

Monitoring and Troubleshooting

This topic contains the following sections:

- Monitor System Activity Through Logs, on page 1
- Troubleshooting, on page 54

Monitor System Activity Through Logs

This topic contains the following sections:

- Overview of Logging, on page 2
- Common Tasks for Logging, on page 2
- Best Practices for Logging, on page 2
- Troubleshooting Web Proxy Issues Using Logs, on page 3
- Log File Types, on page 4
- Adding and Editing Log Subscriptions, on page 8
- Pushing Log Files to Another Server, on page 13
- Archiving Log Files, on page 14
- Log File Names and Appliance Directory Structure, on page 15
- Viewing Log Files, on page 16
- Web Proxy Information in Access Log Files, on page 16
- W3C Compliant Access Log Files, on page 33
- Customizing Access Logs, on page 35
- Traffic Monitor Log Files, on page 40
- Log File Fields and Tags, on page 41
- Troubleshooting Logging, on page 54

Overview of Logging

The Secure Web Appliance records its own system and traffic management activities by writing them to log files. Administrators can consult these log files to monitor and troubleshoot the appliance.

The appliance divides different types of activity into different logging types to simplify the task of finding information on specific activities. The majority of these are automatically enabled by default, but some must be manually enabled as required.

You enable and manage log files through log file subscriptions. Subscriptions allow you to define the settings for creating, customizing, and managing log files.

The two main log files types typically used by administrators are:

- **Access log.** This records all Web Proxy filtering and scanning activity.
- **Traffic Monitor log.** This records all Layer-4 Traffic Monitor activity.

You can view current and past appliance activity using these and other log types. Reference tables are available to help you interpret log file entries.

Related Topics

- Common Tasks for Logging, on page 2
- Log File Types, on page 4

Common Tasks for Logging

Task	Links to Related Topics and Procedures
Add and edit log subscriptions	Adding and Editing Log Subscriptions, on page 8
View log files	Viewing Log Files, on page 16
Interpret log files	Interpreting Access Log Scanning Verdict Entries, on page 27
Customize log files	Customizing Access Logs, on page 35
Push log files to another server	Pushing Log Files to Another Server, on page 13
Archiving log files	Archiving Log Files, on page 14

Best Practices for Logging

- Minimizing the number of log subscriptions will benefit system performance.
- Logging fewer details will benefit system performance.

Troubleshooting Web Proxy Issues Using Logs

By default, the Secure Web Appliance has one log subscription created for Web Proxy logging messages, called the "Default Proxy Logs." This captures basic information on all Web Proxy modules. The appliance also includes log file types for each Web Proxy module so you can read more specific debug information for each module without cluttering up the Default Proxy Logs.

Follow the steps below to troubleshoot Web Proxy issues using the various logs available.

Procedure

Step 1 Read the Default Proxy Logs.

Step 2 If you see an entry that might related to the issue but does not have enough information to resolve it, create a log subscription for the relevant specific Web Proxy module. The following Web Proxy module logs types are available:

Access Control Engine Logs	Logging Framework Logs
AVC Engine Framework Logs	McAfee Integration Framework Logs
Configuration Logs	Memory Manager Logs
Connection Management Logs	Miscellaneous Proxy Modules Logs
Data Security Module Logs	Request Debug Logs
DCA Engine Framework Logs	SNMP Module Logs
Disk Manager Logs	Sophos Integration Framework Logs
FireAMP	WBRS Framework Logs
FTP Proxy Logs	WCCP Module Logs
HTTPS Logs	Webcat Integration Framework Logs
License Module Logs	Webroot Integration Framework Logs

Step 3 Recreate the issue and read the new Web Proxy module log for relevant entries.

Step 4 Repeat as required with other Web Proxy module logs.

Step 5 Remove subscriptions that are no longer required.

What to do next

Related Topics

- Log File Types, on page 4
- Adding and Editing Log Subscriptions, on page 8

Log File Types

Some log types related to the web proxy component are not enabled. The main web proxy log type, called the “Default Proxy Logs,” is enabled by default and captures basic information on all Web Proxy modules. Each Web Proxy module also has its own log type that you can manually enable as required.

The following table describes the Secure Web Appliance log file types.

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
Access Control Engine Logs	Records messages related to the Web Proxy ACL (access control list) evaluation engine.	No	No
Secure Endpoint Engine Logs	Records information about file reputation scanning and file analysis (Secure Endpoint.) See also Log Files.	Yes	Yes
Audit Logs	Records AAA (Authentication, Authorization, and Accounting) events. Records all user interaction with the application and command-line interfaces, and captures committed changes. Some of the audit log details are as follows: • User - Logon • User - Logon failed incorrect password • User - Logon failed unknown user name • User - Logon failed account expired • User - Logoff • User - Lockout • User - Activated • User - Password change • User - Password reset • User - Security settings/profile change • User - Created • User - Deleted/modified • Group/Role - Deletion / modified • Group /Role - Permissions change	Yes	Yes
Access Logs	Records Web Proxy client history.	Yes	Yes
Authentication Framework Logs	Records authentication history and messages.	No	Yes

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
AVC Engine Framework Logs	Records messages related to communication between the Web Proxy and the AVC engine.	No	No
AVC Engine Logs	Records debug messages from the AVC engine.	Yes	Yes
CLI Audit Logs	Records a historical audit of command line interface activity.	Yes	Yes
Configuration Logs	Records messages related to the Web Proxy configuration management system.	No	No
Connection Management Logs	Records messages related to the Web Proxy connection management system.	No	No
Data Security Logs	Records client history for upload requests that are evaluated by the Cisco Data Security Filters.	Yes	Yes
Data Security Module Logs	Records messages related to the Cisco Data Security Filters.	No	No
DCA Engine Framework Logs (Dynamic Content Analysis)	Records messages related to communication between the Web Proxy and the Cisco Web Usage Controls Dynamic Content Analysis engine.	No	No
DCA Engine Logs (Dynamic Content Analysis)	Records messages related to the Cisco Web Usage Controls Dynamic Content Analysis engine.	Yes	Yes
Default Proxy Logs	Records errors related to the Web Proxy. This is the most basic of all Web Proxy related logs. To troubleshoot more specific aspects related to the Web Proxy, create a log subscription for the applicable Web Proxy module.	Yes	Yes
Disk Manager Logs	Records Web Proxy messages related to writing to the cache on disk.	No	No
External Authentication Logs	Records messages related to using the external authentication feature, such as communication success or failure with the external authentication server. Even with external authentication is disabled, this log contains messages about local users successfully or failing logging in.	No	Yes
Feedback Logs	Records the web users reporting misclassified pages.	Yes	Yes

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
FTP Proxy Logs	Records error and warning messages related to the FTP Proxy.	No	No
FTP Server Logs	Records all files uploaded to and downloaded from the Secure Web Appliance using FTP.	Yes	Yes
GUI Logs (Graphical User Interface)	Records history of page refreshes in the web interface. GUI logs also include information about SMTP transactions, for example information about scheduled reports emailed from the appliance.	Yes	Yes
Haystack Logs	Haystack logs record web transaction tracking data processing.	Yes	Yes
HTTPS Logs	Records Web Proxy messages specific to the HTTPS Proxy (when the HTTPS Proxy is enabled).	No	No
ISE Server Logs	Records ISE server(s) connection and operational information.	Yes	Yes
License Module Logs	Records messages related to the Web Proxy's license and feature key handling system.	No	No
Logging Framework Logs	Records messages related to the Web Proxy's logging system.	No	No
Logging Logs	Records errors related to log management.	Yes	Yes
McAfee Integration Framework Logs	Records messages related to communication between the Web Proxy and the McAfee scanning engine.	No	No
McAfee Logs	Records the status of anti-malware scanning activity from the McAfee scanning engine.	Yes	Yes
Memory Manager Logs	Records Web Proxy messages related to managing all memory including the in-memory cache for the Web Proxy process.	No	No
Miscellaneous Proxy Modules Logs	Records Web Proxy messages that are mostly used by developers or customer support.	No	No
AnyConnect Secure Mobility Daemon Logs	Records the interaction between the Secure Web Appliance and the AnyConnect client, including the status check.	Yes	Yes
NTP Logs (Network Time Protocol)	Records changes to the system time made by the Network Time Protocol.	Yes	Yes

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
PAC File Hosting Daemon Logs	Records proxy auto-config (PAC) file usage by clients.	Yes	Yes
Proxy Bypass Logs	Records transactions that bypass the Web Proxy.	No	Yes
Reporting Logs	Records a history of report generation.	Yes	Yes
Reporting Query Logs	Records errors related to report generation.	Yes	Yes
Request Debug Logs	Records very detailed debug information on a specific HTTP transaction from all Web Proxy module log types. You might want to create this log subscription to troubleshoot a proxy issue with a particular transaction without creating all other proxy log subscriptions. **Note:** You can create this log subscription in the CLI only.	No	No
Auth Logs	Records messages related to the Access Control feature.	Yes	Yes
SHD Logs (System Health Daemon)	Records a history of the health of system services and a history of unexpected daemon restarts.	Yes	Yes
SNMP Logs	Records debug messages related to the SNMP network management engine.	Yes	Yes
SNMP Module Logs	Records Web Proxy messages related to interacting with the SNMP monitoring system.	No	No
Sophos Integration Framework Logs	Records messages related to communication between the Web Proxy and the Sophos scanning engine.	No	No
Sophos Logs	Records the status of anti-malware scanning activity from the Sophos scanning engine.	Yes	Yes
Status Logs	Records information related to the system, such as feature key downloads.	Yes	Yes
System Logs	Records DNS, error, and commit activity.	Yes	Yes
Traffic Monitor Error Logs	Records L4TM interface and capture errors.	Yes	Yes
Traffic Monitor Logs	Records sites added to the L4TM block and allow lists.	No	Yes

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
UDS Logs (User Discovery Service)	Records data about how the Web Proxy discovers the user name without doing actual authentication. It includes information about interacting with the Cisco adaptive security appliance for the Secure Mobility as well as integrating with the Novell eDirectory server for transparent user identification.	Yes	Yes
Updater Logs	Records a history of WBRS and other updates.	Yes	Yes
W3C Logs	Records Web Proxy client history in a W3C compliant format. For more information, see W3C Compliant Access Log Files, on page 33.	Yes	No
WBNP Logs (SensorBase Network Participation)	Records a history of Cisco SensorBase Network participation uploads to the SensorBase network.	No	Yes
WBRS Framework Logs (Web Reputation Score)	Records messages related to communication between the Web Proxy and the Web Reputation Filters.	No	No
WCCP Module Logs	Records Web Proxy messages related to implementing WCCP.	No	No
Webcat Integration Framework Logs	Records messages related to communication between the Web Proxy and the URL filtering engine associated with Cisco Web Usage Controls.	No	No
Webroot Integration Framework Logs	Records messages related to communication between the Web Proxy and the Webroot scanning engine.	No	No
Webroot Logs	Records the status of anti-malware scanning activity from the Webroot scanning engine.	Yes	Yes
Welcome Page Acknowledgement Logs	Records a history of web clients who click the Accept button on the end-user acknowledgement page.	Yes	Yes

Adding and Editing Log Subscriptions

You can create multiple log subscriptions for each type of log file. Subscriptions include configuration details for archiving and storage, including these:

- Rollover settings, which determine when log files are archived.

- Compression settings for archived logs.
- Retrieval settings for archived logs, which specifies whether logs are archived onto a remote server or stored on the appliance.

Procedure

Step 1 Choose **System Administration > Log Subscriptions**.

Step 2 To add a log subscription, click **Add Log Subscription**. Or, to edit a log subscription, click the name of the log file in the Log Name field.

Step 3 Configure the subscription:

Option	Description
Log Type	A list of available log file types that you can subscribe to. The other options on the page may change according to log file type you choose. **Note** The Request Debug Logs log type can only be subscribed to using the CLI and does not appear on this list.
Log Name	The name used to refer to the subscription on the Secure Web Appliance. This name is also used for the log directory which will store the log files for the subscription. Enter only ASCII characters ([0-9], [A-Z], [a-z], and_).
Rollover by File Size	The maximum file size to which the current log file can grow before it is archived and a new log file started. Enter a number between 100 kilobytes and 10 gigabytes.
Rollover by Time	The maximum time interval before the current log file is archived and a new log file started. The following interval types are available: • **None.** AsyncOS only performs a rollover when the log file reaches the maximum file size. • **Custom Time Interval.** AsyncOS performs a rollover after a specified amount of time has passed since the previous rollover. Specify the number of days, hours, minutes, and seconds between rollovers using d , h , m , and s as suffixes. • **Daily Rollover.** AsyncOS performs a rollover every day at a specified time. Separate multiple times a day using a comma. Use an asterisk (*) for the hour to have rollover occur every hour during the day. You can also use an asterisk to rollover every minute of an hour. • **Weekly Rollover.** AsyncOS performs a rollover on one or more days of the week at a specified time.
Log Style (Access Logs)	Specifies the log format to use, either Squid, Apache, or Squid Details.

Option	Description

Custom Fields
(Access Logs)
	Allows you to include custom information in each access log entry.
	The syntax for entering format specifiers in the Custom Field is as follows:
	`<format_specifier_1> <format_specifier_2> ...`
	For example: `%a %b %E`
	You can add tokens before the format specifiers to display descriptive text in the access log file. For example:
	`client_IP %a body_bytes %b error_type %E`
	where `client_IP` is the description token for log format specifier `%a`, and so on.

File Name	The name of the log files. Current log files are appended with a `.c` extension and rolled over log files are appended with the file creation timestamp and a `.s` extension.
Log Fields (W3C Access Logs)	Allows you to choose the fields you want to include in the W3C access log. Select a field in the Available Fields list, or type a field in the Custom Field box, and click Add. The order the fields appear in the Selected Log Fields list determines the order of fields in the W3C access log file. You can change the order of fields using the **Move Up** and **Move Down** buttons. You can remove a field by selecting it in the Selected Log Fields list and clicking **Remove**. You can enter multiple user defined fields in the Custom Fields box and add them simultaneously as long as each entry is separated by a new line (click Enter) before clicking **Add**. When you change the log fields included in a W3C log subscription, the log subscription automatically rolls over. This allows the latest version of the log file to include the correct new field headers You can anonymize the *c-ip*, *cs-username*, or *cs-auth-group* log fields of W3C logs, if required. Check the **Anonymization** check box to anonymize *c-ip*, *cs-username*, and *cs-auth-group* fields. After you select the check box, the field names are changed to *c-a-ip*, *cs-a-username,* and *cs-a-auth-group* respectively. **Note** You must enable anonymization only if the external server to which the log files are pushed is compatible to handle the anonymization feature. After the log creation you can deanonymize the anonymized fields, if required. See Deanonymizing W3C Log Fields, on page 13
Passphrase for Anonymization (W3C Access Logs)	Allows you to create passphrase for encrypting the field values. This area will be enabled only when you choose to anonymize *c-ip*, *cs-username*, or *cs-auth-group* log fields. **Note** Sytem applies passphrase rules while configuring passphrase for anonymization. To automatically generate a passphrase, check the check box next to **Auto Generate Passphrase** and click **Generate** **Note** If you have multiple appliances, all the appliances must set the same passphrase.

Option	Description
Log Compression	Specifies whether or not rolled over files are compressed. AsyncOS compresses log files using the gzip compression format.
Log Exclusions (Optional) (Access Logs)	Allows you to specify HTTP status codes (4xx or 5xx only) to exclude the associated transactions from an access log or a W3C access log. For example, entering 401 will filter out authentication failure requests that have that transaction number.
Log Level	Specifies the level of detail for log entries. Choose from: • **Critical**. Includes errors only. This is the least detailed setting and is equivalent to the syslog level "Alert." • **Warning**. Includes errors and warnings. This log level is equivalent to the syslog level "Warning." • **Information**. Includes errors, warnings and additional system operations. This is the default detail level and is equivalent to the syslog level "Info." • **Debug**. Includes data useful for debugging system problems. Use the Debug log level when you are trying to discover the cause of an error. Use this setting temporarily, and then return to the default level. This log level is equivalent to the syslog level "Debug." • **Trace**. This is the most detailed setting. This level includes a complete record of system operations and activity. The Trace log level is recommended only for developers. Using this level causes a serious degradation of system performance and is not recommended. This log level is equivalent to the syslog level "Debug." **Note** More detailed settings create larger log files and have a greater impact on system performance.
Retrieval Method	Specifies where rolled over log files are stored and how they are retrieved for reading. See below for descriptions of the available methods.
Retrieval Method: FTP on Appliance	The FTP on Appliance method (equivalent to FTP Poll) requires a remote FTP client accessing the appliance to retrieve log files using an admin or operator user's username and passphrase. When you choose this method, you must enter the maximum number of log files to store on the appliance. When the maximum number is reached, the system deletes the oldest file. This is the default retrieval method.

Option	Description
Retrieval Method: FTP on Remote Server	The FTP on Remote Server method (equivalent to FTP Push) periodically pushes log files to an FTP server on a remote computer. When you choose this method, you must enter the following information: • FTP server hostname • Directory on FTP server to store the log file • Username and passphrase of a user that has permission to connect to the FTP server **Note** AsyncOS for Web only supports passive mode for remote FTP servers. It cannot push log files to an FTP server in active mode.
Retrieval Method: SCP on Remote Server	The SCP on Remote Server method (equivalent to SCP Push) periodically pushes log files using the secure copy protocol to a remote SCP server. This method requires an SSH SCP server on a remote computer using the SSH2 protocol. The subscription requires a user name, SSH key, and destination directory on the remote computer. Log files are transferred based on a rollover schedule set by you. When you choose this method, you must enter the following information: • SCP server hostname • Directory on SCP server to store the log file • Username of a user that has permission to connect to the SCP server **Note** Currently, we support only SSH-RSA and SSH-DSS in non-FIPS mode as well as SSH-RSA in FIPS mode.
Retrieval Method: Syslog Push	You can only choose syslog for text-based logs. The Syslog Push method sends log messages to a remote syslog server on port 514. This method conforms to RFC 3164. When you choose this method, you must enter the following information: • Syslog server hostname • Protocol to use for transmission, either UDP or TCP • Maximum message size Valid values for UDP are 1024 to 9216. Valid values for TCP are 1024 to 65535. Maximum message size depends on the syslog server configuration. • Facility to use with the log

Step 4 Submit and commit your changes.

What to do next

If you chose SCP as the retrieval method, notice that the appliance displays an SSH key, which you will add to the SCP server host. See Pushing Log Files to Another Server, on page 13.

Related Topics

- Log File Types, on page 4
- Log File Names and Appliance Directory Structure, on page 15

Deanonymizing W3C Log Fields

If you have enabled anonymization feature for field values (*c-ip, cs-username,* and *cs-auth-group*) during log subscription, the destination log server will receive the anonymized values (*c-a-ip*, *cs-a-username*, and *cs-a-auth-group*) of those log fields and not the actual values. If you want to view the actual values you must deanonymize the log fields.

You can deanonymize *c-a-ip*, *cs-a-username*, and *cs-a-auth-group* log field values that are anonymized while adding the W3C log subscription.

Procedure

Step 1 Choose **System Administration** > **Log Subscriptions**.

Step 2 Click **Deanonymization** in the Denonymization column corresponding to the log for which you want to deanonymize the anonymized fields.

Step 3 In the **Method** area, choose any of the following methods to enter the encrypted text for deanonymization.

- Paste encrypted text – Paste only the encrypted text in the Anonymized Text field. You can enter a maximum of 500 entries in this field. You must separate the multiple entries with a comma.
- Upload File –Choose a file that contains the encrypted text. The file can contain a maximum of 1000 entries. The file format should be CSV. The system supports space, new line, tab, and semi colon as the field separator.

Note
If you have changed the passphrase, you must enter the old passphrase to deanonymize the older data.

Step 4 Click **Deanonymize** and the Deanonymization Result table displays the deanonymized log field values.

Pushing Log Files to Another Server

Before you begin

Create or edit the desired log subscription, choosing SCP as the retrieval method. Adding and Editing Log Subscriptions, on page 8

Procedure

Step 1 Add keys to the remote system:

a) Access the CLI.

b) Enter the `logconfig -> hostkeyconfig` command.

c) Use the commands below to display the keys:

Command	Description
Host	Display system host keys. This is the value to place in the remote system's 'known_hosts' file.
User	Displays the public key of the system account that pushes the logs to the remote machine. This is the same key that is displayed when setting up an SCP push subscription. This is the value to place in the remote system's 'authorized_keys' file.

d) Add these keys to the remote system.

Step 2 Still in the CLI, add the remote server's SSH public host key to the appliance:

Command	Description
New	Add a new key.
Fingerprint	Display system host key fingerprints.

Step 3 Commit your changes.

Archiving Log Files

AsyncOS archives (rolls over) log subscriptions when a current log file reaches a user-specified limit of maximum file size or maximum time since last rollover.

These archive settings are included in log subscriptions:

- Rollover by File Size
- Rollover by Time
- Log Compression
- Retrieval Method

You can also manually archive (rollover) log files.

Procedure

Step 1 Choose **System Administration > Log Subscriptions**.

Step 2 Check the checkbox in the Rollover column of the log subscriptions you wish to archive, or check the **All** checkbox to select all the subscriptions.

Step 3 Click **Rollover Now** to archive the selected logs.

What to do next

Related Topics

- Adding and Editing Log Subscriptions, on page 8
- Log File Names and Appliance Directory Structure, on page 15

Log File Names and Appliance Directory Structure

The appliance creates a directory for each log subscription based on the log subscription name. The name of the log file in the directory is composed of the following information:

- Log file name specified in the log subscription
- Timestamp when the log file was started
- A single-character status code, either .c (signifying current) or .s (signifying saved)

The filename of logs are made using the following formula:

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```



Note You should only transfer log files with the saved status.

Reading and Interpreting Log Files

You can read current log file activity as a means of monitoring and troubleshooting the Secure Web Appliance. This is done using the appliance interface.

You can also read archived files for a record of past activity. This can be done using the appliance interface if the archived files are stored on the appliance; otherwise they must be read from their external storage location using an appropriate method.

Each item of information in a log file is represented by a field variable. By determining which fields represent which items of information, you can look up the field function and interpret the log file contents. For W3C compliant access logs, the file header lists field names in the order in which they appear in log entries. For standard Access logs, however, you must consult the documentation regarding this log type for information on its field order.

Related Topics

- Viewing Log Files, on page 16.
- Web Proxy Information in Access Log Files, on page 16.
- Interpreting W3C Access Logs, on page 34.
- Interpreting Traffic Monitor Logs, on page 40.
- Log File Fields and Tags, on page 41.

Viewing Log Files

Before you begin

Be aware that this method of viewing is for log files that are stored on the appliance. The process of viewing files stored externally goes beyond the scope of this documentation.

Procedure

Step 1 Choose **System Administration > Log Subscriptions**.

Step 2 Click the name of the log subscription in the Log Files column of the list of log subscriptions.

Step 3 When prompted, enter the administers username and passphrase for accessing the appliance.

Step 4 When logged in, click one of the log files to view it in your browser or to save it to disk.

Step 5 Refresh the browser for updated results.

Note
If a log subscription is compressed, download, decompress, and then open it.

What to do next

Related Topics

- Web Proxy Information in Access Log Files, on page 16.
- Interpreting W3C Access Logs, on page 34.
- Interpreting Traffic Monitor Logs, on page 40.

Web Proxy Information in Access Log Files

Access log files provides a descriptive record of all Web Proxy filtering and scanning activity. Access log file entries display a record of how the appliance handled each transaction.

Access logs are available in two formats: Standard and W3C compliant. W3C-compliant log files are more customizable with regard to their content and layout than standard Access logs.

The following text is an example access log file entry for a single transaction:

```
1278096903.150 97 172.xx.xx.xx TCP_MISS/200 8187 GET http://my.site.com/ -
DIRECT/my.site.com text/plain DEFAULT_CASE_11-PolicyGroupName-Identity-
OutboundMalwareScanningPolicy-DataSecurityPolicy-ExternalDLPPolicy-RoutingPolicy-NONE
<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-",""-",-,-,IW_comp,-,"-","-",
"Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,
"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e”>
 -
```

Format Specifier	Field Value	Field Description
%t	`1278096903.150`	Timestamp since UNIX epoch.

Format Specifier	Field Value	Field Description
%e	`97`	Elapsed time (latency) in milliseconds.
%a	`172.xx.xx.xx`	Client IP address. **Note:** You can choose to mask the IP address in the access logs using the advancedproxyconfig > authentication CLI command.
%w	`TCP_MISS`	Transaction result code. For more information, see W3C Compliant Access Log Files, on page 33.
%h	`200`	HTTP response code.
%s	`8187`	Response size (headers + body).
%1r %2r	`GET http://my.site.com/`	First line of the request. Note: When the first line of the request is for a native FTP transaction, some special characters in the file name are URL encoded in the access logs. For example, the "@" symbol is written as "%40" in the access logs. The following characters are URL encoded: & # % + , : ; = @ ^ { } [ ]
%A	–	Authenticated username. **Note:** You can choose to mask the username in the access logs using the `advancedproxyconfig` > `authentication` CLI command.

Format Specifier	Field Value	Field Description
%H	`DIRECT`	Code that describes which server was contacted for the retrieving the request content. Most common values include: • **NONE.** The Web Proxy had the content, so it did not contact any other server to retrieve the content. • **DIRECT.** The Web Proxy went to the server named in the request to get the content. • **DEFAULT_PARENT.** The Web Proxy went to its primary parent proxy or an external DLP server to get the content.
%d	`my.site.com`	Data source or server IP address.
%c	`text/plain`	Response body MIME type.
%D	`DEFAULT_CASE_11`	ACL decision tag. **Note:** The end of the ACL decision tag includes a dynamically generated number that the Web Proxy uses internally. You can ignore this number. For more information, see ACL Decision Tags, on page 21.
N/A (Part of the ACL decision tag)	`PolicyGroupName`	Name of policy group responsible for the final decision on this transaction (Access Policy, Decryption Policy, or Data Security Policy). When the transaction matches a global policy, this value is "DefaultGroup." Any space in the policy group name is replaced with an underscore (_).
N/A (Part of the ACL decision tag)	`Identity`	Identity policy group name. Any space in the policy group name is replaced with an underscore (_).

Format Specifier	Field Value	Field Description
N/A (Part of the ACL decision tag)	`OutboundMalwareScanningPolicy`	Outbound Malware Scanning Policy group name. Any space in the policy group name is replaced with an underscore (_).
N/A (Part of the ACL decision tag)	`DataSecurityPolicy`	Cisco Data Security Policy group name. When the transaction matches the global Cisco Data Security Policy, this value is “DefaultGroup.” This policy group name only appears when Cisco Data Security Filters is enabled. “NONE” appears when no Data Security Policy was applied. Any space in the policy group name is replaced with an underscore (_).
N/A (Part of the ACL decision tag)	`ExternalDLPPolicy`	External DLP Policy group name. When the transaction matches the global External DLP Policy, this value is “DefaultGroup.” “NONE” appears when no External DLP Policy was applied. Any space in the policy group name is replaced with an underscore (_).
N/A (Part of the ACL decision tag)	`RoutingPolicy`	Routing Policy group name as *ProxyGroupName/ProxyServerName* . When the transaction matches the global Routing Policy, this value is “DefaultRouting.” When no upstream proxy server is used, this value is “DIRECT.” Any space in the policy group name is replaced with an underscore (_).

Format Specifier	Field Value	Field Description
%Xr	<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,""-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e">	Scanning verdict information. Inside the angled brackets, the access logs include verdict information from various scanning engines. **Note** In AsyncOS version 11.8 and later, the URL category identifier appears in double quotes. For example, "IW_comp". For more information about the values included within the angled brackets, see Interpreting Access Log Scanning Verdict Entries, on page 27 and Malware Scanning Verdict Values, on page 53.
%?BLOCK_SUSPECT_USER_AGENT, MONITOR_SUSPECT_USER_AGENT?% < User-Agent:%!%-%	–	Suspect user agent.

Transaction Result Codes

Transaction result codes in the access log file describe how the appliance resolves client requests. For example, if a request for an object can be resolved from the cache, the result code is `TCP_HIT`. However, if the object is not in the cache and the appliance pulls the object from an origin server, the result code is `TCP_MISS`. The following table describes transaction result codes.

Result Code	Description
`TCP_HIT`	The object requested was fetched from the disk cache.
`TCP_IMS_HIT`	The client sent an IMS (If-Modified-Since) request for an object and the object was found in the cache. The proxy responds with a 304 response.
`TCP_MEM_HIT`	The object requested was fetched from the memory cache.
`TCP_MISS`	The object was not found in the cache, so it was fetched from the origin server.
`TCP_REFRESH_HIT`	The object was in the cache, but had expired. The proxy sent an IMS (If-Modified-Since) request to the origin server, and the server confirmed that the object has not been modified. Therefore, the appliance fetched the object from either the disk or memory cache.

Result Code	Description
TCP_CLIENT_REFRESH_MISS	The client sent a “don’t fetch response from cache” request by issuing the ‘Pragma: no-cache’ header. Due to this header from the client, the appliance fetched the object from the origin server.
TCP_DENIED	The client request was denied due to Access Policies.
UDP_MISS	The object was fetched from the origin server.
NONE	There was an error in the transaction. For example, a DNS failure or gateway timeout.

ACL Decision Tags

An ACL decision tag is a field in an access log entry that indicates how the Web Proxy handled the transaction. It includes information from the Web Reputation filters, URL categories, and the scanning engines.



Note The end of the ACL decision tag includes a dynamically generated number that the Web Proxy uses internally to increase performance. You can ignore this number.

The following table describes the ACL decision tag values.

ACL Decision Tag	Description
ALLOW_ADMIN_ERROR_PAGE	The Web Proxy allowed the transaction to an notification page and to any logo used on that page.
ALLOW_CUSTOMCAT	The Web Proxy allowed the transaction based on custom URL category filtering settings for the Access Policy group.
ALLOW_REFERER	The Web Proxy allowed the transaction based on an embedded/referred content exemption.
ALLOW_WBRS	The Web Proxy allowed the transaction based on the Web Reputation filter settings for the Access Policy group.
AMP_FILE_VERDICT	Value representing a verdict from the Secure Endpoint reputation server for the file: • 1 – Unknown • 2 – Clean • 3 – Malicious • 4 – Unscannable

ACL Decision Tag	Description
ARCHIVESCAN_ALLCLEAR ARCHIVESCAN_BLOCKEDFILETYPE ARCHIVESCAN_NESTEDTOODEEP ARCHIVESCAN_UNKNOWNFMT ARCHIVESCAN_UNSCANABLE ARCHIVESCAN_FILETOOBIG	**Archive scan Verdict** ARCHIVESCAN_ALLCLEAR – There are no blocked file types in the inspected archive. ARCHIVESCAN_BLOCKEDFILETYPE – There is a blocked file type in the inspected archive. The next field in the log entry (Verdict Detail) provides details, specifically the type of file blocked, and the name of the blocked file. ARCHIVESCAN_NESTEDTOODEEP – The archive is blocked because it contains more "encapsulated" or nested archives than the configured maximum. The Verdict Detail field contains "UnScanable Archive-Blocked." ARCHIVESCAN_UNKNOWNFMT – The archive is blocked because it contains a file type of unknown format. The Verdict Detail is "UnScanable Archive-Blocked." ARCHIVESCAN_UNSCANABLE – The archive is blocked because it contain a file which cannot be scanned. The Verdict Detail is "UnScanable Archive-Blocked." ARCHIVESCAN_FILETOOBIG – The archive is blocked because the size of the archive is more than the configured maximum. The Verdict Detail is "UnScanable Archive-Blocked." **Archive scan Verdict Detail** The field following the Verdict field in the log entry provides additional information about the Verdict, such as type of file blocked and name of the blocked file, "UnScanable Archive-Blocked," or "-" to indicate the archive does not contain any blocked file types. For example, if an Inspectable Archive file is blocked (ARCHIVESCAN_BLOCKEDFILETYPE) based on Access Policy: Custom Objects Blocking settings, the Verdict Detail entry includes the type of file blocked, and the name of the blocked file. Refer to Access Policies: Blocking Objects and Archive Inspection Settings for more information about Archive Inspection.
BLOCK_ADC	Transaction blocked based on the configured Application settings for the Access Policy group.
BLOCK_ADMIN	Transaction blocked based on some default settings for the Access Policy group.
BLOCK_ADMIN_CONNECT	Transaction blocked based on the TCP port of the destination as defined in the HTTP CONNECT Ports setting for the Access Policy group.
BLOCK_ADMIN_CUSTOM_USER_AGENT	Transaction blocked based on the user agent as defined in the Block Custom User Agents setting for the Access Policy group.

ACL Decision Tag	Description
BLOCK_ADMIN_TUNNELING	The Web Proxy blocked the transaction based on tunneling of the non HTTP traffic on the HTTP ports for the Access Policy Group.
BLOCK_ADMIN_HTTPS_ NonLocalDestination	Transaction blocked; client tried to bypass authentication using the SSL port as an explicit proxy. To prevent this, if an SSL connection is to the Secure Web Appliance itself, only requests to the actual Secure Web Appliance redirect hostname are allowed.
BLOCK_ADMIN_IDS	Transaction blocked based on the MIME type of the request body content as defined in the Data Security Policy group.
BLOCK_ADMIN_FILE_TYPE	Transaction blocked based on the file type as defined in the Access Policy group.
BLOCK_ADMIN_PROTOCOL	Transaction blocked based on the protocol as defined in the Block Protocols setting for the Access Policy group.
BLOCK_ADMIN_SIZE	Transaction blocked based on the size of the response as defined in the Object Size settings for the Access Policy group.
BLOCK_ADMIN_SIZE_IDS	Transaction blocked based on the size of the request body content as defined in the Data Security Policy group.
BLOCK_AMP_RESP	The Web Proxy blocked the response based on the Secure Endpoint settings for the Access Policy group.
BLOCK_AMW_REQ	The Web Proxy blocked the request based on the Anti-Malware settings for the Outbound Malware Scanning Policy group. The request body produced a positive malware verdict.
BLOCK_AMW_RESP	The Web Proxy blocked the response based on the Anti-Malware settings for the Access Policy group.
BLOCK_AMW_REQ_URL	The Web Proxy suspects the URL in the HTTP request might not be safe, so it blocked the transaction at request time based on the Anti-Malware settings for the Access Policy group.
BLOCK_AVC	Transaction blocked based on the configured Application settings for the Access Policy group.
BLOCK_CONTENT_UNSAFE	Transaction blocked based on the site content ratings settings for the Access Policy group. The client request was for adult content and the policy is configured to block adult content.
BLOCK_CONTINUE_CONTENT_ UNSAFE	Transaction blocked and displayed the Warn and Continue page based on the site content ratings settings in the Access Policy group. The client request was for adult content and the policy is configured to give a warning to users accessing adult content.
BLOCK_CONTINUE_CUSTOMCAT	Transaction blocked and displayed the Warn and Continue page based on a custom URL category in the Access Policy group configured to "Warn."

ACL Decision Tag	Description
BLOCK_CONTINUE_WEBCAT	Transaction blocked and displayed the Warn and Continue page based on a predefined URL category in the Access Policy group configured to “Warn.”
BLOCK_CUSTOMCAT	Transaction blocked based on custom URL category filtering settings for the Access Policy group.
BLOCK_ICAP	The Web Proxy blocked the request based on the verdict of the external DLP system as defined in the External DLP Policy group.
BLOCK_SEARCH_UNSAFE	The client request included an unsafe search query and the Access Policy is configured to enforce safe searches, so the original client request was blocked.
BLOCK_SUSPECT_USER_AGENT	Transaction blocked based on the Suspect User Agent setting for the Access Policy group.
BLOCK_UNSUPPORTED_SEARCH_APP	Transaction blocked based on the safe search settings for the Access Policy group. The transaction was for an unsupported search engine, and the policy is configured to block unsupported search engines.
BLOCK_WBRS	Transaction blocked based on the Web Reputation filter settings for the Access Policy group.
BLOCK_WBRS_IDS	The Web Proxy blocked the upload request based on the Web Reputation filter settings for the Data Security Policy group.
BLOCK_WEBCAT	Transaction blocked based on URL category filtering settings for the Access Policy group.
BLOCK_WEBCAT_IDS	The Web Proxy blocked the upload request based on the URL category filtering settings for the Data Security Policy group.
BLOCK_YTCAT	The Web Proxy blocked the transaction based on the predefined YouTube category filtering settings for the Access Policy group.
BLOCK_CONTINUE_YTCAT	The Web Proxy blocked the transaction and displayed the Warn and Continue page based on a predefined YouTube category in the Access Policy group configured to 'Warn'.
DECRYPT_ADMIN	The Web Proxy decrypted the transaction based on some default settings for the Decryption Policy group.
DECRYPT_ADMIN_EXPIRED_CERT	The Web Proxy decrypted the transaction although the server certificate has expired.
DECRYPT_EUN_ADMIN_DEFAULT_ACTION	The Web Proxy decrypted the transaction based on default settings as drop connection for the decryption policy group when EUN is enabled.
DECRYPT_EUN_ADMIN_EXPIRED_CERT	The Web Proxy decrypted the transaction when HTTPS proxy settings drop an expired certificate with EUN enabled.

ACL Decision Tag	Description
DECRYPT_EUN_ADMIN_INVALID_LEAF_CERT	The Web Proxy decrypted the transaction when HTTPS proxy settings drop an invalid leaf certificate with EUN enabled.
DECRYPT_EUN_ADMIN_MISMATCHED_HOSTNAME	The Web Proxy decrypted the transaction when HTTPS proxy settings drop the mismatched hostname with EUN enabled.
DECRYPT_EUN_ADMIN_OCSP_OTHER_ERROR	The Web Proxy decrypted the transaction when HTTPS proxy settings drop an OCSP with other errors with EUN enabled.
DECRYPT_EUN_ADMIN_OCSP_REVOKED_CERT	The Web Proxy decrypted the transaction when HTTPS proxy settings drop an OCSP revoked certificate with EUN enabled.
DECRYPT_EUN_ADMIN_UNRECOGNIZED_ROOT_CERT	The Web Proxy decrypted the transaction when HTTPS proxy settings drop an unrecognized root authority or issuer certificate with EUN enabled.
DECRYPT_EUN_CUSTOMCAT	The Web Proxy decrypted the transaction based on custom URL category filtering settings for the decryption policy group. If EUN is enabled, the traffic is dropped.
DECRYPT_EUN_WBRS	The Web Proxy decrypted the transaction based on the web reputation filter settings for the decryption policy group. If EUN is enabled, the traffic is dropped.
DECRYPT_EUN_WBRS_NO_SCORE	The Web Proxy decrypted the transaction based on the web reputation filter settings for no score URL in the decryption policy group. If EUN is enabled, the traffic is dropped.
DECRYPT_EUN_WEBCAT	The Web Proxy decrypted the transaction based on URL category filtering settings for the decryption policy group. If EUN is enabled, the traffic is dropped.
DECRYPT_WEBCAT	The Web Proxy decrypted the transaction based on URL category filtering settings for the Decryption Policy group.
DECRYPT_WBRS	The Web Proxy decrypted the transaction based on the web reputation filter settings for the decryption policy group.
DEFAULT_CASE	The Web Proxy allowed the client to access the server because none of the AsyncOS services, such as Web Reputation or anti-malware scanning, took any action on the transaction.
DENY_ADMIN	The Web Proxy denied the transaction. This occurs for HTTPS requests when authentication is required and 'Decrypt for Authentication' is disabled in the HTTPS proxy settings.
DROP_ADMIN	The Web Proxy dropped the transaction based on some default settings for the Decryption Policy group.
DROP_ADMIN_EXPIRED_CERT	The Web Proxy dropped the transaction because the server certificate has expired.

ACL Decision Tag	Description
DROP_WEBCAT	The Web Proxy dropped the transaction based on URL category filtering settings for the Decryption Policy group.
DROP_WBRS	The Web Proxy dropped the transaction based on the Web Reputation filter settings for the Decryption Policy group.
MONITOR_ADC	The Web Proxy monitored the transaction based on the Application settings for the Access Policy group.
MONITOR_ADMIN_EXPIRED_CERT	The Web Proxy monitored the server response because the server certificate has expired.
MONITOR_AMP_RESP	The Web Proxy monitored the server response based on the Secure Endpoint settings for the Access Policy group.
MONITOR_AMW_RESP	The Web Proxy monitored the server response based on the Anti-Malware settings for the Access Policy group.
MONITOR_AMW_RESP_URL	The Web Proxy suspects the URL in the HTTP request might not be safe, but it monitored the transaction based on the Anti-Malware settings for the Access Policy group.
MONITOR_AVC	The Web Proxy monitored the transaction based on the Application settings for the Access Policy group.
MONITOR_CONTINUE_CONTENT_ UNSAFE	Originally, the Web Proxy blocked the transaction and displayed the Warn and Continue page based on the site content ratings settings in the Access Policy group. The client request was for adult content and the policy is configured to give a warning to users accessing adult content. The user accepted the warning and continued to the originally requested site, and no other scanning engine subsequently blocked the request.
MONITOR_CONTINUE_CUSTOMCAT	Originally, the Web Proxy blocked the transaction and displayed the Warn and Continue page based on a custom URL category in the Access Policy group configured to “Warn.” The user accepted the warning and continued to the originally requested site, and no other scanning engine subsequently blocked the request.
MONITOR_CONTINUE_WEBCAT	Originally, the Web Proxy blocked the transaction and displayed the Warn and Continue page based on a predefined URL category in the Access Policy group configured to “Warn.” The user accepted the warning and continued to the originally requested site, and no other scanning engine subsequently blocked the request.
MONITOR_CONTINUE_YTCAT	Originally, the Web Proxy blocked the transaction and displayed the Warn and Continue page based on a predefined YouTube category in the Access Policy group configured to 'Warn.' The user accepted the warning and continued to the originally requested site, and no other scanning engine subsequently blocked the request.

ACL Decision Tag	Description
MONITOR_IDS	The Web Proxy scanned the upload request using either a Data Security Policy or an External DLP Policy, but did not block the request. It evaluated the request against the Access Policies.
MONITOR_SUSPECT_USER_AGENT	The Web Proxy monitored the transaction based on the Suspect User Agent setting for the Access Policy group.
MONITOR_WBRS	The Web Proxy monitored the transaction based on the Web Reputation filter settings for the Access Policy group.
NO_AUTHORIZATION	The Web Proxy did not allow the user access to the application because the user was already authenticated against an authentication realm, but not against any authentication realm configured in the Application Authentication Policy.
NO_PASSWORD	The user failed authentication.
PASSTHRU_ADMIN	The Web Proxy passed through the transaction based on some default settings for the Decryption Policy group.
PASSTHRU_ADMIN_EXPIRED_CERT	The Web Proxy passed through the transaction although the server certificate has expired.
PASSTHRU_WEBCAT	The Web Proxy passed through the transaction based on URL category filtering settings for the Decryption Policy group.
PASSTHRU_WBRS	The Web Proxy passed through the transaction based on the Web Reputation filter settings for the Decryption Policy group.
REDIRECT_CUSTOMCAT	The Web Proxy redirected the transaction to a different URL based on a custom URL category in the Access Policy group configured to "Redirect."
SAAS_AUTH	The Web Proxy allowed the user access to the application because the user was authenticated transparently against the authentication realm configured in the Application Authentication Policy.
OTHER	The Web Proxy did not complete the request due to an error, such as an authorization failure, server disconnect, or an abort from the client.

Interpreting Access Log Scanning Verdict Entries

The access log file entries aggregate and display the results of the various scanning engines, such as URL filtering, Web Reputation filtering, and anti-malware scanning. The appliance displays this information in angled brackets at the end of each access log entry.

The following text is the scanning verdict information from an access log file entry. In this example, the Webroot scanning engine found the malware:

```
<IW_infr,ns,24,"Trojan-Phisher-Gamec",0,354385,12559,-,"-",-,-,-,"-",-,-,"-","-",
-,-,
IW_infr,-,"Trojan Phisher","-","-","Unknown","Unknown","-","-",489.73,0,
```

```
[Local],"-","-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf",

"fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e",

ARCHIVESCAN_BLOCKEDFILETYPE,

EXT_ARCHIVESCAN_VERDICT,

EXT_ARCHIVESCAN_THREATDETAIL,

EXT_WTT_BEHAVIOR,
EXT_YTCAT,
"BlockedFileType: application/x-rpm,
BlockedFile: allfiles/linuxpackage.rp">
```

Note For an example of a whole access log file entry, see Web Proxy Information in Access Log Files, on page 16.

Each element in this example corresponds to a log-file format specifier as shown in the following table:

Position	Field Value	Format Specifier	Description
1	`IW_infr`	%XC	The custom URL category assigned to the transaction, abbreviated. This field shows "nc" when no category is assigned.
2	`ns`	%XW	Web Reputation filters score. This field either shows the score as a number, "ns" for no score, or "dns" when there is a DNS lookup error.
3	`24`	%Xv	The malware scanning verdict Webroot passed to the DVS engine. Applies to responses detected by Webroot only. For more information, see Malware Scanning Verdict Values, on page 53.
4	`"Trojan-Phisher-Gamec"`	"%Xn"	Name of the spyware that is associated with the object. Applies to responses detected by Webroot only.
5	`0`	%Xt	The Webroot specific value associated with the Threat Risk Ratio (TRR) value that determines the probability that malware exists. Applies to responses detected by Webroot only.
6	`354385`	%Xs	A value that Webroot uses as a threat identifier. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by Webroot only.

Position	Field Value	Format Specifier	Description
7	12559	%Xi	A value that Webroot uses as a trace identifier. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by Webroot only.
8	-	%Xd	The malware scanning verdict McAfee passed to the DVS engine. Applies to responses detected by McAfee only. For more information, see Malware Scanning Verdict Values, on page 53.
9	"-"	"%Xe"	The name of the file McAfee scanned. Applies to responses detected by McAfee only.
10	-	%Xf	A value that McAfee uses as a scan error. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by McAfee only.
11	-	%Xg	A value that McAfee uses as a detection type. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by McAfee only.
12	-	%Xh	A value that McAfee uses as a virus type. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by McAfee only.
13	"-"	"%Xj"	The name of the virus that McAfee scanned. Applies to responses detected by McAfee only.
14	-	%XY	The malware scanning verdict Sophos passed to the DVS engine. Applies to responses detected by Sophos only. For more information, see Malware Scanning Verdict Values, on page 53.
15	-	%Xx	A value that Sophos uses as a scan return code. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by Sophos only.
16	"-"	"%Xy"	The name of the file in which Sophos found the objectionable content. Applies to responses detected by Sophos only.

Position	Field Value	Format Specifier	Description
17	"-"	"%Xz"	A value that Sophos uses as the threat name. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by Sophos only.
18	-	%Xl	The Cisco Data Security scan verdict based on the action in the Content column of the Cisco Data Security Policy. The following list describes the possible values for this field: • **0.** Allow • **1.** Block • **- (hyphen).** No scanning was initiated by the Cisco Data Security Filters. This value appears when the Cisco Data Security Filters are disabled, or when the URL category action is set to Allow.
19	-	%Xp	The External DLP scan verdict based on the result given in the ICAP response. The following list describes the possible values for this field: • **0.** Allow • **1.** Block • **- (hyphen).** No scanning was initiated by the external DLP server. This value appears when External DLP scanning is disabled, or when the content was not scanned due to an exempt URL category on the External DLP Policies > Destinations page.
20	`IW_infr`	%XQ	The predefined URL category verdict determined during request-side scanning, abbreviated. This field lists a hyphen (-) when URL filtering is disabled. **Note** In AsyncOS version 11.8 and later, the URL category identifier appears in double quotes. For example, "IW_infr". For a list of URL category abbreviations, see URL Category Descriptions.

Position	Field Value	Format Specifier	Description
21	-	%XA	The URL category verdict determined by the Dynamic Content Analysis engine during response-side scanning, abbreviated. Applies to the Cisco Web Usage Controls URL filtering engine only. Only applies when the Dynamic Content Analysis engine is enabled and when no category is assigned at request time (a value of "nc" is listed in the request-side scanning verdict). For a list of URL category abbreviations, see URL Category Descriptions.
22	"Trojan Phisher"	"%XZ"	Unified response-side anti-malware scanning verdict that provides the malware category independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to server response scanning.
23	"-"	"%Xk"	The Category Name or Threat Type is returned by the Web Reputation filters. The Category Name is returned when the Web Reputation is high and Threat Type returned when the reputation is low.
24	"-"	%X#10#	The URL which is encapsulated inside Google translate engine. If there is no encapsulated URL, the field value will be "-".
25	"Unknown"	"%XO"	The application name as returned by the AVC engine, if applicable. Only applies when the AVC engine is enabled.
26	"Unknown"	"%Xu"	The application type as returned by the AVC engine, if applicable. Only applies when the AVC engine is enabled.
27	"-"	"%Xb"	The application behavior as returned by the AVC engine, if applicable. Only applies when the AVC engine is enabled.
28	"-"	"%XS"	Safe browsing scanning verdict. This value indicates whether either the safe search or the site content ratings feature was applied to the transaction. For a list of the possible values, see Logging Adult Content Access.
29	489.73	%XB	The average bandwidth consumed serving the request, in Kb/sec.

Position	Field Value	Format Specifier	Description
30	`0`	%XT	A value that indicates whether the request was throttled due to bandwidth limit control settings, where “1” indicates the request was throttled, and “0” indicates it was not.
31	`[Local]`	%l	The type of user making the request, either “[Local]” or “[Remote].” Only applies when AnyConnect Secure Mobility is enabled. When it is not enabled, the value is a hyphen (-).
32	`"-"`	“%X3”	Unified request-side anti-malware scanning verdict independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to client request scanning when an Outbound Malware Scanning Policy applies.
33	`"-"`	“%X4”	The threat name assigned to the client request that was blocked or monitored due to an applicable Outbound Malware Scanning Policy. This threat name is independent of which anti-malware scanning engines are enabled.
34	`37`	%X#1#	Verdict from Secure Endpoint file scanning: • 0: File is not malicious • 1: File was not scanned because of its file type • 2: File scan timed out • 3: Scan error • Greater than 3: File is malicious
35	`"W32.CiscoTestVector"`	%X#2#	Threat name, as determined by Secure Endpoint file scanning; "-" indicates no threat.
36	`33`	%X#3#	Reputation score from Secure Endpoint file scanning. This score is used only if the cloud reputation service is unable to determine a clear verdict for the file. For details, see information about the Threat Score and the reputation threshold in File Reputation Filtering and File Analysis .

Position	Field Value	Format Specifier	Description
37	0	%X#4#	Indicator of upload and analysis request: "0" indicates that Secure Endpoint did not request upload of the file for analysis. "1" indicates that Secure Endpoint did request upload of the file for analysis.
38	"WSA-INFECTED-FILE.pdf"	%X#5#	The name of the file being downloaded and analyzed.
39	"fd5ef49d4213e05f448 f11ed9c98253d85829614fba 368a421d14e64c426da5e"	%X#6#	The SHA-256 identifier for this file.
40	ARCHIVESCAN_BLOCKEDFILETYPE	%X#8#	Archive scan Verdict.
41	EXT_ARCHIVESCAN_VERDICT	%Xo	Archive scan Verdict Detail. If an Inspectable Archive file is blocked (ARCHIVESCAN_BLOCKEDFILETYPE) based on Access policy: Custom Objects Blocking settings, this Verdict Detail entry includes the type of file blocked, and the name of the blocked file.
42	EXT_ARCHIVESCAN_THREATDETAIL	%Xm	File verdict by Archive Scanner
43	EXT_WTT_BEHAVIOR	%XU	Web Tap Behavior.
44	EXT_YTCAT	%X#29#	The YouTube URL category assigned to the transaction, abbreviated. This field shows "nc" when no category is assigned.

Refer to Log File Fields and Tags, on page 41 for a description of each format specifier's function.

Related Topics

- Web Proxy Information in Access Log Files, on page 16
- Customizing Access Logs, on page 35
- W3C Compliant Access Log Files, on page 33
- Viewing Log Files, on page 16
- Log File Fields and Tags, on page 41

W3C Compliant Access Log Files

The Secure Web Appliance provides two different log types for recording Web Proxy transaction information: access logs and W3C-formatted access logs. The W3C access logs are World Wide Web Consortium (W3C) compliant, and record transaction history in the W3C Extended Log File (ELF) Format.

• W3C Field Types, on page 34
• Interpreting W3C Access Logs, on page 34

W3C Field Types

When defining a W3C access log subscription, you must choose which log fields to include, such as the ACL decision tag or the client IP address. You can include one of the following types of log fields:

- **Predefined.** The web interface includes a list of fields from which you can choose.
- **User defined.** You can type a log field that is not included in the predefined list.

Interpreting W3C Access Logs

Consider the following rules and guidelines when interpreting W3C access logs:

- Administrators decide what data is recorded in each W3C access log subscription; therefore, W3C access logs have no set field format.
- W3C logs are self-describing. The file format (list of fields) is defined in a header at the start of each log file.
- Fields in the W3C access logs are separated by a white space.
- If a field contains no data for a particular entry, a hyphen (-) is included in the log file instead.
- Each line in the W3C access log file relates to one transaction, and each line is terminated by a LF sequence.

• W3C Log File Headers, on page 34
• W3C Field Prefixes, on page 35

W3C Log File Headers

Each W3C log file contains header text at the beginning of the file. Each line starts with the # character and provides information about the Secure Web Appliance that created the log file. The W3C log file headers also include the file format (list of fields), making the log file self-describing.

The following table describes the header fields listed at the beginning of each W3C log file.

Header Field	Description
Version	The version of the W3C ELF format used.
Date	The date and time at which the header (and log file) was created.
System	The Secure Web Appliance that generated the log file in the format “Management_IP - Management_hostname.”
Software	The Software which generated these logs
Fields	The fields recorded in the log

Example W3C log file:

```
#Version: 1.0
#Date: 2009-06-15 13:55:20
#System: 10.1.1.1 - wsa.qa
#Software: AsyncOS for Web 6.3.0
#Fields: timestamp x-elapsed-time c-ip
x-resultcode-httpstatus sc-bytes cs-method cs-url cs-username
x-hierarchy-origin cs-mime-type x-acltag x-result-code x-suspect-user-agent
```

W3C Field Prefixes

Most W3C log field names include a prefix that identifies from which header a value comes, such as the client or server. Log fields without a prefix reference values that are independent of the computers involved in the transaction. The following table describes the W3C log fields prefixes.

Prefix Header	Description
c	Client
s	Server
cs	Client to server
sc	Server to client
x	Application specific identifier.

For example, the W3C log field “cs-method” refers to the method in the request sent by the client to the server, and “c-ip” refers to the client’s IP address.

Related Topics

- Web Proxy Information in Access Log Files, on page 16.
- Customizing Access Logs, on page 35.
- Traffic Monitor Log Files, on page 40.
- Log File Fields and Tags, on page 41.
- Viewing Log Files, on page 16.

Customizing Access Logs

You can customize regular and W3C access logs to include many different fields to capture comprehensive information about web traffic within the network using predefined fields or user defined fields.

Related Topics

- For a list of predefined fields, see Log File Fields and Tags, on page 41.
- For information on user defined fields, see Access Log User Defined Fields, on page 35.

Access Log User Defined Fields

If the list of predefined Access log and W3C log fields does not include all header information you want to log from HTTP/HTTPS transactions, you can type a user-defined log field in the Custom Fields text box when you configure the access and W3C log subscriptions.

Custom log fields can be any data from any header sent from the client or the server. If a request or response does not include the header added to the log subscription, the log file includes a hyphen as the log field value.

The following table defines the syntax to use for access and W3C logs:

Header Type	Access Log Format Specifier Syntax	W3C Log Custom Field Syntax
Header from the client application	%<*ClientHeaderName* :	cs(*ClientHeaderName*)
Header from the server	%<*ServerHeaderName* :	sc(*ServerHeaderName*)

For example, if you want to log the If-Modified-Since header value in client requests, enter the following text in the Custom Fields box for a W3C log subscription:

```
cs(If-Modified-Since)
```

Related Topics

- Customizing Regular Access Logs, on page 36.
- Customizing W3C Access Logs, on page 37.

Customizing Regular Access Logs

Procedure

Step 1 Choose **System Administration > Log Subscriptions**.

Step 2 Click the access log file name to edit the access log subscription.

Step 3 Enter the required format specifiers in the Custom Field.

The syntax for entering format specifiers in the Custom Field is as follows:

```
<format_specifier_1> <format_specifier_2> ...
```

For example: `%a %b %E`

You can add tokens before the format specifiers to display descriptive text in the access log file. For example:

```
client_IP %a body_bytes %b error_type %E
```

where `client_IP` is the description token for log format specifier `%a` , and so on.

Note
You can create a custom field for any header in a client request or a server response.

Step 4 Submit and commit your changes.

What to do next

Related Topics

- Web Proxy Information in Access Log Files, on page 16.
- Log File Fields and Tags, on page 41.

- Access Log User Defined Fields, on page 35.

Customizing W3C Access Logs

Procedure

Step 1 Choose **System Administration > Log Subscriptions**

Step 2 Click the W3C log file name to edit the W3C log subscription.

Step 3 Type a field in the Custom Field box, and click **Add**.

The order the fields appear in the Selected Log Fields list determines the order of fields in the W3C access log file. You can change the order of fields using the **Move Up** and **Move Down** buttons. You can remove a field by selecting it in the Selected Log Fields list and clicking **Remove**.

You can enter multiple user defined fields in the Custom Fields box and add them simultaneously as long as each entry is separated by a new line (click Enter) before clicking **Add**.

When you change the log fields included in a W3C log subscription, the log subscription automatically rolls over. This allows the latest version of the log file to include the correct new field headers

Note
You can create a custom field for any header in a client request or a server response.

Step 4 Submit and commit your changes.

What to do next

Related Topics

- W3C Compliant Access Log Files, on page 33.
- Log File Fields and Tags, on page 41.
- Access Log User Defined Fields, on page 35.
- Configuring Cisco CTA-specific Custom W3C Logs, on page 37
- Configuring Cisco Cloudlock-specific Custom W3C Logs, on page 39

Configuring Cisco CTA-specific Custom W3C Logs

You can configure your appliance to push Cognitive Threat Analytics (CTA)-specific custom W3C access logs to Cisco Cloud Web Security service for analysis and reporting. Cisco ScanCenter is the administration portal of Cloud Web Security (CWS). See https://www.cisco.com/c/en/us/support/security/cloud-web-security/products-installation-and-configuration-guides-list.html

Before you begin

Create a device account in Cisco ScanCenter for your appliance, selecting SCP (Secure Copy Protocol) as the automatic upload protocol. See the Proxy Device Uploads section of the Cisco ScanCenter Administrator (https://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide.html)

Note the SCP host name and the generated user name for your appliance. The user name is case sensitive and unique for each device.

Procedure

Step 1 Choose **Security Services** > **Cisco Cognitive Threat Analytics**.

Step 2 Click **Edit Settings**.

Step 3 In the **Log Fields** area, add additional log fields, if required. See Adding and Editing Log Subscriptions, on page 8.

Step 4 From the **Selected Log Fields**, check the check boxes next to *c-ip*, *cs-username* or *cs-auth-group* if you want to anonymize these fields individually.

Alternatively, you can check the **Anonymization** check box to anonymize these fields simultaneously. See Adding and Editing Log Subscriptions, on page 8.

Step 5 In the **Retrieval Method** area, enter the username generated for your device in Cisco ScanCenter. The device user name is case sensitive and unique for each proxy device.

Step 6 Modify the **Advanced Options** values, if required.

Step 7 Click **Submit**.

The appliance generates public SSH keys and displays them on the Cisco Cognitive Threat Analytics page.

Step 8 Copy one of the public SSH key to the clipboard.

Step 9 Click the **View Cisco Cognitive Threat Analytics** portal link to switch to the Cisco ScanCenter portal, select the appropriate device account and then paste the public SSH key to the CTA Device Provisioning page. (See the *Proxy Device Uploads* section of the Cisco ScanCenter Administrator Guide).

Log files from your proxy device will be uploaded to the CTA system for analysis on successful authentication between your proxy device and CTA system.

Step 10 Switch back to the appliance and commit your changes.

You can also add CTA W3C logs using **System Administration** > **Log Subscription**. Follow the instructions in Customizing W3C Access Logs, on page 37 to add a new W3C access log subscription with the following options:

- **W3C Logs** as log type
- **Cisco Cognitive Threat Analytics Subscription** as subscription
- **SCP** as file transfer type

See Adding and Editing Log Subscriptions, on page 8 to know more about custom fields.

Note
If you have already configured a CTA log subscription, you must change the log name to *cta_log* to list it on the Cisco Cognitive Threat Analytics page in the appliance.

After log creation, if you want to delete the CTA log, click **Disable** in the Cisco Cognitive Threat Analytics page. You can also delete the CTA log from the Log Subscriptions page (**System Administration** > **Log subscriptions**).

To deanonymize the anonymized CTA-specific W3C log fields, click **Deanonymize** in the Cisco Cognitive Threat Analytics page. See Deanonymizing W3C Log Fields, on page 13

You can also deanonymize the anonymized CTA-specific W3C log fields using **System Administration** > **Log Subscription**. See Deanonymizing W3C Log Fields, on page 13

Configuring Cisco Cloudlock-specific Custom W3C Logs

Cisco Cloudlock is a cloud-native CASB and cloud cybersecurity platform that protects users, data, and applications across Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service. You can configure your appliance to push W3C access logs to Cisco's Cloudlock portal for analysis and reporting. These custom W3C logs provide better visibility into the SaaS usage of the customers.

Before you begin

Create a device account in Cloudlock portal for your appliance, selecting SCP as the automatic upload protocol.

Logon to Cloudlock portal, access the online help and follow the instructions to create device account in the Cloudlock portal.

Procedure

Step 1 Choose **Security Services** > **Cisco Cloudlock**.

Step 2 Click **Edit Settings**.

Note
The log fields are selected by default in the **Log Fields** area.You cannot add additional log fields other than the log fields selected by default. You should not change the order of the log fields displayed in the **Log Fields** area.

You cannot anonymize log fields (*c-ip, cs-username,* or *cs-auth-group*) of Cloudlock log files.

Step 3 In the **Retrieval Method** area, enter the following information:

- Cloudlock server hostname and port number
- Directory on the Cloudlock server to store the log file
- Username of the user who has permission to connect to the Cloudlock server

Step 4 Modify the **Advanced Options** values if required.

Step 5 Click **Submit**.

The appliance generates public SSH keys and displays them on the Cisco Cloudlock page.

Step 6 Copy one of the public SSH key to the clipboard.

Step 7 Click the **View Cloudlock Portal** link to switch to the Cisco Cloudlock portal. Select the appropriate device account and then paste the public SSH key into the Cloudlock Setting page.

Log files from your proxy device will be uploaded to the Cloudlock system for analysis on successful authentication between your proxy device and Cloudlock system.

Step 8 Switch back to the appliance and commit your changes.

You can also add Cloudlock W3C logs using **System Administration** > **Log Subscription**. Follow the instructions in Customizing W3C Access Logs, on page 37 to add a new W3C access log subscription with the following options:

- **W3C Logs** as log type
- **Cisco Cloudlock** as subscription
- **SCP** as file transfer type

See Adding and Editing Log Subscriptions, on page 8 to know more about custom fields.

Note
If you have already configured a Cloudlock log subscription, you must change the log name to **cloudlock_log** to list it on the Cisco Cloudlock page in the appliance.

After log creation, if you want to delete the Cloudlock log, click **Disable** in the Cisco Cloudlock page. You can also delete the Cloudlock log from the Log Subscriptions page (**System Administration** > **Log subscriptions**).

Traffic Monitor Log Files

Layer-4 Traffic Monitor log files provides a detailed record of Layer-4 monitoring activity. You can view Layer-4 Traffic Monitor log file entries to track updates to firewall block lists and firewall allow lists.

Interpreting Traffic Monitor Logs

Use the examples below to interpret the various entry types contains in Traffic Monitor Logs.

Example 1

```
172.xx.xx.xx discovered for blocksite.net (blocksite.net) added to firewall block list.
```

In this example, where a match becomes a block list firewall entry. The Layer-4 Traffic Monitor matched an IP address to a domain name in the block list based on a DNS request which passed through the appliance. The IP address is then entered into the block list for the firewall.

Example 2

```
172.xx.xx.xx discovered for www.allowsite.com (www.allowsite.com) added to firewall allow
list.
```

In this example, a match becomes an allow list firewall entry. The Layer-4 Traffic Monitor matched a domain name entry and added it to the appliance allow list. The IP address is then entered into the allow list for the firewall.

Example 3

```
Firewall noted data from 172.xx.xx.xx to 209.xx.xx.xx (allowsite.net):80.
```

In this example, the Layer-4 Traffic Monitor logs a record of data that passed between an internal IP address and an external IP address which is on the block list. Also, the Layer-4 Traffic Monitor is set to monitor, not block.

Related Topics

- Viewing Log Files, on page 16

Log File Fields and Tags

- Access Log Format Specifiers and W3C Log File Fields, on page 41
- Transaction Result Codes, on page 20
- ACL Decision Tags, on page 21
- Malware Scanning Verdict Values, on page 53

Access Log Format Specifiers and W3C Log File Fields

Log files use variables to represent the individual items of information that make up each log file entry. These variables are called format specifiers in Access logs and log fields in W3C logs and each format specifier has a corresponding log field.

To configure Access Logs to display these values, see Customizing Access Logs, on page 35 and information about custom fields in Adding and Editing Log Subscriptions, on page 8.

The following table describes these variables:

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%:<A	AclTime	To print the total amount of time taken by the Access Control List transaction.
%{	x-id-shared	To print the status of ID sharing with Umbrella. If the ID is shared for a transaction, the corresponding value of the formatter is “ID_SHARED”, else “-“ is displayed in the access log.
%[	x-spoofed-ip	Source IP address used in proxy IP spoofing.
%)	x-proxy-instance-id	Instance ID of proxy if High Performance Mode is enabled, otherwise it logs a hyphen.
%(	cs-domain-map	Resolved domain name which are resolved using domain map.
%X#11#	ext_auth_sgt	Custom field parameter for Secure Group Tags used in ISE integrations.
%$	cipher information	Cipher information of both the legs in the transaction.(Client-proxy cipher info##proxy-server cipher info).The information in the below sequence - <ciphername>, <protocol version>, Kx=<key exchange>, Au=<authentication>, Enc=<symmetric encryption method>, Mac=<message authentication code>

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%:<1	x-p2s-first-byte-time	The time it takes from the moment the Web Proxy starts connecting to the server to the time it is first able to write to the server. If the Web Proxy has to connect to several servers to complete the transaction, it is the sum of those times.
%:<a	x-p2p-auth-wait-time	Wait-time to receive the response from the Web Proxy authentication process, after the Web Proxy sent the request.
%:<b	x-p2s-body-time	Wait-time to write request body to server after header.
%:<d	x-p2p-dns-wait-time	Time taken by the Web Proxy to send the DNS request to the Web Proxy DNS process.
%:<h	x-p2s-header-time	Wait-time to write request header to server after first byte.
%:<r	x-p2p-reputation- wait-time	Wait-time to receive the response from the Web Reputation Filters, after the Web Proxy sent the request.
%:<s	x-p2p-asw-req- wait-time	Wait-time to receive the verdict from the Web Proxy anti-spyware process, after the Web Proxy sent the request.
%:>1	x-s2p-first-byte-time	Wait-time for first response byte from server
%:>a	x-p2p-auth-svc-time	Wait-time to receive the response from the Web Proxy authentication process, including the time required for the Web Proxy to send the request.
%:>b	x-s2p-body-time	Wait-time for complete response body after header received
%:>c	x-p2p-fetch-time	Time required for the Web Proxy to read a response from the disk cache.
%:>d	x-p2p-dns-svc-time	Time taken by the Web Proxy DNS process to send back a DNS result to the Web Proxy.
%:>h	x-s2p-header-time	Wait-time for server header after first response byte
%:>g		SSL server handshake latency information.
%o	-	Time quota consumed.
% O	-	Volume quota consumed.
%X#41#	x-bw-info	The bandwidth quota control level applied, bandwidth pipe number mapped to a request, configured bandwidth quota limit, and the bandwidth quota profile used (level-pipe_no-quota_limit-quota_profile).

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%:>r	x-p2p-reputation-svc- time	Wait-time to receive the verdict from the Web Reputation Filters, including the time required for the Web Proxy to send the request.
%:>s	x-p2p-asw-req-svc- time	Wait-time to receive the verdict from the Web Proxy anti-spyware process, including the time required for the Web Proxy to send the request.
%:1<	x-c2p-first-byte-time	Wait-time for first request byte from new client connection.
%:1>	x-p2c-first-byte-time	Wait-time for first byte written to client.
%:A<	x-p2p-avc-svc-time	Wait-time to receive the response from the AVC process, including the time required for the Web Proxy to send the request.
%:A>	x-p2p-avc-wait-time	Wait-time to receive the response from the AVC process, after the Web Proxy sent the request.
%:b<	x-c2p-body-time	Wait-time for complete client body.
%:b>	x-p2c-body-time	Wait-time for complete body written to client.
%:C<	x-p2p-dca-resp- svc-time	Wait-time to receive the verdict from the Dynamic Content Analysis engine, including the time required for the Web Proxy to send the request.
%:C>	x-p2p-dca-resp- wait-time	Wait-time to receive the response from the Dynamic Content Analysis engine, after the Web Proxy sent the request.
%:h<	x-c2p-header-time	Wait-time for complete client header after first byte
%:h>	x-p2c-header-time	Wait-time for complete header written to client
%:m<	x-p2p-mcafee-resp- svc-time	Wait-time to receive the verdict from the McAfee scanning engine, including the time required for the Web Proxy to send the request.
%:m>	x-p2p-mcafee-resp- wait-time	Wait-time to receive the response from the McAfee scanning engine, after the Web Proxy sent the request.
%:p<	x-p2p-sophos-resp- svc-time	Wait-time to receive the verdict from the Sophos scanning engine, including the time required for the Web Proxy to send the request.
%:p>	x-p2p-sophos-resp- wait-time	Wait-time to receive the response from the Sophos scanning engine, after the Web Proxy sent the request.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%:w<	x-p2p-webroot-resp -svc-time	Wait-time to receive the verdict from the Webroot scanning engine, including the time required for the Web Proxy to send the request.
%:w>	x-p2p-webroot-resp-wait- time	Wait-time to receive the response from the Webroot scanning engine, after the Web Proxy sent the request.
%?BLOCK_SUSPECT_USER_AGENT,MONITOR_SUSPECT_USER_AGENT?%<User-Agent:%!%-	x-suspect-user-agent	Suspect user agent, if applicable. If the Web Proxy determines the user agent is suspect, it will log the user agent in this field. Otherwise, it logs a hyphen. This field is written with double-quotes in the access logs.
%<Referer:	cs(Referer)	Referer
%>Server:	sc(Server)	Server header in the response.
%a	c-ip	Client IP Address.
%A	cs-username	Authenticated user name. This field is written with double-quotes in the access logs.
%b	sc-body-size	Bytes sent to the client from the Web Proxy for the body content.
%B	bytes	Total bytes used (request size + response size, which is %q + %s).
%c	cs-mime-type	Response body MIME type. This field is written with double-quotes in the access logs.
%C	cs(Cookie)	Cookie header. This field is written with double-quotes in the access logs.
%d	s-hostname	Data source or server IP address.
%]	x-http-rewrite-profile-name	HTTP header rewrite profile name.
%D	x-acltag	ACL decision tag.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%e	x-elapsed-time	Elapsed time in milliseconds. For TCP traffic, this is the time elapsed between the opening and closing of the HTTP connection. For UDP traffic, this is the time elapsed between the sending of the first datagram and the time at which the last datagram can be accepted. A large elapsed time value for UDP traffic may indicate that a large timeout value and a long-lived UDP association allowed datagrams to be accepted longer than necessary.
%E	x-error-code	Error code number that may help Customer Support troubleshoot the reason for a failed transaction.(
%f	cs(X-Forwarded-For)	X-Forwarded-For header.
%F	c-port	Client source port
%g	cs-auth-group	Authorized group names. This field is written with double-quotes in the access logs. This field is used for troubleshooting policy/authentication issues to determine whether a user is matching the correct group or policy.
%G		Human-readable timestamp.
%h	sc-http-status	HTTP response code.
%H	s-hierarchy	Hierarchy retrieval.
%i	x-icap-server	IP address of the last ICAP server contacted while processing the request.
%I	x-transaction-id	Transaction ID.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%j	DCF	Do not cache response code; DCF flags. Response code descriptions: • Response code based on client request: • 1 = Request had “no-cache” header. • 2 = Caching is not authorized for the request. • 4 = Request is missing the 'Variant' header. • 8 = Username or passphrase needed for user request. • 20 = Response for specified HTTP method. • Response code based on response received by the appliance: • id="li_7443F05D141F4D9FB788FD416697DB65"> 40 = Response contains “Cache-Control: private” header. • 80 = Response contains “Cache-Control: no-store” header. • 100 = Response indicates that request was a query. • 200 = Response has a small “Expires” value (expires soon). • 400 = Response does not have “Last Modified” header. • 1000 = Response expires immediately. • 2000 = Response file is too big to cache. • 20000 = New copy of file exists. • 40000 = Response has bad/invalid values in “Vary” header. • 80000 = Response requires setting of cookies. • 100000 = Non-cacheable HTTP STATUS Code. • 200000 = Object received by appliance was incomplete (based on size). • 800000 = Response trailers indicate no caching. • 1000000 = Response requires re-write.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%k	s-ip	Data source IP address (server IP address) This value is used to determine a requestor when the IP address is flagged by an intrusion detection device on your network. Allows you to locate a client that visited an IP address that has been so flagged.
%l	user-type	Type of user, either local or remote.
%L	x-local_time	Request local time in human-readable format: DD/MMM/YYYY : hh:mm:ss +nnnn. This field is written with double-quotes in the access logs. Enabling this field allows you to correlate logs to issues without having to calculate local time from epoch time for each log entry.
%m	cs-auth-mechanism	Used to troubleshoot authentication issues. The authentication mechanism used on the transaction. Possible values are: • **BASIC.** The user name was authenticated using the Basic authentication scheme. • **NTLMSSP.** The user name was authenticated using the NTLMSSP authentication scheme. • **NEGOTIATE.** The user name was authenticated using the Kerberos authentication scheme. • **SSO_TUI.** The user name was obtained by matching the client IP address to an authenticated user name using transparent user identification. • **SSO_ISE.** The user was authenticated by an ISE server. (Log shows GUEST if that is chosen as the fall-back mechanism for ISE authentication.) • **SSO_ASA.** The user is a remote user and the user name was obtained from a Cisco ASA using the Secure Mobility. • **FORM_AUTH.** The user entered authentication credentials in a form in the web browser when accessing a application. • **GUEST.** The user failed authentication and instead was granted guest access.
%M	CMF	Cache miss flags: CMF flags.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%N	s-computerName	Server name or destination hostname. This field is written with double-quotes in the access logs.
%p	s-port	Destination port number.
%P	cs-version	Protocol used. Possible values are: • 0 = No protocol used • 1 = HTTP • 2 = HTTPS • 3 = FTP over HTTP • 4 = FTP • 5 = SOCKS • 6 = HTTP2
%q	cs-bytes	Request size (headers + body).
%r	x-req-first-line	Request first line - request method, URI.
%s	sc-bytes	Response size (header + body).
%t	timestamp	Timestamp in UNIX epoch. **Note:** If you want to use a third party log analyzer tool to read and parse the W3C access logs, you might need to include the “timestamp” field. Most log analyzers only understand time in the format provided by this field.
%u	cs(User-Agent)	User agent. This field is written with double-quotes in the access logs. This field helps determine if an application is failing authentication and/or requires different access permissions.
%U	cs-uri	Request URI.
%v	date	Date in YYYY-MM-DD.
%V	time	Time in HH:MM:SS.
%w	sc-result-code	Result code. For example: TCP_MISS, TCP_HIT.
%W	sc-result-code-denial	Result code denial.
%x	x-latency	Latency.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%X0	x-resp-dvs-scanverdict	Unified response-side anti-malware scanning verdict that provides the *malware category number* independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to server response scanning. This field is written with double-quotes in the access logs.
%X1	x-resp-dvs-threat-name	Unified response-side anti-malware scanning verdict that provides the *malware threat name* independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to server response scanning. This field is written with double-quotes in the access logs.
%X2	x-req-dvs-scanverdict	Request side DVS Scan verdict
%X3	x-req-dvs-verdictname	Request side DVS verdict name
%X4	x-req-dvs-threat-name	Request side DVS threat name
%X6	x-as-malware-threat-name	Indicates whether Adaptive Scanning blocked the transaction without invoke any anti-malware scanning engine. The possible values are: • **1.** Transaction was blocked. • **0.** Transaction was not blocked. This variable is included in the scanning verdict information (in the angled brackets at the end of each access log entry).
%XA	x-webcat-resp-code- abbr	The URL category verdict determined during response-side scanning, abbreviated. Applies to the Cisco Web Usage Controls URL filtering engine only.
%Xb	x-avc-behavior	The web application behavior identified by the AVC engine.
%XB	x-avg-bw	Average bandwidth of the user if bandwidth limits are defined by the AVC engine.
%XC	x-webcat-code-abbr	URL category abbreviation for the custom URL category assigned to the transaction.
%Xd	x-mcafee-scanverdict	McAfee specific identifier: (scan verdict).
%Xe	x-mcafee-filename	McAfee specific identifier: (File name yielding verdict) This field is written with double-quotes in the access logs.
%Xf	x-mcafee-av-scanerror	McAfee specific identifier: (scan error).

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%XF	x-webcat-code-full	Full name of the URL category assigned to the transaction. This field is written with double-quotes in the access logs.
%Xg	x-mcafee-av-detecttype	McAfee specific identifier: (detect type).
%XG	x-avc-reqhead-scanverdict	AVC request header verdict.
%Xh	x-mcafee-av-virustype	McAfee specific identifier: (virus type).
%XH	x-avc-reqbody- scanverdict	AVC request body verdict.
%Xi	x-webroot-trace-id	Webroot specific scan identifier: (Trace ID)
%Xj	x-mcafee-virus-name	McAfee specific identifier: (virus name). This field is written with double-quotes in the access logs.
%Xk	x-wbrs-threat-type	Web reputation threat type.
%XK	x-wbrs-threat-reason	Web reputation threat reason.
%Xl	x-ids-verdict	Cisco Data Security Policy scanning verdict. If this field is included, it will display the IDS verdict, or “0” if IDS was active but the document scanned clean, or “-” if no IDS policy was active for the request.
%XL	x-webcat-resp-code- full	The URL category verdict determined during response-side scanning, full name. Applies to the Cisco Web Usage Controls URL filtering engine only.
%XM	x-avc-resphead- scanverdict	AVC response header verdict.
%Xn	x-webroot-threat-name	Webroot specific identifier: (Threat name) This field is written with double-quotes in the access logs.
%XN	x-avc-reqbody-scanverdict	AVC response body verdict.
%XO	x-avc-app	The web application identified by the AVC engine.
%Xp	x-icap-verdict	External DLP server scanning verdict.
%XP	x-acl-added-headers	Unrecognized header. Use this field to log extra headers in client requests. This supports troubleshooting of specialized systems that add headers to client requests as a way of authenticating and redirecting those requests, for example, YouTube for Schools.
%XQ	x-webcat-req-code- abbr	The predefined URL category verdict determined during request-side scanning, abbreviated.
%Xr	x-result-code	Scanning verdict information.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%XR	x-webcat-req-code-full	The URL category verdict determined during request-side scanning, full name.
%Xs	x-webroot-spyid	Webroot specific identifier: (Spy ID).
%XS	x-request-rewrite	Safe browsing scanning verdict. Indicates whether either the safe search or site content ratings feature was applied to the transaction.
%Xt	x-webroot-trr	Webroot specific identifier: (Threat Risk Ratio [TRR]).
%XT	x-bw-throttled	Flag that indicates whether bandwidth limits were applied to the transaction.
%Xu	x-avc-type	The web application type identified by the AVC engine.
%Xv	x-webroot-scanverdict	Malware scanning verdict from Webroot.
%XV	x-request-source-ip	The downstream IP address when the “Enable Identification of Client IP Addresses using X-Forwarded-For” checkbox is enabled for the Web Proxy settings.
%XW	x-wbrs-score	Decoded WBRS score <-10.0-10.0>.
%Xx	x-sophos-scanerror	Sophos specific identifier: (scan return code).
%Xy	x-sophos-file-name	The name of the file in which Sophos found the objectionable content. Applies to responses detected by Sophos only.
%XY	x-sophos-scanverdict	Sophos specific identifier: (scan verdict).
%Xz	x-sophos-virus-name	Sophos specific identifier: (threat name).
%XZ	x-resp-dvs-verdictname	Unified response-side anti-malware scanning verdict that provides the *malware category* independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to server response scanning. This field is written with double-quotes in the access logs.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%X#1#	x-amp-verdict	Verdict from Secure Endpoint file scanning: • 0: File is not malicious. • 1: File was not scanned because of its file type. • 2: File scan timed out. • 3: Scan error. • Greater than 3: File is malicious.
%X#2#	x-amp-malware-name	Threat name, as determined by Secure Endpoint file scanning. "-" indicates no threat.
%X#3#	x-amp-score	Reputation score from Secure Endpoint file scanning. This score is used only if the cloud reputation service is unable to determine a clear verdict for the file. For details, see information about the Threat Score and the reputation threshold in File Reputation Filtering and File Analysis
%X#4#	x-amp-upload	Indicator of upload and analysis request: "0" indicates that Secure Endpoint did not request upload of the file for analysis. "1" indicates that Secure Endpoint did request upload of the file for analysis.
%X#5#	x-amp-filename	The name of the file being downloaded and analyzed.
%X#6#	x-amp-sha	The SHA-256 identifier for this file.
%y	cs-method	Method.
%Y	cs-url	The entire URL.
%:e<	x-p2p-amp-svc-time	Wait-time to receive the verdict from the Secure Endpoint scanning engine, including the time required for the Web Proxy to send the request.
%:e>	x-p2p-amp-wait-time	Wait-time to receive the response from the Secure Endpoint scanning engine, after the Web Proxy sent the request.
N/A	x-hierarchy-origin	Code that describes which server was contacted for the retrieving the request content (for example, DIRECT/www.example.com).

Format Specifier in Access Logs	Log Field in W3C Logs	Description
N/A	x-resultcode-httpstatus	Result code and the HTTP response code, with a slash (/) in between.
N/A	x-archivescan-verdict	Display the verdict of Archive Inspection.
N/A	x-archivescan-verdict- reason	Details of the file blocked by Archive Scan.
%XU	N/A	Reserved for future.

Related Topics

- Web Proxy Information in Access Log Files, on page 16.
- Interpreting W3C Access Logs, on page 34.

Malware Scanning Verdict Values

A malware scanning verdict is a value assigned to a URL request or server response that determines the probability that it contains malware. The Webroot, McAfee, and Sophos scanning engines return the malware scanning verdict to the DVS engine so the DVS engine can determine whether to monitor or block the scanned object. Each malware scanning verdict corresponds to a malware category listed on the Access Policies > Reputation and Anti-Malware Settings page when you edit the anti-malware settings for a particular Access Policy.

The following list presents the different Malware Scanning Verdict Values and each corresponding malware category:

Malware Scanning Verdict Value	Malware Category
-	Not Set
0	Unknown
1	Not Scanned
2	Timeout
3	Error
4	Unscannable
10	Generic Spyware
12	Browser Helper Object
13	Adware
14	System Monitor
18	Commercial System Monitor

Malware Scanning Verdict Value	Malware Category
19	Dialer
20	Hijacker
21	Phishing URL
22	Trojan Downloader
23	Trojan Horse
24	Trojan Phisher
25	Worm
26	Encrypted File
27	Virus
33	Other Malware
34	PUA
35	Aborted
36	Outbreak Heuristics
37	Known Malicious and High-Risk Files

Related Topics

- Web Proxy Information in Access Log Files, on page 16.
- Interpreting W3C Access Logs, on page 34.

Troubleshooting Logging

- Custom URL Categories Not Appearing in Access Log Entries, on page 69
- Logging HTTPS Transactions, on page 69
- Alert: Unable to Maintain the Rate of Data Being Generated, on page 69
- Problem Using Third-Party Log-Analyzer Tool with W3C Access Logs, on page 70

Troubleshooting

This topic contains the following sections:

- General Troubleshooting Best Practices, on page 55
- FIPS Mode Problems, on page 55
- Authentication Problems, on page 56
- Blocked Object Problems, on page 58

- Browser Problems, on page 58
- DNS Problems, on page 59
- Failover Problems, on page 59
- Feature Keys Expired, on page 60
- FTP Problems, on page 60
- Upload/Download Speed Issues, on page 61
- Hardware Issues, on page 62
- HTTPS/Decryption/Certificate Problems, on page 62
- Identity Services Engine Problems, on page 64
- Problems with Custom and External URL Categories, on page 67
- Logging Problems, on page 69
- Policy Problems, on page 70
- Problems with File Reputation and File Analysis , on page 75
- Reboot Issues, on page 75
- Site Access Problems, on page 77
- Upstream Proxy Problems, on page 78
- Virtual Appliances , on page 78
- WCCP Problems, on page 79
- Packet Capture, on page 79
- Working With Support , on page 81

General Troubleshooting Best Practices

Configure your Access Logs to include the following custom fields:

%u, %g, %m, %k, %L (These values are case-sensitive.)

For descriptions of these fields, see Access Log Format Specifiers and W3C Log File Fields, on page 41.

For configuration instructions, see Customizing Access Logs, on page 35 and Adding and Editing Log Subscriptions, on page 8.

FIPS Mode Problems

Check the following topics if you encounter encryption and certificate problems after you upgraded your Secure Web Appliance to AsyncOS 10.5, and enabled FIPS mode and CSP encryption.

- CSP Encryption, on page 56
- Certificate Validation, on page 56

CSP Encryption

For a feature that worked before you enabled FIPS-mode CSP encryption, but doesn't work after encryption is enabled, determine if the CSP encryption is the problem. Disable CSP encryption and FIPS mode and then test the feature. If it works, enable FIPS mode and test it again. If it works, enable CSP encryption and test it again. See Enabling or Disabling FIPS Mode.

Certificate Validation

Certificates which were accepted by your Secure Web Appliance prior to upgrading to AsyncOS 10.5 might be rejected when they are uploaded again, regardless of upload method. (That is, via UI pages such as HTTPS Proxy, Certificate Management, Identity Provider for SaaS, ISE configuration, Authentication configuration, or via the `certconfig` CLI command.)

Ensure that the certificate's signer CAs have been added as "Custom Trusted Certificate Authorities" on the Certificate Management page (Network > Certificate Management). A certificate cannot be uploaded to the Secure Web Appliance if the complete certificate path is untrusted.

Also, when reloading an older configuration, its likely that the included certificates will not be trusted and the reload will fail. Ensure these certificates are replaced while loading the saved configuration.

Note All certificate validation failures are logged in the audit logs (`/data/pub/audit_logs/audit_log.current`).

Authentication Problems

- Troubleshooting Tools for Authentication Issues , on page 56
- Failed Authentication Impacts Normal Operations, on page 56
- LDAP Problems, on page 57
- Basic Authentication Problems, on page 57
- Single Sign-On Problems, on page 58
- Also see:
  - General Troubleshooting Best Practices, on page 55
  - HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, on page 71
  - Cannot Access URLs that Do Not Support Authentication, on page 77
  - Client Requests Fail Upstream Proxy, on page 78

Troubleshooting Tools for Authentication Issues

KerbTray or klist (both part of the Windows Server Resources Kit) for viewing and purging a Kerberos ticket cache. Active Directory Explorer for viewing and editing an Active directory. Wireshark is a packet analyzer you can use for network troubleshooting.

Failed Authentication Impacts Normal Operations

When certain user agents or applications fail to authenticate and are denied access, they repeatedly send requests to the Secure Web Appliance, which in turn repeatedly sends requests to the Active Directory servers with machine credentials, sometimes to the point of impacting normal operations.

For best results, bypass authentication with these user agents. See Bypassing Authentication with Problematic User Agents.

LDAP Problems

- LDAP User Fails Authentication due to NTLMSSP, on page 57
- LDAP Authentication Fails due to LDAP Referral, on page 57

LDAP User Fails Authentication due to NTLMSSP

LDAP servers do not support NTLMSSP. Some client applications, such as Internet Explorer, always choose NTLMSSP when given a choice between NTLMSSP and Basic. When all of the following conditions are true, the user will fail authentication:

- The user only exists in the LDAP realm.
- The Identification Profile uses a sequence that contains both LDAP and NTLM realms.
- The Identification Profile uses the “Basic or NTLMSSP” authentication scheme.
- A user sends a request from an application that chooses NTLMSSP over Basic.

Reconfigure the Identification Profile or the authentication realm or the application such that at least one of the above conditions will be false.

LDAP Authentication Fails due to LDAP Referral

LDAP authentication fails when all of the following conditions are true:

- The LDAP authentication realm uses an Active Directory server.
- The Active Directory server uses an LDAP referral to another authentication server.
- The referred authentication server is unavailable to the Secure Web Appliance.

Workarounds:

- Specify the Global Catalog server (default port is 3268) in the Active Directory forest when you configure the LDAP authentication realm in the appliance.
- Use the `advancedproxyconfig` > `authentication` CLI command to disable LDAP referrals. LDAP referrals are disabled by default.

Basic Authentication Problems

- Basic Authentication Fails, on page 57

Related Problems

- Upstream Proxy Does Not Receive Basic Credentials, on page 78

Basic Authentication Fails

AsyncOS for Web only supports 7-bit ASCII characters for passphrases when using the Basic authentication scheme. Basic authentication fails when the passphrase contains characters that are not 7-bit ASCII.

Single Sign-On Problems

• Users Erroneously Prompted for Credentials, on page 58

Users Erroneously Prompted for Credentials

NTLM authentication does not work in some cases when the Secure Web Appliance is connected to a WCCP v2 capable device. When a user makes a request with a highly locked down version of Internet Explorer that does not do transparent NTLM authentication correctly and the appliance is connected to a WCCP v2 capable device, the browser defaults to Basic authentication. This results in users getting prompted for their authentication credentials when they should not get prompted.

Workaround

In Internet Explorer, add the Secure Web Appliance redirect hostname to the list of trusted sites in the Local Intranet zone (Tools > Internet Options > Security tab).

Blocked Object Problems

• Some Microsoft Office Files Not Blocked, on page 58
• Blocking DOS Executable Object Types Blocks Updates for Windows OneCare, on page 58

Some Microsoft Office Files Not Blocked

When you block Microsoft Office files in the Block Object Type section, it is possible that some Microsoft Office files will not be blocked.

If you need to block all Microsoft Office files, add **application/x-ole** in the Block Custom MIME Types field. However, blocking this custom MIME type also blocks all Microsoft Compound Object format types, such as Visio files and some third-party applications.

Blocking DOS Executable Object Types Blocks Updates for Windows OneCare

When you configure the Secure Web Appliance to block DOS executable object types, the appliance also blocks updates for Windows OneCare.

Browser Problems

• WPAD Not Working With Firefox, on page 58

WPAD Not Working With Firefox

Firefox browsers may not support DHCP lookup with WPAD. For current information, see `https://bugzilla.mozilla.org/show_bug.cgi?id=356831` .

To use Firefox (or any other browser that does not support DHCP) with WPAD when the PAC file is hosted on the Secure Web Appliance, configure the appliance to serve the PAC file through port 80.

Procedure

Step 1 Choose **Security Services > Web Proxy** and delete port 80 from the **HTTP Ports to Proxy** field.

Step 2 Use port 80 as the PAC Server Port when you upload the file to the appliance.

Step 3 If any browsers are manually configured to point to the web proxy on port 80, reconfigure those browsers to point to another port in the HTTP Ports to Proxy field.

Step 4 Change any references to port 80 in PAC files.

DNS Problems

• Alert: Failed to Bootstrap the DNS Cache, on page 59

Alert: Failed to Bootstrap the DNS Cache

If an alert with the message “Failed to bootstrap the DNS cache” is generated when an appliance is rebooted, it means that the system was unable to contact its primary DNS servers. This can happen at boot time if the DNS subsystem comes online before network connectivity is established. If this message appears at other times, it could indicate network issues or that the DNS configuration is not pointing to a valid server.

Failover Problems

• Failover Misconfiguration, on page 59
• Failover Issues on Virtual Appliances , on page 60

Failover Misconfiguration

Misconfiguration of failover groups might result in multiple primary appliances or other failover problems. Diagnose failover problems using the `testfailovergroup` subcommand of the CLI `failoverconfig` command.

For example:

```
wsa.wga> failoverconfig
Currently configured failover profiles:
1.      Failover Group ID: 61
        Hostname: failoverV4P1.wga, Virtual IP: 10.4.28.93/28
        Priority: 100, Interval: 3 seconds
        Status: PRIMARY
Choose the operation you want to perform:
- NEW - Create new failover group.
- EDIT - Modify a failover group.
- DELETE - Remove a failover group.
- PREEMPTIVE - Configure whether failover is preemptive.
- TESTFAILOVERGROUP - Test configured failover profile(s)
[]> testfailovergroup
Failover group ID to test (-1 for all groups):
[]> 61
```

Failover Issues on Virtual Appliances

For deployments on virtual appliances, ensure that you have configured the interface/ virtual switch on the hypervisor to use promiscuous mode.

Feature Keys Expired

If the feature key for the feature you are trying to access (via the web interface) has expired, please contact your Cisco representative or support organization.

FTP Problems

- URL Categories Do Not Block Some FTP Sites, on page 60
- Large FTP Transfers Disconnect, on page 60
- Zero Byte File Appears On FTP Servers After File Upload, on page 60
- Chrome Browser Not Detected As User Agent in FTP-over-HTTP Requests, on page 60
- Also see:
  - Unable to Route FTP Requests Via an Upstream Proxy, on page 78
  - HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, on page 71

URL Categories Do Not Block Some FTP Sites

When a native FTP request is transparently redirected to the FTP Proxy, it contains no hostname information for the FTP server, only its IP address. Because of this, some predefined URL categories and Web Reputation Filters that have only hostname information will not match native FTP requests, even if the requests are destined for those servers. If you wish to block access to these sites, you must create custom URL categories for them using their IP addresses.

Large FTP Transfers Disconnect

If the connection between the FTP Proxy and the FTP server is slow, uploading a large file may take a long time, particularly when Cisco Data Security Filters are enabled. This can cause the FTP client to time out before the FTP Proxy uploads the entire file and you may get a failed transaction notice. The transaction does not fail, however, but continues in the background and will be completed by the FTP Proxy.

You can workaround this issue by increasing the appropriate idle timeout value on the FTP client.

Zero Byte File Appears On FTP Servers After File Upload

FTP clients create a zero byte file on FTP servers when the FTP Proxy blocks an upload due to outbound anti-malware scanning.

Chrome Browser Not Detected As User Agent in FTP-over-HTTP Requests

Chrome browsers do not include a user-agent string in FTP-over-HTTP requests; therefore, Chrome cannot be detected as the user agent in those requests.

Upload/Download Speed Issues

The Secure Web Appliance is designed to handle thousands of client and server connections in parallel, and the sizes of the send and receive buffers are configured to deliver optimal performance, without sacrificing stability. Generally, actual usage is browse traffic, consisting of numerous short-lived connections for which we have receive-packet-steering (RPS) and receive-flow-steering (RFS) data, and for which the Secure Web Appliance has been optimized.

However, at times you may experience a noticeable reduction in upload or download speeds; for example, when transferring large files via proxy. To illustrate: assuming a 10-Mbps line, downloading a 100-MB file that passes through a Secure Web Appliance can be approximately seven to eight times slower than downloading the file directly from its server.

In non-typical environments that include a larger proportion of large-file transfers, you can use the `networktuning` command to increase send and receive buffer size to alleviate this issue, but doing so can also cause network memory exhaustion and affect system stability. See Secure Web Appliance CLI Commands for details of the `networktuning` command.

Caution Exercise care when changing the TCP receive and send buffer control points and other TCP buffer parameters. Use the `networktuning` command only if you understand the ramifications.

To configure the buffer size in `networktuning`, ensure that you have enabled the automatic send and receive options that are provided under `networktuning`.

Here are examples of using the `networktuning` command on two different appliances:

On an S380

```
networktuning
sendspace = 131072
recvspace = 131072
send-auto = 1 [Remember to disable miscellaneous > advancedproxy > send buf auto tuning]
recv-auto = 1 [Remember to disable miscellaneous > advancedproxy > recv buf auto tuning]
mbuf clusters = 98304 * (X/Y)  where is X is RAM in GBs on the system and Y is 4GB.
sendbuf-max = 1048576
recvbuf-max = 1048576
```

Questions

What are these parameters?

The Secure Web Appliance has several buffers and optimization algorithms which can be altered for specific needs. Buffer sizes are originally optimized to suit the “most common” deployment scenarios. However, larger buffer sizes can be used when faster per-connection performance is needed, but note that overall memory usage will increase. Therefore, buffer-size increases should be in line with the memory available on the system. The send- and receive-space variables control the size of the buffers available for storing data for communication over a socket. The send- and receive-auto options are used to enable and disable dynamic scaling of send and receive TCP window sizes. (These parameters are applied in the FreeBSD kernel.)

How were these example values determined?

We tested different sets of values on a customer’s network where this “problem” was observed, and “zeroed in” on these values. We then further tested these changes for stability and performance increase in our labs. You are free to use values other than these at your own risk.

Why are these values not the defaults?

As mentioned, by default the Secure Web Appliance is optimized for the most-common deployments, and operating in a very large number of locations without per-connection performance complaints. Making the changes discussed here will not increase RPS numbers, and in fact may cause them to drop.

Hardware Issues

- Cycling Appliance Power , on page 62
- Appliance Health and Status Indicators , on page 62
- Alert: Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware, on page 62

Cycling Appliance Power

Important! If you need to cycle power to your x80 or x90 appliance, wait at least 20 minutes for the appliance to come up again (all LEDs are green) before pushing the power button.

Appliance Health and Status Indicators

Lights on the front and/or rear panels of your hardware appliance indicate health and status of your appliance. For descriptions of these indicators, see the hardware guides, such as the *Cisco x90 Series Content Security Appliances Installation and Maintenance Guide*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

Specifications for your appliance, such as temperature ranges, are also available in these documents.

Alert: Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware

This alert may or may not indicate a problem. The battery relearn timeout, in itself, does not mean there is any problem with the RAID controller. The controller can recover in the subsequent relearn. Please monitor your email for any other RAID alerts for the next 48 hours, to ensure that this is not the side-effect of any other problem. If you do not see any other RAID-type alerts from the system, then you can safely ignore this alert.

HTTPS/Decryption/Certificate Problems

- Accessing HTTPS Sites Using Routing Policies with URL Category Criteria, on page 63
- HTTPS Request Failures, on page 63
- Bypassing Decryption for Particular Websites, on page 63
- Conditions and Restrictions for Exceptions to Blocking for Embedded and Referred Content, on page 64
- Alert: Problem with Security Certificate, on page 64
- Also see:
  - Logging HTTPS Transactions, on page 69
  - Access Policy not Configurable for HTTPS, on page 70
  - HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, on page 71

Accessing HTTPS Sites Using Routing Policies with URL Category Criteria

For transparently redirected HTTPS requests, the Web Proxy must contact the destination server to determine the server name and therefore the URL category in which it belongs. Due to this, when the Web Proxy evaluates Routing Policy Group membership, it cannot yet know the URL category of an HTTPS request because it has not yet contacted the destination server. If the Web Proxy does not know the URL category, it cannot match the transparent HTTPS request to any user-defined Routing Policy because of insufficient information.

As a result, transparently redirected HTTPS transactions only match Routing Policies if no Routing Policy Group and no identification profile has a membership criteria. If any user-defined Routing Policies or identification profiles define their membership by URL category, then the transparent HTTPS transactions match the Default Routing Policy Group.

HTTPS Request Failures

- HTTPS with IP-based Surrogates and Transparent Requests, on page 63
- Different Client “Hello” Behavior for Custom and Default Categories, on page 63

HTTPS with IP-based Surrogates and Transparent Requests

If the HTTPS request comes from a client that does not have authentication information available from an earlier HTTP request, AsyncOS either fails the HTTPS request or decrypts the HTTPS request in order to authenticate the user, depending on how you configure the HTTPS Proxy. Use the HTTPS Transparent Request setting on the Security Services > HTTPS Proxy page to define this behavior. Refer to the Enabling HTTPS Proxy section in Decryption Policies topic.

Different Client “Hello” Behavior for Custom and Default Categories

When scanning packet captures, you may notice that the “Client Hello” handshake is sent at different times for custom category and default (Web) category HTTPS Decryption pass-through policies.

For an HTTPS page passed through via the default category, the Client Hello is sent before receipt of a Client Hello from the requestor, and the connection fails. For an HTTPS page passed through via a custom URL category, the Client Hello is sent after the Client Hello is received from the requestor, and the connection is successful.

As a remedy, you can create a custom URL category with a pass-through action for SSL 3.0-only-compatible Web pages.

Bypassing Decryption for Particular Websites

Some HTTPS servers do not work as expected when traffic to them is decrypted by a proxy server, such as the Web Proxy. For example, some websites and their associated web applications and applets, such as high security banking sites, maintain a hard-coded list of trusted certificates instead of relying on the operating system certificate store.

You can bypass decryption for HTTPS traffic to these servers to ensure all users can access these types of sites.

Procedure

Step 1 Create a custom URL category that contains the affected HTTPS servers by configuring the Advanced properties.

Step 2 Create a Decryption Policy that uses the custom URL category created in Step 1 as part of its membership, and set the action for the custom URL category to Pass Through.

Conditions and Restrictions for Exceptions to Blocking for Embedded and Referred Content

Referrer-based exceptions are supported only in Access policies. To use this feature with HTTPS traffic, before defining exceptions in Access policies, you must configure HTTPS decryption of the URL Categories that you will select for exception. However, this feature will not work under certain conditions:

Note When time ranges are configured, they receive the highest priority. The referrer will not function if the Time Range quota has been reached.

- If the connection is tunneled and HTTPS decryption is not enabled, this feature will not work for requests going to HTTPS sites.
- According to RFC 2616, a browser client could have a toggle switch for browsing openly/anonymously, which would respectively enable/disable the sending of Referer and from information. The feature is exclusively dependent on the Referer header, and turning off sending them would cause our feature not to work.
- According to RFC 2616, clients should not include a Referer header field in a (non-secure) HTTP request if the referring page was transferred with a secure protocol. So, any request from an HTTPS-based site to an HTTP-based site would not have the Referer header, causing this feature to not work as expected.
- When a Decryption policy is set up such that when a custom category matches the Decryption policy and the action is set to Drop, any incoming request for that category will be dropped, and no bypassing will be done.

Alert: Problem with Security Certificate

Typically, the root certificate information you generate or upload in the appliance is not listed as a trusted root certificate authority in client applications. By default in most web browsers, when users send HTTPS requests, they will see a warning message from the client application informing them that there is a problem with the website's security certificate. Usually, the error message says that the website's security certificate was not issued by a trusted certificate authority or the website was certified by an unknown authority. Some other client applications do not show this warning message to users nor allow users to accept the unrecognized certificate.

Note **Mozilla Firefox browsers:** The certificate you upload must contain "basicConstraints=CA:TRUE" to work with Mozilla Firefox browsers. This constraint allows Firefox to recognize the root certificate as a trusted root authority.

Identity Services Engine Problems

- Tools for Troubleshooting ISE Issues, on page 65
- ISE Server Connection Issues, on page 65
- ISE-related Critical Log Messages, on page 67

Tools for Troubleshooting ISE Issues

The following can be useful when troubleshooting ISE-related issues:

- The ISE test utility, used to test the connection to the ISE server, provides valuable connection-related information. This is the **Start Test** option on the Identity Services Engine page; see Connect to the ISE/ISE-PIC Services.
- ISE and Proxy Logs; see Monitor System Activity Through Logs, on page 1
- ISE-related CLI commands `iseconfig` and `isedata` , particularly `isedata` to confirm security group tag (SGT) download. See Secure Web Appliance CLI Commands for additional information.
- The Web Tracking and Policy Trace functions can be used to debug policy match issues; for example, a user that should be allowed is blocked, and vice versa. See Policy Troubleshooting Tool: Policy Trace, on page 72 for additional information.
- Packet Capture, on page 79 if Working With Support , on page 81.
- For checking certificate status, you can use the openssl Online Certificate Status Protocol (ocsp) utility, available from https://www.openssl.org/ .

ISE Server Connection Issues

Certificate Issues

The Secure Web Appliance and the ISE server(s) use certificates to mutually authenticate for successful connection. Thus, each certificate presented by one entity should be recognizable by other. For example, if the Secure Web Appliance's Client certificate is self-signed, the same certificate must be present in the trusted certificates list on the appropriate ISE server(s). Correspondingly, if the Web Appliance Client certificate is CA-signed, then the CA root certificate must be present on the appropriate ISE server(s). Similar requirements apply to the ISE server-related Admin and pxGrid certificates.

Certificate requirements and installation are described in Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service. If you encounter certificate-related issues, check the following:

- If using CA-signed certificates:
  - Verify that the root CA signing certificate(s) for the Admin and pxGrid certificates are present on the Secure Web Appliance.
  - Verify that the root CA signing certificate for the Web Appliance Client certificate is present in the trusted-certificates list on the ISE server.
- If using self-signed certificates:
  - Verify that the Web Appliance Client certificate—generated on the Secure Web Appliance and downloaded—has been uploaded to the ISE server and is present in the ISE servers trusted-certificates list.
  - Verify that the ISE Admin and pxGrid certificates—generated on the ISE server and downloaded—have been uploaded to the Secure Web Appliance are present in the its certificate list.
- Expired certificates:

- Confirm that certificates which were valid when uploaded have not expired.

Log Output Indicating Certificate Issue

The following ISE-service log snippet shows a client-connection timeout due to a missing or invalid certificate.

```
Tue Mar 24 03:56:14 2015 Debug: ISELoggerThread: Logging queue starting
Tue Mar 24 03:56:14 2015 Info: ISEService: Successfully loaded configuration from: /data/ise/ise_service.
Tue Mar 24 03:56:14 2015 Debug: Statistics loaded from file
Tue Mar 24 03:56:14 2015 Info: ISEService: RPC Server Socket :/tmp/ise_fastrpc.sock
Tue Mar 24 03:56:14 2015 Info: RPCServer: Starting at: /tmp/ise_fastrpc.sock
Tue Mar 24 03:56:14 2015 Info: ISEService: Running
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Creating ISE client attempt 0
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Creating ISE connection with reconnection True
Tue Mar 24 03:56:14 2015 Info: ISEService: Sending ready signal...
Tue Mar 24 03:56:14 2015 Info: ISEDynamicConfigThread: Started Server..
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Successfully created ISE client
Tue Mar 24 03:56:14 2015 Trace: ISEEngineManager: Waiting for client connection, 0 seconds of 30
Tue Mar 24 03:56:17 2015 Trace: ISEEngineManager: Waiting for client connection, 3 seconds of 30
Tue Mar 24 03:56:20 2015 Trace: ISEEngineManager: Waiting for client connection, 6 seconds of 30
Tue Mar 24 03:56:23 2015 Trace: ISEEngineManager: Waiting for client connection, 9 seconds of 30
Tue Mar 24 03:56:26 2015 Trace: ISEEngineManager: Waiting for client connection, 12 seconds of 30
Tue Mar 24 03:56:29 2015 Trace: ISEEngineManager: Waiting for client connection, 15 seconds of 30
Tue Mar 24 03:56:32 2015 Trace: ISEEngineManager: Waiting for client connection, 18 seconds of 30
Tue Mar 24 03:56:35 2015 Trace: ISEEngineManager: Waiting for client connection, 21 seconds of 30
Tue Mar 24 03:56:38 2015 Trace: ISEEngineManager: Waiting for client connection, 24 seconds of 30
Tue Mar 24 03:56:41 2015 Trace: ISEEngineManager: Waiting for client connection, 27 seconds of 30
Tue Mar 24 03:56:44 2015 Trace: ISEEngineManager: Waiting for client connection, 30 seconds of 30
Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Waiting for client connection timed out
Tue Mar 24 03:56:47 2015 Debug: ISEEngineManager: Stopping client...
```

These Trace-level log entries on the Secure Web Appliance show that after 30 seconds the attempts to connect to the ISE server are terminated.

Network Issues

If connection to the ISE server fails during the Start Test on the Identity Services Engine page (Connect to the ISE/ISE-PIC Services), check connectivity to the configured ISE server on ports 443 and 5222.

Port 5222 is the official client-to-server Extensible Messaging and Presence Protocol (XMPP) port, and is used for connection to the ISE server; it is also used by applications such as Jabber and Google Talk. Note that some firewalls are configured to block port 5222.

Tools that can be used to check connectivity include `tcpdump`

Other ISE Server Connectivity Issues

The following issues can cause failure when the Secure Web Appliance attempts to connect with the ISE server:

- Licenses on the ISE server have expired.
- The pxGrid node status is “not connected” on the ISE server’s Administration > pxGrid Services page. Be sure Enable Auto-Registration is selected on this page.

- Outdated Secure Web Appliance clients (specifically “test_client” or “pxgrid_client”) are present on the ISE server. These need to be deleted; see Administration > pxGrid Services > Clients on the ISE server.
- The Secure Web Appliance is attempting to connect to the ISE server before all its services are up and running.

  Some changes on the ISE server, such as certificate updates, require the ISE server or services running on it to restart. Any attempt to connect to the ISE server during this time will fail; however, eventually the connection will succeed.

ISE-related Critical Log Messages

This section contains explanations for ISE-related critical Log messages on the Secure Web Appliance:

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Waiting for client connection timed out`

  The Secure Web Appliance’s ISE process failed to connect to the ISE server for 30 seconds.
- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: WSA Client cert/key missing. Please check ISE config`

  The Web Appliance Client certificate and key were not uploaded or generated on the Secure Web Appliance’s Identity Service Engine configuration page.
- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: ISE service exceeded maximum allowable disconnect duration with ISE server`

  The Secure Web Appliance’s ISE process could not connect to the ISE server for 120 seconds and exited.
- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Subscription to updates failed ...`

  The Secure Web Appliance’s ISE process could not subscribe to the ISE server for updates.
- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Could not create ISE client: ...`

  Internal error when creating the Secure Web Appliance’s ISE client for ISE server connection.
- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Bulk Download thread failed: ...`

  Internal error indicating bulk download of SGTs failed on connection or re-connection.
- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to start service. Error: ...`

  The Secure Web Appliance’s ISE service failed to start.
- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send ready signal ...`

  The Secure Web Appliance’s ISE service was unable to send a ready signal to heimdall .
- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send restart signal ...`

  The Secure Web Appliance’s ISE service was unable to send a restart signal to heimdall .

Problems with Custom and External URL Categories

- Issues Downloading An External Live Feed File, on page 68

• MIME Type Issue on IIS Server for .CSV Files, on page 68
• Malformed Feed File Following Copy and Paste, on page 69

Issues Downloading An External Live Feed File

When Creating and Editing Custom and External URL Categories and providing an **External Live Feed** file (either **Cisco Feed Format** or **Office 365 Feed Format**), you must click the **Get File** button to initiate connection to the specified server, and download and parsing of the file. Progress and results of this process are displayed; if errors occur they are described. Rectify the problems and try downloading the file again.

There are four types of possible error:

- Connect exceptions

  `Failed to resolve server hostname` – the URL provided as the feed-file location is invalid; provide a correct URL to resolve this issue.

- Protocol errors

  `Authentication failed due to invalid credentials` – Server authentication failed; provide the correct user name and passphrase for server connection.

  `The requested file is not found on the server` – The URL provided for the feed file points to an invalid resource. Ensure the correct file is available on the specified server.

- Content validation errors

  `Failed to validate the content of the field` – The content of the feed file is invalid.

- Parsing errors

  - The Cisco Feed Format .csv file must contain one or more entries, where each entry is a site address or a valid regex string, followed by a comma and then the addresstype (which can be either `site` or `regex`). If this convention is not followed for any entry in the feed file, a parsing error is thrown.

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

  - The XML feed file obtained from a Microsoft server is parsed by a standard XML parser. Any inconsistencies in the XML tagging are also flagged as parsing errors.

  The line number of a parsing error is included in the log. For example:

  `Line 8: 'www.anyurl.com' - Line is missing address or address-type field.` Line 8 in the feed file doesn't include a valid address or regex pattern, or an addresstype.

  `Line 12: 'www.test.com' - Unknown address type.` Line 12 has a invalid addresstype; the addresstype can be either `site` or `regex`.

MIME Type Issue on IIS Server for .CSV Files

When providing a .csv file for the **External Live Feed Category** > **Cisco Feed Format** option while Creating and Editing Custom and External URL Categories, you may encounter a "406 not acceptable" error when fetching the file if the Cisco Feed Format server is running Internet Information Services (IIS) version 7 or 8 software. Similarly, the `feedsd` log will report something like: `31 May 2016 16:47:22 (GMT +0200) Warning: Protocol Error: 'HTTP error while fetching file from the server'.`

This is because the default MIME type for .csv files on IIS is `application/csv` rather than `text/csv`. You can remedy the problem by logging into the IIS server and editing the MIME type entry for .csv files to be `text/csv`.

Malformed Feed File Following Copy and Paste

If you copy and paste the contents of a .csv (text) feed file from a UNIX or OS X system to a Windows system, an extra carriage return (`\r`) is added automatically and this can make the feed file malformed.

If you manually create the .csv file, or if you transfer the file from a UNIX or OS X system to a Windows server using SCP, FTP, or POST, there should be no problem.

Logging Problems

- Custom URL Categories Not Appearing in Access Log Entries, on page 69
- Logging HTTPS Transactions, on page 69
- Alert: Unable to Maintain the Rate of Data Being Generated, on page 69
- Problem Using Third-Party Log-Analyzer Tool with W3C Access Logs, on page 70

Custom URL Categories Not Appearing in Access Log Entries

When a web access policy group has a custom URL category set to Monitor and some other component, such as the Web Reputation Filters or the DVS engine, makes the final decision to allow or block a request for a URL in the custom URL category, then the access log entry for the request shows the predefined URL category instead of the custom URL category.

Logging HTTPS Transactions

HTTPS transactions in the access logs appear similar to HTTP transactions, but with slightly different characteristics. What gets logged depends on whether the transaction was explicitly sent or transparently redirected to the HTTPS Proxy:

- **TUNNEL.** This gets written to the access log when the HTTPS request was transparently redirected to the HTTPS Proxy.
- **CONNECT.** This gets written to the access log when the HTTPS request was explicitly sent to the HTTPS Proxy.

When HTTPS traffic is decrypted, the access logs contain two entries for a transaction:

- TUNNEL or CONNECT depending on the type of request processed.
- The HTTP Method and the decrypted URL. For example, “GET https://ftp.example.com”.

The full URL is only visible when the HTTPS Proxy decrypts the traffic.

Alert: Unable to Maintain the Rate of Data Being Generated

AsyncOS for Web sends a critical email message to the configured alert recipients when the internal logging process drops web transaction events due to a full buffer.

By default, when the Web Proxy experiences a very high load, the internal logging process buffers events to record them later when the Web Proxy load decreases. When the logging buffer fills completely, the Web Proxy continues to process traffic, but the logging process does not record some events in the access logs or in the Web Tracking report. This might occur during a spike in web traffic.

However, a full logging buffer might also occur when the appliance is over capacity for a sustained period of time. AsyncOS for Web continues to send the critical email messages every few minutes until the logging process is no longer dropping data.

The critical message contains the following text:

```
Reporting Client: The reporting system is unable to maintain the rate of data being generated.
Any new data generated will be lost.
```

If AsyncOS for Web sends this critical message continuously or frequently, the appliance might be over capacity. Contact Cisco Customer Support to verify whether or not you need additional Secure Web Appliance capacity.

Problem Using Third-Party Log-Analyzer Tool with W3C Access Logs

If you want to use a third party log analyzer tool to read and parse the W3C access logs, you might need to include the "timestamp" field. The timestamp W3C field displays time since the UNIX epoch, and most log analyzers only understand time in this format.

Policy Problems

- Access Policy not Configurable for HTTPS, on page 70
- Blocked Object Problems, on page 58
- Identification Profile Disappeared from Policy, on page 71
- Policy Match Failures, on page 71
- Policy Troubleshooting Tool: Policy Trace, on page 72
- Also see: Accessing HTTPS Sites Using Routing Policies with URL Category Criteria, on page 63

Access Policy not Configurable for HTTPS

With the HTTPS Proxy is enabled, Decryption Policies handle all HTTPS policy decisions. You can no longer define Access and Routing Policy group membership by HTTPS, nor can you configure Access Policies to block HTTPS transactions.

If some Access and Routing Policy group memberships are defined by HTTPS and if some Access Policies block HTTPS, then when you enable the HTTPS Proxy, those Access and Routing Policy groups become disabled. You can choose to enable the policies at any time, but all HTTPS related configurations are removed.

Blocked Object Problems

- Some Microsoft Office Files Not Blocked, on page 58
- Blocking DOS Executable Object Types Blocks Updates for Windows OneCare, on page 58

Some Microsoft Office Files Not Blocked

When you block Microsoft Office files in the Block Object Type section, it is possible that some Microsoft Office files will not be blocked.

If you need to block all Microsoft Office files, add **application/x-ole** in the Block Custom MIME Types field. However, blocking this custom MIME type also blocks all Microsoft Compound Object format types, such as Visio files and some third-party applications.

Blocking DOS Executable Object Types Blocks Updates for Windows OneCare

When you configure the Secure Web Appliance to block DOS executable object types, the appliance also blocks updates for Windows OneCare.

Identification Profile Disappeared from Policy

Disabling an Identification Profile removes it from associated policies. Verify that the Identification Profile is enabled and then add it to the policy again.

Policy Match Failures

- Policy is Never Applied, on page 71
- HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, on page 71
- User Matches Global Policy for HTTPS and FTP over HTTP Requests, on page 71
- User Assigned Incorrect Access Policy , on page 72

Policy is Never Applied

If multiple Identification Profiles have identical criteria, AsyncOS assigns the transactions to the first Identification Profile that matches. Therefore, transactions never match the additional, identical Identification Profiles, and any policies that apply to those subsequent, identical Identification Profiles are never matched or applied.

HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication

Configure the appliance to use IP addresses as the surrogate when credential encryption is enabled.

When credential encryption is enabled and configured to use cookies as the surrogate type, authentication does not work with HTTPS or FTP over HTTP requests. This is because the Web Proxy redirects clients to the Web Proxy itself for authentication using an HTTPS connection if credential encryption is enabled. After successful authentication, the Web Proxy redirects clients back to the original website. In order to continue to identify the user, the Web Proxy must use a surrogate (either the IP address or a cookie). However, using a cookie to track users results in the following behavior if requests use HTTPS or FTP over HTTP:

- **HTTPS.** The Web Proxy must resolve the user identity before assigning a Decryption Policy (and therefore, decrypt the transaction), but it cannot obtain the cookie to identify the user unless it decrypts the transaction.
- **FTP over HTTP.** The dilemma with accessing FTP servers using FTP over HTTP is similar to accessing HTTPS sites. The Web Proxy must resolve the user identity before assigning an Access Policy, but it cannot set the cookie from the FTP transaction.

Therefore, HTTPS and FTP over HTTP requests will match only Access Policies that do not require authentication. Typically, they match the global Access Policy because it never requires authentication.

User Matches Global Policy for HTTPS and FTP over HTTP Requests

When the appliance uses cookie-based authentication, the Web Proxy does not get cookie information from clients for HTTPS and FTP over HTTP requests. Therefore, it cannot get the user name from the cookie.

HTTPS and FTP over HTTP requests still match the Identification Profile according to the other membership criteria, but the Web Proxy does not prompt clients for authentication even if the Identification Profile requires authentication. Instead, the Web Proxy sets the user name to NULL and considers the user as unauthenticated.

Then, when the unauthenticated request is evaluated against a policy, it matches only a policy that specifies "All Identities" and apply to "All Users." Typically, this is the global policy, such as the global Access Policy.

User Assigned Incorrect Access Policy

- Clients on your network use Network Connectivity Status Indicator (NCSI)
- Secure Web Appliance uses NTLMSSP authentication.
- Identification Profile uses IP based surrogates

A user might be identified using the machine credentials instead of the user's own credentials, and as a result, might be assigned to an incorrect Access Policy.

Workaround:

Reduce the surrogate timeout value for machine credentials.

Procedure

Step 1 Use the `advancedproxyconfig > authentication` CLI command.

Step 2 Enter the surrogate timeout for machine credentials.

Policy Trace Mismatch after Modifying Policy Parameters

When you modify policy parameters such as Access Policy, Identification Profiles and Users, Select One or More Identification Profiles, or Selected Groups and Users, the changes will take a few minutes to take effect.

Policy Troubleshooting Tool: Policy Trace

- About the Policy Trace Tool, on page 72
- Tracing Client Requests, on page 73
- Advanced: Request Details, on page 74
- Advanced: Response Detail Overrides, on page 75

About the Policy Trace Tool

The Policy Trace Tool can emulate a client request and then detail how the Web Proxy processes that request. It can be used to trace client requests and debug policy processing when troubleshooting Web Proxy issues. You can perform a basic trace, or you can enter advanced trace settings and override options.

Note When you use the Policy Trace tool, the Web Proxy does not record the requests in the access log or reporting database.

The Policy Trace tool evaluates requests against polices used by the Web Proxy only. These are Access, Encrypted HTTPS Management, Routing, Data Security, and Outbound Malware Scanning polices.

Note SOCKS and External DLP polices are not evaluated by the Policy Trace tool.

Tracing Client Requests

Note You can use the CLI command `maxhttpheadersize` to change the maximum HTTP header size for proxy requests. Increasing this value can alleviate Policy Trace failures that can occur when the specified user belongs to a large number of authentication groups, or when the response header is larger than the current maximum header size. See Secure Web Appliance CLI Commands for more information about this command.

Procedure

Step 1 Choose **System Administration** > **Policy Trace**.

Step 2 Enter the URL you wish to trace to in the Destination URL field.

Step 3 (Optional) Enter additional emulation parameters:

To emulate...	Enter...
The client source IP used to make the request.	An IP address in the Client IP Address field. **Note** If an IP address is not specified, AsyncOS uses localhost. Also, SGTs (security group tags) cannot be fetched and policies based on SGTs will not be matched.
The authentication/identification credentials used to make the request.	A user name in the User Name field, and then choose Identity Services Engine or an authentication realm from the Authentication/Identification drop-down list. **Note** Only enabled option(s) are available. That is, authentication options and the ISE option are available only if they are both enabled. For authentication of the user you enter here, the user must have already successfully authenticated through the Secure Web Appliance.

Step 4 Click **Find Policy Match.**

The Policy Trace output is displayed in the Results pane.

Note
For a Pass Through HTTPS transaction, the Policy Trace tool bypasses further scanning and no Access policy is associated with the transaction. Similarly, for a Decrypt HTTPS transaction, the tool cannot actually decrypt the transaction to determine the applied Access policy. In both cases, as well as for Drop transactions, the trace results display: “Access policy: Not Applicable.”

Note

If the client IP address provided is not routable, the trace results display: "Connection Trace: Connection to Origin Server: Failed".

What to do next

Related Topics

- Advanced: Request Details, on page 74
- Advanced: Response Detail Overrides, on page 75

Advanced: Request Details

You can use the settings in the Request Details pane of the Policy Trace page, Advanced section, to tune the outbound malware scan request for this policy trace.

Procedure

Step 1 Expand the **Advanced** section on the Policy Trace page.

Step 2 Complete the fields in the Request Details pane as required:

Setting	Description
Proxy Port	Select a specific proxy port to use for the trace request to test policy membership based on proxy port.
User Agent	Specify the User Agent to simulate in the request.
Time of Request	Specify the Date and Time of day to simulate in the request.
Upload File	Choose a local file to simulate uploading in the request. When you specify a file to upload here, the Web Proxy simulates an HTTP POST request instead of a GET request.
Object Size	Enter the size of the request object in bytes. You can enter K, M, or G to represent Kilobytes, Megabytes, or Gigabytes.
MIME Type	Enter the MIME type.
Anti-malware Scanning Verdicts	To override a Webroot, McAfee, or Sophos scanning verdict, choose the specific type of verdict to be overridden.

Step 3 Click **Find Policy Match.**

The Policy Trace output is displayed in the Results pane.

Advanced: Response Detail Overrides

You can use the settings in the Response Detail Overrides pane of the Policy Trace page, Advanced section, to “tweak” aspects of the Web Access Policies response for this trace.

Procedure

Step 1 Expand the **Advanced** section on the Policy Trace page.

Step 2 Complete the fields in the Response Detail Overrides pane as required:

Setting	Description
URL Category	Use this setting to override the URL transaction category of the trace response. Choose a category which is to replace the URL category in the response results.
Application	Similarly, use this setting to override the application category of the trace response. Choose a category which is to replace the application category in the response results.
Object Size	Enter a size for the response object in bytes. You can enter K, M, or G to represent Kilobytes, Megabytes, or Gigabytes.
MIME Type	Enter a MIME type.
Web Reputation Score	Enter a web reputation score from -10.0 to 10.0. The web reputation score -100 means 'No Score.'
Anti-malware Scanning Verdicts	Use these options to override specific anti-malware scanning verdicts provided in the trace response. Choose verdicts which are to replace the Webroot, McAfee, and Sophos scanning verdicts in the response results.

Step 3 Click **Find Policy Match.**

The Policy Trace output is displayed in the Results pane.

Problems with File Reputation and File Analysis

See Troubleshooting File Reputation and Analysis

Reboot Issues

- Virtual Appliance Running on KVM Hangs on Reboot , on page 76
- Hardware Appliances: Remotely Resetting Appliance Power , on page 76

Virtual Appliance Running on KVM Hangs on Reboot

Note This is a KVM issue and may change at any time.

For more information, see https://www.mail-archive.com/kvm@vger.kernel.org/msg103854.html and https://bugs.launchpad.net/qemu/+bug/1329956.

Procedure

Step 1 Check the following:

```
cat /sys/module/kvm_intel/parameters/enable_apicv
```

Step 2 If the above value is set to Y:

a) Stop your virtual appliances and reinstall the KVM kernel module:

```
rmmod kvm_intel  modprobe kvm_intel enable_apicv=N
```

b) Restart your virtual appliance.

Hardware Appliances: Remotely Resetting Appliance Power

Before you begin

- Obtain and set up a utility that can manage devices using IPMI version 2.0.
- Understand how to use the supported IPMI commands. See the documentation for your IPMI tool.

If a hardware appliance requires a hard reset, you can reboot the appliance chassis remotely using a third-party Intelligent Platform Management Interface (IPMI) tool.

Restrictions

- Remote power cycling is available only on certain hardware. For specifics, see Enabling Remote Power Cycling.
- If you want be able to use this feature, you must enable it in advance, before you need to use it. For details, see Enabling Remote Power Cycling.
- Only the following IPMI commands are supported: status, on, off, cycle, reset, diag, soft. Issuing unsupported commands will produce an “insufficient privileges” error.

Procedure

Step 1 Use IPMI to issue a supported power-cycling command to the IP address assigned to the Remote Power Cycle port, which you configured earlier, along with the required credentials.

For example, from a UNIX-type machine with IPMI support, you might issue the command:

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P passphrase chassis power reset
```

For S195, S395, and S695 models, use :

```
ipmitool -I lanplus -H 192.0.2.1 -U remoteresetuser -P password chassis power reset
```

where `192.0.2.1` is the IP address assigned to the Remote Power Cycle port and remoteresetuser and passphrase are the credentials that you entered while enabling this feature.

Step 2 Wait at least eleven minutes for the appliance to reboot.

Site Access Problems

- Cannot Access URLs that Do Not Support Authentication, on page 77
- Cannot Access Sites With POST Requests , on page 77
- Also see: Bypassing Decryption for Particular Websites, on page 63

Cannot Access URLs that Do Not Support Authentication

This is a partial list of applications cannot be used when the Secure Web Appliance is deployed in transparent mode because they do not support authentication.

- Mozilla Thunderbird
- Adobe Acrobat Updates
- HttpBridge
- Subversion, by CollabNet
- Microsoft Windows Update
- Microsoft Visual Studio

Workaround: Create a class of user for the URL that does not require authentication.

Related Topics

- Bypassing Authentication

Cannot Access Sites With POST Requests

When the user's first client request is a POST request and the user still needs to authenticate, the POST body content is lost. This might be a problem when the POST request is for a application with the Access Control single sign-on feature in use.

Workarounds:

- Have users first authenticate with the Web Proxy by requesting a different URL through the browser before connecting to a URL that uses POST as a first request.
- Bypass authentication for URLs that use POST as a first request.



Note When working with Access Control, you can bypass authentication for the Assertion Consumer Service (ACS) URL configured in the Application Authentication Policy.

Related Topics

- Bypassing Authentication.

Upstream Proxy Problems

- Upstream Proxy Does Not Receive Basic Credentials, on page 78
- Client Requests Fail Upstream Proxy, on page 78

Upstream Proxy Does Not Receive Basic Credentials

If both the appliance and the upstream proxy use authentication with NTLMSSP, depending on the configurations, the appliance and upstream proxy might engage in an infinite loop of requesting authentication credentials. For example, if the upstream proxy requires Basic authentication, but the appliance requires NTLMSSP authentication, then the appliance can never successfully pass Basic credentials to the upstream proxy. This is due to limitations in authentication protocols.

Client Requests Fail Upstream Proxy

Configuration:

- Secure Web Appliance and upstream proxy server use Basic authentication.
- Credential Encryption is enabled on the downstream Secure Web Appliance.

Client requests fail on the upstream proxy because the Web Proxy receives an “Authorization” HTTP header from clients, but the upstream proxy server requires a “Proxy-Authorization” HTTP header.

Unable to Route FTP Requests Via an Upstream Proxy

If your network contains an upstream proxy that does not support FTP connections, then you must create a Routing Policy that applies to all Identities and to just FTP requests. Configure that Routing Policy to directly connect to FTP servers or to connect to a proxy group whose proxies all support FTP connections.

Virtual Appliances

- Do Not Use Force Reset, Power Off, or Reset Options During AsyncOS Startup , on page 78
- Network Connectivity on KVM Deployments Works Initially, Then Fails , on page 79
- Slow Performance, Watchdog Issues, and High CPU Usage on KVM Deployments , on page 79
- General Troubleshooting for Virtual Appliances Running on Linux Hosts , on page 79

Do Not Use Force Reset, Power Off, or Reset Options During AsyncOS Startup

The following actions on your virtual host are the equivalent of pulling the plug on a hardware appliance and are not supported, especially during AsyncOS startup:

- In KVM, the Force Reset option.
- In VMWare, the Power Off and Reset options. (These options are safe to use after the appliance has come up completely.)

Network Connectivity on KVM Deployments Works Initially, Then Fails

Problem

Network connectivity is lost after previously working.

Solution

This is a KVM issue. See the section on "KVM: Network connectivity works initially, then fails" in the OpenStack documentation at
http://docs.openstack.org/admin-guide-cloud/content/section_network-troubleshoot.html

Slow Performance, Watchdog Issues, and High CPU Usage on KVM Deployments

Problem

Appliance performance is slow, watchdog issues occur, and the appliance shows unusually high CPU usage when running on an Ubuntu virtual machine.

Solution

Install the latest Host OS updates from Ubuntu.

General Troubleshooting for Virtual Appliances Running on Linux Hosts

Problem

Issues with virtual appliances running on KVM deployments may be related to host OS configuration issues.

Solution

See the troubleshooting section and other information in the *Virtualization Deployment and Administration Guide* available from:

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Virtualization_Deployment_and_Administration_Guide/Red_Hat_Enterprise_Linux-7-Virtualization_Deployment_and_Administration_Guide-en-US.pdf.

WCCP Problems

- Maximum Port Entries, on page 79

Maximum Port Entries

In deployments using WCCP, the maximum number of port entries is 30 for HTTP, HTTPS , and FTP ports combined.

Packet Capture

- Starting a Packet Capture, on page 80
- Managing Packet Capture Files, on page 81

The appliance provides the ability to capture and display TCP/IP and other packets being transmitted or received over the network to which the appliance is attached.



Note The packet capture feature is similar to the Unix tcpdump command.

Secure Web Appliance does not support packet capture for the NIC paired interfaces. The packet capture will be applied only for the active interface. For example, if both P1 and P2 are paired, both P1 and P2 will not be configured in the user interface or the CLI.

Starting a Packet Capture

Procedure

Step 1 Choose **Support and Help > Packet Capture**.

Step 2 (Optional) Click **Edit Settings** to change the packet capture settings.

Option	Description
Capture File Size Limit	Specifies the maximum size that the capture file can reach. One the limit is reached, the data will be discarded and a new file started, unless the Capture Duration setting is 'Run Capture Until File Size Limit Reached.'
Capture Duration	Options for if and when the capture automatically stops. Choose from: • **Run Capture Until File Size Limit Reached**. The capture runs until the file limit set above is reached. • **Run Capture Until Time Elapsed Reaches.** The capture runs for a specified duration. If you enter the amount of time without specifying the units, AsyncOS uses seconds by default. • **Run Capture Indefinitely.** The packet capture runs until you manually stop it. **Note** The capture can be ended manually at any time.
Interfaces	The interfaces from which traffic will be captured.
Filters	The filtering options to apply when capturing packets. Filtering allows you to capture required packets only. Choose from: • **No Filters.** All packets will be captured. • **Predefined Filters.** The predefined filters provide filtering by port and/or IP addresses. If left blank, all traffic will be captured. • **Custom Filter.** Use this option if you already know the exact syntax of the packet capture options that you need. Use standard tcpdump syntax.

(Optional) Submit and commit your packet capture changes.

Note

When you change the packet capture settings without committing the changes and then start a packet capture, AsyncOS uses the new settings. This allows you to use the new settings in the current session without enforcing the settings for future packet capture runs. The settings remain in effect until you clear them.

Step 3 Click **Start Capture**. To manually stop a running capture, click **Stop Capture**.

Managing Packet Capture Files

The appliance saves the captured packet activity to a file and stores the file locally. You can send packet capture files using FTP to Cisco Customer Support for debugging and troubleshooting purposes.

• Downloading or Deleting Packet Capture Files, on page 81

Downloading or Deleting Packet Capture Files



Note You can also connect to the appliance using FTP and retrieving packet capture files from the captures directory.

Procedure

Step 1 Choose **Support and Help > Packet Capture**.

Step 2 Select the packet capture file you wish to use from the Manage Packet Capture Files pane. If this pane is not visible then no packet capture files have been stored on the appliance.

Step 3 Click **Download File** or **Delete Selected Files** as required.

Working With Support

• Gathering Information for Efficient Service , on page 81
• Opening a Technical Support Request, on page 81
• Getting Support for Virtual Appliances , on page 82
• Enabling Remote Access to the Appliance , on page 83

Gathering Information for Efficient Service

Before contacting Support:

- Enable custom logging fields as described in General Troubleshooting Best Practices, on page 55.
- Consider doing a packet capture. See Packet Capture, on page 79.

Opening a Technical Support Request

Before you begin

- Verify that your Cisco.com user ID is associated with your service agreement contract for this appliance. To view a list of service contracts that are currently associated with your Cisco.com profile, visit the

Cisco.com Profile Manager at https://sso.cisco.com/autho/forms/CDClogin.html. If you do not have a Cisco.com user ID, register to get one.

You can use the appliance to send a non-urgent request for assistance to Cisco Customer Support. When the appliance sends the request, it also sends the configuration of the appliance. The appliance must be able to send mail to the Internet to send a support request.



Note If you have an urgent issue, please call a Cisco Worldwide Support Center.

Procedure

Step 1 Choose **Support And Help > Contact Technical Support**.

Step 2 (Optional) Choose additional recipients for the request. By default, the support request and configuration file is sent to Cisco Customer Support.

Step 3 Enter your contact information.

Step 4 Enter the issue details.

- If you have a customer support ticket already for this issue, enter it.

Step 5 Click **Send**. A trouble ticket is created with Cisco.

Getting Support for Virtual Appliances

If you file a support case for a Cisco content security virtual appliance, you must provide your Virtual License Number (VLN), your contract number, and your Product Identifier code (PID).

You can identify your PID based on the software licenses running on your virtual appliance, by referencing your purchase order, or from the following table:

Functionality	PID	Description
Web Security Essentials	WSA-WSE-LIC=	Includes: • Web Usage Controls • Web Reputation
Web Security Premium	WSA-WSP-LIC=	Includes: • Web Usage Controls • Web Reputation • Sophos and Webroot Anti-Malware signatures
Web Security Anti-Malware	WSA-WSM-LIC=	Includes Sophos and Webroot Anti-Malware signatures
McAfee Anti-Malware	WSA-AMM-LIC=	—

Functionality	PID	Description
Secure Endpoint	WSA-AMP-LIC=	—

Enabling Remote Access to the Appliance

The Remote Access option allows Cisco Customer Support to remotely access your appliance for support purposes.

Procedure

Step 1 Choose **Support And Help > Remote Access**.

Step 2 Click **Enable**.

Step 3 Complete the Customer Support Remote Access options:

Option	Description
Seed String	If you enter a string, the string should not match any existing or future pass phrase. The string will appear near the top of the page after you click Submit. You will give this string to your support representative.
Secure Tunnel (recommended)	Specifies whether or not to use a secure tunnel for remote access connections. When enabled, the appliance creates an SSH tunnel over the specified port to the server upgrades.ironport.com, over port 443 (by default). Once a connection is made, Cisco Customer Support is able to use the SSH tunnel to obtain access to the appliance. Once the techsupport tunnel is enabled, it will remain connected to upgrades.ironport.com for 7 days. After 7 days, no new connections can be made using the techsupport tunnel, though any existing connections will continue to exist and work. The Remote Access account will remain active until specifically deactivated.
Appliance Serial Number	The serial number of the appliance.

Step 4 Submit and commit your changes.

Step 5 Look for the seed string in the Success message near the top of the page and make a note of it.

For security reasons, this string is not stored on the appliance and there is no way to locate this string later.

Keep this seed string in a safe place.

Step 6 Give the seed string to your Support representative.