Forcepoint Security Information Event Management (SIEM) Solutions

SIEM Solutions | Web Protection Solutions| v8.5.x | 08-Jun-2020

Forcepoint web protection solutions allow Internet activity logging data and, with v8.5.4, audit log data to be passed to a third-party SIEM product, like ArcSight or Splunk. See *Integrating with third-party SIEM products*, page 1.

- For information about the other types of alerting offered by web protection solutions, see the Administrator Help.
- For information about alerts on a Forcepoint appliance, see the Forcepoint Appliances CLI Guide.
- For information about alarms using Content Gateway, see the Content Gateway Manager Help.

Use web protection reporting tools or SIEM integration to report on Internet activity when alerts reveal a potential issue.

Integrating with third-party SIEM products

Your web protection software can be configured to pass Internet activity (log) data and audit log data (v8.5.4 only) to a third-party SIEM product. To enable this configuration:

1. An instance of **Multiplexer** is installed with each Policy Server instance in your network.

   In appliance-based deployments, Policy Server runs on the full policy source appliance and all user directory and filtering appliances.
2. Use the **Web > Settings > General > SIEM Integration** page of the Security Managert to activate the integration and configure the system to send log data to your SIEM product in the format you specify.

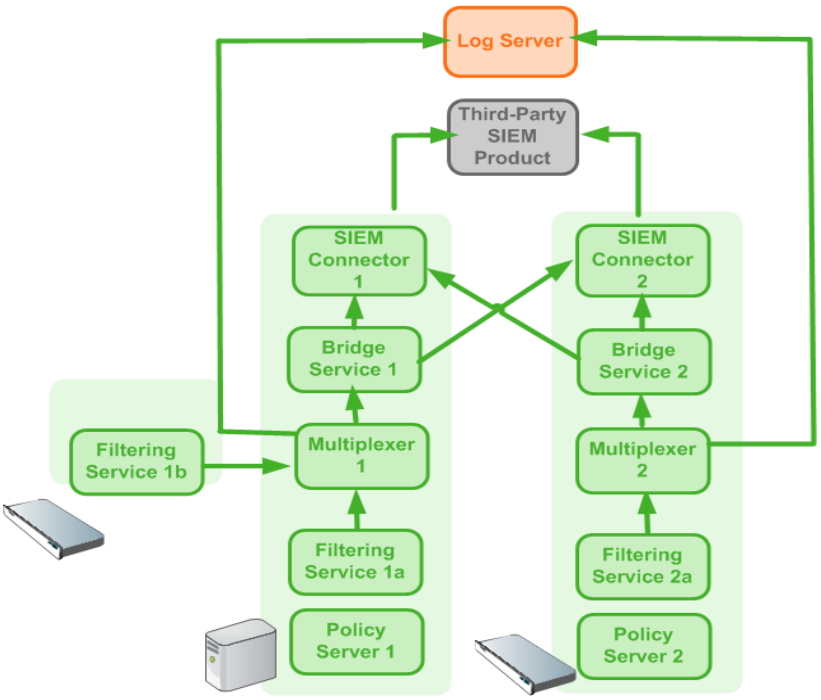
   See *Enabling and configuring SIEM integration*, page 3.

Multiplexer can run on supported Windows or Linux platforms, or on Forcepoint appliances and is automatically installed with each Policy Server instance in your deployment.

Configuration for each Multiplexer instance is stored by its Policy Server. This means that you can configure different settings for each Multiplexer instance, if, for example, you use a different SIEM product in different regions.

SIEM with Forcepoint Web Security, V8.5 and v8.5.3

The following diagram shows a possible configuration for SIEM integration for v8.5 and v8.5.3:



This deployment includes 2 Policy Server instances, each with its own Multiplexer instance.

- There are 2 Filtering Service instances associated with Policy Server 1; both pass Internet activity data to Multiplexer 1.
- Each Multiplexer instance passes the data that it receives from its associated Filtering Service instances to both Log Server and a third-party SIEM product.

The illustration shows 2 Forcepoint appliances and an additional server; all web protection components shown in the diagram could be deployed on a supported Windows or Linux server, or an appliance.

Data for each Policy Server (including those without a SIEM solution enabled) is sent to all SIEM solutions configured for other Policy Servers assigned to the same Policy Broker. This is true whether Policy Server was installed and assigned to a specific

Policy Broker, or Policy Server was connected to a Policy Broker using the **Settings > General > Policy Broker** page of Security Manager.

> **Important**
> To avoid duplication of data when using the same SIEM solution for each Policy Server assigned to the same Policy Broker, make sure that the details entered on the **Settings > General > SIEM Integration** page match for each Policy Server. If IP address or hostname, Port, and SIEM format do not match, the SIEM integration is handled as a different SIEM solution.

If data that is sent to a specific SIEM solution should not be forwarded to other SIEM solutions, install a replica Policy Broker and associate the corresponding Policy Server to that replica.

SIEM with Forcepoint Web Security, v8.5.4

In a basic configuration of SIEM integration for v8.5.4, data for each Policy Server is sent to each of the SIEM solutions configured in the **Internet Activity Log Data** section of **Web > Settings > General > SIEM Integration**. Data is not also sent to SIEM integrations configured for associated Policy Servers. To send data from multiple Policy Servers to the same SIEM integration, each Policy Server must be configured to use the same SIEM solution or solutions.

The **Audit Log Data** section is available for the primary Policy Server and, when **Enable SIEM integration for audit log data for this Policy Server** is selected, data viewable on **Web > Status > Audit Log** showing which administrators have accessed the Forcepoint Security Manager, as well as any changes made to policies and settings, is forwarded to the configured SIEM integration. Note that this feature is available only for the primary Policy Server and does not appear if you switch to a secondary Policy Server.

Enabling and configuring SIEM integration

Log on to the Web Security module of the Forcepoint Security Manager and navigate to **Settings > General > SIEM Integration** to activate and configure SIEM integration.

Perform this procedure for each Policy Server instance in your deployment.

In the **Internet Activity Log Data** section (titled in v8.5.3):

1. For 8.5.4: Click **Add** to open a new window where you will continue configuring your SIEM integration.

   For v8.5 and v8.5.3: Select **Enable SIEM integration for Internet activity log data for this Policy Server** (in v8.5, select **Enable SIEM integration for this Policy Server**) to turn on the SIEM integration feature. Follow these steps for

each Policy Server instance in your deployment to pass log data to a third-party SIEM product.

2. Provide the **IP address or hostname** of the machine hosting the SIEM product. Then, provide the communication **Port** to use for sending SIEM data.
3. Specify the **Transport protocol** (UDP or TCP) to use when sending data to the SIEM product.
4. Select the **SIEM format** to use. This determines the syntax of the string used to pass log data to the integration.
   - The available formats are syslog/CEF (ArcSight), syslog/key-value pairs (Splunk and others), syslog/LEEF (QRadar), and Custom.
   - If you select Custom, a text box is displayed. Enter or paste the string that you want to use. Click **View SIEM format strings** for a set of sample strings to use as a reference or template.
   - If you select a non-custom option, a sample **Format string** showing fields and value keys is displayed.

   See *Working with SIEM integration format strings*, page 5, for more information about format strings and the data included in records sent to the integration.
5. Click **OK** to cache your changes. Changes are not implemented until you click **Save and Deploy**.

After the changes have been saved, Multiplexer distributes the log data it receives from Filtering service to both Log Server and the selected SIEM integration.

With v8.5.4, perform these steps in the **Audit Log Data** section for the primary Policy Server in your deployment to pass audit log data to a third-party SIEM product. (See Viewing and exporting the audit log in Administrator Help for more information about the audit log.)

1. Check **Enable SIEM integration for audit log data for this Policy Server** to enable the feature.

   Note that this feature is available only for the primary Policy Server and does not appear if you switch to a secondary Policy Server.
2. Provide the **IP address or hostname** of the machine hosting the SIEM product, as well as the communication **Port** to use for sending the audit log data.
3. Specify the **Transport protocol** (UDP or TCP) to use when sending audit log data to the SIEM product.
4. Select the **SIEM format** to use. This determines the syntax of the string used to pass audit log data to the integration.
   - If you select Custom, enter or paste the string that you want to use in the text box that displays. Click **View SIEM format strings** for samples to use as a reference.
   - If you select a non-custom format, a sample **Format string** displays.
5. Click **OK** to cache your changes. Changes are not implemented until you click **Save and Deploy.**

When you save your changes, records written to the audit log are forwarded to the SIEM solution.

Working with SIEM integration format strings

When the SIEM integration is enabled, log data can be sent to the SIEM server using a custom or predefined format. Predefined format strings are available for syslog/CEF (ArcSight), syslog/key-value pairs (Splunk and others), and syslog/LEEF (QRadar).

Tip

Pre-defined strings can be copied and pasted into the Custom string field for modification.

A sample format string looks like this:

```
<159>%<:%b %d %H:%M:%S> %<-sourceServer>
CEF:0|Forcepoint|Security|%<productVersion>|%<categoryNumber
>|Transaction %<dispositionString>|%<severity>|
act=%<dispositionString> app=%<protocol> dvc=%<sourceServer>
dst=%<destination> dhost=%<urlHost> dpt=%<port>
src=%<source> spt=%<clientSourcePort> suser=%<=userPath>
loginID=%<=loginID>
destinationTranslatedPort=%<proxySourcePort> rt=%<time>
in=%<bytesReceived> out=%<bytesSent> requestMethod=%<method>
requestClientApplication=%<=userAgent>
reason=%<scanReasonString> cs1Label=Policy
cs1=%<policyNames> cs2Label=DynCat cs2=%<dynamicCategory>
cs3Label=ContentType cs3=%<=contentType>
cn1Label=DispositionCode cn1=%<=dispositionNumber>
cn2Label=ScanDuration cn2=%<scanDuration> request=%<=url>
logRecordSource=%<logRecordSource>
```

With log data incorporated, the result looks like this:

```
<159>Feb 14 16:36:56 10.10.10.121
CEF:0|Forcepoint|Security|8.5.0|148|Transaction permitted|1|
act=permitted app=http dvc=10.10.10.121 dst=204.15.67.17
dhost=testdatabasewebsense.com dpt=80 src=10.10.10.7
spt=65252 suser=LDAP://10.10.10.254
CN\=Users,DC\=forcepoint,DC\=local/win7 loginID=win7
destinationTranslatedPort=0 rt=1518655016 in=0 out=0
requestMethod=GET requestClientApplication=Mozilla/5.0
(Windows NT 6.1; Win64; x64; rv:58.0) Gecko/20100101
Firefox/58.0 reason=- cs1Label=Policy cs1=Super
Administrator**Default cs2Label=DynCat cs2=0
cs3Label=ContentType cs3=text/html cn1Label=DispositionCode
cn1=1048 cn2Label=ScanDuration cn2=14 request=http://
```

```
testdatabasewebsense.com/images/site_bg.gif
logRecordSource=OnPrem
```

When audit log data is sent to the SIEM server, predefined format strings are also available for syslog/CEF (ArcSight), syslog/key-value pairs (Splunk and others), and syslog/LEEF (QRadar).

A sample syslog/key-value pairs format string looks like this:

```
<156>%<:%b %d %H:%M:%S> %<-sourceServer> vendor=Forcepoint
product=Security product_version=%<productVersion>
action=%<action value> user=%<_userPath> reason=%<_details>
```

Field reference for SIEM integration

The string used to format data may include any of several keys, listed in the table below. Each key appears as follows in the format string:

```
%<key_name>
```

Key names are case sensitive.

- To include literal text in the string, simply enter the text. No special formatting is required.
- To include a timestamp, use the format:

  ```
  %<:%b %d %H:%M:%S %Z>
  ```

  See documentation for the **strftime** function for information about how to customize the string to suit your needs.
- To insert a line feed, use the format:

  ```
  %<\n>
  ```

Escape codes

Escape codes are needed in some string formats to render the needed output.

In CEF, for example, the equal sign is not allowed within values. For example, the equal sign embedded in the URL below is not allowed:

```
request=http://foo.com/x=42
```

An escape character must be added before the equal sign for the value to be rendered properly. The correct syntax is:

```
request=http://foo.com/x\=42
```

To support this, the format string syntax allows specific escape codes in front of the key name. For example, if you specify “%<=url>”, its meaning is the same as “%<url>”, except that all equal signs are escaped with a backslash, as are all linefeeds (LF), carriage returns (CR), and backslashes, resulting in: \=, \n, \r, and \\ respectively (each escape code is 2 characters long).

Supported escape codes include:

Code	Description
`%<=name>`	Escape equal signs, carriage returns, linefeeds, and the backslash character.
`%<$name>`	Escape end-of-line (replace LF with \n and CR with \r).
`%<|name>`	Escape the vertical bar (|), plus CR/LF; this is useful for the CEF prefix, where a vertical bar is not allowed unless escaped.
`%<"name>`	Escape the following special characters with a backslash: ● Backslash (to \\) ● Single quotes ('), double quotes ("), and backtick (‘) ● Dollar sign ($), equal sign (=), and vertical bar (|) ● Space, tab, CR, LF ● Colon and semi-colon
`%<_name>`	Turn the following characters into underscores: ● Backslash ● All three quote types ● All whitespace
`%<-name>`	The “-” (dash) escape has no effect in current versions. It was designed to signify “use value as-is; substitute a dash if there’s no value”. However, this is the default behavior; there is no need for the escape option.

In all the escaped cases, an empty string is replaced with “-” to support positional fields (e.g. in extended.log formats).

Keys

The keys that can be included in records sent to the SIEM integration are:

Key Name	Description
bytesReceived	Bytes received in response to the request
bytesSent	Bytes sent as part of the request
categoryNumber	Integer representing the category assigned to the URL (see *Category number reference*, page 11)
categoryReasonCode	The reason the URL was assigned to the listed category (see *Category reason code*, page 18)
ccaResultAttr	An ID from scanning results indicating which scanning process was used.
clientDestinationPort	Destination port of client connection; e.g., 8080 with Content Gateway explicit proxy
clientSourcePort	Source port of the client connection
cloudAppId	An internal ID assigned to the cloud application.
cloudAppName	Name of the requested cloud application.
cloudAppRiskLevel	Risk level (high, medium, or low) assigned to the cloud application.
cloudAppType	Type of cloud application requested (for example, Finance).
contentStripped	When Content Gateway content stripping is enabled, a three-bit map of the content that was removed. Bit 0 indicates ActiveX Bit 1 indicates JavaScript Bit 2 indicates VBScript For example, “000” indicates that no content was stripped. On the other hand, “010” indicates only JavaScript is stripped, while “111” indicates that ActiveX, JavaScript, and VBScript data are all stripped.
contentType	The Content Type value from the request header (for example, image/gif)
customerId	ID provided to each customer who purchases the Forcepoint Web Security Hybrid Module. (hybrid data)
destination	Translated IPv4 or IPv6 address of the destination machine (resolved by DNS from the requested URL).
dispositionNumber	The numeric code associated with the action (e.g., category permitted, file type blocked) applied to the request (see *Disposition reference*, page 16)
dispositionString	Permitted or Blocked, based on the value of dispositionNumber
DSSexternalIncidentID	The Forcepoint DLP ID number associated with an incident in the forensics repository

Key Name	Description
DSStimeStamp	The Forcepoint DLP timestamp for the forensic data
dynamicCategory	If non-zero, the category determined by real-time content analysis (e.g., Real-Time Security Scanning, Advanced File Analysis, etc.)
fileName	The name of the file associated with the request
fileTypeCode	The file type associated with the request (see *File type code*, page 19)
keyword	Keyword used to block a request. Empty if the request was not blocked by keyword.
loginID	Login ID of the user to whom the policy was applied. NOTE: output can now be configured to replace the full LDAP user path with domain/userID. Contact Technical Support for assistance.
logRecordSource	The source of the log record. (Hybrid or on-premises (OnPrem))
lookupDuration	How long it took to look up category or protocol information in the Master Database (milliseconds)
method	Method associated with the request (for example, GET, POST, PUT, and so on)
networkDirection	Inbound (0) or outbound (1)
policyNames	The name of the policy or policies that could be applied to the request. (Multiple policies may be found, for example, for a user who belongs to multiple groups.)
port	Integer representing the TCP port of the origin server
productVersion	Web protection product version, as determined by Multiplexer (for example, 8.2.0)
protocol	The protocol name (custom or defined in the Master Database)
protocolId	Signed protocol identifier. A negative number indicates a custom protocol.
protocolVersion	HTTP Version (Byte.Byte)
proxySourceAddress	The IP address of the proxy (on-premises data) or the SIEMConnector IP address (hybrid data)
proxySourcePort	Source port of proxy-server connection
proxyStatusCode	Proxy HTTP response code
refererUrl	URL of the referer site associated with the request
requestCount	The number of requests to a given site.
roleId	A number associated with the delegated administration role in which the policy applied to the request was created. The identifier for the Super Administrator role is 8.
scanDuration	If Content Gateway analysis was performed, how long it took (milliseconds)

Key Name	Description
scanReasonString	Scanning analytic result, if any; the string might look like: 0-1404-Threat.Malicious.Web.RealTime.
severity	1 if permitted, 7 if blocked This severity entry does not relate to the severity levels assigned to incidents that appear on the Threats dashboard in Security Manager.
serverStatusCode	Origin server HTTP response code
source	IPv4 or IPv6 address of the client (requesting) machine
sourceServer*	IP address (in integer format) of the server that originated the message, either Content Gateway or Network Agent
time	A positive, long number representing the number of seconds (v8.5) or milliseconds (v8.5.3) since midnight Jan. 1, 1970
url	Full requested URL. Does not include protocol or port.
urlHost	Host (domain) portion of the requested URL
userAgent	Contents of the User-Agent HTTP header, if present
userPath	Contains NameSpace, Domain, and UserName information for the user to whom the policy was applied.

Important

*SIEM server will identify the proper sourceServer/host only if the custom string starts with this header: <159>%<:%b %d %H:%M:%S> %<-sourceServer>"

The keys that can be included in audit log records sent to the SIEM integration are:

Key Name	Description
action value	Type of change made, such as log on, log off, add, delete, or change
details	Specific information about the change that was made.
productVersion	Web protection product version, as determined by Multiplexer (for example, 8.5.0)
sourceServer	For changes that affect the Policy Server, such as changes made to Settings options, the IP address or name of machine running the Policy Server affected by the change. For changes made to policies or to global settings, the IP address of the primary Policy Broker.
userPath	User name of the administrator who made the change.

Category number reference

If you are using an SIEM integration to send log data to a third-party SIEM product, use the following table to map the ID shown in the **categoryNumber** field to a predefined category name.

ID	Parent Category	Child Category
1	Adult Material	
2	Business and Economy	
3	Education	
4	Government	
5	News and Media	
6	Religion	
7	Society and Lifestyles	
8	Special Events	
9	Information Technology	
10	Abortion	
11	Advocacy Groups	
12	Entertainment	
13	Gambling	
14	Games	
15	Illegal or Questionable	
16	Job Search	
17	Shopping	
18	Sports	
19	Tasteless	
20	Travel	
21	Vehicles	
22	Violence	
23	Weapons	
24	Drugs	
25	Militancy and Extremist	
26	Intolerance	
27	Health	
28	Information technology	Website Translation
29	Productivity	Advertisements

ID	Parent Category	Child Category
64	User-Defined	
65	Adult Material	Nudity
66	Adult Material	Adult Content
67	Adult Material	Sex
68	Business and Economy	Financial Data and Services
69	Education	Cultural Institutions
70	Entertainment	Media File Download
72	Government	Military
73	Government	Political Organizations
74	Internet Communication	General Email
75	Information Technology	Proxy Avoidance
76	Information Technology	Search Engines and Portals
78	Information Technology	Web Hosting
79	Internet Communication	Web Chat
80	Information Technology	Hacking
81	News and Media	Alternative Journals
82	Religion	Non-Traditional Religions
83	Religion	Traditional Religions
84	Society and Lifestyles	Restaurants and Dining
85	Society and Lifestyles	Gay or Lesbian or Bisexual Interest
86	Society and Lifestyles	Personals and Dating
87	Society and Lifestyles	Alcohol and Tobacco
88	Drugs	Prescribed Medications
89	Drugs	Nutrition
90	Drugs	Abused Drugs
91	Internet Communication	
92	Abortion	Pro-Choice
93	Abortion	Pro-Life
94	Adult Material	Sex Education
95	Adult Material	Lingerie and Swimsuit
96	Productivity	Online Brokerage and Trading
97	Education	Educational Institutions
98	Productivity	Instant Messaging

ID	Parent Category	Child Category
99	Productivity	Application and Software Download
100	Productivity	Pay-to-Surf
101	Shopping	Internet Auctions
102	Shopping	Real Estate
103	Society and Lifestyles	Hobbies
107	Sport	Sport Hunting and Gun Clubs
108	Bandwidth	Internet Telephony
109	Bandwidth	Streaming Media
110	Productivity	
111	Drugs	Marijuana
112	Productivity	Message Boards and Forums
113	Bandwidth	Personal Network Storage and Backup
114	Bandwidth	Internet Radio and TV
115	Bandwidth	Peer-to-Peer File Sharing
116	Bandwidth	
117	Society and Lifestyles	Social Networking
118	Education	Educational Materials
121	Education	Reference Materials
122	Social Organizations	
123	Social Organizations	Service and Philanthropic Organizations
124	Social Organizations	Social and Affiliation Organizations
125	Social Organizations	Professional and Worker Organizations
126	Security	
128	Security	Malicious Websites
138	Information Technology	Computer Security
146	Miscellaneous	
147	Miscellaneous	Web Infrastructure
148	Miscellaneous	Web Images
149	Miscellaneous	Private IP Addresses
150	Miscellaneous	Content Delivery Networks
151	Miscellaneous	Dynamic Content

ID	Parent Category	Child Category
152	Miscellaneous	Network Errors
153	Miscellaneous	Uncategorized
154	Security	Spyware
156	Miscellaneous	File Download Servers
164	Security	Phishing and Other Frauds
166	Security	Keyloggers
167	Security	Potentially Unwanted Software
172	Security	Bot Networks
191	Extended Protection	
192	Extended Protection	Elevated Exposure
193	Extended Protection	Emerging Exploits
194	Extended Protection	Suspicious Content
195	Internet Communication	Organizational Email
196	Internet Communication	Text and Media Messaging
200	Information Technology	Web and Email Spam
201	Information Technology	Web Collaboration
202	Parked Domain	
203	Business and Economy	Hosted Business Applications
204	Society and Lifestyles	Blogs and Personal Sites
205	Security	Malicious Embedded Link
206	Security	Malicious Embedded iFrame
207	Security	Suspicious Embedded Link
208	Bandwidth	Surveillance
209	Bandwidth	Educational Video
210	Bandwidth	Entertainment Video
211	Bandwidth	Viral Video
212	Extended Protection	Dynamic DNS
213	Security	Potentially Exploited Documents
214	Security	Mobile Malware
215	Information Technology	Unauthorized Mobile Marketplaces
216	Security	Custom-Encrypted Uploads
217	Security	Files Containing Passwords
218	Security	Advanced Malware Command and Control

ID	Parent Category	Child Category
219	Security	Advanced Malware Payloads
220	Security	Compromised Websites
221	Extended Protection	Newly Registered Websites
222	Collaboration - Office	
223	Collaboration - Office	Office - Mail
224	Collaboration - Office	Office - Drive
225	Collaboration - Office	Office - Documents
226	Collaboration - Office	Office - Apps
227	Information Technology	Web Analytics
228	Information Technology	Web and Email Marketing
1500	Social Web - Facebook	
1501	Social Web - LinkedIn	LinkedIn Updates
1502	Social Web - LinkedIn	LinkedIn Mail
1503	Social Web - LinkedIn	LinkedIn Connections
1504	Social Web - LinkedIn	LinkedIn Jobs
1505	Social Web - Facebook	Facebook Posting
1506	Social Web - Facebook	Facebook Commenting
1507	Social Web - Facebook	Facebook Friends
1508	Social Web - Facebook	Facebook Photo Upload
1509	Social Web - Facebook	Facebook Mail
1510	Social Web - Facebook	Facebook Events
1511	Social Web - YouTube	YouTube Commenting
1512	Social Web - YouTube	YouTube Video Upload
1513	Social Web - Facebook	Facebook Apps
1514	Social Web - Facebook	Facebook Chat
1516	Social Web - Facebook	Facebook Questions
1517	Social Web - Facebook	Facebook Video Upload
1518	Social Web - Facebook	Facebook Groups
1519	Social Web - Twitter	Twitter Posting
1520	Social Web - Twitter	Twitter Mail
1521	Social Web - Twitter	Twitter Follow
1523	Social Web - YouTube	YouTube Sharing
1524	Social Web - Facebook	Facebook Games
1525	Social Web - YouTube	
1526	Social Web - Twitter	

ID	Parent Category	Child Category
1527	Social Web - LinkedIn	
1528	Social Web - Various	
1529	Social Web - Various	Classifieds Posting
1530	Social Web - Various	Blog Posting
1531	Social Web - Various	Blog Commenting
1801	Non-HTTP	

Disposition reference

If you are using an SIEM integration to send log data to a third-party SIEM product, use the following table to map the ID shown in the **dispositionNumber** field to the action applied to the request.

The table also shows how each number is summarized in the **dispositionString** field.

ID	Description	Summary
1024	Category permitted, not set	Permitted
1025	Category blocked	Blocked
1026	Category permitted	Permitted
1027	Custom URL, category blocked	Blocked
1028	Custom URL, category permitted	Permitted
1029	Always blocked	Blocked
1030	Never blocked	Permitted
1031	Blocked by limited access filter	Blocked
1032	Blocked by keyword	Blocked
1033	Blocked – subscription level exceeded	Blocked
1034	Permitted – subscription level exceeded	Permitted
1035	Password override page	Blocked
1037	Permitted by password override	Permitted
1040	Permitted with Confirm option	Permitted
1041	Blocked – authentication required	Blocked
1042	Permitted – category not purchased	Permitted
1043	Permitted by quota	Permitted
1044	Permitted with keyword match	Permitted

ID	Description	Summary
1045	Blocked due to network bandwidth	Blocked
1046	Blocked due to protocol bandwidth	Blocked
1047	File type blocked	Blocked
1048	File type permitted	Permitted
1049	Protocol blocked	Blocked
1050	Protocol permitted	Permitted
1051	Protocol permitted, not set	Permitted
1052	Permitted by limited access filter	Permitted
1053	Redirected by search filtering	Blocked
1054	Blocked with Confirm option	Blocked
1055	Blocked by quota	Blocked
1056	Permitted – protocol not purchased	Permitted
1057	Blocked by security override	Blocked
1058	Blocked by Hosted Anti-Virus Scanning - Inbound	Blocked
1059	Blocked by Hosted Anti-Virus Scanning - Outbound	Blocked
1060	Permitted by Policy Exception	Permitted
1061	Blocked by Policy Exception	Blocked
1062	Permitted by Tunneled Protocol Quota	Permitted
1063	Permitted by Tunneled Protocol Continue	Permitted
1064	Blocked by Web DLP	Blocked
1065	Permitted by Referer	Permitted
1066	File Blocked: Over Max Scan Size	Blocked
1067	Cloud app permitted	Permitted
1068	Cloud app blocked	Blocked
1069	Protected cloud app request forwarded	Permitted
1281	Category blocked real time	Blocked
1282	Category permitted real time	Permitted
1293	Permitted by password override real time	Permitted
1296	Permitted with confirm option real time	Permitted
1299	Permitted by quota real time	Permitted
1301	Blocked due to network bandwidth real time	Blocked
1302	Blocked due to protocol bandwidth real time	Blocked
1303	File type blocked real time	Blocked
1304	File type permitted real time	Permitted

ID	Description	Summary
1310	Blocked with confirm option real time	Blocked
1311	Blocked by quota real time	Blocked
1313	Blocked by security override real time	Blocked
1314	Blocked Inbound: Cloud Antivirus	Blocked
1315	Blocked Outbound: Cloud Antivirus	Blocked
1316	Permitted by Exception: Real Time	Permitted
1317	Blocked by Exception: Real Time	Blocked
1537	Permitted by scanning link analysis	Permitted
1538	Web 2.0 request permitted	Permitted
1539	Permitted after Web 2.0 scanning and link analysis	Permitted
1553	Blocked by scanning link analysis	Blocked
1554	Web 2.0 request blocked	Blocked
1555	Blocked after Web 2.0 scanning and link analysis	Blocked
1556	Zipbomb permitted Real Time	Permitted
1557	Zipbomb blocked Real Time	Blocked

Category reason code

If you are using an SIEM integration to send log data to a third-party SIEM product, use the following table to map the ID shown in the **categoryReasonCode** field to the reason the URL was placed in the category indicated in the **categoryNumber** field.

ID	Description
0	None
1	Found in the Master Database
2	Regular expression matched in the Master Database
3	Found in a Real-Time Database Update or Real-Time Security Update database
4	Regular expression matched in a Real-Time Database Update or Real-Time Security Update database
5	Custom URL - permit
6	Custom URL - deny
7	Private IP address
8	Categorized by keyword
9	Categorized by Content Gateway analysis

ID	Description
10	Multi-term search
11	Categorized by the hybrid service (*requires the Web Hybrid module*)

File type code

If you are using an SIEM integration to send log data to a third-party SIEM product, use the following table to map the ID shown in the **fileTypeCode** field to the file type identified for the request, if any.

ID	Description
0	No file downloaded; can result when the request (GET) is blocked
3	Executables
4	Compressed Files
5	Multimedia
6	Text
7	Images
8	Documents
9	Threats
10	Rich Internet Applications
11	Unknown