Understand Secure Web Appliance Accesslogs

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Accesslog Structure

- Epoch time
- Elapsed Time
- Source IP address
- Transaction Result Code
- HTTP Response Code
- Total Size Transferred
- HTTP Method
- Destination
- User name and Authentication Realm
- Access Type
- Server Address
- MIME content-type/subtype
- ACL Decision Tag
- Policy Name
- Identity Policy
- Data SecurityPolicy Group
- External DLP Policy Group
- Routing Policy Group
- Web Traffic Tap
- URL Category Abbreviation
- Web Reputation Score
- Webroot Scanning
- McAfee Scanning
- Sophos Scanning
- Cisco Data Security Scan Verdict
- External DLP Scan Verdict
- Predefined URL Category Verdict
- URL Category Verdict
- Unified Inbound DVS Verdict
- Web Reputation Filter Threat Type
- Google Translate Encapsulated URL
- Application Control (AVC/ADC)
- Safe Browsing Verdict
- Average Bandwidth

Bandwidth Limit Control

User Type

Outbound Malware Scanning

Advanced Malware Protection

Archive Scan

Web Tap

YouTube URL category

HTTP Response Code

ACL DecisionTag

Malware Scanning Verdict Values

Related Content

Introduction

This document describes the structure of Secure Web Appliance (SWA) Accesslog.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Access To Command Line Interface (CLI) of SWA.

- Administrative Access to the SWA.
- Basic understanding of the SWA work flow.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Accesslog Structure

In this article the Accesslog structure is explained by this sample:

```
1726597763.348 68855 192.168.1.10 TCP_MISS/200 97645 TCP_CONNECT 10.37.145.84:443 "AMOJARRA\amirhossein
```

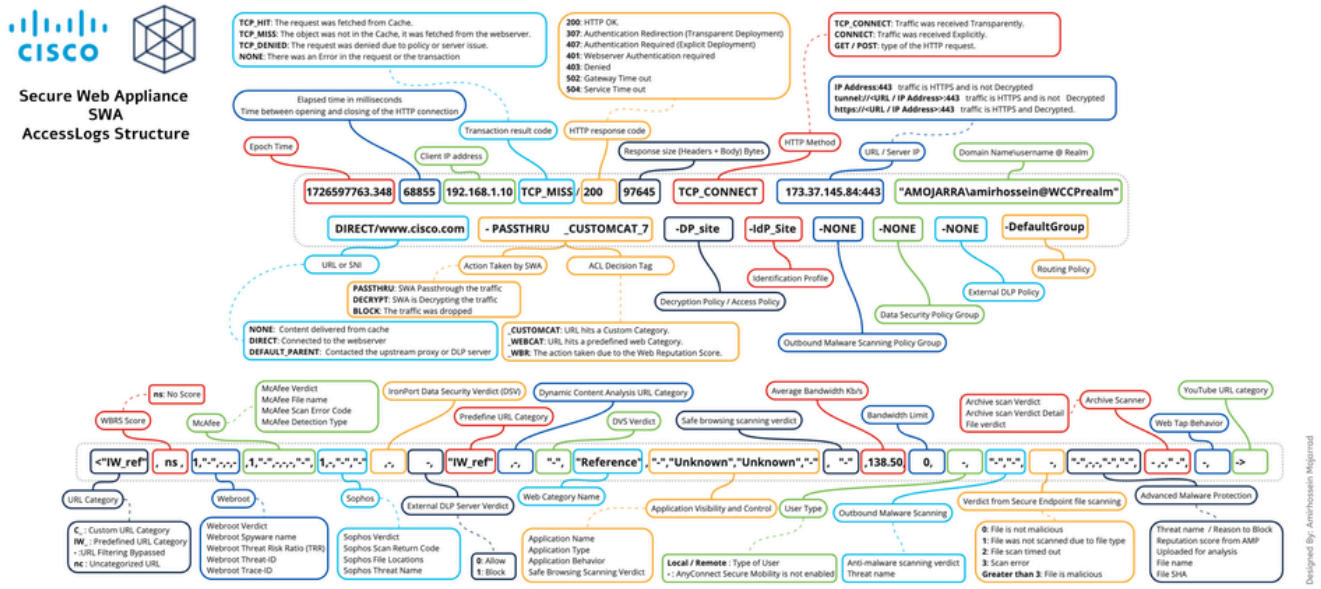


Image - Accesslog Structure

Note: The structure of Access Logs depends on the version of SWA. At the beginning of each Accesslog file there is a line that shows its structure and the order of the Format Specifier.

Section	Sample from Accesslog	Format Specifier	Details
Epoch time	1726597763.348	**%t**	Epoch time (often called Unix time or POSIX time by counting the total number of seconds that have elapsed since January 1, 1970, at 00 The Epoch time of when the transaction was You can convert this value by online Epoch t operating system.
Elapsed Time	68855	**%e**	The amount of milliseconds the request took and the connection closed.
Source IP address	192.168.1.10	**%a**	Client/Source IP address.

Transaction Result Code	TCP_MISS	**%w**	Transaction Result Code indicates how the S Here are the list of the Transaction Result Co
			TCP_HIT
			TCP_IMS_HIT
			TCP_MEM_HIT
			TCP_MISS
			TCP_REFRESH_HIT
			TCP_CLIENT_REFRESH_MISS
			TCP_DENIED
			TCP_DENIED_SSL HTTPS

			TCP_CLIENT_REFRESH_MISS_SSL
			TCP_MISS_SSL HTTPS
HTTP Response Code	/200	**%h**	The HTTP Response Code represents the sta server in response to the client HTTP request Here are the list of the most important HTTP information kindly visit **HTTP Response Co**

Status code	**Meaning**
000	000 is a nonstandard response c in communication during TLS transfer.
2xx Successful	
200	OK
204	No Content
206	Partial Content (also known as
3xx Redirection	
301	Permanent Redirection.
302	Temporary Redirection
304	Not Modified
307	Temporary Redirect for Auther (Usually seen in the transparen authenticating the user)
4xx Client Error	
400	Bad Request
401	Web server authentication requ transparent deployment while S

			403 Forbidden **404** Not Found **407** Explicit Proxy Authentication **5xx Server Error** **500** Internal Server Error **502** Bad Gateway **503** Service Unavailable **504** Gateway Timeout
Total Size Transferred	97645	**%s**	Total transferred Bytes for the request.
HTTP Method	TCP_CONNECT	**%1r**	An HTTP method is a standardized way for a action to be performed on a resource by a we with GET or submitting data with POST. **GET** The HTTP GE from a server. information an body. In simple **POST** The HTTP PO a server, typica request. It is co forms, uploadi changes the ser **CONNECT** The HTTP CO establish a tunn allowing the cl connection to t often used for encrypted com Indicates that t the SWA, mea use the proxy d **TCP_CONNECT** Indicates that t **transparently** or Layer 4 redi

<table>
<tr><td>Destination</td><td>10.37.145.84:443</td><td>%2r</td><td>This section shows the destination server UR

In transparent redirection, before the traffic g
destination IP address and port number.

If the URL starts with tunnel:// it means SW

If the URL starts with https:// it means SWA</td></tr>
<tr><td>User name and Authentication Realm</td><td>AMOJARRA\amirhossein@WCCPrealm</td><td>%A</td><td>Credentials used for this connection.

If the request gets authenticated, SWA logs t
Authentication realms as:

<Domain Name> \ <User Name> @ <Auth

If the request is not authenticated yet or is ex
log you see hyphen "-"</td></tr>
<tr><td>Access Type</td><td>DIRECT/</td><td>%H</td><td>Code that describes which server was contact
content.

Most common values include:

<table><tr><td>NONE</td><td>The Web Proxy had
any other server to re</td></tr><tr><td>DIRECT</td><td>The Web Proxy wen
request to get the cor</td></tr><tr><td>DEFAULT_PARENT</td><td>The Web Proxy wen
external Data Loss P
content.</td></tr></table></td></tr>
<tr><td>Server Address</td><td>www.cisco.com</td><td>%d</td><td>Data source or server IP address.</td></tr>
<tr><td>MIME content-type/subtype</td><td>-</td><td>%c</td><td>Multipurpose Internet Mail Extensions (MIM
format of a document, file or assortment of b
standardized in IETF RFC 6838

Two primary MIME types are important for t

• text/plain is the default value for textu
human-readable and must not contain b
• application/octet-stream is the defaul
unknown file type must use this type. I
when manipulating these files, to prote</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td>vulnerabilities and possible dangerous

To get a full list of MIME type please visit: M</td></tr>
<tr><td>ACL Decision Tag</td><td>PASSTHRU_CUSTOMCAT_7-</td><td>%D</td><td>An ACL decision tag is a field in an access lo
Web Proxy handled the transaction. It includ
Reputation filters, URL categories, and the sc

Note: The end of the ACL decision tag
generated number that the Web Proxy u
performance. You can ignore this numb

Here is a list of the most important ACL Dec
please visit ACL Decision Tag section in thi

ACL Decision Tag

ALLOW_CUSTOMCAT

ALLOW_WBRS

AMP_FILE_VERDICT

BLOCK_ADMIN

BLOCK_ADMIN_CONNECT

BLOCK_ADMIN_CUSTOM_USER_AG

BLOCK_ADMIN_TUNNELING</td></tr>
</table>

			BLOCK_ADMIN_FILE_TYPE
			BLOCK_ADMIN_PROTOCOL
			BLOCK_AMP_RESP
			BLOCK_AVC
			BLOCK_CONTENT_UNSAFE
			BLOCK_CUSTOMCAT
			BLOCK_ICAP
			BLOCK_WBRS
			BLOCK_WEBCAT
			BLOCK_YTCAT
			DECRYPT_ADMIN

			DECRYPT_EUN_CUSTOMCAT
			DECRYPT_EUN_WBRS
			DECRYPT_EUN_WEBCAT
			DECRYPT_WEBCAT
			DECRYPT_WBRS
			DROP_ADMIN
			DROP_WEBCAT
			DROP_WBRS
			PASSTHRU_ADMIN
			PASSTHRU_WEBCAT

			PASSTHRU_WBRS **OTHER**
Policy Name	DP_site-	**N/A**	Depends on the type of the traffic, this shows • **Decryption Policy name**: If the traffic yet • **Access Policy name**: If the traffic is H
Identity Policy	IdP_Site-	**N/A**	Shows the Identification Profile name
Outbound Malware Scanning Policy Group	NONE-	**N/A**	Outbound Malware Scanning Policy group n Any space in the policy group name is replac
Data Security Policy Group	NONE-	**N/A**	Cisco Data Security Policy group name. Whe global Cisco Data Security Policy, this value group name only appears when Cisco Data S appears when no Data Security Policy was ap Any space in the policy group name is replac
External DLP Policy Group	NONE-	**N/A**	When the transaction matches the global Ext **DefaultGroup**. **NONE** appears when no Ext Any space in the policy group name is replac
Routing Policy Group	DefaultGroup-	**N/A**	Routing Policy group name as **ProxyGroupN** When the transaction matches the global Rou **DefaultRouting**. When no upstream proxy s **DIRECT** Any space in the policy group name is replac

<table>
<tr><td>Web Traffic Tap</td><td>NONE</td><td>N/A</td><td>Web Traffic Tap Policy name.</td></tr>
<tr><td>URL Category Abbreviation</td><td><"C_Cisc",</td><td>%XC</td><td>URL Category that that the request is matchi<table>
<tr><td>-</td><td>URL Filtering Bypassed</td></tr>
<tr><td>nc</td><td>Not Categorized URLs</td></tr>
<tr><td>err</td><td>URL Filtering Bypassed</td></tr>
<tr><td>imp</td><td>Impossible</td></tr>
<tr><td>IW_</td><td>If the category name starts with
this means the request was hitt
Cisco Predefined URL Categor</td></tr>
<tr><td>C_</td><td>If the category name starts with
this means the request was hitt
Custom URL Category</td></tr>
</table></td></tr>
<tr><td>Web Reputation Score</td><td>-,</td><td>%XW</td><td>This field shows the Web Reputation (WBRS

ns means the URL has no score.</td></tr>
<tr><td>Webroot Scanning</td><td>-,"-",-,-,-,</td><td></td><td>These 5 fields are related to Webroot scannin<table>
<tr><td>Webroot Verdict,</td><td>%Xv</td><td>The r
Webr
Appl
Webr

For m
Verd
Scan
articl</td></tr>
<tr><td>Webroot Spyname,</td><td>“%Xn”</td><td>Name
with
detec</td></tr>
</table></td></tr>
</table>

			Webroot TRR,	**%Xt**	The W with value that r respo
			Webroot ThreatID,	**%Xs**	A val ident can u troub respo
			Webroot TraceID,	**%Xi**	A val ident can u troub respo
McAfee Scanning	-,"-",-,-,-,"-",		These 6 fields are related to McAfee scannin		
			McAfee Verdict,	**%Xd**	The r passe respo For m Verd **Scan** articl
			McAfee File name,	**“%Xe”**	The r Appl McA
			McAfee Scan Error Code,	**%Xf**	A val error this v issue McA
			McAfee Detection Type,	**%Xg**	A val detec Supp troub respo
			McAfee Virus Type,	**%Xh**	A val

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td></td><td>type.
this v
issue
McA</td></tr>
<tr><td>McAfee Virus Name,</td><td>“%Xj”</td><td>The n
scann
by M</td></tr>
</table>
</td></tr>
<tr><td>Sophos Scanning</td><td>-,-,"-","-",</td><td></td><td>
These 4 fields are related to Sophos scanning
<table>
<tr><td>Sophos Verdict,</td><td>%XY</td><td>The n
passe
respo

For m
Verd
Scan
articl</td></tr>
<tr><td>Sophos Scan Return Code,</td><td>%Xx</td><td>A val
return
can u
troub
respo</td></tr>
<tr><td>Sophos File Locations,</td><td>“%Xy”</td><td>The n
found
Appli
Soph</td></tr>
<tr><td>Sophos Threat Name,</td><td>“%Xz”</td><td>A val
name
use th
issue
Soph</td></tr>
</table>
</td></tr>
<tr><td>Cisco Data Security Scan Verdict</td><td>-,</td><td>%Xl</td><td>
The Cisco Data Security scan verdict based o
column of the Cisco Data Security Policy.

This list describes the possible values for this

0. Allow

1. Block

- (hyphen). No scanning was initiated by the
</td></tr>
</table>

			value appears when the Cisco Data Security URL category action is set to Allow.
External DLP Scan Verdict	-,	**%Xp**	The External DLP scan verdict based on the Content Adaptation Protocol (ICAP) respons This list describes the possible values for this **0.** Allow **1.** Block **- (hyphen)**. No scanning was initiated by the appears when External DLP scanning is disa scanned due to an exempt URL category on t Destinations page.
Predefined URL Category Verdict	"-",	**%XQ**	The predefined URL category verdict determ scanning, abbreviated. This field lists a hyphen (**-**) when URL filte If the request hits a Custom URL Category, y URL category name in your Accesslog but th custom URL category. For a list of URL category abbreviations, see
URL Category Verdict	-,	**%XA**	The URL category verdict determined by the (DCA) engine during response-side scanning Applies to the Cisco Web Usage Controls UR **nc**: This value appears in the request-side sca Content Analysis engine is enabled and no U request time, indicating the URL is un-catego phase before response-side scanning categori
Unified Inbound DVS Verdict	"-",	**%XZ**	Unified response-side Anti-Malware scannin Malware category independent of which scan Applies to transactions blocked or monitored
Web Reputation Filter Threat Type	"-",	**%Xk**	The Category Name or Threat Type is return The Category Name is returned when the We Type returned when the reputation is low. Typically, this field is populated for sites at r

<table>
<tr><td>Google Translate Encapsulated URL</td><td>"-",</td><td>%X#10#</td><td>The URL which is encapsulated inside Goog
encapsulated URL, the field value be -.</td></tr>
<tr><td>Application Control (AVC/ADC)</td><td>"-","-","-",</td><td></td><td>In these 3 fields statistics of Application Visi
Application Discovery and Control (ADC) ar
<table><tr><td>AVC/ADC Application Name</td><td>"%XO"</td><td>The ap
AVC c
Only a
engine</td></tr><tr><td>AVC/ADC Application Type</td><td>“%Xu”</td><td>The ap
AVC c
Only a
engine</td></tr><tr><td>AVC/ADC Application Behavior</td><td>“%Xb”</td><td>The ap
the AV
Only a
engine

It is _ f</td></tr></table></td></tr>
<tr><td>Safe Browsing Verdict</td><td>"-",</td><td>%XS</td><td>This value indicates whether either the safe s
feature was applied to the transaction.
<table><tr><td>ensrch</td><td>The original client request was unsa
applied.</td></tr><tr><td>encrt</td><td>The original client request was unsa
feature was applied.</td></tr><tr><td>unsupp</td><td>The original client request was to an</td></tr><tr><td>err</td><td>The original client request was unsa
the site content ratings feature could</td></tr><tr><td>-</td><td>Neither the safe search nor the site c
to the client request because the feat
the transaction was allowed in a cust
was made from an unsupported appl</td></tr></table></td></tr>
</table>

<table>
<tr><td>Average Bandwidth</td><td>11.35,</td><td>%XB</td><td>The average bandwidth consumed serving th</td></tr>
<tr><td>Bandwidth Limit Control</td><td>0,</td><td>%XT</td><td>A value that indicates whether the request wa control settings.

“1” indicates the request was throttled.

“0” indicates the request was not throttled.</td></tr>
<tr><td>User Type</td><td>-,</td><td>%l</td><td>The type of user making the request, either [I

Only applies when AnyConnect Secure Mob

When it is not enabled, the value is a hyphen</td></tr>
<tr><td>Outbound Malware Scanning</td><td>"-","-",</td><td></td><td>These 2 fields applies to transactions blocked request scanning when an Outbound Malwar<table><tr><td>Unified Outbound DVS Verdict</td><td>“%X3”</td><td>Unified scannin scannin transac client r Outbou applies</td></tr><tr><td>Outbound Threat Name</td><td>“%X4”</td><td>The thr request due to a Scannin

This th which a are ena</td></tr></table></td></tr>
<tr><td>Advanced Malware Protection</td><td>-,"-",-,-,"-","-",</td><td></td><td>These 6 fields are related to Secure Endpoint Malware Protection):<table><tr><td>File verdict</td><td>%X#1#</td></tr></table></td></tr>
</table>

			Threat Name	**%X#2#**
			Reputation Score	**%X#3#**
			Upload action for analysis	**%X#4#**
			File name	**%X#5#**
			File SHA	**%X#6#**
Archive Scan	-,-,"-",		These 3 fields indicates the status of the Arch	
			Archive scan Verdict	**%X#8#** Archive scan Verdict. **ARCHIVESCAN_ALLC**

					ARCHIVESCAN_BLOC
					ARCHIVESCAN_NESTI
					ARCHIVESCAN_UNKN
					ARCHIVESCAN_UNSC

					ARCHIVESCAN_FILET
			Archive scan Verdict Detail	**%Xo**	Archive scan Verdict Detai blocked (**ARCHIVESCAN** based on Access policy: Cu this Verdict Detail entry in and the name of the blocke "**UnScanable Archive-Blo** does not contain any block
			File verdict	**%Xm**	File verdict by Archive Sca
Web Tap	-,	**%XU**	Web Tap Behavior.		
YouTube URL category	->	**%X#29#**	The YouTube URL category assigned to the field shows **nc** when no category is assigned.		

HTTP Response Code

Here is the full list of HTTP Response Code

Status code	**Meaning**

1xx Information	
100	Continue
101	Switching protocols
102	Processing
103	Early Hints
2xx Successful	
200	OK
201	Created
202	Accepted
203	Non-Authoritative Information
204	No Content
205	Reset Content
206	Partial Content
207	Multi-Status
208	Already Reported
226	IM Used
3xx Redirection	
300	Multiple Choices
301	Moved Permanently
302	Found (Previously "Moved Temporarily")
303	See Other
304	Not Modified
305	Use Proxy
306	Switch Proxy
307	Temporary Redirect for Authentication (Usually seen in the transparent deployment while SWA is authenticating the user)
308	Permanent Redirect

4xx Client Error	
400	Bad Request
401	Web server authentication required (Usually seen in the transparent deployment while SWA is authenticating the user)
402	Payment Required
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not Acceptable
407	Explicit Proxy Authentication Required
408	Request Timeout
409	Conflict
410	Gone
411	Length Required
412	Precondition Failed
413	Payload Too Large
414	URI Too Long
415	Unsupported Media Type
416	Range Not Satisfiable
417	Expectation Failed
418	I am a Teapot
421	Misdirected Request
422	Unprocessable Entity
423	Locked
424	Failed Dependency
425	Too Early
426	Upgrade Required
428	Precondition Required
429	Too Many Requests
431	Request Header Fields Too Large
451	Unavailable For Legal Reasons

5xx Server Error	
500	Internal Server Error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Gateway Timeout
505	HTTP Version Not Supported
506	Variant Also Negotiates
507	Insufficient Storage
508	Loop Detected
510	Not Extended
511	Network Authentication Required

ACL Decision Tag

Here is the full list of the ACL decision tags:

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
ARCHIVESCAN_ALLCLEAR	Archive scan Verdict
ARCHIVESCAN_BLOCKEDFILETYPE	**ARCHIVESCAN_ALLCLEAR –** There are no blocked file types in the inspected archive.
ARCHIVESCAN_NESTEDTOODEEP	**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_UNKNOWNFMT	**ARCHIVESCAN_NESTEDTOODEEP** – The archive is blocked because it contains more “encapsulated” or nested archives than the configured maximum. The Verdict Detail field contains “Un-Scanable Archive-Blocked".
ARCHIVESCAN_UNSCANABLE	**ARCHIVESCAN_UNKNOWNFMT** – The archive is blocked because it contains a file type of unknown format. The Verdict Detail is “Un-Scannable Archive-Blocked”.
ARCHIVESCAN_FILETOOBIG	**ARCHIVESCAN_UNSCANABLE –** The archive is blocked because it contain a file which cannot be scanned. The Verdict Detail is “Un-Scannable Archive-Blocked”.
	ARCHIVESCAN_FILETOOBIG – The archive is blocked because the size of the archive is more than the configured maximum. The Verdict Detail is “UnScannable Archive-Blocked.”

	Archive scan Verdict Detail.
	The field and 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, “Un-Scannable 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_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.
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 SWA itself, only requests to the actual SWA redirect host name 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 can 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**.
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.
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 host name with EUN enabled.

DECRYPT_EUN_ADMIN_OCSP_OTHER_ERROR	The Web Proxy decrypted the transaction when HTTPS proxy settings drop an Online Certificate Status Protocol (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 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.
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_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 can 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.
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.

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.

This 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
19	Dialer
20	Hijacker

Malware Scanning Verdict Value	Malware Category
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 Content

- User Guide for AsyncOS 15.2 for Cisco Secure Web Appliance
- Use Secure Web Appliance Best Practices
- Ensure Proper Virtual WSA HA Group Functionality in a VMware Environment
- Configure Performance Parameter in Access Logs
- Understand HTTPS Accesslog Format in Secure Web Appliance
- Access Secure Web Appliance Logs