Notify End-Users of Proxy Actions

This topic contains the following sections:

- End-User Notifications Overview, on page 1
- Configuring General Settings for Notification Pages, on page 2
- End-User Acknowledgment Page, on page 2
- End-User Notification Pages , on page 6
- Configuring the End-User URL Filtering Warning Page, on page 9
- Configuring FTP Notification Messages, on page 10
- Custom Messages on Notification Pages, on page 11
- Editing Notification Page HTML Files Directly , on page 12
- Notification Page Types, on page 16

End-User Notifications Overview

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

Option	Description	Further information
End-user acknowledgement page	Informs end users that their web activity is being filtered and monitored. An end-user acknowledgment page is displayed when a user first accesses a browser after a certain period of time.	End-User Acknowledgment Page, on page 2
End-user notification pages	Page shown to end users when access to a particular page is blocked, specific to the reason for blocking it.	End-User Notification Pages , on page 6
End-user URL filtering warning page	Warns end users that a site they are accessing does not meet your organization's acceptable use policies, and allows them to continue if they choose.	Configuring the End-User URL Filtering Warning Page, on page 9
FTP notification messages	Gives end users the reason a native FTP transaction was blocked.	Configuring FTP Notification Messages, on page 10.

Option	Description	Further information
Time and Volume Quotas Expiry Warning Page	Notifies end users when their access is blocked because they have reached the configured data volume or time limit.	Configure these settings on the Security Services > End User Notification page, Time and Volume Quotas Expiry Warning Page section. See also Time Ranges and Quotas.

Configuring General Settings for Notification Pages

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

Procedure

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

Step 2 Click **Edit Settings**.

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

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

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

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

Step 5 Submit and Commit Changes.

What to do next

Related Topics

- Caveats for URLs and Logos in Notification Pages , on page 11

End-User Acknowledgment Page

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

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

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

- Access HTTPS and FTP Sites with the End-User Acknowledgment Page, on page 3
- About the End-user Acknowledgment Page, on page 3
- Configuring the End-User Acknowledgment Page, on page 4

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

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

- **HTTPS.** The Web Proxy tracks whether the user has acknowledged the end-user acknowledgment page with a cookie, but it cannot obtain the cookie unless it decrypts the transaction. You can choose to either bypass (pass through) or drop HTTPS requests when the end-user acknowledgment page is enabled and tracks users using session cookies. Do this using the advancedproxyconfig > EUN CLI command, and choose bypass for the "Action to be taken for HTTPS requests with Session based EUA ("bypass" or "drop")." command.
- **FTP over HTTP.** Web browsers never send cookies for FTP over HTTP transactions, so the Web Proxy cannot obtain the cookie. To work around this, you can exempt FTP over HTTP transactions from requiring the end-user acknowledgment page. Do this by creating a custom URL category using "ftp://" as the regular expression (without the quotes) and defining and Identity policy that exempts users from the end-user acknowledgment page for this custom URL category.

About the End-user Acknowledgment Page

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

Configuring the End-User Acknowledgment Page

Before you begin

- To configure the display language and customize the displayed logo, see Configuring General Settings for Notification Pages, on page 2.
- If you will customize the message shown to end users, see Custom Messages on Notification Pages, on page 11. If you require more customization than the Custom Message box allows, see Editing Notification Page HTML Files Directly , on page 12.

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

In the CLI, use `advancedproxyconfig > eun`.

Procedure

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

Step 2 Click **Edit Settings**.

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

Step 4 Enter options:

Setting	Description
Time Between Acknowledgements	The Time Between Acknowledgments determines how often the Web Proxy displays the end-user acknowledgment page for each user. This setting applies to users tracked by username and users tracked by IP address or session cookie. You can specify any value from 30 to 2678400 seconds (one month). Default is one day (86400 seconds). When the Time Between Acknowledgments changes and is committed, the Web Proxy uses the new value even for users who have already acknowledged the Web Proxy.
Inactivity Timeout	The Inactivity Timeout determines how long a user tracked and acknowledged by IP address or session cookie (unauthenticated users only) can be idle before the user is no longer considered to have agreed to the acceptable use policy. You can specify any value from 30 to 2678400 seconds (one month). Default is four hours (14400 seconds).

Setting	Description
Surrogate Type	Determines which method the Web Proxy uses to track the user: • **IP Address.** The Web Proxy allows the user at that IP address to use any web browser or non-browser HTTP process to access the web once the user clicks the link on the end-user acknowledgment page. Tracking the user by IP address allows the user to access the web until the Web Proxy displays a new end-user acknowledgment page due to inactivity or the configured time interval for new acknowledgments. Unlike tracking by a session cookie, tracking by IP address allows the user to open up multiple web browser applications and not have to agree to the end-user acknowledgment unless the configured time interval has expired. **Note** When IP address is configured and the user is authenticated, the Web Proxy tracks users by username instead of IP address. • **Session Cookie.** The Web Proxy sends the user's web browser a cookie when the user clicks the link on the end-user acknowledgment page and uses the cookie to track their session. Users can continue to access the web using their web browser until the Time Between Acknowledgments value expires, they have been inactive longer than the allotted time, or they close their web browser. If the user using a non-browser HTTP client application, they must be able to click the link on the end-user acknowledgment page to access the web. If the user opens a second web browser application, the user must go through the end-user acknowledgment process again in order for the Web Proxy to send a session cookie to the second web browser. **Note** Using a session cookie to track users when the client accesses HTTPS sites or FTP servers using FTP over HTTP is not supported.
Custom message	Customize the text that appears on every end-user acknowledgment page. You can include some simple HTML tags to format the text. **Note** You can only include a custom message when you configure the end-user acknowledgment page in the web interface, versus the CLI. See also Custom Messages on Notification Pages, on page 11.

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

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

Step 6 Submit and Commit Changes.

End-User Notification Pages

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

To	See
Display predefined, customizable pages that are hosted on the Web Security Appliance .	Configuring On-Box End-User Notification Pages, on page 6
Redirect the user to HTTP end-user notification pages at a specific URL.	Off-Box End-User Notification Pages , on page 7

Configuring On-Box End-User Notification Pages

Before you begin

- To configure the display language and customize the displayed logo, see Configuring General Settings for Notification Pages, on page 2.
- If you will customize the message displayed using on-box notifications, review the topics under Custom Messages on Notification Pages, on page 11. If you require more customization than the Custom Message box allows, see Editing Notification Page HTML Files Directly , on page 12.

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

Procedure

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

Step 2 Click **Edit Settings**.

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

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

Setting	Description
Custom Message	Include any additional text required on each notification page. When you enter a custom message, AsyncOS places the message before the last sentence on the notification page which includes the contact information.
Contact Information	Customize the contact information listed on each notification page. AsyncOS displays the contact information sentence as the last sentence on a page, before providing notification codes that users can provide to the network administrator.

Setting	Description
End-User Misclassification Reporting	When enabled, users can report misclassified URLs to Cisco. An additional button appears on the on-box end-user notification pages for sites blocked due to suspected malware or URL filters. This button allows the user to report when they believe the page has been misclassified. It does not appear for pages blocked due to other policy settings. **Note** • You must enable SensorBase Network Participation. See Enabling Participation in The Cisco SensorBase Network for more information. • You must have a valid Cisco account linked to the serial number/s of your appliance/s. • Reporting of misclassified URLs does not work on virtual Web Security Appliance .

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

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

Step 6 Submit and Commit Changes.

Off-Box End-User Notification Pages

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

- Displaying the Correct Off-Box Page Based on the Reason for Blocking Access , on page 7
- URL Criteria for Off-Box Notification Pages , on page 7
- Off-Box End-User Notification Page Parameters, on page 8
- Redirecting End-User Notification Pages to a Custom URL (Off-Box) , on page 9

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

By default, AsyncOS redirects all blocked websites to the URL regardless of the reason why it blocked the original page. However, AsyncOS also passes parameters as a query string appended to the redirect URL so you can ensure that the user sees a unique page explaining the reason for the block. For more information on the included parameters, see Off-Box End-User Notification Page Parameters, on page 8.

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

URL Criteria for Off-Box Notification Pages

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

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

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

And you have the following access log entry:

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

Then AsyncOS creates the following redirected URL:

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

Off-Box End-User Notification Page Parameters

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

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

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

Parameter Name	Description
Time	Date and time of the transaction.
ID	Transaction ID.
Client_IP	IP address of the client.
User	Username of the client making the request, if available.
Site	Hostname of the destination in the HTTP request.
URI	URL path specified in the HTTP request.
Status_Code	HTTP status code for the request.
Decision_Tag	ACL decision tag as defined in the Access log entry that indicates how the DVS engine handled the transaction.
URL_Cat	URL category that the URL filtering engine assigned to the transaction request. **Note:** AsyncOS for Web sends the entire URL category name for both predefined and user defined URL categories. It performs URL encoding on the category name, so spaces are written as “%20”.
WBRS	WBRS score that the Web Reputation Filters assigned to the URL in the request.
DVS_Verdict	Malware category that the DVS engine assigns to the transaction.

Parameter Name	Description
DVS_ThreatName	The name of the malware found by the DVS engine.
Reauth_URL	A URL that users can click to authenticate again if the user is blocked from a website due to a restrictive URL filtering policy. Use this parameter when the "Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction" global authentication setting is enabled and the user is blocked from a website due to a blocked URL category. To use this parameter, make sure the CGI script performs the following steps: 1. Get the value of `Reauth_Url` parameter. 2. URL-decode the value. 3. Base64 decode the value and get the actual re-authentication URL. 4. Include the decoded URL on the end-user notification page in some way, either as a link or button, along with instructions for users informing them they can click the link and enter new authentication credentials that allow greater access.

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

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

Procedure

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

Step 2 Click **Edit Settings**.

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

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

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

Step 6 Submit and Commit Changes.

Configuring the End-User URL Filtering Warning Page

Before you begin

- If you will customize the message displayed using on-box notifications, review the topics under Custom Messages on Notification Pages, on page 11. If you require more customization than the Custom Message box allows, see Editing Notification Page HTML Files Directly , on page 12.

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

Procedure

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

Step 2 Click **Edit Settings**.

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

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

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

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

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

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

Step 7 Submit and Commit Changes.

Configuring FTP Notification Messages

Before you begin

If you will customize the message displayed using on-box notifications, review the topics under Custom Messages on Notification Pages, on page 11. If you require more customization than the Custom Message box allows, see Editing Notification Page HTML Files Directly , on page 12.

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

Procedure

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

Step 2 Click **Edit Settings**.

Step 3 Scroll down to the Native FTP section.

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

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

Step 6 Submit and Commit Changes.

Custom Messages on Notification Pages

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

- Supported HTML Tags in Custom Messages on Notification Pages, on page 11
- Caveats for URLs and Logos in Notification Pages , on page 11

Supported HTML Tags in Custom Messages on Notification Pages

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

You can use the following HTML tags.

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

For example, you can make some text italic:

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

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

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

Note If you need greater flexibility or wish to add JavaScript to your notification pages, you must edit the HTML notification files directly. JavaScript entered into the Custom Message box for notifications in the web user interface will be stripped out. See Editing Notification Page HTML Files Directly , on page 12.

Caveats for URLs and Logos in Notification Pages

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

- Enter text into the “Custom Message” box for any notification on the Edit End User Notification page

- Directly edit HTML files for on-box notifications
- Use a custom logo

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

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

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

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

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

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

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

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

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

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

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

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

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

Editing Notification Page HTML Files Directly

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

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

- Requirements for Editing Notification HTML Files Directly , on page 12
- Editing Notification Page HTML Files Directly , on page 12
- Using Variables in Notification HTML Files , on page 14
- Variables for Customizing Notification HTML Files , on page 14

Requirements for Editing Notification HTML Files Directly

- Each notification page file must be a valid HTML file. For a list of HTML tags you can include, see Supported HTML Tags in Custom Messages on Notification Pages, on page 11.

- The customized notification page file names must exactly match the file names shipped with the Web Security Appliance .

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

Editing Notification HTML Files Directly

Before you begin

- Understand the requirements in Requirements for Editing Notification HTML Files Directly , on page 12.
- See Variables for Customizing Notification HTML Files , on page 14 and Using Variables in Notification HTML Files , on page 14.

Procedure

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

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

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

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

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

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

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

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

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

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

Step 10 Commit your change.

Step 11 Close the SSH client.

Using Variables in Notification HTML Files

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

The table describes the different conditional variable formats.

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

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

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

Any variable included in Variables for Customizing Notification HTML Files , on page 14 can be used as a conditional variable. However, the best variables to use in conditional statements are the ones that relate to the *client request* instead of the server response, and the variables that may or may not evaluate to TRUE instead of the variables that always evaluate to TRUE.

Variables for Customizing Notification HTML Files

You can use variables in the notification HTML files to display specific information to the user. You can also turn each variable into a conditional variable to create if-then statements. For more information, see Using Variables in Notification HTML Files , on page 14.

Variable	Description	Always Evaluates to TRUE if Used as Conditional Variable
%a	Authentication realm for FTP	No
%A	ARP address	Yes
%b	User-agent name	No
%B	Blocking reason, such as BLOCK-SRC or BLOCK-TYPE	No

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

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

Notification Page Types

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

Most notification pages display a different set of codes that may help administrators or Cisco Customer Support troubleshoot any potential problem. Some codes are for Cisco internal use only. The different codes that might appear in the notification pages are the same as the variables you can include in customized notification pages, as shown in Variables for Customizing Notification HTML Files , on page 14.

The table describes the different notification pages users might encounter.

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

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

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

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

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

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

File Name and Notification Title	Notification Description	Notification Text
ERR_PROXY_UNACKNOWLEDGED Policy Acknowledgment	End-user acknowledgment page. For more information, see End-User Notification Pages , on page 6.	Please acknowledge the following statements before accessing the Internet. Your web transactions will be automatically monitored and processed to detect dangerous content and to enforce organization's policies. By clicking the link below, you acknowledge this monitoring and accept that data about the sites you visit may be recorded. You will be periodically asked to acknowledge the presence of the monitoring system. You are responsible for following organization's polices on Internet access. Click here to accept this statement and access the Internet.
ERR_PROXY_UNLICENSED Proxy Not Licensed	Block page that is displayed when there is no valid license key for the Web Security Appliance Web Proxy.	Internet access is not available without proper licensing of the security device. Please contact <*contact name*> <*email address*> and provide the code shown below. **Note** To access the management interface of the security device, enter the configured IP address with port.
ERR_RANGE_NOT_SATISFIABLE Range Not Satisfiable	Error page that is displayed when the requested range of bytes cannot be satisfied by the web server.	The system cannot process this request. A non-standard browser may have generated an invalid HTTP request. If you are using a standard browser, please retry the request.
ERR_REDIRECT_PERMANENT Redirect Permanent	Internal redirection page.	The page <*URL*> is being redirected to <*redirected URL*>.
ERR_REDIRECT_REPEAT_REQUEST Redirect	Internal redirection page.	Please repeat your request.

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

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