Protecting Against Malicious or Undesirable URLs

This chapter contains the following sections:

- URL-Related Protections and Controls , on page 1
- URL Retrospective Verdict and URL Remediation, on page 2
- Setting Up URL Filtering, on page 3
- Taking Action Based on the Reputation or Category of URLs in Messages , on page 10
- Handling Unscannable Messages for URL Filtering, on page 14
- Remediating Malicious URLs in Mailboxes, on page 15
- Detecting Malicious URLs in Messages Using Content Filter, on page 16
- Detecting Malicious URLs in Messages Using Message Filter, on page 17
- Monitoring URL Filtering Results , on page 18
- Displaying URL Details in Message Tracking , on page 19
- Troubleshooting URL Filtering, on page 19
- About URL Categories, on page 25

URL-Related Protections and Controls

Control and protection against malicious or undesirable links is incorporated into the anti-spam, outbreak, content, and message filtering processes in the work queue. These controls:

- Increase the effectiveness of protection from malicious URLs in messages and attachments.

  URL filtering is incorporated into Outbreak Filtering. This strengthened protection is useful even if your organization already has a Cisco Web Security Appliance or similar protection from web-based threats, because it blocks threats at the point of entry.

  You can also use content or message filters to take action based on the Web Based Reputation Score (WBRS) of URLs in messages.

Note As a best practice, Cisco recommends rewriting URLs with a questionable, neutral, and favorable or unknown reputation to redirect them to the Cisco Web Security Proxy for click-time evaluation of their safety.

- Better identify spam

  The email gateway uses the reputation and category of links in messages, in conjunction with other spam-identification algorithms, to help identify spam. For example, if a link in a message belongs to a marketing web site, the message is more likely to be a marketing message.

- Support enforcement of corporate acceptable use policies

  The category of URLs (for example, Adult Content or Illegal Activities) can be used in conjunction with content and message filters to enforce corporate acceptable use policies.

- Allow you to identify users in your organization who most frequently clicked a URL in a message that has been rewritten for protection, as well as links that have most frequently been clicked.

Related Topics

- Which URLs Are Evaluated , on page 2
- Web Interaction Tracking Page

Which URLs Are Evaluated

URLs in incoming and outgoing messages (including attachments) are evaluated. Any valid string for a URL is evaluated, including strings with the following:

- http, https, or www
- domain or IP address
- port number preceded by a colon (:)
- uppercase or lowercase letters

When evaluating URLs to determine whether a message is spam, if necessary for load management, the system prioritizes screening of incoming messages over outgoing messages.

URL Retrospective Verdict and URL Remediation

The URLs are filtered based on the URL reputation and category provided by cloud based Talos Intelligence Services. The URL reputation can change as new information emerges. A URL may not be initially evaluated as malicious, and the message may therefore be released to the recipient. But later, these URL reputations can turn malicious anytime, even after it has reached the user's mailbox. Talos Intelligence Services monitors the URL verdicts in a sandbox server. The email gateway polls for the retrospective verdict update of the URLs from Talos every two minutes for a period of 168 hours. If any URL reputation changes to 'Malicious', Talos sends the retrospective verdict update to the email gateway. The email gateway sends alerts on the retrospective verdict update so that necessary action can be taken.

Cisco Secure Email Gateway handles the URL Retrospective verdicts generated within 7 days of the URLs sent for analysis. The email gateway does not perform the configured policy action for verdicts received after 7 days.

Additionally, you can configure the Mailbox Auto Remediation service to remediate the message with a malicious URL from the user's mailbox. For example, you can configure your email gateway to delete the message from the recipient's mailbox when the reputation of the URL changes to malicious. The configured policy action is applied only to the delivered messages.

Note The URL Retrospective Verdict and Remediation feature is available for incoming mails only.

The URL Retrospective Verdict traffic from Secure Email Gateway cannot be decrypted. Only pass-through proxy mode is supported. However, the polling response data can be decrypted.

All emails with the same subject line are remediated if one of them contains a malicious URL.

The firewall rules of Secure Email Gateway must be updated to allow the following hostnames to access the URL Retrospection global registration and polling service:

- prod-register-api.uce.cmd.cisco.com
- prodap-retro-api.uce.cmd.cisco.com
- prodeu-retro-api.uce.cmd.cisco.com
- produs-retro-api.uce.cmd.cisco.com

The email gateway gets connected to the URL Retrospection registration and polling service in one of the geographical regions (for example, APJC, EU, and Americas) based on the DNS server configured for the host name (prod-register-api.uce.cmd.cisco.com).

Note If you are upgrading from an earlier version of AsyncOS with the URL Retrospective service enabled, the geographic region to register the URL Retrospective service after the upgrade is selected automatically based on the name resolution for the global registration service hostname received from the DNS server.

Related Topics

- Remediating Malicious URLs in Mailboxes, on page 15

Setting Up URL Filtering

- Requirements for URL Filtering , on page 3
- Enable URL Filtering, on page 4
- About the Connection to Talos Intelligence Services , on page 6
- Web Interaction Tracking , on page 7
- URL Filtering in Cluster Configurations, on page 7
- Creating Allowed Lists for URL Filtering , on page 8
- Customizing the Notification That End Users See If a Site Is Malicious , on page 9

Requirements for URL Filtering

In addition to enabling URL filtering, you must enable other features depending on desired functionality.

For enhanced protection against spam:

- Anti-spam scanning must be enabled globally and per applicable mail policy. This can be either the IronPort Anti-Spam or the Intelligent Multi-Scan feature. See the anti-spam chapter.

  For enhanced protection against malware:

- The Outbreak Filters feature must be enabled globally and per applicable mail policy. See the Outbreak Filters chapter.

  To take action based on URL reputation, or to enforce acceptable use policies using message and content filters:

- The Outbreak Filters feature must be enabled globally. See the Outbreak Filters chapter.

Enable URL Filtering

You can enable URL filtering using the **Security Services > URL Filtering** page in the web interface or the **`websecurityconfig`** command in CLI.

Before You Begin

- Ensure that the requirements for the individual URL filtering features that you want to use have been met. See Requirements for URL Filtering , on page 3.
- (Optional) Create a list of URLs that you want all URL filtering functionalities to ignore. See Creating Allowed Lists for URL Filtering , on page 8.

Procedure

Step 1 Select **Security Services > URL Filtering**.

Step 2 Click **Enable**.

Step 3 Select the **Enable URL Category and Reputation Filters** check box.

Note
When you enable URL Filtering, the URL Retrospective Service is also automatically enabled and connected to the AMERICAS region. You can change it anytime later. For more information, see URL Retrospective Verdict and URL Remediation, on page 2.

Step 4 (Optional) If you have created a list of URLs to exempt from URL filtering when evaluating messages for spam and malware, and from all content and message filtering, select that list.

This setting does not cause the message to bypass anti-spam or Outbreak Filters processing generally.

Step 5 [Optional] Enable **Web Interaction Tracking**. See Web Interaction Tracking , on page 7.

Step 6 Under the **URL Retrospective Service**, choose the geographic region to which you want to register the URL Retrospective Service, from the **Region** drop-down list.

Step 7 [Optional] Enable **QR Code URL Scanning** to extract URLs by scanning QR code images in the message body and attachments.

Note

- Enabling **QR Code URL Scanning** feature also enables image extraction and QR code scanning from attachments, which may lead to email processing delays. You can disable image extraction from

attachments via the CLI to minimize the performance impact.. For more details, refer to the `websecurityconfig` section in the CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway.

- The supported image types for QR Code Scanning are jpeg, jpg, png, bmp.
- **QR Code URL Scanning** supports a maximum of 5 images per attachment and an overall limit of 5 images per email. Images are scanned sequentially across attachments. Once the email-level limit is reached, scanning stops and no additional images from the current or subsequent attachments are scanned.

Step 8 [Optional] Click **Advanced Settings** and enter the required parameters described in the following table to configure advanced URL filtering settings:

Parameter	Description
URL Lookup Timeout	Enter the time taken for the URL to request the IP address for a certain domain name.
Maximum Number of URLs scanned in Message Body	Enter the maximum number of URLs that you want the email gateway to scan in a message body
Maximum Number of URLs scanned in Message Attachments	Enter the maximum number of URLs that you want the email gateway to scan in message attachments.
Rewrite URL text and HREF in Message	Select the **Yes** radio button if you want the entire rewritten URL to appear in the message body. OR Select the **No** radio button if you want the entire rewritten URL to only appear in the HREF for HTML messages.
URL Logging	Select the **Enable** radio button if you want to display URL details in Mail Logs and Message Tracking. The URL details are logged in Mail Logs and Message Tracking based on any one of the following conditions: • Category of any URL in the message matches the URL category filters. • Reputation score of any URL in the message matches URL reputation filters. • Outbreak Filters (if enabled) rewrites any URL in the message.

Step 9 Submit and commit your changes.

If you have met the applicable prerequisites, and you have already configured Outbreak Filters and Anti-Spam protection, then you do not need to make additional configurations to benefit from enhanced automatic detection of spam and malicious URLs.

What to do next

- To take action based on the reputation of URLs in messages, see Taking Action Based on the Reputation or Category of URLs in Messages , on page 10.
- To use URL categories in content and message filters, for example to enforce acceptable use policies, see Taking Action Based on the Reputation or Category of URLs in Messages , on page 10.
- To redirect all URLs in suspected spam messages to the Cisco Web Security proxy service, see Using Custom Headers to Redirect URLs in Suspected Spam to the Cisco Web Security Proxy: Configuration Example.
- (Optional) To customize the appearance of end user notification page, see Customizing the Notification That End Users See If a Site Is Malicious , on page 9.
- Ensure that you receive alerts about issues related to this feature. See Future URL Category Set Changes , on page 38, the release notes for your AsyncOS release, and Adding Alert Recipients.

About the Connection to Talos Intelligence Services

URL reputation and category are provided by cloud-based Talos Intelligence Services.

The email gateway connects to the Talos Intelligence Services either directly or through a web proxy, using the port specified for URL filtering services in Firewall Information Communication is over HTTPS with mutual certificate authentication. Certificates are updated automatically (see Service Updates.) For additional information about required certificates, see the Release Notes available from the location specified in Certificates for URL Filtering Features , on page 6.

If an HTTP or HTTPS proxy has been configured on the **Security Services > Service Updates** page, the email gateway will use it when communicating with Talos Intelligence Services. For more information about using a proxy server, see Configuring Server Settings for Downloading Upgrades and Updates.

Note Certificates are not saved with a configuration file.

Related Topics

- Certificates for URL Filtering Features , on page 6
- Alert: Beaker Connector: Error Fetching Enrollment Certificate , on page 21
- Alert: Beaker Connector: Certificate Is Invalid , on page 22

Certificates for URL Filtering Features

AsyncOS is designed to automatically deploy and update the certificates needed for communications with cloud services used for URL filtering features. However, if for any reason the system is unable to update these certificates, you will receive an alert that requires action from you.

Ensure that the email gateway is configured to send you these alerts (System type, Warning severity). For instructions, see Alerts.

If you receive an alert about an invalid certificate, contact Cisco TAC, which can provide the required replacement certificate. For instructions to use the replacement certificate, see Manually Configuring a Certificate for Communication with Talos Intelligence Services , on page 25.

Web Interaction Tracking

The web interaction tracking feature provides information about the end users who clicked on rewritten URLs and the action (allowed, blocked, or unknown) associated with each user click. Once you enable this feature, you can use the Web Interaction Tracking report to view information such as top malicious URLs clicked, top users who clicked on malicious URLs, and so on. For more information about the Web Interaction Tracking report, see Web Interaction Tracking Page.

Web Interaction Tracking data is provided by a cloud-based Cisco Aggregator Server.

Related Topics

- Configuring Web Interaction Tracking, on page 7
- About the Connection to Cisco Aggregator Server, on page 7

Configuring Web Interaction Tracking

Depending on your requirements, you can enable web interaction tracking on one of the global settings pages:

- **Outbreak Filters**. Track end users who clicked URLs rewritten by Outbreak Filters. See Configuring Outbreak Filters Global Settings.
- **URL Filtering**. Track end users who clicked URLs rewritten by policies (using content and message filters). See Enable URL Filtering, on page 4.

About the Connection to Cisco Aggregator Server

The email gateway connects to the Cisco Aggregator Server every 30 minutes (non-configurable), either directly or through a web proxy, using the port specified for URL filtering services in Firewall Information Communication is over HTTPS with mutual certificate authentication. Certificates are updated automatically (see Service Updates.)

If an HTTP or HTTPS proxy has been configured on the **Security Services** > **Service Updates** page, the email gateway will use it when communicating with the Cisco Aggregator Server. For more information about using a proxy server, see Configuring Server Settings for Downloading Upgrades and Updates.

Note Certificates are not saved with a configuration file.

URL Filtering in Cluster Configurations

- You can enable URL filtering at the machine, group or cluster level.
- If URL filtering is enabled at machine level, URL allowed lists and web interaction tracking can be configured at machine, group or cluster level.
- If URL filtering is enabled at group level, URL allowed lists and web interaction tracking must be configured at group or cluster level.
- If URL filtering is enabled at cluster level, URL allowed lists and web interaction tracking must be configured at cluster level.
- The standard rules for clusters for Message Filters and Content Filters apply.

Creating Allowed Lists for URL Filtering

If you specify a global allowed list when configuring the URL Filtering feature, then URLs on the allowed list are not evaluated for reputation or category, for anti-spam, Outbreak Filtering, or content and message filtering. However, the messages that contain these URLs are evaluated as usual by anti-spam scanning and Outbreak Filters. You can also specify a URL allowed list in each URL Filtering condition (rule) and action in content and message filters, to supplement the global URL allowed list.

To categorize allowed list URLs from Outbreak Filtering generally, use the Bypass Domain Scanning option that you configure on the Mail Policies: Outbreak Filters page. URL allowed lists for URL filtering are similar to, but independent of, Bypass Domain Scanning. For more information about that feature, see URL Rewriting and Bypassing Domains.

There is no relationship between URL filtering allowed lists described in this section and the allowd list used for sender reputation filtering based on IP Reputation score.

Before You Begin

Consider importing a list of URLs instead of creating one in the web interface. See Importing a URL List , on page 8.

Procedure

Step 1 Select **Mail Policies > URL Lists**.

Step 2 Select **Add URL List** or click a list to edit.

Be sure all URLs that you want to designate globally as an allowed list are in a single list. You can select only one global allowed list for URL filtering.

Step 3 Create and submit the URL list.

To view a list of supported URL formats, enter a semicolon (;) into the **URLs** box and click **Submit**. Then click the **more...** link that appears.

Each URL, domain, or IP address can be on a separate line, or separate each with a comma.

Step 4 Commit your changes.

What to do next

- To designate a URL list as the global allowed list, see Enable URL Filtering, on page 4.
- To designate a URL list as the allowed list for a specific condition (rule) or action in a content or message filter, see Taking Action Based on the Reputation or Category of URLs in Messages , on page 10 and Content Filter Actions. For message filters, see also URL Category Actions and URL Category Rule.

Related Topics

- Importing a URL List , on page 8

Importing a URL List

You can import a URL list to use as a allowed list for URL filtering.

Procedure

Step 1 Create the text file to import:

- The first line must be the name of the URL list.
- Each URL must be on a separate line.

Step 2 Upload the file to the `/configuration` directory on the appliance.

Step 3 Use the `urllistconfig > new` command in the command-line interface.

Customizing the Notification That End Users See If a Site Is Malicious

If an end user clicks a malicious URL identified by Outbreak Filtering or a Policy (using Content or Message Filters), the Cisco Web Security proxy displays a notification in the end user's web browser. This notification states that the site is malicious and access to it has been blocked.

When an end user clicks on a URL rewritten using Outbreak Filtering, the notification page is displayed for 10 seconds and then is redirected to the Cisco Web Security proxy for click-time evaluation.

You can customize the appearance of this notification page and display your organization's branding such as company logo, contact information, and so on.

Note If you do not customize the notification page, end users see a Cisco branded notification page.

Before You Begin

- Enable URL filtering. See Enable URL Filtering, on page 4.

Procedure

Step 1 Select **Security Services** > **Block Page Customization**.

Step 2 Click **Enable**.

Step 3 Check the **Enable Block Page customization** check box and enter the following details:

- URL of the organization's logo. It is recommended that the logo image is hosted on a publicly accessible server.
- Organization's name
- Organization's contact information

Step 4 Choose the language of the notification. You can choose any one of the languages supported by the web interface.

Note

The default language of the end user's browser takes precedence over the language you have selected here. Also, if the default language of the end user's browser is not supported by AsyncOS, then the notification is displayed in the language you have selected here.

Step 5 (Optional) Preview the notification page by clicking **Preview Block Page Customization** link.

Step 6 Submit and commit your changes.

Next Steps

Set up URL rewriting in one of the following ways:

- Using Outbreak Filters. See Redirecting URLs.
- Using Content or Message Filters. See Taking Action Based on the Reputation or Category of URLs in Messages , on page 10.

Taking Action Based on the Reputation or Category of URLs in Messages

You can take action based on the reputation or category of URL links in the message body or message attachment using message filters and content filters in incoming and outgoing mail policies.

Because Outbreak Filters take many factors into consideration when evaluating messages for malware, and URL reputation alone may not trigger aggressive message handling, you may want to create filters based on URL reputation.

For example, you can use URL Reputation filters to:

- (For URLs in message body only) Rewrite URLs of neutral or unknown reputation to redirect them to the Cisco cloud Web Security proxy service for click-time evaluation.
- Drop messages that include URLs that have reputation scores in the Untrusted range.

You can use URL Category filters to:

- Filter categories of URLs to enforce organizational policies for acceptable web use, for example to prevent users from visiting adult or gambling sites while at the office.
- Provide enhanced protection from malicious sites, which may not exist long enough to be classified. (For URLs in message body only) You can redirect all URLs in the Unclassified category to the Cisco cloud Web Security proxy service for evaluation at the time a user clicks a link.

Related Topics

- Using URL-Related Conditions (Rules) and Actions , on page 11
- Filtering by URL Reputation or URL Category: Conditions and Rules , on page 11
- Modifying URLs in Messages: Using URL Reputation and URL Category Actions in Filters , on page 12
- Redirected URLs: What Does the End User Experience? , on page 14

Using URL-Related Conditions (Rules) and Actions

To	Example	Do This
Take action on the message as a whole.	Drop or quarantine messages.	Create a URL Reputation or URL Category condition or rule, then pair it with any action other than a URL Reputation or URL Category action. Exception: Do not pair a URL Reputation condition or rule with a Bounce action.
(For URls in message body only) Modify URLs in a message, or modify their behavior.	Replace a URL in the message with a text note, or make the URL unclickable.	Create a URL Reputation or URL Category action only; do not use a separate URL filtering condition.

As always, you must specify a content filter in a mail policy in order to use it.

Related Topics

- Filtering by URL Reputation or URL Category: Conditions and Rules , on page 11
- Modifying URLs in Messages: Using URL Reputation and URL Category Actions in Filters , on page 12

Filtering by URL Reputation or URL Category: Conditions and Rules

You can perform actions on messages based on the reputation or category of URLs in the message body and message attachments. If you want to perform any action other than modifying URLs or their behavior, add a **URL Reputation** or **URL Category** condition and select the reputation scores or URL categories for which you want to apply the action.

For example, if you want to apply the **Drop (Final Action)** action to all messages that include URLs in the Adult category, add a condition of type **URL Category** with the **Adult** category selected.

If you do not specify a category, the action you choose is applied to all messages.

URL reputation score ranges for trusted, neutral, and untrusted URLs are predefined and not editable. However, you can specify a custom range instead. The specified endpoints are included in the range you specify. For example, if you create a custom range from -8 to -10, then -8 and -10 are included in the range. Use "Unknown" for URLs for which a reputation score cannot be determined.

Note Neutral URL reputation means that URLs are currently clean, but may turn malicious in future, as they are prone to attacks. For such URLs, administrators can create non-blocking policies, for example, redirecting them to the Cisco Web Security Proxy for click-time evaluation.

URLs that are included on the selected URL allowed list or on the global URL allowed list not evaluated.

The action that you pair with this condition is taken if any URL in the message matches the reputation score or any category specified in the condition.

If you want to modify URLs in a message, or modify their behavior, configure only a URL Reputation or URL Category action. You do not need a separate URL Reputation or URL Category condition or rule for this purpose.

Note Do not pair a URL Reputation condition with a Bounce action.

Tip To check the category of a particular URL, visit the link in Reporting Uncategorized and Misclassified URLs , on page 38.

Related Topics

- Creating Allowed Lists for URL Filtering , on page 8
- Content Filters

Modifying URLs in Messages: Using URL Reputation and URL Category Actions in Filters

Use a URL Reputation or URL Category action to modify URLs in a message, or their behavior, based on the reputation or category of the URL.

URL Reputation and URL Category actions do not require a separate condition. Instead, the selected action is applied based on the reputation or categories that you select in the URL Reputation or URL Category action.

The action is applied only to URLs that meet the criteria specified in the action. Other URLs in the message are not modified.

If you do not specify a category, the action you choose is applied to all messages.

URL reputation score ranges for trusted, neutral, and untrusted URLs are predefined and not editable. However, you can specify a custom range instead. The specified endpoints are included in the range you specify. For example, if you create a custom range from -8 to -10, then -8 and -10 are included in the range. Use “Unknown” for URLs for which a reputation score cannot be determined.

Note Neutral URL reputation means that URLs are currently clean, but may turn malicious in future, as they are prone to attacks. For such URLs, administrators can create non-blocking policies, for example, redirecting them to the Cisco Web Security Proxy for click-time evaluation.

The following URL-related actions are only applicable for URLs in the message body::

- Defang a URL so that it is unclickable. Message recipients can still see and copy the URL.
- Redirect a URL so that if the message recipient clicks the link, the transaction is routed to a Cisco web security proxy in the cloud, which blocks access if the site is malicious.

Example: You might want to redirect all URLs in the **Uncategorized** category to the Cisco Cloud Web Security proxy service, as malicious sites used in phishing attacks often do not exist long enough to be classified.

See also Redirected URLs: What Does the End User Experience? , on page 14.

To redirect URLs to a different proxy, see the example in the following bullet.

Note The Cisco Cloud Web Security proxy service has no configurable options in this release. For example, there is no threat score threshold to adjust or action to specify based on threat score.

- Replace the URL with any text.

  To include the original URL in the text that appears in the message, use the $URL variable.

  Examples:

  - Replace all URLs in the **Illegal Downloads** category with a note:

    ```
    Message from your system administrator: A link to an illegal downloads web site has
    been removed from this message.
    ```

  - Include the original URL along with a warning:

    ```
    WARNING! The following URL may contain malware: $URL
    ```

    This becomes: WARNING: The following URL may contain malware: http://example.com.

  - Redirect to a custom proxy or web security service:

    ```
    http://custom_proxy/$URL
    ```

    This becomes: http://custom_proxy/http://example.com

Remote Browser Isolation (RBI) provides a secure way to open web links by running the browsing session in an isolated cloud environment instead of your local machine.

Note You must have a valid Menlo Security account to utilize the RBI feature. Ensure your account is provisioned and accessible before configuring RBI settings on the gateway.

Menlo link: https://isolate.menlosecurity.com/account/login

RBI rewrites a URL so that, when clicked, it opens in an isolated remote browser environment hosted on the Menlo Security platform.

The Menlo environment loads the site in isolation, allowing you to safely view and interact with the page, even if it contains unsafe or malicious elements. Harmful components are stripped, blocked, or neutralized, and only safe, sanitized content is rendered in your local browser.

This approach prevents direct interaction between your system and potentially harmful websites, mitigating the risk of malicious activity while still enabling secure access to the information on suspicious pages.

The reputation and category of URLs that are included on the selected URL allowed list or on the global URL allowed list are not evaluated.

If you defang or replace URLs, you can choose to ignore URLs in signed messages.

Pairing a URL Reputation or URL Category action with a URL Reputation or URL Category condition (or rule) is not recommended. If you pair a condition (rule) and action that include different categories, then no match occurs.

Tip To check the category of a particular URL, visit the link in Reporting Uncategorized and Misclassified URLs , on page 38.

Related Topics

- Creating Allowed Lists for URL Filtering , on page 8
- Using Custom Headers to Redirect URLs in Suspected Spam to the Cisco Web Security Proxy: Configuration Example
- Content Filters
- URL Reputation Rules
- URL Category Rule

Redirected URLs: What Does the End User Experience?

Based on the evaluation by the Cisco Cloud Web Security proxy service:

- If the site is benign, the user is directed to the target web site and has no knowledge that the link has been redirected.
- If the site is malicious, the user sees a notice that the site is malicious and access to it has been blocked.

  You can customize the appearance of end user notification page and display your organization's branding such as company logo, contact information, and so on. See Customizing the Notification That End Users See If a Site Is Malicious , on page 9.

- If communication with the Cisco Cloud Web Security proxy service times out, the user is allowed to access the target web site.
- If any other error occurs, the user sees a notice.

Related Topics

- Modifying URLs in Messages: Using URL Reputation and URL Category Actions in Filters , on page 12

Handling Unscannable Messages for URL Filtering

In the following scenarios, the URL filtering scanning fails, and the following header - *X-URL-LookUp-ScanningError* is added to the message:

- Unable to obtain the URL Reputation and Category
- Unable to expand the shortened URLs in the message

- Number of URLs in the message body or message attachments exceeds the maximum URL scan limit

You can add a content filter, select the *X-URL-LookUp-ScanningError* header in the Other Header condition, and configure appropriate actions to take on the message.

Remediating Malicious URLs in Mailboxes

URLs with any reputation can turn malicious anytime, even after it has reached the user's mailbox. You can configure URL filtering on your email gateway to send alerts based on the URL retrospective verdicts received from Talos. You can also configure your email gateway to perform auto-remedial actions on the messages in user mailbox when the URL verdict changes to malicious.

Before You Begin

- Ensure that the requirements for the individual URL filtering features that you want to use have been met. See Requirements for URL Filtering , on page 3.
- Ensure that the URL filtering is enabled. See Enable URL Filtering, on page 4.
- Ensure that the license keys to access the cloud services are activated on your email gateway.
- Ensure that the Mailbox Auto Remediation feature is enabled on your email gateway. See Enabling Account Settings on Email Gateway.

Procedure

Step 1 Select **Security Services > URL Filtering**.

Step 2 Click **Enable** under **Mailbox Auto Remediation**.

Step 3 Select the **Enable Mailbox Auto Remediation** checkbox.

Step 4 Configure the remedial actions to be performed on messages delivered to end users when the URL reputation verdict turns malicious.

- Forward to an email address - Select this option to forward the message with malicious URL to a specified user, for example, an email administrator.
- Delete the message - Select this option to permanently delete the message with malicious URL from the end user's mailbox.
- Forward to an email address and delete the message. Select this option to forward the message with malicious URL to a specified user, for example, an email administrator and permanently delete that message from the end user's mailbox.

Note
Messages from certain folders (for example, Deleted Items) cannot be deleted as Office 365 services do not support deletion of messages from these folders.

Note
Before configuring the Mailbox Auto Remediation settings, review Remediating Messages in Mailboxes.

Step 5 Submit and commit the changes.

Detecting Malicious URLs in Messages Using Content Filter

Use the ‘URL Reputation’ content filter to detect URLs in messages categorized as malicious by the ETF engine and take appropriate actions on such messages.

You can configure the 'URL Reputation' content filter for ETF in any one of the following ways:

- Use the 'URL Reputation' condition with any appropriate action.
- Use the 'URL Reputation' action with any or no condition.
- Use the 'URL Reputation' condition and action.

The following procedure is used to detect malciicous URLs using the 'URL Reputation' condition and action:

Note

- If you only want to use the 'URL Reputation' condition with any appropriate action, do not follow steps 11-20 of the procedure.
- If you only want to use the 'URL Reputation' action with any or no condition., do not follow steps 4-10 of the procedure.

Before you begin

- Make sure that you enable URL filtering on your email gateway. To enable URL filtering, go to *Security Services* > *URL Filtering* page in the web interface. For more information, see Protecting Against Malicious or Undesirable URLs, on page 1.
- Make sure that you enable Outbreak Filters on your email gateway. To enable Outbreak Filters, go to *Security Services* > *Outbreak Filters* page in the web interface. For more information, see Outbreak Filters.
- Make sure that you enable Anti-Spam engine on your email gateway. To enable the Anti-Spam engine, go to *Security Services* > *Anti-Spam* page in the web interface. For more information, see Managing Spam and Graymail.
- (Optional) Create a URL list. To create one, go to *Mail Polices* > *URL Lists* page in the web interface. For more information, see Protecting Against Malicious or Undesirable URLs, on page 1.

Procedure

Step 1 Go to **Mail Policies > Incoming Content Filters**.

Step 2 Click **Add Filter**.

Step 3 Enter a name and description for the content filter.

Step 4 Click **Add Condition**.

Step 5 Click **URL Reputation**.

Step 6 Select **External Threat Feeds**.

Step 7 Select the ETF source(s) to detect malicious URLs.

Step 8 (Optional) Select the list of allow listed URLs that you do not want the email gateway to detect for threats.

Step 9 Select the required **Check URLs within** option to detect malicious URLs in the message body and subject and/or message attachments.

Step 10 Click **OK**.

Step 11 Click **Add Action**.

Step 12 Click **URL Reputation**.

Step 13 Select **External Threat Feeds**.

Step 14 Make sure that you select the same ETF source(s) that you selected in the condition (Step 7).

Step 15 (Optional) Select the same list of allow listed URLs that you selected in Step 8.

Step 16 Select the required **Check URLs within** option to detect malicious URLs in the 'message body and subject' and/or 'message attachments'

Step 17 Select the required action that you want to perform on the URLs within the message body and subject and/or message attachments.

Note
In Step 16, if you choose the 'Check URLs within' option as 'Attachments', you can only strip the attachment from the message.

Step 18 Select whether you want to take actions on all messages or unsigned messages.

Step 19 Click **OK**.

Step 20 Submit and commit your changes.

Note
If you have configured URL Reputation content filters for Web Based Reputation Score (WBRS) and ETF on your email gateway, it is recommended to set the order of the WBRS URL Reputation content filter higher than the order of the ETF URL Reputation filter, to improve the performance of your emal gateway.

Detecting Malicious URLs in Messages Using Message Filter

As an example, use the ‘URL Reputation’ message filter rule syntax to detect malicious URLs in messages using the ETF engine, and to defang the URL.

Syntax:

```
 defang_url_in_message: if (url-external-threat-feeds (['etf_source1'],
 <'URL_allowedlist'>,
<’message_attachments'> , <’message_body_subject’> ,))
 { url-etf-defang(['etf-source1'], "", 0); } <’URL_allowedlist’> ,
<’Preserve_signed’>)}
```

Where

- `‘url-external-threat-feeds’` is the URL Reputation rule.
- `‘etf_source1’` is the ETF source(s) used to detect malicious URLs in the messages or message attachments.

- `'URL_allowedlist'` is the name of a URL allowed list. If a URL allowed list is not present, it is displayed as "".
- `'message_attachments'` is used to check for malicious URLs in the message attachments. A value of '1' is used to detect malicious URLs in the message attachments.
- `'message_body_subject'` is used to check for malicious URLs in the message body and subject. A value of '1' is used to detect malicious URLs in the message body and subject.

Note A value of "1,1" is used to detect malciocus URLs in the message body, subject, and message attachments.

- `'url-etf-defang'` is one of the actions that you can take on messages that contain malicious URLs.

  The following examples are the ETF-based actions that you can apply on messages that contain malicious URLs:

  - url-etf-strip(['etf_source1'], "None", 1)
  - url-etf-defang-strip(['etf_source1'], "None", 1, "Attachment removed")
  - url-etf-defang-strip(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect-strip(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect-strip(['etf_source1'], "None", 1, " Attachment removed")
  - url-etf-replace(['etf_source1'], "", "None", 1)
  - url-etf-replace(['etf_source1'], "URL removed", "None", 1)
  - url-etf-replace-strip(['etf_source1'], "URL removed ", "None", 1)
  - url-etf-replace-strip(['etf_source1'], "URL removed*", "None", 1, "Attachment removed")

- `'Preserve_signed'` is represented by '1' or '0'. '1' indicates that this action applies to unsigned messages only and '0' indicates that this action applies to all messages.

In the following example, if a URL in the message attachment is detected as malicious by the ETF engine, the attachment is stripped.

```
Strip_Malicious_URLs: if (true) {url-etf-strip(['threat_feed_source'], "", 0);}
```

Monitoring URL Filtering Results

To view data about malicious and neutral URLs detected, select **Monitor** > **URL Filtering**. For important information about the data on this page, see URL Filtering Page.

To view data about messages with malicious URL that are remediated form user's mailbox, see URL Retrospection Page.

Displaying URL Details in Message Tracking

To display details in Message Tracking for URLs caught by outbreak filters and relevant content filters:

- Message Tracking must be enabled.
- Outbreak filters and/or content filters based on URL reputation or URL Category must be operational.
- For outbreak filters, URL Rewriting must be enabled. See URL Rewriting and Bypassing Domains.
- URL logging must be enabled. See Enabling Logging of URLs and Message Tracking Details for URLs.
- Mailbox remediation must be enabled to display details in Message Tracking about messages with malicious URLs that are remediated from user's mailbox based on URL retrospective verdict update. See Remediating Messages in Mailboxes.

For more information about the data displayed, see Message Tracking Details.

To manage administrative user access to these potentially sensitive details, see Controlling Access to Sensitive Information in Message Tracking.

Troubleshooting URL Filtering

Related Topics

- Viewing Logs , on page 21
- Alert: Beaker Connector: Error Fetching Enrollment Certificate , on page 21
- Alert: Beaker Connector: Certificate Is Invalid , on page 22
- Unable to Connect to Talos Intelligence Services, on page 22
- Alert: Unable to Connect to the Cisco Aggregator Server, on page 22
- Alert: Unable to Retrieve Web Interaction Tracking Information from the Cisco Aggregator Server, on page 23
- Using the websecurityadvancedconfig Command , on page 23
- Message Tracking Search Does Not Find Messages with Specified Category , on page 23
- Malicious URLs and Marketing Messages Are Not Caught by Anti-Spam or Outbreak Filters , on page 24
- URLs in a Filtered Category Are Not Handled Correctly , on page 24
- End User Reaches Malicious Site via Rewritten URL , on page 24
- Manually Configuring a Certificate for Communication with Talos Intelligence Services , on page 25

Viewing Alerts

The following table lists the system alerts generated by the URL Filtering engine, including a description of the alert and the alert severity.

Component/Alert Name	Message and Description	Parameters
ECS REMEDIATION_INITIATION	Alert Text: "Mail remediation initiated for messages messages with malicious URLs: $message_id : $url" Information: Alert sent when the mailbox remediation initiated by the remediation service to remediate malicious URL that is already delivered to user's mailbox is success or failure.	• **message_id** - The message ID of the message that contains the URL. • **url** - The URL for which the retrospective verdict is received.
ECS INFO	Alert Text: "Verdict update received from URL retrospective service. The message IDs, MIDs, and URLs are as below in the format: $message_id : $mid : $url" Information: Alert sent when your email gateway receives a URL retrospective verdict from the retrospective server.	• **message_id** - The message ID of the message that contains the URL. • **mid** - Message identifier number. • **url** - The URL for which the retrospective verdict is received.
ECS CRITICAL	Alert Text: Polling to receive retrospective verdict on URL reputation failed with invalid certificate error. Contact Cisco TAC for assistance. Warning: Alert sent when your email gateway fails to receive the URL retrospective verdict from the retrospective server because of invalid certificate. Contact Cisco TAC for assistance.	N/A
ECS WARN	Alert Text: Restart URL retrospective polling service to fix the incorrect request format. Warning: Alert sent to restart the URL retrospective polling service to correct the format of the polling request.	N/A

Component/Alert Name	Message and Description	Parameters
ECS CRITICAL	Connection Error: Unable to connect to retrospective registration service. Contact Cisco TAC for assistance. Reasons for failure: • Invalid certificate error. • Cloud service is unavailable. • Connection request is rejected (for example, invalid certificate key).	N/A

Viewing Logs

URL filtering information is posted to the following logs:

- Mail Logs (mail_logs). Information related to the result of scanning a URL (action taken of a message depending on the URL) is posted to this log.
- URL Filtering Logs (web_client). Information related to errors, timeouts, network issues, and so on while attempting the URL lookup are posted this log.
- Remediation Logs. Information related to the mailbox remediation based on URL retrospective service is posted to this log.
- Email Cloud Scanner Logs. Information related to the URL retrospective verdicts received from the Retrospective cloud scanner.

Most information is at Info or Debug level. For more information on logs, see Logging.

Logs do not include information about what happens when a user clicks a redirected link in a message.

"SDS" and in logs refers to URL reputation services. "Beaker Connector" refers to Talos engine.

Alert: Beaker Connector: Error Fetching Enrollment Certificate

Problem

You receive an info-level alert about an error fetching the enrollment client certificate.

Solution

This certificate is required to connect to the following cloud-based services: Talos Intelligence Services (to obtain URL reputation and category) and Cisco Aggregator Server (to obtain web interaction tracking data). Try the following:

1. Check for networking issues such as incorrect proxy settings or firewall issues.
2. Verify that your URL Filtering feature key is valid and active.
3. If the problem persists, contact Cisco TAC.

Alert: Beaker Connector: Certificate Is Invalid

Problem

You receive a critical alert about an invalid Beaker connector certificate.

Solution

This certificate is required to connect to Talos Intelligence Services in the cloud in order to obtain URL reputation and category.

To obtain and manually install a certificate, see Manually Configuring a Certificate for Communication with Talos Intelligence Services , on page 25.

Unable to Connect to Talos Intelligence Services

Problem

The **Security Services > URL Filtering** page persistently indicates an issue connecting to Talos Intelligence Services.

Solution

- If you have enabled URL filtering but have not yet committed the change, commit the change.
- Check for recent alerts related to the connection with Talos Intelligence Services. See Viewing Recent Alerts. If applicable, see Alert: Beaker Connector: Error Fetching Enrollment Certificate , on page 21 and Alert: Beaker Connector: Certificate Is Invalid , on page 22.
- If you are connecting via a proxy specified in **Security Services > Service Updates**, verify that this is configured and working properly.
- Check for other network issues that might prevent connection.
- If you see errors in the URL Filtering Logs related to timed out requests to the Talos client, use the websecuritydiagnostics command and the **`websecurityadvancedconfig`** command in the command-line interface to investigate and make changes:
    - If the diagnostics show that Response Time is not less than the configured URL Lookup Timeout, increase the URL Lookup Timeout value accordingly.
- Check the URL Filtering Logs for non-timeout errors in communications with the URL scanner, Cisco Web Security Services, or Talos client. "Talos client" in logs represents Talos Intelligence Services. If you see such log messages, contact TAC.

Alert: Unable to Connect to the Cisco Aggregator Server

Problem

You receive the following warning alert: Unable to Connect to the Cisco Aggregator Server.

Solution

Do the following:

1. Check the connectivity between the email gateway and the Cisco Aggregator Server by pinging the hostname of the server from the email gateway. Use the aggregatorconfig command in CLI to view the hostname of the Cisco Aggregator Server.
2. If you are connecting via a proxy specified in Security Services > Service Updates, verify that this is configured and working properly.

3. Check for other network issues that might prevent connection.
4. Check if the DNS service is running.
5. If the problem persists, contact Cisco TAC.

Alert: Unable to Retrieve Web Interaction Tracking Information from the Cisco Aggregator Server

Problem

You receive the following warning alert: Unable to retrieve web interaction tracking information from the Cisco Aggregator Server.

Solution

Do the following:

1. If you are connecting via a proxy specified in **Security Services > Service Updates**, verify that this is configured and working properly.
2. Check for other network issues that might prevent connection.
3. Check if the DNS service is running.
4. If the problem persists, contact Cisco TAC.

Alert: Email Cloud Scanner (ECS): Certificate Is Invalid

Problem

You receive a critical alert about an invalid ECS connector certificate.

Solution

Retrospective server certicate validation failed by the Email Cloud Scanner client. This certificate is required to connect to the client to obtain the URL retrospective update. To fix this error, contact Cisco Support.

Alert: Email Cloud Scanner (ECS): Network is Unreachable

Problem

You receive a critical alert when your email gateway is unable to reach the URL Retrospective cloud scanner service.

Solution

Verify your firewall settings. Contact your network administrator for assistance.

Using the websecurityadvancedconfig Command

Except for changes explicitly described in this document, make no other changes using the websecurityadvancedconfig command without guidance from TAC.

Message Tracking Search Does Not Find Messages with Specified Category

Problem

Messages that contain URLs in a particular category are not found when searching by that category.

Solution

See Expected Messages Are Missing from Search Results.

Malicious URLs and Marketing Messages Are Not Caught by Anti-Spam or Outbreak Filters

Problem

Malicious URLs and messages containing marketing links are not caught by the anti-spam or outbreak filters.

Solution

- This can occur because web site reputation and category are only two among many criteria that anti-spam and outbreak filters use to determine their verdicts. You can increase the sensitivity of these filters by lowering the thresholds required to take action such as rewriting or replacing URLs with text, or quarantining or dropping messages. For details, see The Outbreak Filters Feature and Mail Policies and Defining Anti-Spam Policies. Alternatively, create content or message filters based on URL reputation score.
- This can also occur if the email gateway is unable to connect to the Talos Intelligence Services. See Unable to Connect to Talos Intelligence Services, on page 22.

URLs in a Filtered Category Are Not Handled Correctly

Problem

The defined action in a content or message filter based on URL category is not applied.

Solution

- Use the Trace feature (described in the Troubleshooting chapter) to follow the message processing path.
- This can occur if the email gateway is unable to connect to the Talos Intelligence Services. See Unable to Connect to Talos Intelligence Services, on page 22.
- If there are no connection issues, the URLs may not yet be categorized, or may be miscategorized. See Reporting Uncategorized and Misclassified URLs , on page 38. You can use this site to determine the category of a URL.

End User Reaches Malicious Site via Rewritten URL

Problem

A malicious URL was redirected to the Cisco Web Security Proxy, but the end user was able to access the site anyway.

Solution

This can occur if:

- The site was not yet identified as a malicious site.
- The connection to the Cisco Web Security Proxy timed out, which should be a rare occurrence. Ensure that network issues are not interfering with the connection.

Manually Configuring a Certificate for Communication with Talos Intelligence Services

Use this procedure if the email gateway is unable to automatically obtain a certificate for communication with Talos Intelligence Services.

Procedure

Step 1 Obtain the required certificate.

Step 2 Upload the certificate using **Network > Certificates,** or use the certconfig command in the command-line interface.

Step 3 In the command-line interface, enter the **`websecurityconfig`** command.

Step 4 Follow the prompts to set the client certificate for Talos Intelligence Services Authentication.

About URL Categories

Related Topics

- URL Category Descriptions , on page 25
- Determining the Category of a URL , on page 38
- Reporting Uncategorized and Misclassified URLs , on page 38
- Future URL Category Set Changes , on page 38

URL Category Descriptions

These URL categories are the same categories that are used on recent releases of AsyncOS for Web Security appliances.

URL Category	Abbrev ia-tion	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.adultnetline.com

URL Category	Abbrevia-tion	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 Nutrition.” Bars and restaurants are classified as “Dining and Drinking.”	www.samueladams.com www.whisky.com
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	Abbrev ia-tion	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.staples.com
Chat and Instant Messaging	chat	1040	Web-based instant messaging and chat rooms.	www.icq.com www.meebo.com
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.	—
Computer Security	csec	1065	Offering security products and services for corporate and home users.	www.computersecurity.com www.symantec.com

URL Category	Abbrevia-tion	Code	Description	Example URLs
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 clip art. “Freeware and Shareware” is a separate category.	www.xml.com www.w3.org
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.all-yours.net www.delivr.net
Dining and Drinking	food	1061	Eating and drinking establishments; restaurants, bars, taverns, and pubs; restaurant guides and reviews.	www.hideawaybrewpub.com www.restaurantrow.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 http://dynalink.co.jp http://ipadsl.net
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

URL Category	Abbrev ia-tion	Code	Description	Example URLs
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 Nutrition.”	www.fashion.net www.findabeautysalon.com
File Transfer Services	fts	1071	File transfer services with the primary purpose of providing download services and hosted file sharing	www.rapidshare.com www.yousendit.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.”	finance.yahoo.com www.bankofamerica.com
Freeware and Shareware	free	1068	Providing downloads of free and shareware software.	www.freewarehome.com www.shareware.com

URL Category	Abbrevia-tion	Code	Description	Example URLs
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 Nutrition." 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

URL Category	Abbrev ia-tion	Code	Description	Example URLs
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.nazi.org
Health and Nutrition	hlth	1009	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); food in general; food and beverage; cooking and recipes; food and nutrition, health, and dieting; cooking, including recipe and culinary websites; alternative medicine.	www.health.com www.webmd.com
Humor	lol	1079	Jokes, sketches, comics and other humorous content. Adult humor likely to offend is classified as “Adult.”	www.humor.com www.jokes.com
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.thedisease.net

URL Category	Abbrevia-tion	Code	Description	Example URLs
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.keygenguru.com www.zcrack.com
Illegal Drugs	drug	1047	Information about recreational drugs, drug paraphernalia, drug purchase and manufacture.	www.cocaine.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
Internet Telephony	voip	1067	Telephonic services using the Internet.	www.evaphone.com www.skype.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 swim wear, especially when modeled.	www.swimsuits.com www.victoriassecret.com
Lotteries	lotr	1034	Sweepstakes, contests and state-sponsored lotteries.	www.calottery.com www.flalottery.com
Mobile Phones	cell	1070	Short Message Services (SMS); ring tones and mobile phone downloads. Cellular carrier websites are included in the "Business and Industry" category.	www.cbfsms.com www.zedge.net

URL Category	Abbrev ia-tion	Code	Description	Example URLs
Nature	natr	1013	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); animals, pets, livestock, and zoology; biology; botany.	www.enature.com www.nature.org
News	news	1058	News; headlines; newspapers; television stations; magazines; weather; ski conditions.	www.cnn.com 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.artenuda.com www.naturistsociety.com
Online Communities	comm	1024	Affinity groups; special interest groups; web newsgroups; message boards. Excludes websites classified as “Professional Networking” or “Social Networking.”	www.igda.org www.ieee.org
Online Storage and Backup	osb	1066	Offsite and peer-to-peer storage for backup, sharing, and hosting.	www.adrive.com www.dropbox.com

URL Category	Abbrevia-tion	Code	Description	Example URLs
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.scottrade.com
Organizational Email	pem	1085	Websites used to access business email (often via Outlook Web Access).	—
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.parked.com
Peer File Transfer	p2p	1056	Peer-to-peer file request websites. This does not track the file transfers themselves.	www.bittorrent.com www.limewire.com
Personal Sites	pers	1081	Websites about and from private individuals; personal homepage servers; websites with personal contents; personal blogs with no particular theme.	www.karymullis.com www.stallman.org
Photo Searches and Images	img	1090	Facilitating the storing and searching for, images, photographs, and clip-art.	www.flickr.com www.photobucket.com
Politics	pol	1083	Websites of politicians; political parties; news and information on politics, elections, democracy, and voting.	www.politics.com www.thisnation.com

URL Category	Abbrevia-tion	Code	Description	Example URLs
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
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
Reference	ref	1017	City and state guides; maps, time; reference sources; dictionaries; libraries.	www.wikipedia.org www.yellowpages.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.	kids.discovery.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

URL Category	Abbrev ia-tion	Code	Description	Example URLs
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.childcare.gov www.familysearch.org
Software Updates	swup	1053	Websites that host updates for software packages.	www.softwarepatch.com www.versiontracker.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
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 Nutrition.”	www.bat.com www.tobacco.org

URL Category	Abbrev ia-tion	Code	Description	Example URLs
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
Unclassified	—	—	Websites which are not in the Cisco database are recorded as unclassified for reporting purposes. This may include mistyped 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 Hosting	whst	1037	Website hosting; bandwidth services.	www.bluehost.com www.godaddy.com
Web Page Translation	tran	1063	Translation of web pages between languages.	babelfish.yahoo.com translate.google.com

URL Category	Abbrev ia-tion	Code	Description	Example URLs
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."	mail.yahoo.com www.hotmail.com

Determining the Category of a URL

To look up the category of a particular URL, visit the site shown in Reporting Uncategorized and Misclassified URLs , on page 38.

Reporting Uncategorized and Misclassified URLs

To report URLs that have been miscategorized, and URLs that are not categorized but should be, visit:

https://talosintelligence.com/reputation_center/support

To check the status of submitted URLs, click the **Status on Submitted URLs** tab on this page.

Future URL Category Set Changes

Rarely, the set of URL categories may change as a result of emerging trends and technologies. For example, a category may be added or removed, renamed, merged with another category, or split into two categories. These changes can affect the results from existing filters, so if changes occur, the email gateway will send an alert (System type, Warning severity). If you receive such an alert, you should evaluate and possibly update content and message filters to work with the updated categories. Existing filters will not automatically be changed. To ensure that you receive these alerts, see Adding Alert Recipients.

The following changes do not require category set changes and will not generate alerts:

- Routine categorization of newly-categorized sites.
- Recategorization of misclassified sites.