Monitor System Activity Through Logs

This topic contains the following sections:

- Overview of Logging, on page 1
- Common Tasks for Logging, on page 2
- Best Practices for Logging, on page 2
- Troubleshooting Web Proxy Issues Using Logs, on page 2
- Log File Types, on page 3
- 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 34
- Customizing Access Logs, on page 36
- Traffic Monitor Log Files, on page 40
- Log File Fields and Tags, on page 41
- Troubleshooting Logging, on page 54

Overview of Logging

The Web Security 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 3

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 36
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 Web Security 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 3
- 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 Web Security 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
AMP Engine Logs	Records information about file reputation scanning and file analysis (Advanced Malware Protection.) See also Log Files.	Yes	Yes

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
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
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

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
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
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 Web Security 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

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
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 Web Security 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
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

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
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
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

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
W3C Logs	Records Web Proxy client history in a W3C compliant format. For more information, see W3C Compliant Access Log Files, on page 34.	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 Web Security 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 3
- 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 Web Security 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.
%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 34.
%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 AMP 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 Web Security Appliance itself, only requests to the actual Web Security 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 Advanced Malware Protection 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 Advanced Malware Protection 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 Advanced Malware Protection 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 Advanced Malware Protection file scanning; "-" indicates no threat.

Position	Field Value	Format Specifier	Description
36	33	%X#3#	Reputation score from Advanced Malware Protection 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 . .
37	0	%X#4#	Indicator of upload and analysis request: “0” indicates that Advanced Malware Protection did not request upload of the file for analysis. “1” indicates that Advanced Malware Protection 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 36

- W3C Compliant Access Log Files, on page 34
- Viewing Log Files, on page 16
- Log File Fields and Tags, on page 41

W3C Compliant Access Log Files

The Web Security 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 Web Security 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 Web Security 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 36.
- 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 36.

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 36.

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 34.
- Log File Fields and Tags, on page 41.

- Access Log User Defined Fields, on page 36.
- Configuring Cisco CTA-specific Custom W3C Logs, on page 38
- 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 36 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-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.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%(	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>
%:<l	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.
%:>l	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.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%:>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.
%:>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.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%: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.
%: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 Advanced Malware Protection 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 Advanced Malware Protection file scanning. "-" indicates no threat.
%X#3#	x-amp-score	Reputation score from Advanced Malware Protection 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 Advanced Malware Protection did not request upload of the file for analysis. "1" indicates that Advanced Malware Protection 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 AMP 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 AMP 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
- Logging HTTPS Transactions
- Alert: Unable to Maintain the Rate of Data Being Generated
- Problem Using Third-Party Log-Analyzer Tool with W3C Access Logs