Example URLs
Regional Restricted Sites (Italy)	xita	1124	URLs that are restricted in Italy due to content which may be unlawful as determined by the regional government.	
Regional Restricted Sites (Poland)	xpol	1126	URLs that are restricted in Poland due to content which may be unlawful as determined by the regional government.	www.betsafe62.com www.tornadobet69.com
Religion	rel	1086	Religious content, information about religions; religious communities.	www.religionfacts.com www.religioustolerance.org
SaaS and B2B	saas	1080	Web portals for online business services; online meetings.	www.netsuite.com www.salesforce.com
Safe for Kids	kids	1057	Directed at, and specifically approved for, young children.	www.discoverykids.com www.nickjr.com
Science and Technology	sci	1012	Science and technology, such as aerospace, electronics, engineering, mathematics, and other similar subjects; space exploration; meteorology; geography; environment; energy (fossil, nuclear, renewable); communications (telephones, telecommunications).	www.physorg.com www.science.gov
Search Engines and Portals	srch	1020	Search engines and other initial points of access to information on the Internet.	www.bing.com www.google.com
Sex Education	sxed	1052	Factual websites dealing with sex; sexual health; contraception; pregnancy.	www.avert.org www.scarleteen.com
Shopping	shop	1005	Bartering; online purchasing; coupons and free offers; general office supplies; online catalogs; online malls.	www.amazon.com www.shopping.com
Social Networking	snet	1069	Social networking. See also “Professional Networking.”	www.facebook.com www.twitter.com
Social Science	socs	1014	Sciences and history related to society; archaeology; anthropology; cultural studies; history; linguistics; geography; philosophy; psychology; women's studies.	www.archaeology.org www.anthropology.net
Society and Culture	scty	1010	Family and relationships; ethnicity; social organizations; genealogy; seniors; child-care.	www.childcareaware.org www.familysearch.org

URL Category	Abbre viation	Code	Description	Example URLs
Software Updates	swup	1053	Websites that host updates for software packages.	www.softwarepatch.com www.windowsupdate.com
Sports and Recreation	sprt	1008	All sports, professional and amateur; recreational activities; fishing; fantasy sports; public parks; amusement parks; water parks; theme parks; zoos and aquariums; spas.	www.espn.com www.recreation.gov
Streaming Audio	aud	1073	Real-time streaming audio content including Internet radio and audio feeds.	www.live-radio.net www.shoutcast.com
Streaming Video	vid	1072	Real-time streaming video including Internet television, web casts, and video sharing.	www.hulu.com www.youtube.com
Terrorism and Violent Extremism	terr	1119	Terrorist or extremist websites that promote death or violence as part of their ideology. Sites may contain graphic or disturbing images, videos, and text. Some sites may not advocate terrorism but share first-hand material of a violent nature.	
Tobacco	tob	1078	Pro-tobacco websites; tobacco manufacturers; pipes and smoking products (not marketed for illegal drug use). Tobacco addiction is classified as “Health and Medicine.”	www.bat.com www.tobacco.org
Transportation	trns	1044	Personal transportation; information about cars and motorcycles; shopping for new and used cars and motorcycles; car clubs; boats, airplanes, recreational vehicles (RVs), and other similar items. Note, car and motorcycle racing is classified as “Sports and Recreation.”	www.cars.com www.motorcycles.com
Travel	trvl	1046	Business and personal travel; travel information; travel resources; travel agents; vacation packages; cruises; lodging and accommodation; travel transportation; flight booking; airfares; car rental; vacation homes.	www.expedia.com www.lonelyplanet.com
URL Shorteners	shrt	1120	Domains used to shorten long URLs, brand URLs, or may obscure the final destination of a hyperlink.	www.bit.ly www.tinyurl.com

URL Category	Abbreviation	Code	Description	Example URLs
Weapons	weap	1036	Information relating to the purchase or use of conventional weapons such as gun sellers, gun auctions, gun classified ads, gun accessories, gun shows, and gun training; general information about guns; other weapons and graphic hunting sites may be included. Government military websites are classified as "Government and Law."	www.coldsteel.com www.gunbroker.com
Web Cache and Archives	cach	1108	Cached or archived web content often stored for preservation or to decrease load times.	www.archive.org www.webcache.googleusercontent.com
Web Hosting	whst	1037	Website hosting; bandwidth services.	www.bluehost.com www.godaddy.com
Web Page Translation	tran	1063	Translation of web pages between languages.	www.babelfish.com www.translate.google.com
Web-based Email	mail	1038	Public web-based email services. Websites enabling individuals to access their company or organization's email service are classified as "Organizational Email."	www.mail.yahoo.com www.outlook.com

Related Topics

- Managing Updates to the Set of URL Categories , on page 15
- Reporting Uncategorized and Misclassified URLs, on page 13

Create Decryption Policies to Control HTTPS Traffic

This topic contains the following sections:

- Overview of Create Decryption Policies to Control HTTPS Traffic, on page 58
- Managing HTTPS Traffic through Decryption Policies Best Practices, on page 59
- Decryption Policies , on page 59
- Root Certificates, on page 65
- Routing HTTPS Traffic, on page 72
- Troubleshooting Decryption/HTTPS/Certificates, on page 72

Overview of Create Decryption Policies to Control HTTPS Traffic

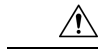
Decryption policies define the handling of HTTPS traffic within the web proxy:

- When to decrypt HTTPS traffic.
- How to handle requests that use invalid or revoked security certificates.

You can create decryption policies to handle HTTPS traffic in the following ways:

- Pass through encrypted traffic
- Decrypt traffic and apply the content-based access policies defined for HTTP traffic. This also makes malware scanning possible

  .
- Drop the HTTPS connection
- Monitor the request (take no final action) as the web proxy continues to evaluate the request against policies that may lead to a final drop, pass through, or decrypt action.



Caution **Handle personally identifiable information with care:** If you choose to decrypt an end-user's HTTPS session, the Secure Web Appliance access logs and reports may contain personally identifiable information. The Administrator can configure how much URI text is stored in the logs using the `advancedproxyconfig` CLI command and the `HTTPS` subcommand. You can log the entire URI, or a partial form of the URI with the query portion removed. However, even when you choose to strip the query from the URI, personally identifiable information may still remain.

Managing HTTPS Traffic through Decryption Policies Task Overview

Step	Task List for Managing HTTPS Traffic through Decryption Policies	Links to Related Topics and Procedures
1	Enabling the HTTPS proxy	Enabling the HTTPS Proxy, on page 61
2	Upload or Generate a certificate and key	• Uploading a Root Certificate and Key, on page 67 • Generating a Certificate and Key for the HTTPS Proxy, on page 68
3	Configuring Decryption options	Configuring Decryption Options, on page 64
5	(Optional) Configure invalid certificate handling	Configuring Invalid Certificate Handling, on page 68
6	(Optional) Enabling real-time revocation status checking	Enabling Real-Time Revocation Status Checking, on page 70
7	(Optional) Manage trusted and blocked certificates	Trusted Root Certificates, on page 71

Managing HTTPS Traffic through Decryption Policies Best Practices

Create fewer, more general Decryption Policy groups that apply to all users or fewer, larger groups of users on the network. Then, if you need to apply more granular control to decrypted HTTPS traffic, use more specific Access Policy groups.

Decryption Policies

The appliance can perform any of the following actions on an HTTPS connection request:

Option	Description
Monitor	Monitor is an intermediary action that indicates the Web Proxy should continue evaluating the transaction against the other control settings to determine which final action to ultimately apply.
Drop	The appliance drops the connection and does not pass the connection request to the server. The appliance does not notify the user that it dropped the connection.
Pass through	The appliance passes through the connection between the client and the server without inspecting the traffic content. However, with a standard pass-through policy, the Secure Web Appliance does check the validity of the requested server by initiating an HTTPS handshake with the server. This validity check includes server certificate validation. If the server fails the check, the transaction is blocked. You can skip validation checks for specific sites by configuring policies that incorporate custom categories which include these sites, thereby indicating that these sites are trustworthy—these sites are passed through without validity checks. Exercise care when configuring policies that allow validity checks to be skipped.
Decrypt	The appliance allows the connection, but inspects the traffic content. It decrypts the traffic and applies Access Policies to the decrypted traffic as if it were a plaintext HTTP connection. By decrypting the connection and applying Access Policies, you can scan the traffic for malware.

All actions except Monitor are “final actions” the Web Proxy applies to a transaction. A final action is an action that causes the Web Proxy to stop evaluating the transaction against other control settings. For example, if a Decryption Policy is configured to monitor invalid server certificates, the Web Proxy makes no final decision on how to handle the HTTPS transaction if the server has an invalid certificate. If a Decryption Policy is configured to block servers with a low Web reputation score, then any request to a server with a low reputation score is dropped without considering the URL category actions.

The following diagram shows how the Web Proxy evaluates a client request against the Decryption Policy groups. Applying Decryption Policy Actions shows the order the Web Proxy uses when evaluating control settings for Decryption Policies. Figure 8: Applying Access Policy Actions, on page 91 shows the order the Web Proxy uses when evaluating control settings for Access Policies.

Figure 3: Applying Decryption Policy Actions

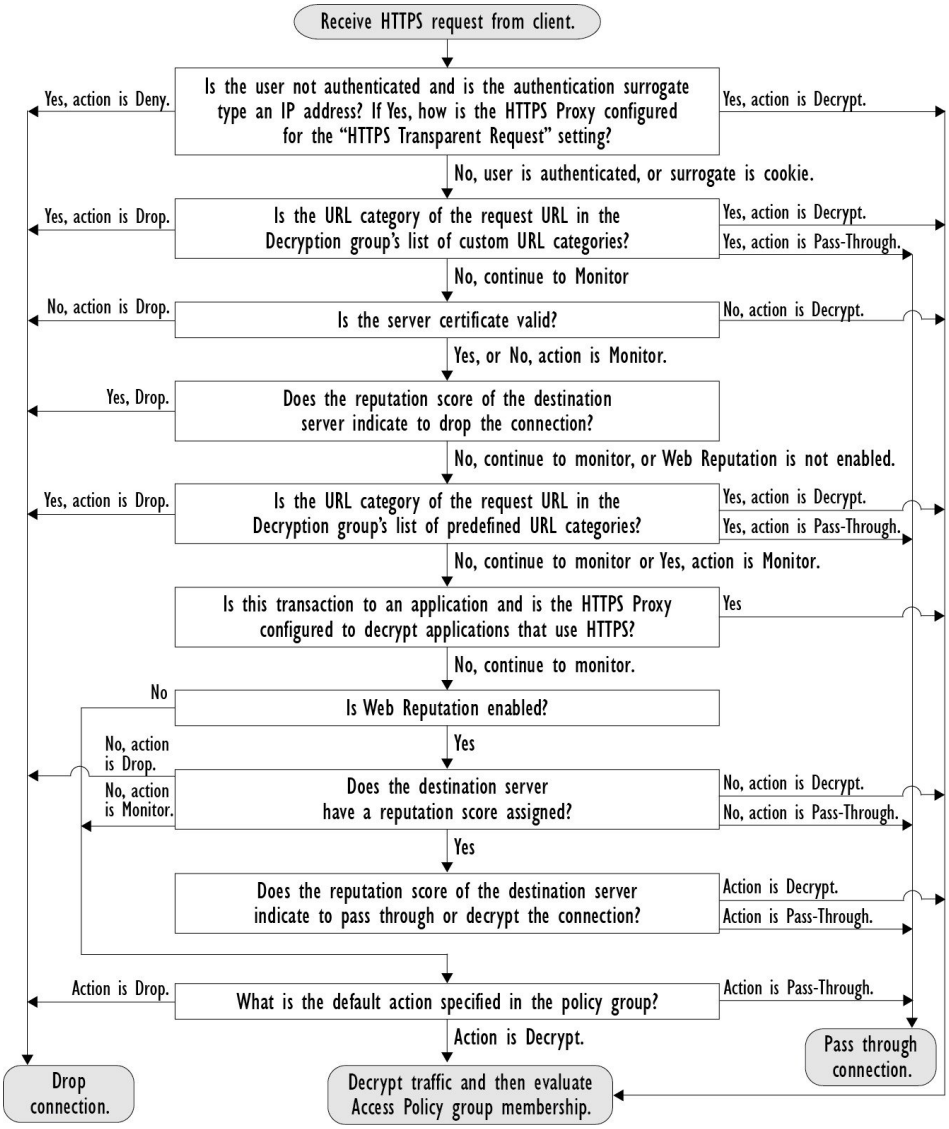
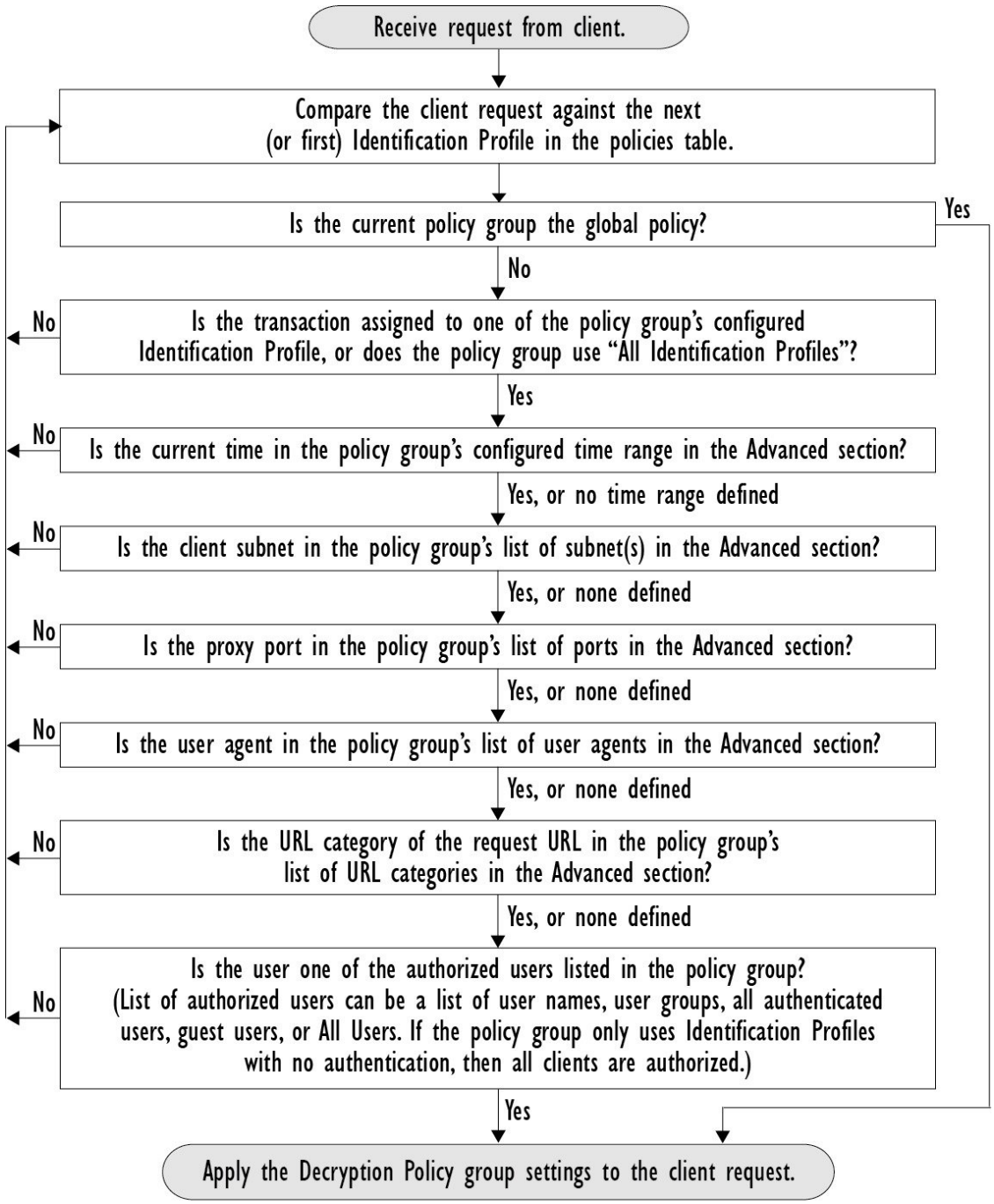


Figure 4: Policy Group Transaction Flow for Decryption Policies



Enabling the HTTPS Proxy

To monitor and decrypt HTTPS traffic, you must enable the HTTPS Proxy. When you enable the HTTPS Proxy, you must configure what the appliance uses for a root certificate when it sends self-signed server certificates to the client applications on the network. You can upload a root certificate and key that your

organization already has, or you can configure the appliance to generate a certificate and key with information you enter.

Once the HTTPS Proxy is enabled, all HTTPS policy decisions are handled by Decryption Policies. Also on this page, you can configure what the appliance does with HTTPS traffic when the server certificate is invalid.

Before you begin

When the HTTPS proxy is enabled, HTTPS-specific rules in access policies are disabled and the web proxy processes decrypted HTTPS traffic using rules for HTTP.

Procedure

Step 1 **Security Services** > **HTTPS Proxy**, click **Enable and Edit Settings**.

The HTTPS Proxy License Agreement appears.

Step 2 Read the terms of the HTTPS Proxy License Agreement, and click **Accept**.

Step 3 Verify the Enable HTTPS Proxy field is enabled.

Step 4 In the **HTTPS Ports to Proxy** field, enter the ports the appliance should check for HTTPS traffic. Port 443 is the default port.

Note
Secure Web Appliance can use maximum of 30 ports as proxy:3 ports are always reserved for FTP proxy, and 27 ports can be configured as HTTP and HTTPS proxy.

Step 5 Upload or generate a root/signing certificate to use for decryption.

Note
If the appliance has both an uploaded certificate and key pair and a generated certificate and key pair, it only uses the certificate and key pair currently selected in the Root Certificate for Signing section.

Step 6 In the HTTPS Transparent Request section, select one of the following options:

- Decrypt the HTTPS request and redirect for authentication
- Deny the HTTPS request

This setting only applies to transactions that use IP address as the authentication surrogate and when the user has not yet been authenticated.

Note
This field only appears when the appliance is deployed in transparent mode.

Step 7 In the Applications that Use HTTPS section, choose whether to enable decryption for enhanced application visibility and control or application discovery and control.

Note
Decryption may cause some applications to fail unless the root certificate for signing is installed on the client. For more information on the appliance root certificate, see Managing Certificate Validation and Decryption for HTTPS, on page 66.

Step 8 Submit and commit your changes.

What to do next

Related Topics

- Managing Certificate Validation and Decryption for HTTPS, on page 66

Controlling HTTPS Traffic

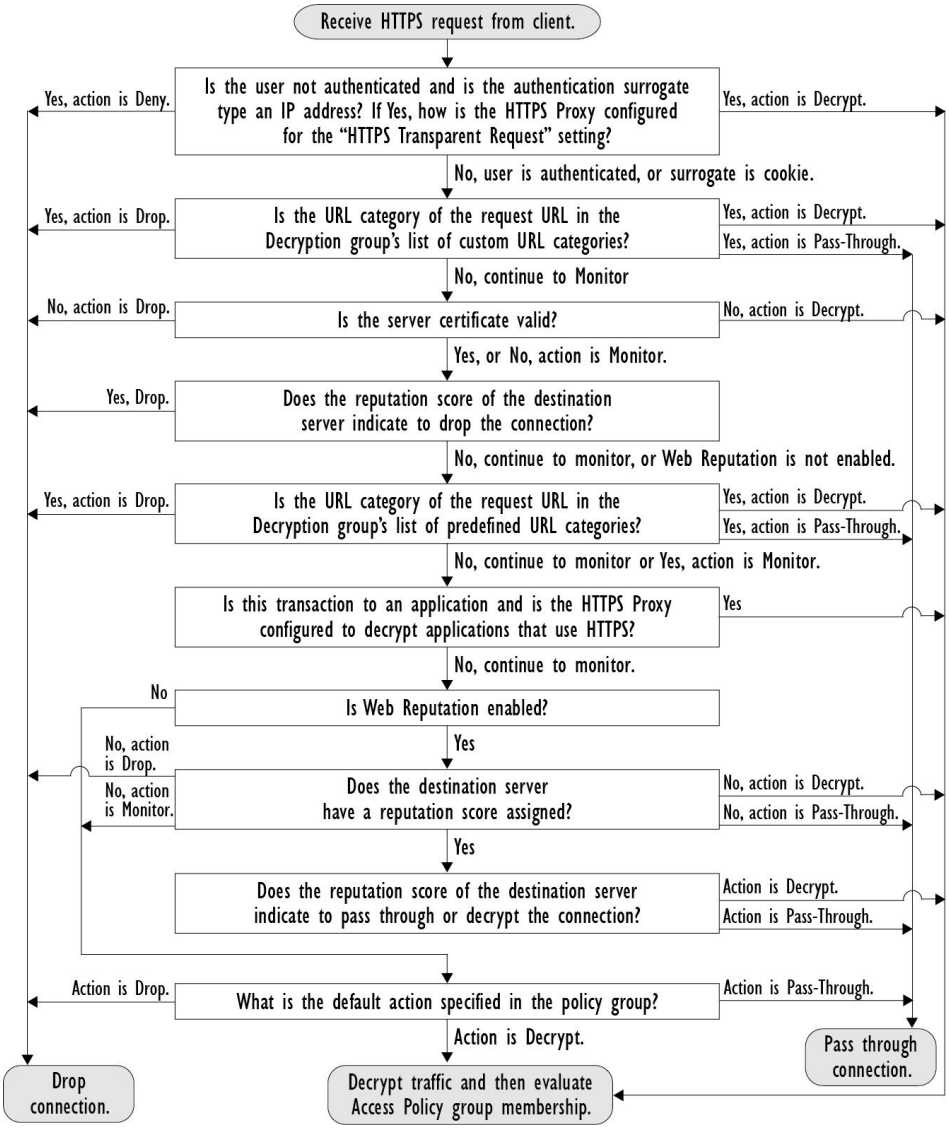
After the Secure Web Appliance assigns an HTTPS connection request to a Decryption Policy group, the connection request inherits the control settings of that policy group. The control settings of the Decryption Policy group determine whether the appliance decrypts, drops, or passes through the connection:

Option	Description
URL Categories	You can configure the action to take on HTTPS requests for each predefined and custom URL category. Click the link under the URL Filtering column for the policy group you want to configure. **Note** If you want to *block* (with end-user notification) a particular URL category for HTTPS requests instead of drop (with no end-user notification), choose to decrypt that URL category in the Decryption Policy group and then choose to block the same URL category in the Access Policy group.
Web Reputation	You can configure the action to take on HTTPS requests based on the web reputation score of the requested server. Click the link under the Web Reputation column for the policy group you want to configure.
Default Action	You can configure the action the appliance should take when none of the other settings apply. Click the link under the Default Action column for the policy group you want to configure. **Note** The configured default action only affects the transaction when no decision is made based on URL category or Web Reputation score. If Web Reputation filtering is disabled, the default action applies to all transactions that match a Monitor action in a URL category. If Web Reputation filtering is enabled, the default action is used only if the Monitor action is selected for sites with no score.

To bypass encrypted traffic having a good web reputation score, make sure that you disable the **Decrypt for Application Detection** option in the **Decryption Options** section of the HTTPS Proxy Settings page.

The following diagram shows how the appliance determines which action to take on an HTTPS request after it has assigned a particular Decryption Policy to the request. The Web reputation score of the destination server is evaluated only once, but the result is applied at two different points in the decision flow. For example, note that a Web reputation score Drop action overrides any action specified for predefined URL categories.

Figure 5: Applying Decryption Policy Actions



Configuring Decryption Options

Before you begin

Verify that the HTTPS proxy is enabled as described in Enabling the HTTPS Proxy, on page 61.

Procedure

Step 1 **Security Services** > **HTTPS Proxy**.

Step 2 Click **Edit Settings**.

Step 3 Enable the decryption options.

Note
Enabling this option will improve the efficacy of detection for some HTTPS applications. However, decryption may cause other HTTPS applications to fail unless the root certificate for signing is installed on the client. Choosing ADC or AVC in Acceptable Use Controls, decrypts to identify the application.

Decryption Option	Description
Decrypt for Authentication	For users who have not been authenticated prior to this HTTPS transaction, allow decryption for authentication.
Decrypt for End-User Notification	Allow decryption so that AsyncOS can display the end-user notification. **Note** If the certificate is invalid and invalid certificates are set to drop, when running a policy trace, the first logged action for the transaction will be “decrypt”.
Decrypt for End-User Acknowledgment	For users who have not acknowledged the web proxy prior to this HTTPS transaction, allow decryption so that AsyncOS can display the end-user acknowledgment.
Decrypt for Application Detection	Enhances the ability of AsyncOS to detect HTTPS applications.

Authentication and HTTPS Connections

Authentication at the HTTPS connection layer is available for these types of requests:

Option	Description
Explicit requests	• secure client authentication disabled or • secure client authentication enabled and an IP-based surrogate
Transparent requests	• IP-based surrogate, decryption for authentication enabled or • IP-based surrogate, client previously authenticated using an HTTP request

Root Certificates

The HTTPS proxy uses the root certificates and private key files that you upload to the appliance to decrypt traffic. The root certificate and private key files you upload to the appliance must be in PEM format; DER format is not supported.

You can enter root certificate information in the following ways:

- **Generate.** You can enter some basic organization information and then click a button so the appliance generates the rest of the certificate and a private key.
- **Upload.** You can upload a certificate file and its matching private key file created outside of the appliance.

Note You can also upload an intermediate certificate that has been signed by a root certificate authority. When the Web Proxy mimics the server certificate, it sends the uploaded certificate along with the mimicked certificate to the client application. That way, as long as the intermediate certificate is signed by a root certificate authority that the client application trusts, the application will trust the mimicked server certificate, too. See About Certificates and Keys for more information.

You can choose how to handle the root certificates issued by the Secure Web Appliance:

- **Inform users to accept the root certificate.** You can inform the users in your organization what the new policies are at the company and tell them to accept the root certificate supplied by the organization as a trusted source.
- **Add the root certificate to client machines.** You can add the root certificate to all client machines on the network as a trusted root certificate authority. This way, the client applications automatically accept transactions with the root certificate.

Procedure

Step 1 Security Services > HTTPS Proxy.

Step 2 Click **Edit Settings**.

Step 3 Click the Download Certificate link for either the generated or uploaded certificate.

Note
To reduce the possibility of client machines getting a certificate error, submit the changes after you generate or upload the root certificate to the Secure Web Appliance, then distribute the certificate to client machines, and then commit the changes to the appliance.

Managing Certificate Validation and Decryption for HTTPS

The Secure Web Appliance validates certificates before inspecting and decrypting content.

Valid Certificates

Qualities of a valid certificate:

- **Not expired.** The certificate's validity period includes the current date.
- **Recognized certificate authority.** The issuing certificate authority is included in the list of trusted certificate authorities stored on the Secure Web Appliance.
- **Valid signature.** The digital signature was properly implemented based on cryptographic standards.
- **Consistent naming.** The common name matches the hostname specified in the HTTP header.
- **Not revoked.** The issuing certificate authority has not revoked the certificate.

Related Topics

- Enabling Real-Time Revocation Status Checking, on page 70
- Configuring Invalid Certificate Handling, on page 68
- Options for Certificate Revocation Status Checking, on page 69

Invalid Certificate Handling

The appliance can perform one of the following actions for invalid server certificates:

- **Drop.**
- **Decrypt.**
- **Monitor.**

Certificates that are Invalid for Multiple Reasons

For server certificates that are invalid due to both an unrecognized root authority and an expired certificate, the HTTPS proxy performs the action that applies to unrecognized root authorities.

In all other cases, for server certificates that are invalid for multiple reasons simultaneously, the HTTPS Proxy performs actions in order from the most restrictive action to the least restrictive action.

Untrusted Certificate Warnings for Decrypted Connections

When the Secure Web Appliance encounters an invalid certificate and is configured to decrypt the connection, AsyncOS creates an untrusted certificate that requires the end-user to accept or reject the connection. The common name of the certificate is “Untrusted Certificate Warning.”

Adding this untrusted certificate to the list of trusted certificates will remove the end user’s option to accept or reject the connection.

When AsyncOS generates one of these certificates, it creates a proxy log entry with the text “Signing untrusted key” or “Signing untrusted cert”.

Uploading a Root Certificate and Key

Before you begin

Enable the HTTPS Proxy. Enabling the HTTPS Proxy, on page 61.

Procedure

Step 1 **Security Services** > **HTTPS Proxy**.

Step 2 Click **Edit Settings**.

Step 3 Select **Use Uploaded Certificate and Key**.

Step 4 Click **Browse** for the Certificate field to navigate to the certificate file stored on the local machine.

If the file you upload contains multiple certificates or keys, the Web Proxy uses the first certificate or key in the file.

Step 5 Click **Browse** for the Key field to navigate to the private key file.

Note
The key length must be 512, 1024, or 2048 bits.

Step 6 Select **Key is Encrypted** if the key is encrypted.

Step 7 Click **Upload Files** to transfer the certificate and key files to the Secure Web Appliance.

The uploaded certificate information is displayed on the Edit HTTPS Proxy Settings page.

Step 8 (Optional) Click **Download Certificate** so you can transfer it to the client applications on the network.

Step 9 Submit and commit your changes.

Generating a Certificate and Key for the HTTPS Proxy

Before you begin

Enable the HTTPS Proxy. Enabling the HTTPS Proxy, on page 61.

Procedure

Step 1 **Security Services** > **HTTPS Proxy**.

Step 2 Click **Edit Settings**.

Step 3 Select **Use Generated Certificate and Key**.

Step 4 Click **Generate New Certificate and Key**.

Step 5 In the Generate Certificate and Key dialog box, enter the information to display in the root certificate.

You can enter any ASCII character except the forward slash (/) in the **Common Name** field.

Step 6 Click **Generate**.

Step 7 The generated certificate information is displayed on the Edit HTTPS Proxy Settings page.

Step 8 (Optional) Click **Download Certificate** so you can transfer it to the client applications on the network.

Step 9 (Optional) Click the **Download Certificate Signing Request** link. so you can submit the Certificate Signing Request (CSR) to a certificate authority (CA).

Step 10 (Optional) Upload the signed certificate to the Secure Web Appliance after receiving it back from the CA. You can do this at anytime after generating the certificate on the appliance.

Step 11 Submit and Commit Changes.

Configuring Invalid Certificate Handling

Before you begin

Verify that the HTTPS proxy is enabled as described in Enabling the HTTPS Proxy, on page 61.

Procedure

Step 1 **Security Services** > **HTTPS Proxy**.

Step 2 Click **Edit Settings**.

Step 3 For each type of certificate error, define the proxy response: **Drop**, **Decrypt**, or **Monitor**.

Certificate Error Type	Description
Expired	The current date falls outside of the range of validity for the certificate.
Mismatched hostname	The hostname in the certificate does not match the hostname the client was trying to access. **Note** The Web Proxy can only perform hostname match when it is deployed in explicit forward mode. When it is deployed in transparent mode, it does not know the hostname of the destination server (it only knows the IP address), so it cannot compare it to the hostname in the server certificate.
Unrecognized root authority/issuer	Either the root authority or an intermediate certificate authority is unrecognized.
Invalid signing certificate	There was a problem with the signing certificate.
Invalid leaf certificate	There was a problem with the leaf certificate, for example, a rejection, decoding, or mismatch problem.
All other error types	Most other error types are due to the appliance not being able to complete the SSL handshake with the HTTPS server. For more information about additional error scenarios for server certificates, see http://www.openssl.org/docs/apps/verify.html.

Step 4 Submit and Commit Changes.

Options for Certificate Revocation Status Checking

To determine whether the issuing certificate authority has revoked a certificate, the Secure Web Appliance can check with the issuing certificate authority in these ways:

- **Certificate Revocation List (Comodo certificates only).** The Secure Web Appliance checks Comodo's certificate revocation list. Comodo maintains this list, updating it according to their own policies. Depending on when it was last updated, the certificate revocation list may be out of date at the time the Secure Web Appliance checks it.
- **Online Certificate Status Protocol (OCSP).** The Secure Web Appliance checks the revocation status with the issuing certificate authority in real time. If the issuing certificate authority supports OCSP, the certificate will include a URL for real-time status checking. This feature is enabled by default for fresh installations and disabled by default for updates.

Note The Secure Web Appliance only performs the OCSP query for certificates that it determines to be valid in all other respects and that include the OCSP URL.

Related Topics

- Enabling Real-Time Revocation Status Checking, on page 70
- Configuring Invalid Certificate Handling, on page 68

Enabling Real-Time Revocation Status Checking

Before you begin

Ensure the HTTPS Proxy is enabled. See Enabling the HTTPS Proxy, on page 61.

Procedure

Step 1 **Security Services > HTTPS Proxy**.

Step 2 Click **Edit Settings**.

Step 3 Select **Enable Online Certificate Status Protocol (OCSP)**.

Step 4 Configure the **OCSP Result Handling** properties,

Cisco recommends configuring the OCSP Result Handling options to the same actions as Invalid Certificate Handling options. For example, if you set Expired Certificate to Monitor, configure Revoked Certificate to monitor.

Step 5 (Optional) Expand the Advanced configuration section and configure the settings described below.

Field Name	Description
OCSP Valid Response Cache Timeout	Time to wait before rechecking a valid OCSP response in seconds (s), minutes (m), hours (h), or days (d). Default unit is seconds. Valid range is from 1 second to 7 days.
OCSP Invalid Response Cache Timeout	Time to wait before rechecking an invalid OCSP response in seconds (s), minutes (m), hours (h), or days (d). Default unit is seconds. Valid range is from 1 second to 7 days.
OCSP Network Error Cache Timeout	Time to wait before attempting to contact the OCSP responder again after failing to get a response in seconds (s), minutes (m), hours (h), or days (d). Valid range from 1 second to 24 hours.
Allowed Clock Skew	Maximum allowed difference in time settings between the Secure Web Appliance and the OCSP responder in seconds (s) or minutes (m). Valid range from 1 second to 60 minutes.
Maximum Time to Wait for OCSP Response	Maximum time to wait for a response from the OCSP responder. Valid range is from 1 second to 10 minutes. Specify a shorter duration to reduce delays in end user access to HTTPS requests in the event that the OCSP responder is unavailable.
Use upstream proxy for OCSP checking	Group Name of the upstream proxies.

Field Name	Description
Servers exempt from upstream proxy	IP addresses or hostnames of the servers to exempt. May be left blank.

Step 6 Submit and Commit Changes.

Trusted Root Certificates

The Secure Web Appliance ships with and maintains a list of trusted root certificates. Web sites with trusted certificates do not require decryption.

You can manage the trusted certificate list, adding certificates to it and functionally removing certificates from it. While the Secure Web Appliance does not delete certificates from the primary list, it allows you to override trust in a certificate, which functionally removes the certificate from the trusted list.

Adding Certificates to the Trusted List

Before you begin

Verify that the HTTPS Proxy is enabled. See Enabling the HTTPS Proxy, on page 61.

Procedure

Step 1 **Security Services** > **HTTPS Proxy**.

Step 2 Click **Manage Trusted Root Certificates.**

Step 3 Click **Import**.

Step 4 Click **Browse** and navigate to the certificate file.

Step 5 **Submit** and **Commit** Changes.

Look for the certificate you uploaded in the **Custom Trusted Root Certificates** list.

Removing Certificates from the Trusted List

Procedure

Step 1 Select **Security Services** > **HTTPS Proxy**.

Step 2 Click **Manage Trusted Root Certificates.**

Step 3 Select the **Override Trust** checkbox corresponding to the certificate you wish to remove from the list.

Step 4 **Submit** and **Commit** Changes.

Routing HTTPS Traffic

The ability of AsyncOS to route HTTPS transactions based on information stored in client headers is limited and is different for transparent and explicit HTTPS.

Option	Description
Transparent HTTPS	In the case of transparent HTTPS, AsyncOS does not have access to information in the client headers. Therefore, AsyncOS cannot enforce routing policies if any routing policy or identification profile relies on the information in client headers.
Explicit HTTPS	In the case of explicit HTTPS, AsyncOS has access to the following information in client headers: • URL • Destination port number Therefore, for explicit HTTPS transactions, it is possible to match a routing policy based on URL or port number.

Troubleshooting Decryption/HTTPS/Certificates

- Accessing HTTPS Sites Using Routing Policies with URL Category Criteria
- HTTPS with IP-based Surrogates and Transparent Requests
- Bypassing Decryption for Particular Websites
- Alert: Problem with Security Certificate

Create Policies to Control Internet Requests

This topic contains the following sections:

- Overview of Policies: Control Intercepted Internet Requests, on page 73
- Managing Web Requests Through Policies Task Overview, on page 74
- Managing Web Requests Through Policies Best Practices, on page 75
- Policies, on page 75
- Policy Configuration, on page 84
- Block, Allow, or Redirect Transaction Requests, on page 90
- Client Applications, on page 91
- Time Ranges and Quotas, on page 93
- Access Control by URL Category, on page 96
- Remote Users, on page 98
- Troubleshooting Policies, on page 101

Overview of Policies: Control Intercepted Internet Requests

When the user creates a web request the configured Secure Web Appliance intercepts the requests and manages the process of which the request travels to get to its final outcome, be that accessing a particular web site, an email or even accessing an online application. In configuring the Secure Web Appliance policies are created to define the criteria and actions of requests made by the user.

Policies are the means by which the Secure Web Appliance identifies and controls web requests. When a client sends a web request to a server, the Web Proxy receives the request, evaluates it, and determines to which policy it belongs. Actions defined in the policy are then applied to the request.

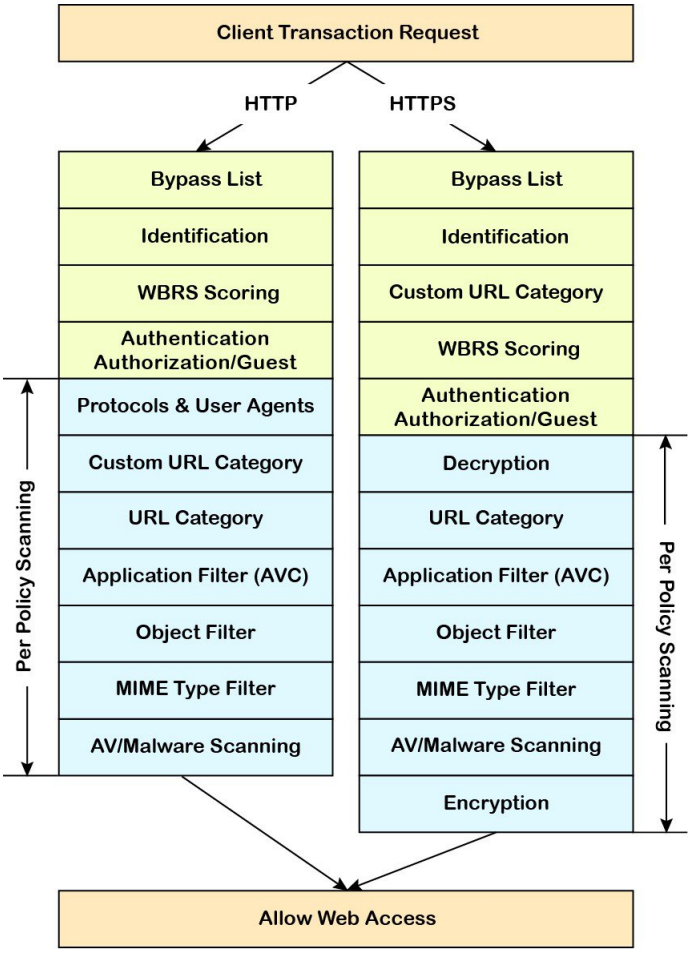
The Secure Web Appliance uses multiple policy types to manage different aspects of web requests. Policy types might fully manage transactions by themselves or pass transactions along to other policy types for additional processing. Policy types can be groups by the functions they perform, such as access, routing, or security.

AsyncOS evaluates transactions based on policies before it evaluates external dependencies to avoid unnecessary external communication from the appliance. For example, if a transaction is blocked based on a policy that blocks uncategorized URLs, the transaction will not fail based on a DNS error.

Intercepted HTTP/HTTPS Request Processing

The following diagram depicts the flow of an intercepted Web request as it is processed by the appliance.

Figure 6: HTTP/HTTPS Transaction Flow



Also see the following diagrams depicting various transaction processing flows:

- Figure 1: Identification Profiles and Authentication Processing – No Surrogates and IP-based Surrogates, on page 9
- Figure 2: Identification Profiles and Authentication Processing – Cookie-based Surrogates, on page 10
- Figure 7: Policy Group Transaction Flow for Access Policies, on page 78
- Figure 4: Policy Group Transaction Flow for Decryption Policies, on page 61
- Controlling HTTPS Traffic, on page 63

Managing Web Requests Through Policies Task Overview

Step	Task List for Managing Web Requests through Policies	Links to Related Topics and Procedures
1	Set up and sequence Authentication Realms	Authentication Realms

Step	Task List for Managing Web Requests through Policies	Links to Related Topics and Procedures
2	(For upstream proxies) Create a proxy group.	Creating Proxy Groups for Upstream Proxies
2	(Optional) Create Custom Client Applications	Client Applications, on page 91
3	(Optional) Create Custom URL Categories	Creating and Editing Custom URL Categories, on page 28
4	Create Identification Profiles	Classifying Users and Client Software, on page 3
5	(Optional) Create time ranges to Limit Access by Time of Day	Time Ranges and Quotas, on page 93
6	Create and Order Policies	• Creating a Policy , on page 79 • Policy Order, on page 78

Managing Web Requests Through Policies Best Practices

If you want to use Active Directory user objects to manage web requests, do not use primary groups as criteria. Active Directory user objects do not contain the primary group.

Policies

- Policy Types, on page 75
- Policy Order, on page 78
- Creating a Policy , on page 79

Policy Types

Policy Type	Request Type	Description	Link to task
Access	• HTTP • Decrypted HTTPS • FTP	Block, allow or redirect inbound HTTP, FTP, and decrypted HTTPS traffic. Access policies also manage inbound encrypted HTTPS traffic if the HTTPS proxy is disabled.	Creating a Policy , on page 79
SOCKS	• SOCKS	Allow or block SOCKS communication requests.	Creating a Policy , on page 79

Policy Type	Request Type	Description	Link to task
Application Authentication	• application	Allow or deny access to a Software as a Service (SaaS) application. Use single sign-on to authenticate users and increase security by allowing access to applications to be quickly disabled. To use the single sign-on feature of policies you must configure the Secure Web Appliance as an identity provider and upload or generate a certificate and key for SaaS.	Creating SaaS Application Authentication Policies, on page 104
Encrypted HTTPS Management	• HTTPS	Decrypt, pass through, or drop HTTPS connections. AsyncOS passes decrypted traffic to Access policies for further processing.	Creating a Policy , on page 79
Data Security	• HTTP • Decrypted HTTPS • FTP	Manage data uploads to the web. Data Security policies scan outbound traffic to ensure it complies to company rules for data uploads, based on its destination and content. Unlike External DLP policies, which redirect outbound traffic to external servers for scanning, Data Security policies use the Secure Web Appliance to scan and evaluate traffic.	Creating a Policy , on page 79
External DLP (Data Loss Prevention)	• HTTP • Decrypted HTTPS • FTP	Send outbound traffic to servers running 3rd-party DLP systems, which scan it for adherence to company rules for data uploads. Unlike Data Security policies, which also manage data uploads, External DLP policies move scanning work away from the Secure Web Appliance, which frees resources on the appliance and leverages any additional functionality offered by 3rd-party software.	Creating a Policy , on page 79
Outbound Malware Scanning	• HTTP • Decrypted HTTPS • FTP	Block, monitor, or allow requests to upload data that may contain malicious data. Prevent malware that is already present on your network from being transmitted to external networks.	Creating a Policy , on page 79

Policy Type	Request Type	Description	Link to task
Routing	• HTTP • HTTPS • FTP	Direct web traffic through upstream proxies or direct it to destination servers. You might want to redirect traffic through upstream proxies to preserve your existing network design, to off-load processing from the Secure Web Appliance, or to leverage additional functionality provided by 3rd-party proxy systems. If multiple upstream proxies are available, the Secure Web Appliance can use load balancing techniques to distribute data to them. Retian the client's source IP address, change it to the web proxy IP, or a custom IP using IP Spooing profile.	Creating a Policy , on page 79

Each policy type uses a policy table to store and manage its policies. Each policy table comes with a predefined, global policy, which maintains default actions for a policy type. Additional, user-defined policies are created and added to the policy table as required. Policies are processed in the order in which they are listed in the policy table.

Individual policies define the user-request types they manage, and the actions they perform on those requests. Each policy definition has two main sections:

- **Identification Profiles and Users** – Identification Profiles are used in policy membership criteria and are particularly important as they contain many options for identifying web transaction. They also share many properties with policies.
- **Advanced** – The criteria used to identify users to which the policy applies. One or more criteria can be specified in a policy, and all must be match for the criteria to be met.
  - **Protocols** – Allow the transfer of data between various networking devices such as http, https, ftp, etc.
  - **Proxy Ports** – the numbered port by which the request accesses the web proxy,
  - **Subnets** – The logical grouping of connected network devices (such as geographic location or Local Area Network [LAN]), where the request originated
  - **Time Range** – Time ranges can be created for use in policies to identify or apply actions to web requests based on the time or day the requests were made. The time ranges are created as individual units.
  - **URL Categories** – URL categories are predefined or custom categories of websites, such as News, Business, Social Media, etc. These can be used to identify or apply actions to web requests.
  - **User Agents** – These are the client applications (such as updaters and Web browsers) used to make requests. You can define policy criteria based on user agents, and you can specify control settings based on user agents. You can also exempt user agents from authentication, which is useful for applications that cannot prompt for credentials. You can define custom user agents but cannot re-use these definitions other policies.

Note When you define multiple membership criteria, the client request must meet all criteria to match the policy.

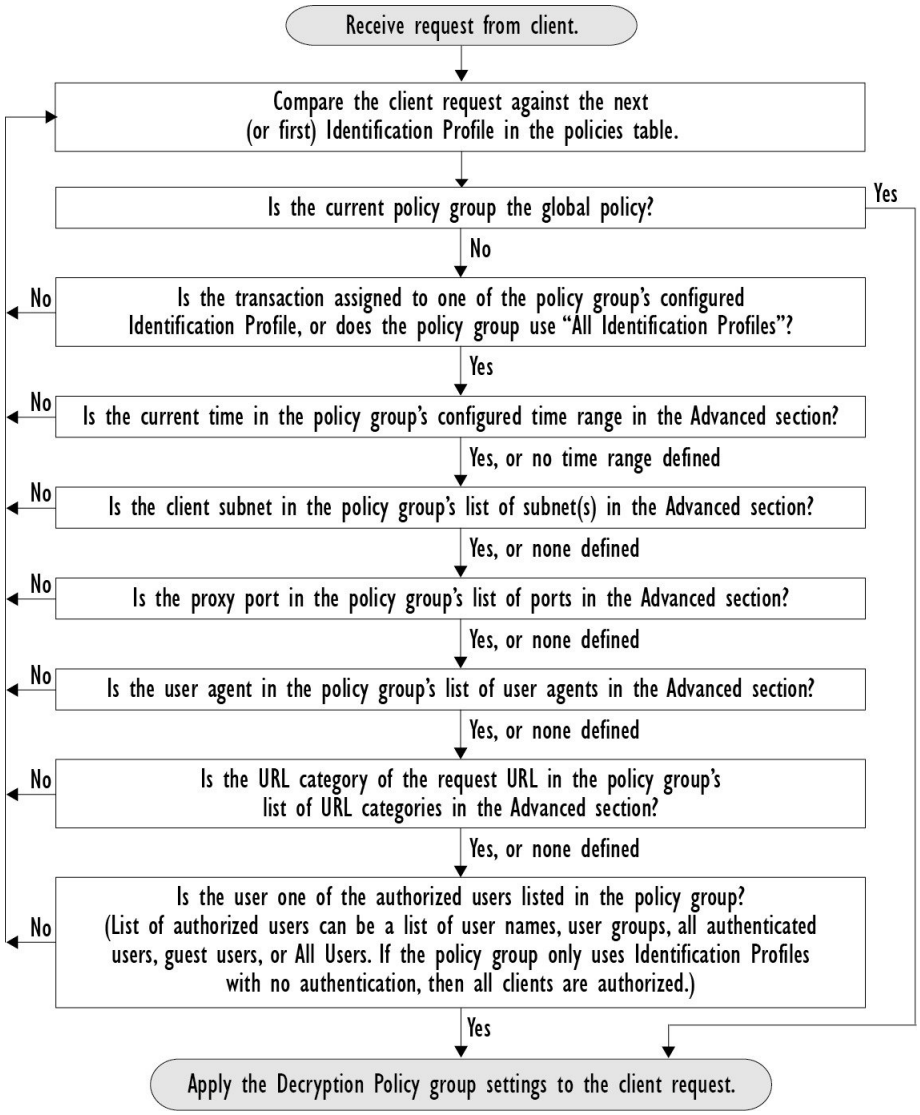
Policy Order

The order in which policies are listed in a policy table determines the priority with which they are applied to Web requests. Web requests are checked against policies beginning at the top of the table and ending at the first policy matched. Any policies below that point in the table are not processed.

If no user-defined policy is matched against a Web request, then the global policy for that policy type is applied. Global policies are always positioned last in Policy tables and cannot be re-ordered.

The following diagram depicts the flow of a client request through the Access policies table.

Figure 7: Policy Group Transaction Flow for Access Policies



Creating a Policy

Before you begin

- Enable the appropriate proxy:
  - Web Proxy (for HTTP, decrypted HTTPS, and FTP)
  - HTTPS Proxy
  - SOCKS Proxy
- Create associated Identification Profiles.
- Understand Policy Order, on page 78.
- (Encrypted HTTPS only) Upload or generate a Certificate and Key.
- (Data Security only) Enable Cisco Data Security Filters Settings.
- (External DLP only) Define an External DLP server.
- (Routing only) Define the associated upstream proxy on the Secure Web Appliance.
- (Optional) Create associated client applications.
- (Optional) Create associated time ranges. See Time Ranges and Quotas, on page 93.
- (Optional) Create associated URL categories. See Creating and Editing Custom URL Categories, on page 28.

Procedure

Step 1 In the **Policy Settings** section, use the **Enable Identity** check box to enable this policy, or to quickly disable it without deleting it.

Step 2 Assign a unique policy **Name**.

Step 3 A **Description** is optional.

Step 4 From the Insert Above drop-down list, choose where this policy is to appear in the table.

Note
Arrange policies such that, from top to bottom of the table, they are in most-restrictive to least-restrictive order. See Policy Order, on page 78 for more information.

Step 5 In the **Policy Expires** area, check the **Set Expiration for Policy** check box to set the expiry time for the policy. Enter the date and time for the policy expiration that you want to set. The policies are automatically disabled once they exceed the set expiry time.

Note
System checks the policies every minute to disable the policies which get expired during the minute. For example, if a policy is set to expire at 11:00, at maximum it will be disabled by 11:01.

Policy Expiry feature is applicable only for Access, Decryption, and Web Traffic Tap policies.

You will receive an email prior to three days of the policy expiry and another one upon policy expiry.

Note
To receive alerts, you must enable Policy Expiration alerts using **System Administration** > **Alerts** . See Policy Expiration Alerts

You can set the policy expiration time through Cisco Content Security Management Appliances as well. The policies will get expired after the set expiry time but will not be shown as disabled in the Cisco Content Security Management Appliances GUI.

Once you set the policy expiration feature, the expiry happens based on the appliance's local time settings.

Step 6 In the **Policy Member Definition** section, specify how user and group membership is defined: from the Identification Profiles and Users list, choose one of the following:

- **All Identification Profiles** – This policy will apply to all existing profiles. You must also define at least one **Advanced** option.
- **Select One or More Identification Profiles** – A table for specifying individual Identification Profiles appears, one profile-membership definition per row.

Step 7 If you chose **All Identification Profile**s:

a) Specify the authorized users and groups to which this policy applies by selecting one of the following options:

- **All Authenticated Users** – All users identified through authentication or transparent identification.
- **Selected Groups and Users** – Specified users and groups are used.

  To add or edit the specified **ISE Secure Group Tags** (SGTs) and the specified Users, click the link following the appropriate label. For example, click the list of currently specified users to edit that list. See Adding and Editing Secure Group Tags for a Policy, on page 82 for more information.

  If you use ISE, you can add or edit ISE Secure Group Tags. This is not supported in ISE-PIC deployments. To add or edit the specified **ISE Groups**, click the link following the label. This option is specific to ISE-PIC.
- **Guests** – Users connected as guests and those failing authentication.
- **All Users** – All clients, whether authenticated or not. If this option is selected, at least one **Advanced** option also must be provided.

Step 8 If you chose **Select One or More Identification Profiles**, a profile-selection table appears.

a) Choose an Identification Profile from the Select Identification Profile drop-down list in the Identification Profiles column.

b) Specify the Authorized Users and Groups to which this policy applies:

- **All Authenticated Users** – All users identified through authentication or transparent identification.
- **Selected Groups and Users** – Specified users and groups are used.

  To add or edit the specified ISE Secure Group Tags (SGTs) and the specified Users, click the link following the appropriate label. For example, click the list of currently specified users to edit that list. See Adding and Editing Secure Group Tags for a Policy, on page 82 for more information.
- **Guests** – Users connected as guests and those failing authentication.

c) To add a row to the profile-selection table, click **Add Identification Profile**. To delete a row, click the trash-can icon in that row.

Repeat steps (a) through (c) as necessary to add all desired Identification Profiles.

Step 9 Expand the **Advanced** section to define additional group membership criteria. (This step may be optional depending on selection in the **Policy Member Definition** section. Also, some of the following options will not be available, depending on the type of policy you are configuring.) .

Advanced Option	Description
Protocols	Select the protocols to which this policy will apply. **All others** means any protocol not selected. If the associated identification profile applies to specific protocols, this policy applies to those same protocols
Proxy Ports	Applies this policy only to traffic using specific ports to access the web proxy. Enter one or more port numbers, separating 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. **Note** If the associated identification profile applies only to specific proxy ports, you cannot enter proxy ports here.
Subnets	Applies this policy only to traffic on specific subnets. Select **Specify subnets** and enter the specific subnets, separated by commas. Leave **Use subnets from selected Identities** selected if you do not want additional filtering by subnet. **Note** If the associated identity applies to specific subnets, you can further restrict the application of this policy to a subset of the addresses to which the identity applies.
Time Range	You can apply time ranges for policy membership: • Time Range – Choose a previously defined time range (Time Ranges and Quotas, on page 93). • Match Time Range – Use this option to indicate whether this time range is inclusive or exclusive. In other words, whether to match only during the range specified, or at all times except those in the specified range.
URL Categories	You can restrict policy membership by specific destinations (URLs) and by categories of URLs. Select all desired custom and predefined categories. See Creating and Editing Custom URL Categories, on page 28 for information about custom categories.

Advanced Option	Description

User Agents	You can select specific user agents, and define custom agents using regular expressions, as part of membership definition for this policy.
	• **Common User Agents**
	  • **Browsers** – Expand this section to select various Web browsers.
	  • **Others** – Expand this section to select specific non-browser agents such as application updaters.
	• **Custom User Agents** – You can enter one or more regular expressions, one per line, to define custom user agents.
	• **Match User Agents** – Use this option to indicate whether these user-agent specifications are inclusive or exclusive. In other words, whether membership definition includes only the selected user agents, or specifically excludes the selected user agents.

Adding and Editing Secure Group Tags for a Policy

To change the list of Secure Group Tags (SGTs) assigned to a particular Identification Profile in a policy, click the link following the ISE Secure Group Tags label in the Selected Groups and Users list on the Add/Edit Policy page. (See Creating a Policy , on page 79.) This link is either "No tags entered," or it is a list of currently assigned tags. The link opens the Add/Edit Secure Group Tags page.

All SGTs currently assigned to this policy are listed in the Authorized Secure Group Tags section. All SGTs available from the connected ISE server are listed in the Secure Group Tag Search section.

Procedure

Step 1 To add one or more SGTs to the Authorized Secure Group Tags list, select the desired entries in the Secure Group Tag Search section, and then click **Add**.

Note

- The SGTs already added, are highlighted in green. To quickly find a specific SGT in the list of those available, enter a text string in the **Search** field.
- When a Secure Web Appliance is connected to ISE/ISE-PIC, default SGTs from ISE/ISE-PIC are also displayed. These SGTs will not have users assigned. Ensure that you select the correct SGTs.

Step 2 To remove one or more SGTs from the Authorized Secure Group Tags list, select those entries and then click **Delete**.

Step 3 Click Done to return to the Add/Edit Group page.

What to do next

Related Topics

- Time Ranges and Quotas, on page 93
- Using Client Applications in Policies, on page 92

Adding Routing Destination and IP Spoofing Profile to Routing Policy

You can configure how the web proxy forwards the web traffic and the requests the source IP address by configuring the routing destination and IP spoofing profile in routing policies.

Note

- The global routing policy is enabled by default even if an upstream proxy group is not configured on the appliance.
- IP spoofing profiles are not related to routing destination, and can be configured independently.
- Routing Policy can be enabled without configuring an upstream proxy.

Note To configure an upstream proxy group for a routing policy in Security Management appliance, save the configuration file of the Secure Web Appliance and import it on the Security Management appliance. Otherwise, the Security Management appliance shows the upstream proxy as "Not Found" and the routing policy will be disabled after the config push.

Procedure

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

Step 2 On the **Routing Policies** page, click the link under **Routing Destination** column for the routing policy that you want to configure the upstream proxy group.

Step 3 Choose an appropriate upstream proxy group for the selected policy from the following:

Action	Description
Use Global Policy Settings	The web proxy uses the settings defined in the Global Policy. This is the default action for user defined policy groups. By default, the routing destination for Global Routing Policy is set as **Direct Connection**. Applies to user defined policy groups only.
Direct Connection	The web proxy forwards web traffic directly to its destination web server.
Custom upstream proxy group	The web proxy redirects the web traffic to an external upstream proxy group. For more information about creating upstream proxy groups, see Upstream Proxies.

Step 4 On the **Routing Policies** page, click the link under **IP Spoofing** column for the routing policy that you want to configure the IP spofing profile.

Step 5 Choose an appropriate IP spoofing profile for the selected policy from the following:

Action	Description
Use Global Policy Settings	The web proxy uses the settings defined in the Global Policy. This is the default action for user defined policy groups. By default, the IP spoofing is disabled for the Global Routing Policy. Applies to user defined policy groups only.
Do No Use IP Spoofing	The web proxy changes the request source IP address to match its own address to increase security.
Use Client IP	The web proxy retains the source address so that it appears to originate from the source client rather than from the Secure Web Appliance.
Custom spoofing profile name	The web proxy changes the request source IP address to custom IP defined in the selected custom IP spoofing profile name.

Step 6 **Submit** and **Commit** your changes.

What to do next

Related Topics

- Upstream Proxies
- Web Proxy IP Spoofing

Policy Configuration

Each row in a table of policies represents a policy definition, and each column displays current contains a link to a configuration page for that element of the policy.

Note Of the following policy-configuration components, you can specify the "Warn" option only with URL Filtering.

Option	Description
Protocols and User Agents	Used to control policy access to protocols and configure blocking for particular client applications, such as instant messaging clients, web browsers, and Internet phone services. You can also configure the appliance to tunnel HTTP CONNECT requests on specific ports. With tunneling enabled, the appliance passes HTTP traffic through specified ports without evaluating it.

Option	Description
URL Filtering	AsyncOS for Web allows you to configure how the appliance handles a transaction based on the URL category of a particular HTTP or HTTPS request. Using a predefined category list, you can choose to block, monitor, warn, or set quota-based or time-based filters. You can also create custom URL categories and then choose to block, redirect, allow, monitor, warn, or apply quota-based or time-based filters for Websites in the custom categories. See Creating and Editing Custom URL Categories, on page 28 for information about creating custom URL categories. In addition, you can add exceptions to blocking of embedded or referred content.
Applications	The AVC or ADC engine is an acceptable use policy component which inspects web traffic to gain deeper understanding and control of web traffic used for applications. You can configure the web proxy to be configured to block or allow application based on the application types, and by individual applications. Starting with AsyncOS 15.0, you can use either AVC or ADC engine to monitor web traffic. By default, AVC is enabled. While the AVC engine operates the same as ADC, the AVC engine supports a limited number of applications. In AVC you can also apply controls to particular application behaviors, such as, file transfer within a particular application. See Managing Access to Web Applications for configuration information **Note** In the post-configuration of ADC activities, the ADC application engine searches or evalutes for the activity information for a particular traffic. Due to the ADC signature database update, even if the entire category is set to *Block*, any new applications added will be set to *Monitor* by default.
Objects	These options let you configure the Web Proxy to block file downloads based on file characteristics, such as file size, file type, and MIME type. An object is, generally, any item that can be individually selected, uploaded, downloaded and manipulated. See Access Policies: Blocking Objects, on page 86 for information about specifying blocked objects.
Anti-Malware and Reputation	Web reputation filters allow for a web-based reputation score to be assigned to a URL to determine the probability of it containing URL-based malware. Anti-malware scanning identifies and stops web-based malware threats. Advanced Malware Protection identifies malware in downloaded files. The Anti-Malware and Reputation policy inherits global settings respective to each component. Within **Security Services** > **Anti-Malware and Reputation**, malware categories can be customized to monitor or block based on malware scanning verdicts and web reputation score thresholds can be customized. Malware categories can be further customized within a policy. There are also global settings for file reputation and analysis services. For more information, see Anti-Malware and Reputation Settings in Access Policies and Configuring File Reputation and Analysis Features.

Option	Description
HTTP ReWrite Profile	You can configure custom header profiles for HTTP requests and can create multiple headers under a header rewrite profile. The header rewrite profile feature enables the appliance to pass the user and group information to another upstream device after successful authentication. The upstream proxy considers the user as authenticated, bypasses further authentication, and provides access to the user based on the defined access policies. See Web Proxy Custom Headers Per Policy.
Clone Policy	If an existing policy has most of the settings that you want in a new policy, you can save time by cloning the existing policy and then modifying it. Although the cloned policy shares the same grouping attributes, it has its own unique identity, such as the display name, IP address, host, and domain name. The following policies with cloning option in Secure Web Appliance can also be managed by Cisco Secure Email and Web Manager (SMA). • Access • Decryption • Identification • Routing • External DLP • Outbound Malware Scanning • HTTP ReWrite Profile • Cisco Data Security **Note** You can clone only one policy at an instance.
Delete	Deletes the created policy.

Access Policies: Blocking Objects

You can use the options on the Access Policies: Objects page to block file downloads based on file characteristics, such as file size, file type, and MIME type. An object is, generally, any item that can be individually selected, uploaded, downloaded and manipulated.

You can specify a number of types of objects to be blocked by each individual Access policy, and by the Global policy. These object types include Archives, Document Types, Executable Code, Web Page Content, and so on.

Procedure

Step 1 On the Access Policies page (**Web Security Manager** > **Access Policies**), click the link in the **Objects** column of the row representing the policy you wish to edit.

Step 2 Choose the desired type of object blocking for this Access policy:

- **Use Global Policy Objects Blocking Settings** – This policy uses the object-blocking settings defined for the Global Policy; these settings are displayed in read-only mode. Edit the settings for the Global Policy to change them.
- **Define Custom Objects Blocking Settings** – You can edit all object-blocking settings for this policy.
- **Disable Object Blocking for this Policy** – Object blocking is disabled for this policy; no object-blocking options are presented.

Step 3 If you chose **Define Custom Objects Blocking Settings** in the previous step, select and deselect object-blocking options on the Access Policies: Objects page as needed.

Object Size	You can block objects based on their download size: • **HTTP/HTTPS Max Download Size** – Either provide the maximum object size for HTTP/HTTPS download (objects larger than this will be blocked), or indicate that there is no maximum size for object download via HTTP/HTTPS. • **FTP Max Download Size** – Either provide the maximum object size for FTP download (objects larger than this will be blocked), or indicate that there is no maximum size for object download via FTP.
Block Object Type	
Archives	Expand this section to select types of Archive files that are to be blocked. This list includes Archive types such as ARC, BinHex, and StuffIt.

Inspectable Archives	Expand this section to select whether to **Allow**, **Block**, or **Inspect** specific types of Inspectable Archive files. Inspectable Archives are archive or compressed files that the Secure Web Appliance can inflate to inspect each of the contained files in order to apply the file-type block policy. The Inspectable Archives list includes archive types such as 7zip, Microsoft CAB, RAR, and TAR.
	
	The following points apply to archive inspection:
	
	• Only archive types marked **Inspect** will be inflated and inspected.
	
	• Only one archive will be inspected at a time, Additional concurrent inspectable archives may not be inspected.
	
	• If an inspected archive contains a file type that is assigned the Block action by the current policy, the entire archive will be blocked, regardless of any allowed file types it may contain.
	
	• An inspected archive that contains an unsupported archive type will be marked as "unscannable." If it contains a blocked archive type, it will be blocked.
	
	• Password-protected and encrypted archives are not supported and will be marked as "unscannable."
	
	• An inspectable archive which is incomplete or corrupt is marked as "unscannable."
	
	• The **DVS Engine Object Scanning Limits** value specified for the **Anti-Malware and Reputation** global settings also applies to the size of an inspectable archive; an object exceeding this size is marked as "unscannable." See Enabling Anti-Malware and Reputation Filters for information about this object size limit.
	
	• An inspectable archive marked as "unscannable" can be either Blocked in its entirety or Allowed in its entirety.
	
	• When access policies are configured to block custom MIME types, and archive inspection is enabled:
	
	  • If the appliance directly downloads a file with the custom MIME type as part of the content-type header, access is blocked.
	
	  • If the same file is part of a ZIP/archive file, the appliance inspects the archive and determines the MIME type based on its own MIME evaluation. If the MIME evaluated by the appliance's engine does not match the configured custom MIME type, the content is not blocked.
	
	• The appliance can inspect configured archives but it has the limitation to inspect certain archives such as RAR and 7-Zip.
	
	See Archive Inspection Settings, on page 89 for information about configuring archive inspection.

Document Types	Expand this section to select types of text documents to be blocked. This list includes document types such as FrameMaker, Microsoft Office, and PDF.
Executable Code	Expand this section to select types of executable code to be blocked. The list includes Java Applet, UNIX Executable and Windows Executable.

Installers	Types of installers to be blocked; the list includes UNIX/LINUX Packages.
Media	Types of media files to be blocked. The list includes Audio, Video and Photographic Image Processing Formats (TIFF/PSD).
P2P Metafiles	This list includes BitTorrent Links (`.torrent`).
Web Page Content	This list includes Flash and Images.
Miscellaneous	This list includes Calendar Data.
Custom MIME Types	You can define additional objects/files to be blocked based on MIME type. Enter one or more MIME types in the **Block Custom MIME Types** field, one per line.

Step 4 Click **Submit**.

Archive Inspection Settings

You can Allow, Block, or Inspect specific types of Inspectable Archives for individual Access policies. Inspectable Archives are archive or compressed files that the Secure Web Appliance can inflate to inspect each of the contained files in order to apply the file-type block policy. See Access Policies: Blocking Objects, on page 86 for more information about configuring archive inspection for individual Access policies.

Note During archive inspection, nested objects are written to disk for examination. The amount of disk space that can be occupied at any given time during file inspection is 1 GB. Any archive file exceeding this maximum disk-use size will be marked unscannable.

The Secure Web Appliance's Acceptable Use Controls page provides system-wide Inspectable Archives Settings; that is, these settings apply to archive extraction and inspection whenever enabled in an Access policy.

Procedure

Step 1 Choose **Security Services** > **Acceptable Use Controls**.

Step 2 Click the **Edit Archives Settings** button.

Step 3 Edit the Inspectable Archives Settings as needed.

- **Maximum Encapsulated Archive Extractions** – Maximum number of "encapsulated" archives to be extracted and inspected. That is, maximum depth to inspect an archive containing other inspectable archives. An encapsulated archive is one that is contained in another archive file. This value can be zero through five; depth count begins at one with the first nested file.

  The external archive is considered file zero. If the archive has files nested beyond this maximum nested value, the archive is marked as unscannable. Note that this will impact performance.

- **Block Uninspectable Archives** – If checked, the Secure Web Appliance will block archives it failed to inflate and inspect.

Step 4 **Submit** and **Commit Changes**.

Block, Allow, or Redirect Transaction Requests

The web proxy controls web traffic based on the policies that you create for groups of transaction requests.

- **Allow.** The Web Proxy permits the connection without interruption. Allowed connections may not have been scanned by the DVS engine.
- **Block.** The Web Proxy does not permit the connection and instead displays an end user notification page explaining the reason for the block.
- **Redirect.** The Web Proxy does not allow the connection to the originally requested destination server and instead connects to a different specified URL, see Redirecting Traffic in the Access Policies, on page 36.



Note The preceding actions are final actions that the Web Proxy takes on a client request. The Monitor action that you can configure for Access Policies is not a final action.

Generally, different types of policies control traffic based on the transport protocol.

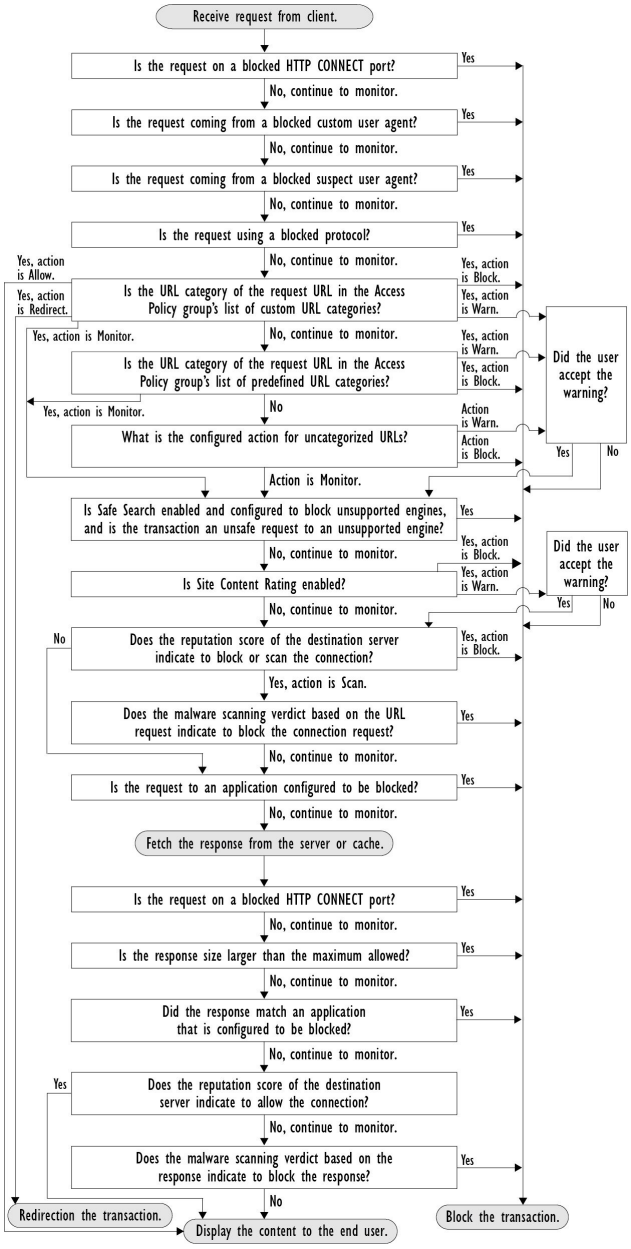
Policy Type	Protocols				Actions Supported			
	HTTP	HTTPS	FTP	SOCKS	Block	Allow	Redirect	Monitor
Access	x	x	x		x	x	x	x
SOCKS				x	x	x		
SAAS	x	x						
Decryption	x	x						x
Data Security	x	x	x		x			x
External DLP	x	x	x				x	
Outbound Malware Scanning	x	x	x		x			x
Routing	x	x	x				x	



Note Decryption policy takes precedence over Access policy.

The following diagram shows how the Web Proxy determines which action to take on a request after it has assigned a particular Access Policy to the request. The Web reputation score of the destination server is evaluated only once, but the result is applied at two different points in the decision flow.

Figure 8: Applying Access Policy Actions



Client Applications

About Client Applications

Client Applications (such as a web browser) are used to make requests. You can define policy membership based on client applications, and you can specify control settings and exempt client applications from authentication, which is useful for applications that cannot prompt for credentials.

Using Client Applications in Policies

Defining Policy Membership Using Client Applications

Procedure

Step 1 Choose a policy type from the Web Security Manager menu.

Step 2 Click a policy name in the policies table.

Step 3 Expand the Advanced section and click the link in the Client Applications field.

Step 4 Define one or more of the client applications:

Option	Method
Choose a predefined client application	Expand the Browser and Other sections and check the required client application check boxes. **Tip** Choose only the Any Version options when possible, as this provides better performance than having multiple selections.
Define a custom client application	Enter an appropriate regular expression in the Custom Client Applications field. Enter additional regular expressions on new lines as required. **Tip** Click **Example Client Applications Patterns** for examples of regular expressions.

Step 5 (Optional) Click the Match All Except The Selected **Client Applications** Definitions radio button to base the policy membership on all client applications **except** those you have defined.

Step 6 Click **Done**.

Defining Policy Control Settings Using Client Applications

Procedure

Step 1 Choose a policy type from the Web Security Manager menu.

Step 2 Find the required policy name in the policies table.

Step 3 Click the cell link in the Protocols and Client Applications column on the same row.

Step 4 Choose **Define Custom Settings** from the drop-down list in the Edit Protocols and Client Applications Settings pane (if not already set).

Step 5 Enter a regular expression in the Custom Client Applications field that matches the client application you wish to define. Enter additional regular expressions on new lines as required.

Tip
Click **Example Client Application Patterns** for examples of regular expressions.

Step 6 Submit and commit your changes.

Exempting Client Applications from Authentication

Procedure

	Command or Action	Purpose
Step 1	Create an Identification Profile that does not require authentication.	Classifying Users and Client Software, on page 3
Step 2	Set the Identification Profile membership as the client application to exempt.	Using Client Applications in Policies, on page 92
Step 3	Place the Identification Profile above all other Identification Profiles in the policies table that require authentication.	Policy Order, on page 78

Time Ranges and Quotas

You can apply time ranges and time and volume quotas to access policies and decryption policies to restrict when a user has access, as well as their maximum connection time or data volume (also referred to as a "bandwidth quota").

- Time Ranges for Policies and Acceptable Use Controls, on page 93
- Time and Volume Quotas, on page 94

Time Ranges for Policies and Acceptable Use Controls

Time ranges are defined periods of time during which policies and acceptable use controls apply.

Note You cannot use time ranges to define the times at which users must authenticate. Authentication requirements are defined in Identification Profiles, which do not support time ranges.

- Creating a Time Range, on page 93

Creating a Time Range

Procedure

Step 1 Choose **Web Security Manager** > **Define Time Ranges and Quotas**.

Step 2 Click **Add Time Range**.

Step 3 Enter a name for the time range.

Step 4 Choose a **Time Zone** option:

- Use **Time Zone Setting From Appliance** – Use the same time zone as the Secure Web Appliance.

- **Specify Time Zone for this Time Range** – Define a different time zone, either as a GMT Offset, or as a region, country and a specific time zone in that country.

Step 5 Check one or more **Day of Week** check boxes.

Step 6 Select a **Time of Day** option:

- **All Day** – Use the full 24-hour period.
- **From** and **To** – Define a specific range of hours: enter a start time and end time in HH:MM (24-hour format).

Tip
Each time range defines a start time and an end-time boundary. For example, entering 8:00 through 17:00 matches 8:00:00 through 16:59:59, but not 17:00:00. Midnight must be specified as 00:00 for a start time, and as 24:00 for an end time.

Step 7 Submit and commit your changes.

Time and Volume Quotas

Quotas allow individual users to continue accessing an Internet resource (or a class of Internet resources) until they exhaust the data volume or time limit imposed. AsyncOS enforces defined quotas on HTTP, HTTPS and FTP traffic.

As a user approaches either their time or volume quota, AsyncOS displays first a warning, and then a block page.

Please note the following regarding use of time and volume quotas:

- If AsyncOS is deployed in transparent mode and HTTPS proxy is disabled, there is no listening on port 443, and requests are dropped. This is standard behavior. If AsyncOS is deployed in explicit mode, you can set quotas in your access policies.

  When HTTPS proxy is enabled, possible actions on a request are pass-through, decrypt, drop, or monitor. Overall, quotas in decryption policies are applicable only to the pass-through categories.

  With pass-through, you will also have the option to set quotas for tunnel traffic. With decrypt, this option is not available, as the quotas configured in the access policy will be applied to decrypted traffic.

- If URL Filtering is disabled or if its feature key is unavailable, AsyncOS cannot identify the category of a URL, and the **Access Policy** > **URL Filtering** page is disabled. Thus, the feature key needs to be present, and Acceptable Use Policies enabled, to configure quotas..
- Many websites such as Facebook and Gmail auto-update at frequent intervals. If such a website is left open in an unused browser window or tab, it will continue to consume the user's quota of time and volume.
- When you restart the proxy and the high-performance mode is:
  - **Enabled** - Time and volume quotas are not reset. Quotas are automatically reset once within the 24-hour window based on the configured time.
  - **Disabled** - Time and volume quotas are reset. The reset impact remains only for the current 24-hour window as the quotas are automatically reset once within 24 hours. Proxy may restart due to configuration changes or proxy process crash.
- Your EUN pages (both warning and block) cannot be displayed for HTTPS even when decrypt-for-EUN option is enabled.

Note The most restrictive quota will always apply when more than one quota applies to any given user.

- Volume Quota Calculations, on page 95
- Time Quota Calculations, on page 95
- Defining Time, Volume, and Bandwidth Quotas, on page 95

Volume Quota Calculations

Calculation of volume quotas is as follows:

- HTTP and decrypted HTTPS traffic – The HTTP request and response body are counted toward quota limits. The request headers and response headers will not be counted toward the limits.
- Tunnel traffic (including tunneled HTTPS) – AsyncOS simply shuttles the tunneled traffic from the client to the server, and vice versa. The entire data volume of the tunnel traffic is counted toward quota limits.
- FTP – The control-connection traffic is not counted. The size of the file uploaded and downloaded is counted toward quota limits.

Note Only client-side traffic is counted toward quota limits. Cached content also counts toward the limit, as client-side traffic is generated even when a response is served from the cache.

Time Quota Calculations

Calculation of time quotas is as follows:

- HTTP and decrypted HTTPS traffic – The duration of each connection to the same URL category, from formation to disconnect, plus one minute, is counted toward the time quota limit. If multiple requests are made to the same URL category within one minute of each other, they are counted as one continuous session and the one minute is added only at the end of this session (that is, after at least one minute of "silence").
- Tunnel traffic (including tunneled HTTPS) – The actual duration of the tunnel, from formation to disconnect, counts toward quota limits. The above calculation for multiple requests applies to tunneled traffic as well.
- FTP – The actual duration of the FTP control session, from formation to disconnect, counts toward quota limits. The above calculation for multiple requests applies to FTP traffic as well.

Defining Time, Volume, and Bandwidth Quotas

Before you begin

- Go to **Security Services** > **Acceptable Use Controls** to enable Acceptable Use Controls.
- Define a time range unless you want the quota to apply as a daily limit.

Procedure

Step 1 Navigate to **Web Security Manager > Define Time Ranges and Quotas**.

Step 2 Click **Add Quota**.

Step 3 Enter a unique **Quota Name** in the field.

Step 4 To reset the Time and Volume quota every day, select **Reset Time and Volume quota daily at** and enter a time in the 12-hour format in the field, then choose **AM** or **PM** from the menu. Alternatively, select **Select a predefined time range profile**.

Note
Using reset quota option does not reset the configured bandwidth quota value.

Step 5 To set a time quota, select the **Time Quota** check box and choose the number of hours from the **hrs** menu and the number of minutes from the **mins** menu, from zero (always blocked) to 23 hours and 59 minutes.

Step 6 To set a volume quota enter a number in the field and choose **KB** (kilobytes), MB (megabytes), or **GB** (gigabytes) from the menu.

Step 7 To set a bandwidth quota enter a number in the field and choose **Kbps** (kilobytes per second) or **Mbps** (megabytes per second) from the menu.

- You cannot configure both the URL bandwidth quota and the overall web activity quota for the same access or decryption policies.
- Bandwidth quota cannot be configured if the overall bandwidth limit or AVC bandwidth limit is enabled or vice-versa.
- Cached content is also taken into account for bandwidth quota.
- While editing quota profile, do not add bandwidth quota to any existing time or volume quota profile that is mapped to CDS policy.
- To have the URLs throttled using overall web activities bandwidth quota in the decryption policy, the URLs must be configured to passthrough.
- The following configuration is required for uncategorized URL to throttle through Deeper Bandwidth control:
  - Access Policies—Uncategorized URLs in decryption policy set to Decrypt/Monitor and Monitor in Access Policies and Overall web activities bandwidth quota respectively.
  - Decryption Policies—Uncategorized URLs in decryption policy is set to Passthrough and Overall web activities bandwidth quota.

Note
Delete all quota profiles whose bandwidth quota was configured before upgrading to AsyncOS Release 15.0.

Step 8 Click **Submit** and then click **Commit Changes** to apply your changes. Alternatively, click **Cancel** to abandon your changes.

What to do next

(Optional) Navigate to **Security Services > End-User Notification** to configure end-user notifications for quotas.

Access Control by URL Category

You can identify and action Web requests based on the category of Website they address. The Secure Web Appliance ships with many predefined URL categories, such as Web-based Email and others.

Predefined categories, and the Websites associated with them, are defined within filtering databases that reside on the Secure Web Appliance. These databases are automatically kept up to date by Cisco. You can also create custom URL categories for host names and IP addresses that you specify.

URL categories can be used by all policies except policies to identify requests. They can also be used by Access, Encrypted HTTPS Management and Data Security policies to apply actions to requests.

See Creating and Editing Custom URL Categories, on page 28 for information about creating custom URL categories.

Using URL Categories to Identify Web Requests

Before you begin

- Enable Acceptable Use Control, see Configuring the URL Filtering Engine , on page 14.
- (Optional) Create Custom URL Categories, see Creating and Editing Custom URL Categories, on page 28.

Procedure

Step 1 Choose a policy type (except SaaS) from the Web Security Manager menu.

Step 2 Click a policy name in the policies table (or add a new policy).

Step 3 Expand the **Advanced** section and click the link in the URL Categories field.

Step 4 Click the Add column cells corresponding to URL Categories you wish to identify web requests by. Do this for the Custom URL Categories and Predefined URL Categories lists as required.

Step 5 Click **Done**.

Step 6 Submit and commit your changes.

Using URL Categories to Action Web Request

Before you begin

- Enable Acceptable Use Control, see Configuring the URL Filtering Engine , on page 14.
- (Optional) Create Custom URL Categories, see Creating and Editing Custom URL Categories, on page 28.



Note If you have used URL categories as criteria within a policy then those categories alone are available to specify actions against within the same policy. Some of the options described below may differ or be unavailable because of this.

Procedure

Step 1 Choose one of **Access Policies**, **Cisco Data Security Policies**, or **Encrypted HTTPS Management** from the Web Security Manager menu.

Step 2 Find the required policy name in the policies table.

Step 3 Click the cell link in the URL Filtering column on the same row.

Step 4 (Optional) Add custom URL categories:

a) Click **Select Custom Categories**.

b) Choose which custom URL categories to include in this policy and click **Apply**.

Choose which custom URL categories the URL filtering engine should compare the client request against. The URL filtering engine compares client requests against included custom URL categories, and ignores excluded custom URL categories. The URL filtering engine compares the URL in a client request to included custom URL categories before predefined URL categories.

The custom URL categories included in the policy appear in the Custom URL Category Filtering section.

Step 5 Choose an action for each custom and predefined URL category.

Note
Available actions vary between custom and predefined categories and between policy types.

Step 6 In the Uncategorized URLs section, choose the action to take for client requests to web sites that do not fall into a predefined or custom URL category.

Step 7 Submit and commit your changes.

Remote Users

- About Remote Users, on page 98
- How to Configure Identification of Remote Users, on page 99
- Display Remote User Status and Statistics for ASAs, on page 100

About Remote Users

Cisco AnyConnect Secure Mobility extends the network perimeter to remote endpoints, enabling the integration of web filtering services offered by the Secure Web Appliance.

Remote and mobile users use the Cisco AnyConnect Secure VPN (virtual private network)client to establish VPN sessions with the Adaptive Security Appliance (ASA). The ASA sends web traffic to the Secure Web Appliance along with information identifying the user by IP address and user name. The Secure Web Appliance scans the traffic, enforces acceptable use policies, and protects the user from security threats. The security appliance returns all traffic deemed safe and acceptable to the user.

When Secure Mobility is enabled, you can configure identities and policies to apply to users by their location:

- **Remote users.** These users are connected to the network from a remote location using VPN. The Secure Web Appliance automatically identifies remote users when both the Cisco ASA and Cisco AnyConnect

client are used for VPN access. Otherwise, the Secure Web Appliance administrator must specify remote users by configuring a range of IP addresses.

- **Local users.** These users are connected to the network either physically or wirelessly.

When the Secure Web Appliance integrates with a Cisco ASA, you can configure it to identify users by an authenticated user name transparently to achieve single sign-on for remote users.

How to Configure Identification of Remote Users

Task	Further information
1. Configure identification of remote users.	Configuring Identification of Remote Users, on page 99
2. Create an identity for remote users.	Classifying Users and Client Software, on page 3 **1.** In the "Define Members by User Location" section, select Remote Users Only. **2.** In the "Define Members by Authentication" section, select "Identify Users Transparently through Cisco ASA Integration."
3. Create a policy for remote users.	Creating a Policy , on page 79

Configuring Identification of Remote Users

Procedure

Step 1 Security Services > AnyConnect Secure Mobility, and click **Enable**.

Step 2 Read the terms of the AnyConnect Secure Mobility License Agreement, and click **Accept**.

Step 3 Configure how to identify remote users.

Option	Description	Additional Steps
IP Address	Specify a range of IP addresses that the appliance should consider as assigned to remote devices.	**a.** Enter a range of IP addresses in the IP Range field. **b.** Go to step 4

Option	Description	Additional Steps
Cisco ASA Integration	Specify one or more Cisco ASA the Secure Web Appliance communicates with. The Cisco ASA maintains an IP address-to-user mapping and communicates that information with the Secure Web Appliance. When the Web Proxy receives a transaction, it obtains the IP address and determines the user by checking the IP address-to-user mapping. When users are determined by integrating with a Cisco ASA, you can enable single sign-on for remote users.	**a.** Enter the Cisco ASA host name or IP address. **b.** Enter the port number used to access the ASA. The default port number for the Cisco ASA is 11999. **c.** If multiple Cisco ASA are configured in a cluster, click **Add Row** and configure each ASA in the cluster. **Note** If two Cisco ASA are configured for high availability, enter only one host name or IP address for the *active* Cisco ASA. **d.** Enter the access passphrase for the Cisco ASA. **Note** The passphrase you enter here must match the access passphrase configured for the specified Cisco ASA. **e.** Optional, click **Start Test** to verify the Secure Web Appliance can connect to the configured Cisco ASA.

Step 4 Submit and Commit Changes.

Note
Enable AnyConnect Security Mobility (**Security Services** > **AnyConnect Security Mobility**) to make the Define Members by User Location option available on the Secure Web Appliance. By default, this option is available on the Cisco Content Security Management Appliance (**Web** > **Configuration Master** > **Identification Profiles**). When you use the Define Members by User Location option to configure an identification profile in the Security Management Appliance and publish that configuration to the Secure Web Appliance where AnyConnect Security Mobility is not enabled, the identification profile is disabled.

Display Remote User Status and Statistics for ASAs

Use this command to display information related to Secure Mobility when the Secure Web Appliance is integrated with an ASA.

Command	Description
`musstatus`	This command displays the following information: • The status of the Secure Web Appliance connection with each ASA. • The duration of the Secure Web Appliance connection with each ASA in minutes. • The number of remote clients from each ASA. • The number of remote clients being serviced, which is defined as the number of remote clients that have passed traffic through the Secure Web Appliance. • The total number of remote clients.

Troubleshooting Policies

- Access Policy not Configurable for HTTPS
- Some Microsoft Office Files Not Blocked
- Blocking DOS Executable Object Types Blocks Updates for Windows OneCare
- Identification Profile Disappeared from Policy
- Policy is Never Applied
- HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication
- User Matches Global Policy for HTTPS and FTP over HTTP Requests
- User Assigned Incorrect Access Policy
- Policy Troubleshooting Tool: Policy Trace

SaaS Access Control

This topic contains the following sections:

- Overview of SaaS Access Control, on page 101
- Configuring the Appliance as an Identity Provider, on page 102
- Using SaaS Access Control and Multiple Appliances, on page 104
- Creating SaaS Application Authentication Policies, on page 104
- Configuring End-user Access to the Single Sign-on URL, on page 106

Overview of SaaS Access Control

The Secure Web Appliance uses the Security Assertion Markup Language (SAML) to authorize access to SaaS applications. It works with SaaS applications that are strictly compliant with SAML version 2.0.

Cisco SaaS Access Control allows you to:

- Control which users can access SaaS applications and from where.
- Quickly disable access to all SaaS applications when users are no longer employed by the organization.
- Reduce the risk of phishing attacks that ask users to enter their SaaS user credentials.
- Choose whether users are transparently signed in (single sign-on functionality) or prompted to enter their authentication user name and pass phrase.

SaaS Access Control only works with SaaS applications that require an authentication mechanism that is supported by the Secure Web Appliance. Currently, the Web Proxy uses the "PasswordProtectedTransport" authentication mechanism.

To enable SaaS Access Control, you must configure settings on both the Secure Web Appliance and the SaaS application:

Procedure

	Command or Action	Purpose
Step 1	Configure the Secure Web Appliance as an identity provider.	Configuring the Appliance as an Identity Provider, on page 102
Step 2	Create an authentication policy for the SaaS application.	Creating SaaS Application Authentication Policies, on page 104
Step 3	Configure the SaaS application for single sign-on.	Configuring End-user Access to the Single Sign-on URL, on page 106
Step 4	(Optional) Configue multiple Secure Web Appliances.	Using SaaS Access Control and Multiple Appliances, on page 104

Configuring the Appliance as an Identity Provider

When you configure the Secure Web Appliance as an identity provider, the settings you define apply to all SaaS applications it communicates with. The Secure Web Appliance uses a certificate and key to sign each SAML assertion it creates.

Before you begin

- (Optional) Locate a certificate (PEM format) and key for signing SAML assertions.
- Upload the certificate to each SaaS application.

Procedure

Step 1 Choose **Network > Identity Provider for SaaS**.

Step 2 Click **Edit Settings**.

Step 3 Check **Enable SaaS Single Sign-on Service**.

Step 4 Enter a virtual domain name in the **Identity Provider Domain Name** field.

Step 5 Enter a unique text identifier in the **Identity Provider Entity ID** field (a URI formatted string is recommended).

Step 6 Either upload or generate a certificate and key:

Method	Additional Steps
Upload a certificate and key	**a.** Select **Use Uploaded Certificate and Key**. **b.** In the **Certificate** field, click Browse; locate the file to upload. **Note** The Web Proxy uses the first certificate or key in the file. The certificate file must be in PEM format. DER format is not supported. **c.** In the **Key** field, click Browse; locate the file to upload. If the key is encrypted, select **Key is Encrypted**. **Note** The key length must be 512, 1024, or 2048 bits. The private key file must be in PEM format. DER format is not supported. **d.** Click **Upload Files**. **e.** Click **Download Certificate** to download a copy of the certificate for transfer to the SaaS applications with which the Secure Web Appliance will communicate.
Generate a certificate and key	**a.** Select **Use Generated Certificate and Key**. **b.** Click **Generate New Certificate and Key**. **1.** In the Generate Certificate and Key dialog box, enter the information to display in the signing certificate. **Note** You can enter any ASCII character except the forward slash (/) in the Common Name field. **2.** Click **Generate**. **c.** Click **Download Certificate** to transfer the certificate to the SaaS applications with which the Secure Web Appliance will communicate. **d.** (Optional) To use a signed certificate, click the **Download Certificate Signing Request** (DCSR) link to submit a request to a certificate authority (CA). After you receive a signed certificate from the CA, click **Browse** and navigate to the signed certificate location. Click **Upload File**. (bug 37984)

Note
If the appliance has both an uploaded certificate and key pair and a generated certificate and key pair, it only uses the certificate and key pair currently selected in the Signing Certificate section.

Step 7 Make note of the settings when you configure the appliance as an identity provider. Some of these settings must be used when configuring the SaaS application for single sign-on.

Step 8 Submit and Commit Changes.

What to do next

After specifying the certificate and key to use for signing SAML assertions, upload the certificate to each SaaS application.

Related Topics

- Configuring End-user Access to the Single Sign-on URL, on page 106

Using SaaS Access Control and Multiple Appliances

Before you begin

Configuring the Appliance as an Identity Provider, on page 102

Procedure

Step 1 Configure the same Identity Provider Domain Name for each Secure Web Appliance.

Step 2 Configure the same Identity Provider Entity ID for each Secure Web Appliance.

Step 3 Upload the same certificate and private key to each appliance on the **Network > Identity Provider for SaaS** page.

Step 4 Upload this certificate to each SaaS application you configure.

Creating SaaS Application Authentication Policies

Before you begin

- Create associated identities.
- Configure Identity Provider, see Configuring the Appliance as an Identity Provider, on page 102.
- Provide an Identity Provider Signing Certificate and Key: Network > Identity Provider for SaaS > Enable and Edit Settings.
- Create an Authentication Realm, Authentication Realms.

Procedure

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

Step 2 Click **Add Application**.

Step 3 Configure the settings:

Property	Description
Application Name	Enter a name to identify the SaaS application for this policy; each application name must be unique. The Secure Web Appliance uses the application name to generate a single sign-on URL.
Description	(Optional) Enter a description for this SaaS policy.
Metadata for Service Provider	Configure the metadata that describes the service provider referenced in this policy. You can either describe the service provider properties manually or upload a metadata file provided by the SaaS application. The Secure Web Appliance uses the metadata to determine how to communicate with the SaaS application (service provider) using SAML. Contact the SaaS application to learn the correct settings to configure the metadata. **Configure Keys Manually** – If you select this option, provide the following: • **Service Provider Entity ID**. Enter the text (typically in URI format) the SaaS application uses to identify itself as a service provider. • **Name ID Format**. Choose from the drop-down list the format the appliance should use to identify users in the SAML assertion it sends to service providers. The value you enter here must match the corresponding setting configured on the SaaS application. • **Assertion Consumer Service URL**. Enter the URL to which the Secure Web Appliance is to send the SAML assertion it creates. Read the SaaS application documentation to determine the correct URL to use (also known as the login URL). **Import File from Hard Disk** – If you select this option, click Browse, locate the file, and then click **Import**. **Note** This metadata file is an XML document, following the SAML standard, that describes a service provider instance. Not all SaaS applications use metadata files, but for those that do, contact the SaaS application provider for the file.
User Identification / Authentication for SaaS SSO	Specify how users are identified/authenticated for SaaS single sign-on: • Always prompt users for their local authentication credentials. • Prompt users for their local authentication credentials if the Web Proxy obtained their user names transparently. • Automatically sign in SaaS users using their local authentication credentials. Choose the authentication realm or sequence the Web Proxy should use to authenticate users accessing this SaaS application. Users must be a member of the authentication realm or authentication sequence to successfully access the SaaS application. If an Identity Services Engine is used for authentication, and LDAP was selected, the realm will be used for the SAML user names and attribute mapping.

Property	Description
SAML User Name Mapping	Specify how the Web Proxy should represent user names to the service provider in the SAML assertion. You can pass the user names as they are used inside your network (**No mapping**), or you can change the internal user names into a different format using one of the following methods: • **LDAP query**. The user names sent to the service provider are based on one or more LDAP query attributes. Enter an expression containing LDAP attribute fields and optional custom text. You must enclose attribute names in angled brackets. You can include any number of attributes. For example, for the LDAP attributes "user" and "domain," you could enter <user>@<domain>.com. • **Fixed Rule Mapping**. The user names sent to the service provider are based on the internal user name with a fixed string added before or after the internal user name. Enter the fixed string in the **Expression Name** field, with %s either before or after the string to indicate its position in the internal user name.
SAML Attribute Mapping	(Optional) You can provide to the SaaS application additional information about the internal users from the LDAP authentication server if required by the SaaS application. Map each LDAP server attribute to a SAML attribute.
Authentication Context	Choose the authentication mechanism the Web Proxy uses to authenticate its internal users. **Note** The authentication context informs the service provider which authentication mechanism the identity provider used to authenticate the internal users. Some service providers require a particular authentication mechanism to allow users to access the SaaS application. If a service provider requires an authentication context that is not supported by an identity provider, users cannot access the service provider using single sign-on from the identity provider.

Step 4 Submit and Commit Changes.

What to do next

Set up the single sign-on settings on the SaaS application side, using the same parameters to configure the application.

Configuring End-user Access to the Single Sign-on URL

After you configure the Secure Web Appliance as an identity provider and create a SaaS Application Authentication Policy for the SaaS application, the appliance creates a single sign-on URL (SSO URL). The Secure Web Appliance uses the application name configured in the SaaS Application Authentication Policy to generate the single sign-on URL; the SSO URL format is:

http://*IdentityProviderDomainName* /SSOURL/*ApplicationName*

Procedure

Step 1 Obtain the single sign-on URL from the **Web Security Manager > SaaS Policies** page.

Step 2 Make the URL available to end-users depending on which flow type.

Step 3 If you choose Identity provider initiated flow, the appliance redirects users to the SaaS application.

Step 4 If you choose Service Provider initiated flows, you must configure this URL in the SaaS application.

- Always prompt SaaS users for proxy authentication. After entering valid credentials, users are logged into the SaaS application.
- Transparently sign in SaaS users. Users are logged into the SaaS application automatically.

Note
To achieve single sign-on behavior using explicit forward requests for all authenticated users when the appliance is deployed in transparent mode, select "**Apply same surrogate settings to explicit forward requests**" when you configure the Identity group.

Scan Outbound Traffic for Existing Infections

This topic contains the following sections:

- Overview of Scanning Outbound Traffic, on page 107
- Understanding Upload Requests, on page 108
- Creating Outbound Malware Scanning Policies, on page 109
- Controlling Upload Requests , on page 111
- Logging of DVS Scanning, on page 112

Overview of Scanning Outbound Traffic

To prevent malicious data from leaving the network, the Secure Web Appliance provides the Outbound Malware Scanning feature. Using policy groups, you can define which uploads are scanned for malware, which anti-malware scanning engines to use for scanning, and which malware types to block.

The Cisco Dynamic Vectoring and Streaming (DVS) engine scans transaction requests as they leave the network. By working with the Cisco DVS engine, the Secure Web Appliance enables you to prevent users from unintentionally uploading malicious data.

You can perform the following tasks:

Task	Link to Task
Create policies to block malware	Creating Outbound Malware Scanning Policies, on page 109
Assign upload requests to outbound malware policy groups	Controlling Upload Requests , on page 111

User Experience When Requests Are Blocked by the DVS Engine

When the Cisco DVS engine blocks an upload request, the Web Proxy sends a block page to the end user. However, not all Websites display the block page to the end user. Some Web 2.0 Websites display dynamic

content using Javascript instead of a static Webpage and are not likely to display the block page. Users are still properly blocked from uploading malicious data, but they may not always be informed of this by the Website.

Understanding Upload Requests

Outbound Malware Scanning Policies define whether or not the Web Proxy blocks HTTP requests and decrypted HTTPS connections for transactions that upload data to a server (upload requests). An upload request is an HTTP or decrypted HTTPS request that has content in the request body.

When the Web Proxy receives an upload request, it compares the request to the Outbound Malware Scanning policy groups to determine which policy group to apply. After it assigns the request to a policy group, it compares the request to the policy group's configured control settings to determine whether to block the request or monitor the request. When an Outbound Malware Scanning Policy determines to monitor a request, it is evaluated against the Access Policies, and the final action the Web Proxy takes on the request is determined by the applicable Access Policy.



Note Upload requests that try to upload files with a size of zero (0) bytes are not evaluated against Outbound Malware Scanning Policies.

Criteria for Group Membership

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

The Web Proxy follows a specific process for matching the group membership criteria. It considers the following factors for group membership:

Criteria	Description
Identification Profile	Each client request either matches an **Identification Profile**, fails authentication and is granted guest access, or fails authentication and is terminated.
Authorized users	If the assigned **Identification Profile** requires authentication, the user must be in the list of authorized users in the Outbound Malware Scanning 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 Outbound Malware Scanning Policy group membership. Some options, such as proxy port and URL category, can also be defined within the **Identification Profile**. When an advanced option is configured in the **Identification Profile**, it is not configurable in the Outbound Malware Scanning Policy group level.

Matching Client Requests to Outbound Malware Scanning Policy Groups

The Web Proxy 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 Outbound Malware Scanning Policies

You can create Outbound Malware Scanning Policy groups based on combinations of several criteria, such as one or more Identities 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 Identities.

Procedure

Step 1 Choose **Web Security Manager** > **Outbound Malware Scanning**.

Step 2 Click **Add Policy**.

Step 3 Enter a name and an optional description for the policy group.

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, select where in the policies table to place the policy group.

When configuring multiple policy groups, you must specify a logical order for each group.

Step 5 In the **Identification Profiles** and Users section, select one or more Identity 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. 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 select to use the addresses that may be defined with the associated Identity, or you can enter specific addresses here. **Note** If the Identity 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 Identity. 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.

Step 8 Submit your changes.

Step 9 Configure Outbound Malware Scanning Policy group control settings to define how the Web Proxy handles transactions.

The new Outbound Malware Scanning Policy group automatically inherits global policy group settings until you configure options for each control setting.

Step 10 Submit and Commit Changes.

Controlling Upload Requests

Each upload request is assigned to an Outbound Malware Scanning Policy group and inherits the control settings of that policy group. After the Web Proxy receives the upload request headers, it has the information necessary to decide if it should scan the request body. The DVS engine scans the request and returns a verdict to the Web Proxy. The block page appears to the end user, if applicable.

Procedure

Step 1 Choose **Web Security Manager > Outbound Malware Scanning**.

Step 2 In the **Destinations** column, click the link for the policy group you want to configure.

Step 3 In the **Edit Destination Settings** section, select **Define Destinations Scanning Custom Settings** from the drop-down menu.

Step 4 In the **Destinations to Scan** section, select one of the following:

Option	Description
Do not scan any uploads	The DVS engine scans no upload requests. All upload requests are evaluated against the Access Policies
Scan all uploads	The DVS engine scans all upload requests. The upload request is blocked or evaluated against the Access Policies, depending on the DVS engine scanning verdict
Scan uploads to specified custom URL categories	The DVS engine scans upload requests that belong in specific custom URL categories. The upload request is blocked or evaluated against the Access Policies, depending on the DVS engine scanning verdict. Click **Edit custom categories list** to select the URL categories to scan

Step 5 Submit your changes.

Step 6 In the **Anti-Malware Filtering** column, click the link for the policy group.

Step 7 In the **Anti-Malware Settings** section, select **Define Anti-Malware Custom Settings**.

Step 8 In the **Cisco DVS Anti-Malware Settings** section, select which anti-malware scanning engines to enable for this policy group.

Step 9 In the **Malware Categories** section, select whether to monitor or block the various malware categories.

The categories listed in this section depend on which scanning engines you enable.

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 10 Submit and Commit Changes.

Logging of DVS Scanning

The access logs indicate whether or not the DVS engine scanned an upload request for malware. The scanning verdict information section of each access log entry includes values for the DVS engine activity for scanned uploads. You can also add one of the fields to the W3C or access logs to more easily find this DVS engine activity:

Table 1: Log Fields in W3C Logs and Format Specifiers in Access Logs

W3C Log Field	Format Specifier in Access Logs
x-req-dvs-scanverdict	%X2
x-req-dvs-threat-name	%X4
x-req-dvs-verdictname	%X3

When the DVS engine marks an upload request as being malware and it is configured to block malware uploads, the ACL decision tag in the access logs is BLOCK_AMW_REQ.

However, when the DVS engine marks an upload request as being malware and it is configured to *monitor* malware uploads, the ACL decision tag in the access logs is actually determined by the Access Policy applied to the transaction.

To determine whether or not the DVS engine scanned an upload request for malware, view the results of the DVS engine activity in the scanning verdict information section of each access log entry.