Forcepoint Security Information Event Management (SIEM) Solutions

Applies to:	TRITON AP-WEB and Web Filter & Security, v8.3.x

Forcepoint web protection solutions can issue alerts using SNMP trap data when integrated with a supported Security Information Event Management (SIEM) system.

SNMP traps send alerts to system administrators about significant events that affect the security of your network. These alerts include:

- *System, usage, and suspicious activity alerts*, page 2
- *Content Gateway (software) alarms*, page 17

Forcepoint web protection solutions also allow Internet activity logging data to be passed to a third-party SIEM product, like ArcSight or Splunk. See *Integrating with third-party SIEM products*, page 19.

- For information about the other types of alerting offered by web protection solutions, see the Administrator Help.
- For information about alarms using Content Gateway, see the Content Gateway Manager Help.

Use SNMP alerting to maintain system health and keep your organization protected, and use web protection reporting tools or SIEM integration to report on Internet activity when alerts reveal a potential issue.

System, usage, and suspicious activity alerts

To facilitate tracking and management of both web protection software and client Internet activity, Super Administrators can configure the following alerts to be sent when selected events occur:

- **System alerts** notify administrators of events relating to subscription status and Master Database activity, as well as Content Gateway events, including loss of contact to a domain controller, log space issues, and more.
- **Usage alerts** notify administrators when Internet activity for selected categories or protocols reaches configured thresholds.

  Usage alerts can be generated for both pre-defined and custom categories or protocols.
- **Suspicious activity alerts** notify administrators when threat-related events of a selected threat severity level reach configured thresholds or, for TRITON AP-WEB customers who have enabled Advanced File Analysis, when a file that was sent for analysis is found to be malicious.

All alerts can be sent to selected recipients via email or SNMP.

Note that alerting must be enabled and configured before system, usage, or suspicious activity alerts can be generated. See *Enabling system, usage, and suspicious activity alerts*, page 7.

User-configurable controls help avoid generating excessive numbers of alert messages. Define realistic alerting limits and thresholds to avoid creating excessive numbers of alerts for noncritical events. See *Flood control*, page 8.

System alerts

Filtering Service alerts monitor events such as database download failure, changes to the database, and subscription issues. They apply to both TRITON AP-WEB and Web Filter & Security deployments:

Alert Event	**Possible Causes**	**Recommended Severity**
A Master Database download failed.	● Unable to complete download (general) ● Unable to download for 15 days ● Unsupported product version ● Operating system error or incompatibility ● Invalid subscription key ● Expired subscription	Error
The number of current users exceeds your subscription level.	More clients are making Internet requests than are covered by your subscription.	Error
The number of current users has reached 90% of your subscription level.	The number of clients in your network is very close to the maximum number of clients covered by your subscription.	Warning
The search engines supported by Search Filtering have changed.	A search engine was either added to or removed from the list of search engines for which your product can enable search filtering.	Information
The Master Database has been updated.	● URL categories added or removed ● Network protocols added or removed	Information
Your subscription expires in one month.	Your subscription is approaching its renewal date	Information
Your subscription expires in one week.	Your subscription has not been renewed	Warning

Additional Content Gateway alerts are available for TRITON AP-WEB customers:

Alert Event	Possible Causes	Severity Recommendation
A domain controller is down.	● Domain controller shut down or restarted ● Network problem	Warning
Decryption and inspection of secure content has been disabled.	Feature turned off	Information
Log space is critically low.	Not enough disk space in the partition for storing Content Gateway logs	Warning
Subscription information could not be reviewed.	Local or remote problem	Warning
Non-critical alerts have been received.	● Content Gateway process reset ● Cache configuration issue ● Unable to create cache partition ● Unable to initialize cache ● Unable to open configuration file ● Invalid fields in configuration file ● Unable to update configuration file ● Clustering peer operating system mismatch ● Could not enable virtual IP addressing ● Connection throttle too high ● Host database disabled ● Logging configuration error ● Unable to open Content Gateway Manager ● ICMP echo failed for a default gateway ● HTTP origin server is congested ● Congestion alleviated on the HTTP origin server ● Content scanning skipped ● WCCP configuration error	Varies

A system alert for a database download failure, delivered via email, might look like this:

```
Alert: Database Download Failure
Filtering Service: 10.80.187.244
Subscription Key: EXAMPLEDO77K33LF

Filtering Service is unable to download the Master Database
because your software version is no longer supported.
Contact Forcepoint LLC or your authorized reseller for
information about upgrades.
```

Usage alerts

Usage alerts warn an administrator when Internet activity for selected URL categories or protocols reaches a defined threshold.

For configuring usage alerts, see *Configuring category usage alerts*, page 11, and *Configuring protocol usage alerts*, page 12.

Alert Event	Severity Recommendation
Configured threshold exceeded for category	Information
Configured threshold exceeded for protocol	Information

A category usage alert delivered via email might look like this:

```
Alert: Threshold exceeded for Blocked Category (1 of 20
alerts for today)

A client has exceeded a configured daily Internet usage
threshold.

For more information, run investigative or presentation
reports in the TRITON Manager. See the Administrator Help
for details.

User name: JSmith
User IP address: 123.1.2.3
Threshold (in visits): 40
Category: Sports
Action: Blocked

--Most recent request--
URL: http://www.extremepingpong.com
IP address: 216.251.32.98
Port: 80
```

Suspicious activity alerts

Suspicious activity alerts notify administrators when threat-related events of a selected severity level (Critical, High, Medium, Low) reach configured thresholds.

Because Content Gateway is required to detect critical and high severity alerts, it is not possible to configure alerting for those severity levels in Web Filter & Security deployments.

TRITON AP-WEB customers who have enabled Advanced File Analysis can enable email or SNMP alerts to be sent when a file submitted for analysis is determined to be malicious.

Threat-related events can be monitored and investigated via the **Threats** dashboard in the Web module of the TRITON Manager (see Threats dashboard).

To configure suspicious activity alerts, see *Configuring suspicious activity alerts*, page 13.

A suspicious activity alert delivered via email might look like this:

```
Alert: High Severity Suspicious Activity Alert (1 of 100 max
alerts for today)

Date: 5/15/2012 12:04:53 PM
Type: Information
Source: Forcepoint Usage Monitor

Suspicious activity has exceeded the alerting threshold for
this severity level.

Severity: High
Category: Malware: Command and Control
Filtering action: Blocked
Threshold (in hits): 15

Log on to the TRITON Manager and access the Threats dashboard
for more details about these incidents.

Access TRITON Manager here: <link>

---Most recent incident---

User: bjones
IP address: 10.1.20.55
Hostname: lt-bjones
URL: http://<full_url>
Destination IP address: 153.x.x.x  Port: 8080
Threat details: trojan.downloader.win32.W32/
CeeInject.AE.gen!Eldorado
```

Enabling system, usage, and suspicious activity alerts

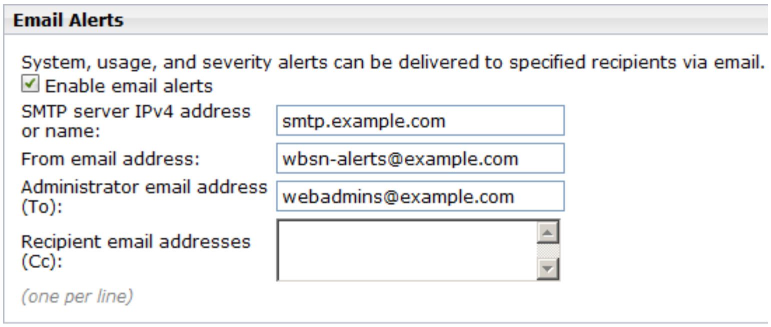
To enable alerting, go to the **Settings** > **Alerts** > **Enable Alerts** page in the Web module of the TRITON Manager.

1. Set the **Maximum daily alerts per usage type** value to limit the total number of alerts generated daily.

   For example, you might configure usage alerts to be sent every 5 times (threshold) someone requests a site in the Sports category. Depending on the number of users and their Internet use patterns, that could generate hundreds of alerts each day.

   If you enter 10 as the maximum daily alerts per usage type, only 10 alert messages are generated each day for the Sports category. In this example, these messages alert you to the first 50 requests for Sports sites (5 requests per alert multiplied by 10 alerts).

2. Mark **Enable email alerts** to configure email notifications, then provide information about the location of the SMTP server and the alert sender and recipients.



Email Alerts

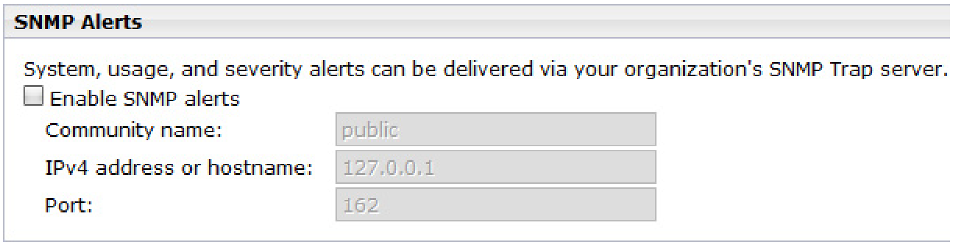
System, usage, and severity alerts can be delivered to specified recipients via email.

☑ Enable email alerts

SMTP server IPv4 address or name:	smtp.example.com
From email address:	wbsn-alerts@example.com
Administrator email address (To):	webadmins@example.com
Recipient email addresses (Cc): *(one per line)*	

SMTP server IPv4 address or name	IPv4 address or hostname for the SMTP server through which email alerts should be routed.
From email address	Email address to use as the sender for email alerts.
Administrator email address (To)	Email address of the primary recipient of email alerts.
Recipient email addresses (Cc)	Email address for up to 50 additional recipients. Each address must be on a separate line.

3. Mark **Enable SNMP alerts** to enable delivery of alert messages through an SNMP trap system installed in your network, then provide trap server information (described below).



SNMP Alerts

System, usage, and severity alerts can be delivered via your organization's SNMP Trap server.

□ Enable SNMP alerts

Community name: public

IPv4 address or hostname: 127.0.0.1

Port: 162

Community name	Name of the trap community on your SNMP trap server.
Server IP or name	IP address or name of the SNMP Trap server.
Port	Port number SNMP message use.

4. Click **OK** to cache changes. Changes are not implemented until you click **Save and Deploy**.

Once alerting is enabled, to configure specific types of alerts, see:

- *Configuring system alerts*, page 10
- *Configuring category usage alerts*, page 11
- *Configuring protocol usage alerts*, page 12
- *Configuring suspicious activity alerts*, page 13

SNMP alert information

When your software sends an SNMP alert, the following fields may be populated in the SNMP trap:

- Filtering Service (IP address)
- Time (year, month, and day)
- User name
- Threshold (usage alerts)
- Protocol
- URL (hat triggered the alert)
- Port (protocol port)
- Policy Server (IP address)
- Subscription key
- User IP address
- Category
- Action (e.g., Blocked, Permitted)
- IP address (of the URL that triggered the alert)

Flood control

There are built-in controls for usage alerts to avoid generating excessive numbers of alert messages. Use the **Maximum daily alerts per usage type** setting on the

Settings > Alerts > Enable Alerts page to specify a limit for how many alerts are sent in response to user requests for particular categories and protocols.

You can also set threshold limits for each category and protocol usage alert, and for each suspicious activity alert. For example, if you set a threshold limit of 10 for a certain category, an alert is generated after 10 requests for that category (by any combination of clients).

Suppose that the maximum daily alerts setting is 20, and the category alert threshold is 10. Administrators are only alerted the first 20 times category requests exceed the threshold. That means that only the first 200 occurrences result in alert messages (threshold of 10 multiplied by alert limit of 20).

Configuring system, usage, and suspicious activity alerts

Use the topics in this section sequentially, or jump to the type of alert you want to configure.

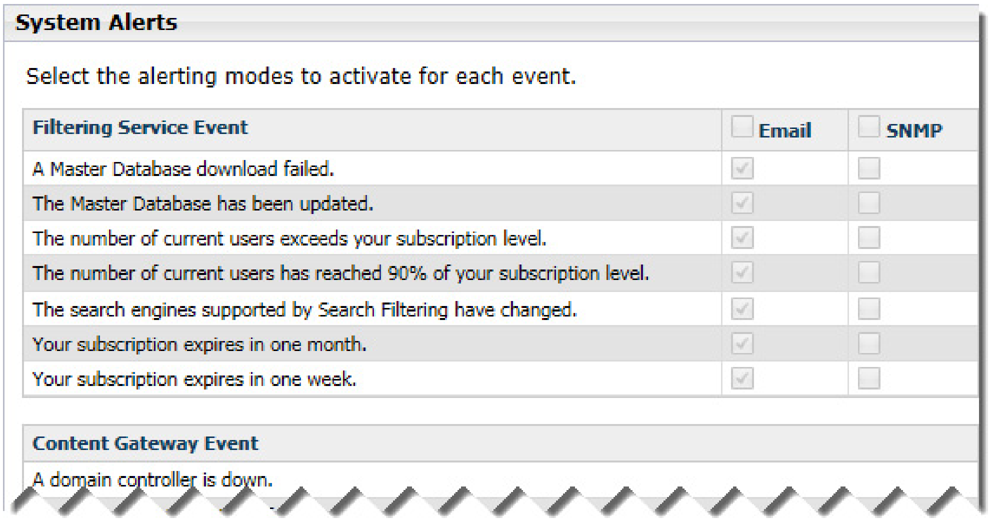
- *Configuring system alerts*, page 10
- *Configuring category usage alerts*, page 11
- *Configuring protocol usage alerts*, page 12
- *Configuring suspicious activity alerts*, page 13

Configuring system alerts

Configure system alerts on the **Settings > Alerts** > **System** page in the Web module of the TRITON Manager. Select a delivery mechanism for each system event that you want to have trigger an alert message.

Note
System events do not have threshold values. A single system event occurrence will trigger a system alert.

TRITON AP-WEB administrators have the option to enable system alerts for both Filtering Service events and Content Gateway events.



System Alerts

Select the alerting modes to activate for each event.

Filtering Service Event	□ Email	□ SNMP
A Master Database download failed.	☑	□
The Master Database has been updated.	☑	□
The number of current users exceeds your subscription level.	☑	□
The number of current users has reached 90% of your subscription level.	☑	□
The search engines supported by Search Filtering have changed.	☑	□
Your subscription expires in one month.	☑	□
Your subscription expires in one week.	☑	□

Content Gateway Event
A domain controller is down.

1. Select an alert delivery method for each event. Delivery methods must be enabled on the **Settings** > **Alerts** > **Enable Alerts** page before they can be selected.

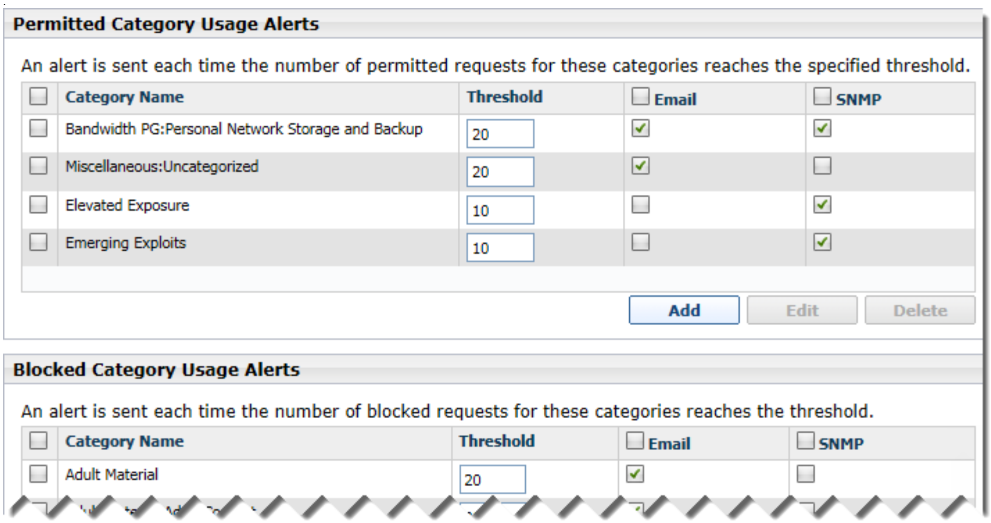
2. Click **OK** to cache your changes. Changes are not implemented until you click **Save and Deploy**.

Configuring category usage alerts

Category usage alerts can be configured to send notifications when Internet activity for particular URL categories reaches a defined threshold. You can define alerts for permitted requests or for blocked requests to the category.

For example, you might want to be alerted each time 50 requests for sites in the Shopping category have been permitted, to help decide whether to place restrictions on that category. Or, you might want to receive an alert each time 100 requests for sites in the Entertainment category have been blocked, to see whether users are adapting to a new Internet use policy.

Use the **Settings > Alerts** > **Category Usage** page to review the default set of alerts, and to add, edit, or remove alerts.



Permitted Category Usage Alerts

An alert is sent each time the number of permitted requests for these categories reaches the specified threshold.

☐	Category Name	Threshold	☐ Email	☐ SNMP
☐	Bandwidth PG:Personal Network Storage and Backup	20	☑	☑
☐	Miscellaneous:Uncategorized	20	☑	☐
☐	Elevated Exposure	10	☐	☑
☐	Emerging Exploits	10	☐	☑

Blocked Category Usage Alerts

An alert is sent each time the number of blocked requests for these categories reaches the threshold.

☐	Category Name	Threshold	☐ Email	☐ SNMP
☐	Adult Material	20	☑	☐

- Review the **Permitted Category Usage Alerts** and **Blocked Category Usage Alerts** lists to see if the default set of alerts is relevant to your organization.
- Click **Add** below the appropriate list to open the Add Category Usage Alerts page (see *Adding category usage alerts*, page 15) and configure alerts for additional categories.
- To change an alert (for example, by updating the threshold or changing the delivery method), mark the check box next to the affected category or categories and click **Edit**.
- Mark the check box next to any categories that you want to remove from the list, then click **Delete**.

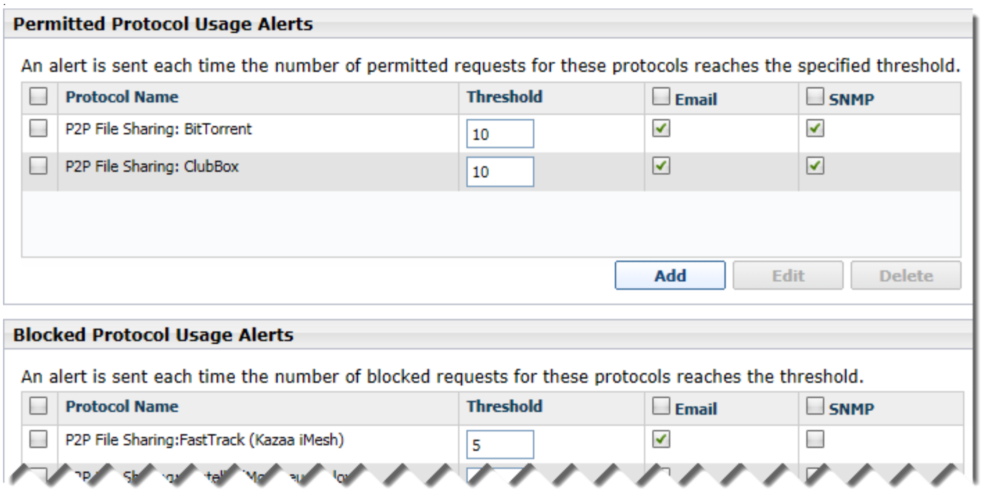
When you are finished making changes to category usage alerts, click **OK** to cache your changes. Changes are not implemented until you click **Save and Deploy**.

Configuring protocol usage alerts

Protocol usage alerts can be configured to send notifications when Internet activity for a particular protocol reaches a defined threshold. You can define alerts for permitted or blocked requests for the selected protocol.

For example, you might want to be alerted each time 50 requests for a particular instant messaging protocol are permitted, to help decide whether to place restrictions on that protocol. Or, you might want to receive an alert each time 100 requests for a particular peer-to-peer file sharing protocol have been blocked, to see whether users are adapting to a new Internet use policy.

Use the **Settings > Alerts** > **Protocol Usage** page to review the default set of alerts, or to add, edit, or delete protocol usage alerts.



Permitted Protocol Usage Alerts

An alert is sent each time the number of permitted requests for these protocols reaches the specified threshold.

□	Protocol Name	Threshold	□ Email	□ SNMP
□	P2P File Sharing: BitTorrent	10	☑	☑
□	P2P File Sharing: ClubBox	10	☑	☑

Blocked Protocol Usage Alerts

An alert is sent each time the number of blocked requests for these protocols reaches the threshold.

□	Protocol Name	Threshold	□ Email	□ SNMP
□	P2P File Sharing:FastTrack (Kazaa iMesh)	5	☑	□

- Review the **Permitted Protocol Usage Alerts** and **Blocked Protocol Usage Alerts** lists to see if the default set of alerts is relevant to your organization.
- Click **Add** below the appropriate list to open the Add Protocol Usage Alerts page (see *Adding protocol usage alerts*, page 16) and configure alerts for additional protocols.
- To change an alert (for example, by updating the threshold or changing the delivery method), mark the check box next to the affected protocol or protocols and click **Edit**.
- Mark the check box next to any protocols that you want to remove from the list, then click **Delete**.

When you are finished making changes to category usage alerts, click **OK** to cache your changes. Changes are not implemented until you click **Save and Deploy**.

Configuring suspicious activity alerts

Suspicious activity alerts can be configured to send notifications when events of a specified severity level reach a defined threshold. You can define alerts for permitted requests and blocked requests at each severity level.

Content Gateway is required to detect critical and high severity alerts. With Web Filter & Security, it is not possible to configure alerting for those severity levels.

TRITON AP-WEB customers who have have enabled Advanced Filte Analysis can enable email or SNMP alerts to be sent when a file submitted for advanced analysis is determined to be malicious.

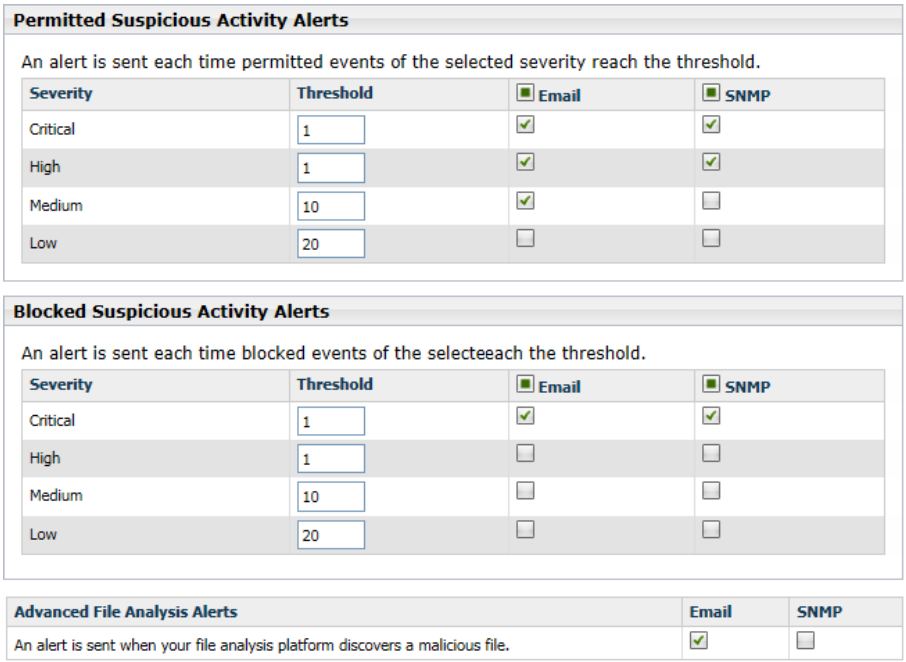
Use the **Settings > Alerts > Suspicious Activity** page to enable, disable, or change alerting configuration for alerts associated with suspicious events in your network.

The page includes 3 tables: **Permitted Suspicious Activity Alerts**, **Blocked Suspicious Activity Alerts**, and **Advanced File Analysis Alerts**.

For suspicious activity alerts, each table shows:

- The **Severity** level (critical, high, medium, low), as determined by the identified threat type.
- The alerting **Threshold**. By default, the threshold for critical and high severity alerts, both permitted and blocked, is **1**.
- One or more notification methods.

For advanced file analysis, you can enable alerting via email, SNMP, or both when an analyzed file is found to be malicious.



Permitted Suspicious Activity Alerts

An alert is sent each time permitted events of the selected severity reach the threshold.

Severity	Threshold	▣ Email	▣ SNMP
Critical	1	☑	☑
High	1	☑	☑
Medium	10	☑	□
Low	20	□	□

Blocked Suspicious Activity Alerts

An alert is sent each time blocked events of the selecteeach the threshold.

Severity	Threshold	▣ Email	▣ SNMP
Critical	1	☑	☑
High	1	□	□
Medium	10	□	□
Low	20	□	□

Advanced File Analysis Alerts	Email	SNMP
An alert is sent when your file analysis platform discovers a malicious file.	☑	□

To configure suspicious activity alerts:

1. For each severity level, enter a number in the **Threshold** field to specify the number of suspicious events that cause an alert to be generated.
2. Select the notification method or methods to use to deliver suspicious activity alerts.

   If you do not want to receive alerts for a severity level, do not select either delivery method.
3. If the Advanced File Analysis option has been enabled, mark the check box or boxes in the Advanced File Analysis Alerts section to cause an email or SNMP alert to be sent when a file sent for analysis is found to be malicious.

   Each check box is enabled only if the corresponding alert type (email or SNMP) is enabled on the Enable Alerts page.

   Note that threats related to advanced file analysis are not included on the Threats dashboard.
4. Click **OK** to cache your changes. Changes are not implemented until you click **Save and Deploy**.

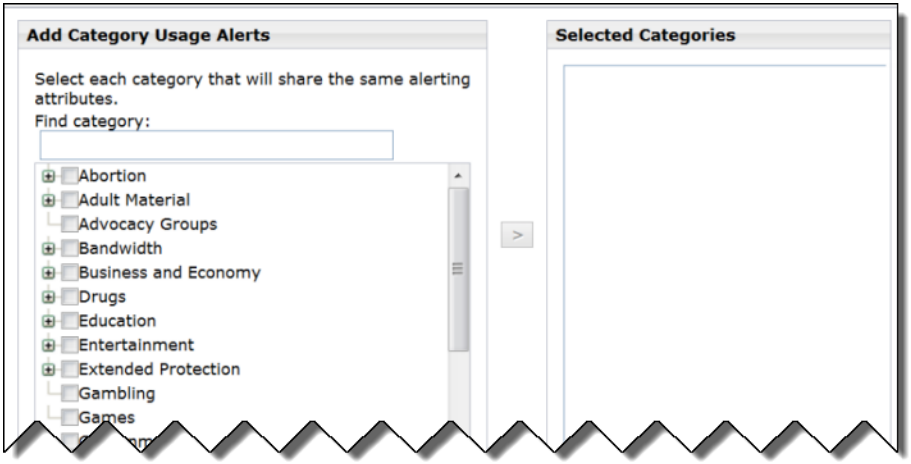
Adding usage alerts

Use the topics in this section sequentially, or jump to the type of alert you want to add.

- *Adding category usage alerts*, page 15
- *Adding protocol usage alerts*, page 16

Adding category usage alerts

The **Add Category Usage Alerts** page appears when you click **Add** on the Category Usage page. Here, you can select new categories for usage alerts, establish the threshold for these alerts, and select the alert methods.



Add Category Usage Alerts

Select each category that will share the same alerting attributes.

Find category:

- ⊞ □ Abortion
- ⊞ □ Adult Material
- □ Advocacy Groups
- ⊞ □ Bandwidth
- ⊞ □ Business and Economy
- ⊞ □ Drugs
- ⊞ □ Education
- ⊞ □ Entertainment
- ⊞ □ Extended Protection
- □ Gambling
- □ Games

Selected Categories

1. Mark the check box beside each category to be added with the same threshold and alert methods.

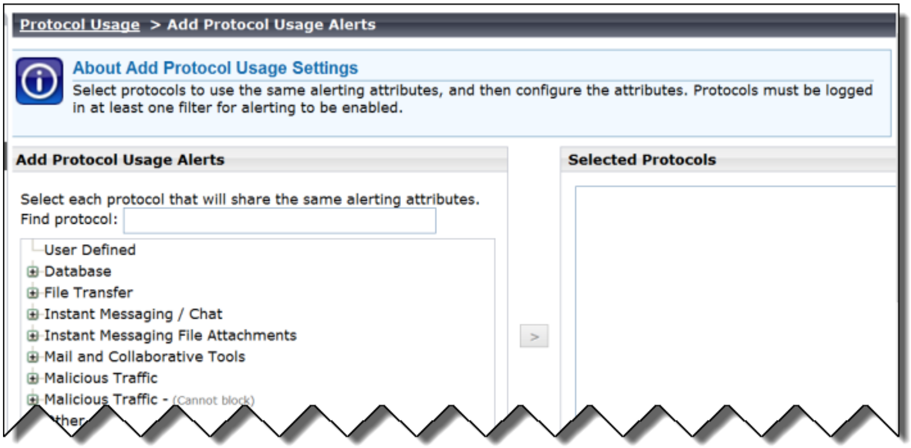
> **Note**
>
> Categories that are not logged cannot be selected for alerting. By default, logging is enabled for all categories. See Configuring how requests are logged for more information about disabling or enabling logging for specific categories.

2. Set the **Threshold** by selecting the number of requests that cause an alert to be generated.
3. Mark the check box for each desired alert method for these categories.

   Only the alert methods that have been enabled on the Alerts page are available for selection.
4. Click **OK** to cache your changes and return to the Category Usage page (see *Content Gateway (software) alarms*, page 17). Changes are not implemented until you click **Save and Deploy**.

Adding protocol usage alerts

Use the **Protocol Usage** > **Add Protocol Usage Alerts** page to select new protocols for usage alerts, establish the threshold for these alerts, and select the alert methods.



Protocol Usage > Add Protocol Usage Alerts

About Add Protocol Usage Settings

Select protocols to use the same alerting attributes, and then configure the attributes. Protocols must be logged in at least one filter for alerting to be enabled.

Add Protocol Usage Alerts

Select each protocol that will share the same alerting attributes.

Find protocol:

- User Defined
- ⊞ Database
- ⊞ File Transfer
- ⊞ Instant Messaging / Chat
- ⊞ Instant Messaging File Attachments
- ⊞ Mail and Collaborative Tools
- ⊞ Malicious Traffic
- ⊞ Malicious Traffic - (Cannot block)
- ther

Selected Protocols

1. Mark the check box beside each protocol to be added with the same threshold and alert methods.

Note

You cannot select a protocol for alerting unless it is configured for logging in one or more protocol filters.

Protocol alerts only reflect usage by clients governed by a protocol filter that logs the protocol. See Editing a protocol filter for more information.

2. Set the **Threshold** by selecting the number of requests that cause an alert to be generated.
3. Select each desired alert method for each alert.

   Only the alert methods that have been enabled on the Enable Alerts page are available for selection.
4. Click **OK** to cache changes and return to the Protocol Usage page. Changes are not implemented until you click **Save and Deploy**.

Content Gateway (software) alarms

In a TRITON AP-WEB deployment with a software-based Content Gateway, Content Gateway signals an alarm for any detected failure condition. You can configure Content Gateway to send email or page support personnel when an alarm occurs.

> **Note**
>
> For information on alarms using Content Gateway, see Working with alarms in the Content Gateway Manager Help.

Configuring SNMP alerting on Content Gateway (software)

Before configuring SNMP to monitor and report on Content Gateway processes, make sure you have installed Net-SNMP and performed a basic SNMP configuration.

1. Add the process names and MAX/MIN process values to the “Process checks” section of snmpd.conf. You also need to add the v2 trap specification.
2. Edit **/etc/snmp/snmpd.conf** and add the following lines in the “Process checks” area:

```
proc content_cop 1 1
proc content_gateway 1 1
proc content_manager 1 1
proc DownloadService 1 1
proc microdasys 2 1
proc microdasysws 1 1
# send v2 traps
trap2sink IP_address_of_SNMP_Manager:162
informsink IP_address_of_SNMP_Manager: 162
rwuser all
agentSecName all
defaultMonitors yes
```

If Filtering Service is also running on the Content Gateway machine and you want to monitor it, add:

```
proc EIMServer 1 1
```

To verify that SNMP Agent is sending trap messages:

1. On the SNMP Agent/Content Gateway machine, start a network packet analyzer and terminate the DownloadService process.
2. In the packet capture data, look for an SNMPv2-Trap message for DownloadService going to the SNMP Manager. The trap message might be similar to:

```
Value: STRING: Too few DownloadService running (# = 0)
```

To verify that SNMP Manager is receiving trap messages:

1. On the SNMP Agent/Content Gateway machine, terminate the DownloadService process. Note that it may take several minutes from the time the trap occurs until the trap is sent to the SNMP Manager.
2. On the SNMP Manager machine, check the SNMP trap log for an entry for DownloadService. The name and location of the log file is specified in the snmptrapd startup command (example provided above). Here is one way to find the message if it is being logged in /var/log/messages:

   ```
   cat /var/log/messages | grep DownloadService
   ```

An entry might look like:

```
Nov 25 15:09:42 localhost snmptrapd[11980]: 10.10.10.10]:
Trap,
DISPAN-EV = STRING , DISMAN-EVENT-MIB::mteHotOID = OID ,
DISMAN-EVENT-IB::prErrMessage.4 = STRING: Too few
DownloadService
running (# = 0)
```

Grep for “snmptrapd” to see all log entries related to snmptrapd.

Use **nc** (netcat) to test basic UDP connectivity between the Agent and the Manager. For example, this command could be run on either side of the connection to test the designated UDP ports.

```
[root]# nc -u -v -z -w2 10.228.85.10 161-162
```

Here, “-u” indicates UPD, “-v” indicates verbose output, “-z” means to scan for listening daemons, and “-w2” indicates to wait 2 seconds before timing out.

Sample results:

```
10.228.85.10: inverse host lookup failed: Unknown host
(UNKNOWN) [10.228.85.10] 161 (snmp) open
```

Integrating with third-party SIEM products

Your web protection software can be configured to pass Internet activity (log) data 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.

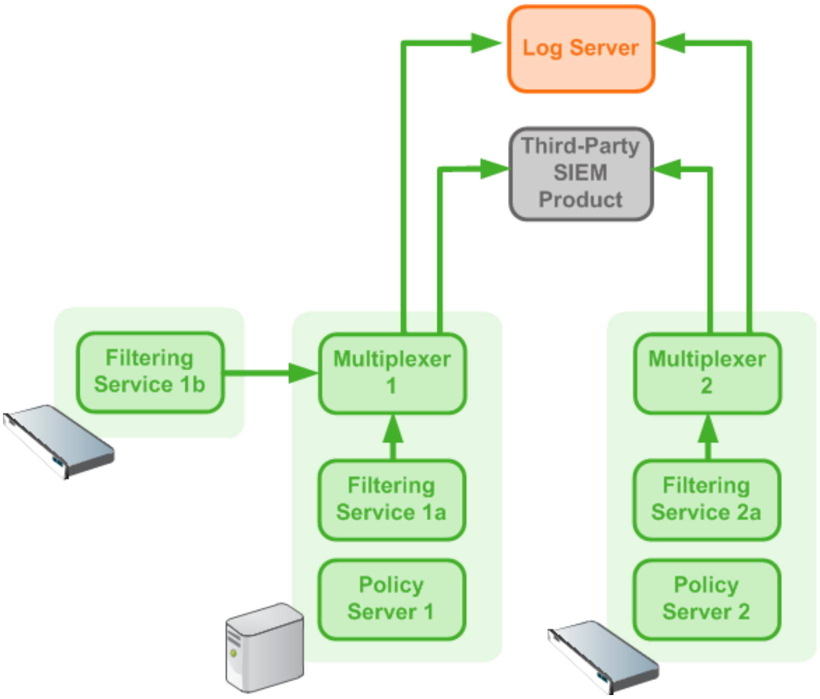
2. Use the **Settings > General > SIEM Integration** page in the Web module of the TRITON Manager to activate the integration and configure the system to send log data to your SIEM product in the format you specify.

   See *Enabling and configuring SIEM integration*, page 20.

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.

The following diagram shows a possible configuration for SIEM integration:



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.

Enabling and configuring SIEM integration

Log on to the Web module of the TRITON Manager to activate and configure SIEM integration.

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

1. Navigate to the **Settings > General > SIEM Integration** page and select **Enable SIEM integration for this Policy Server**.
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 21, 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.

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>
destinationTranslatedPort=%<proxySourcePort> rt=%<time>000
in=%<bytesSent> out=%<bytesReceived> 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>
```

With log data incorporated, the result looks like this:

```
<159>Nov 03 15:34:47 10.203.89.17
CEF:0|Forcepoint|Security|8.3.0|153|Transaction permitted|1|
act=permitted app=http dvc=10.203.89.17 dst=204.15.67.17
dhost=testdatabasewebsense.com dpt=80 src=10.203.89.7
spt=53512 suser=LDAP://10.203.89.254
CN\=Users,DC\=forcepoint,DC\=local/Win1 Tester
destinationTranslatedPort=21528 rt=1478212487000 in=390
out=101198 requestMethod=GET
requestClientApplication=Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.71
Safari/537.36 reason=3-10618-Content.None.Web.RTC
cs1Label=Policy cs1=Super Administrator**Default
cs2Label=DynCat cs2=153 cs3Label=ContentType cs3=text/html;
charset\=utf-8 cn1Label=DispositionCode cn1=1282
cn2Label=ScanDuration cn2=64 request=http://
testdatabasewebsense.com/
```

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.

Code	Description
`%<"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 26)
categoryReasonCode	The reason the URL was assigned to the listed category (see *Category reason code*, page 35)
clientDestinationPort	Destination port of client connection; e.g., 8080 with Content Gateway explicit proxy
clientSourcePort	Source port of the client connection
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)

Key Name	Description
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 32)
dispositionString	Permitted or Blocked, based on the value of dispositionNumber
DSSexternalIncidentID	The TRITON AP-DATA ID number associated with an incident in the forensics repository
DSStimeStamp	The TRITON AP-DATA 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 35)
keyword	Keyword used to block a request. Empty if the request was not blocked by keyword.
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
proxySourcePort	Source port of proxy-server connection
proxyStatusCode	Proxy HTTP response code
refererUrl	URL of the referer site associated with the request
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.

Key Name	Description
scanDuration	If Content Gateway analysis was performed, how long it took (milliseconds)
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 the Web module of the TRITON 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 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.

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
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

ID	Description	Summary
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
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
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

ID	Description	Summary
1556	Zipbomb permitted Real Time	Permitted
1557	Zipbomb blocked Real Time	Blocked

Category reason and file type reference

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
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

ID	Description
5	Multimedia
6	Text
7	Images
8	Documents
9	Threats
10	Rich Internet Applications
11	Unknown