F5® BIG-IQ® Centralized Management: Fraud Protection Service

Version 5.3

Table of Contents

Configuring How BIG-IQ FPS Processes Alerts

Before you start managing alerts

Before you can start using Fraud Protection Service (FPS) to manage alerts, you need to deploy a data collection device (DCD) cluster. This cluster includes the BIG-IQ® Centralized Management devices and Data Collection devices needed to manage and store the alert data generated from your BIG-IP® devices. Additionally, you need to configure your BIG-IP devices to send their FPS alerts to the DCD cluster. These tasks are detailed in the document *Planning and Implementing an F5®BIG-IQ® Centralized Management Deployment*.

Configure a web service

Before you can perform this task, you must be logged in as Admin and, if you plan to use a proxy for WebService traffic, you must have configured a proxy server that your data collection device cluster can access.

Important: *To use a proxy, you must configure a proxy on each device (data collection devices and BIG-IQ® devices) in the cluster. Additionally, the proxy names you specify for each node in the cluster must match exactly.*

You can add or remove a WebService configuration. You need a web service to download new alert transform rules from the SOC. You also need a web service so you can forward received alerts to the Security Operations Center (SOC) so that the SOC can inspect them.

1. At the top of the screen, click **Monitoring**.
2. On the left, expand **EVENTS** > **Fraud Protection Service** > **Configuration**.
3. Click **WebService Configuration**, and then select the web service you want to configure.
   - To configure an existing service, click the name of the service.
   - To configure a new service click **Create**.

   Note: *If you create a web service with a particular set of SOC credentials, and then use that web service in forwarding rules or scheduled alert rule downloads and later delete and recreate it with a different name, then attempts to restore that snapshot will fail. To successfully restore snapshots, you must recreate the web service with the same name.*

   Important: *When you make changes to your web service configuration, allow up to 5 minutes for these changes to propagate to all of your managed FPS devices before you look for the impact of the configuration changes.*
4. For the **WebService Name**, type a name for the web service that you would like to forward alerts to. The Security Operations Center (SOC) is the only option.
5. For **Description**, type a description of the account that you would like to send alerts to.
6. For **WebService URI**, use the default value supplied by the BIG-IQ.
7. For **Remote Account ID**, type the remote account ID provided by the SOC.
8. For **SOC User**, type the user name provided by the SOC.
9. For **SOC Password**, type the password provided by the SOC.

10. If you want the alert traffic for this web service to route through a proxy, select **Use Proxy**, and then select the proxy you want to use.
11. For **Test SOC Connection**, click the **Test** button to make sure the alert goes through.

Important: *A successful test confirms only that the alert was successfully sent (or, if you specified a proxy, that the alert reached the proxy server). You should confirm with the recipient that the test message is received.*

12. Click **Save & Close**

You have configured a web service that can down load alert rules from the SOC and forward alerts to the SOC.

Create an alert transform rule

Before you can perform this task, you must be logged in as Admin.

An alert transform rule is used to modify alerts matching a set of criteria. It might take a few minutes after alert transform rules are added before they take effect.

When you create an alert transform rule, you create a set of criteria that tells your system what to do with incoming alerts. An example of this would be if the system finds a particular string in the alert query when there is generic malware present. If the alert matches all of the criteria that you set up, then the system should change the alert severity, details, recommendation, and status. You can use alert transform rules to ignore a type of alert that is harmless, or you can use alert transform rules to change the alert severity to a high percentage and change the alert status to monitor.

1. At the top of the screen, click **Monitoring**.
2. On the left, expand **EVENTS** > **Fraud Protection Service** > **Configuration**.
3. Click **Alert Transform Rules**.
4. To add an alert transform rule, click the **Create** button.
   The New Alert Transform Rule screen opens.
5. Complete the New Alert Transform Rule screen:
   a) In **Transform Rule Name**, type a name for the alert rule.
   b) In **Description**, type a description of the alert rule.
   c) In **Find**, type the string that you would like to search for.
   d) For the **Where** setting, use the arrow key to move a location that you would like to search to the **Selected** column.
      The alerts you specify will be searched for instances of the **Find** string specified in the previous step.
   e) For the **When** setting, add an alert category to the **Selected** column.
   f) For the **Accounts** setting, retain the default, **All Accounts**, or clear that check box, and select a specific fraud protection account.
      The Alert Transform Rule then only acts on the alerts that the account is set to receive.
   g) For **Alert Severity**, add a severity number to the alert.
      By default, most alerts are given a severity number of 50.
   h) In **Alert Details**, type in details about the alert.
   i) In **Alert Recommendation**, type in an alert recommendations.
   j) For **Alert Status**, select a status for the alert.
   k) Select the **Advanced** check box if you want to extract the user name from the alert using regular expression.
6. If you select the **Use regex to obfuscate the user name from selected fields** check box, there are two more settings to do.

a) In the **User Regular Expression** field, type a regular expression.

   If the alert contains a string that matches the regular expression you specified, BIG-IQ replaces that string with `username`. This hides the information in the alert.

b) In the **Match User Regular Expression on** setting, move the alert fields that you want to search and replace from the **Available** list to the **Selected** list.
   The system searches the selected fields for strings that match the specified regular expression and replaces them with `username`.

7. Click **Save & Close**.

Creating a schedule to import transform rules

Before you can create a new download schedule, you must configure a web service.

You can set up a schedule to import transform rules from the Security Operations Center (SOC). You can start imports immediately, or repeat them on a daily, weekly, or monthly basis. You can only create one repeating schedule. However, you can create a new schedule that will run immediately.

1. At the top of the screen, click **Monitoring**.
2. On the left, expand **EVENTS** > **Fraud Protection Service** > **Configuration**, and then click **Transform Rule Import Schedule**.
3. Click the **Create** button.
   The New FPS Download Schedule screen opens.
4. Type a **Name** and **Description** for the transform rule import schedule.
5. From the **WebService** list, select the service you want to use.
6. For **Import Alert Rules Frequency**, select how often you want the transform rules to import.
7. For **Start Date**, specify the date and time that you want the import to start.
8. For **End Date**, either select **No End Date**, or specify the date and time that you want the import to stop.
9. Click **Save & Close**

You have now created an import schedule for alert transform rules.

Importing a CSV file with alert rules

Importing alert transform rules from a CSV file is helpful if you do not want to schedule a download of the alert transform rules from the Security Operations Center (SOC) over the Internet.

You can save alert rules (called *signatures*) from the SOC into a CSV file, then use the steps in this task to import the CSV file into FPS.

1. At the top of the screen, click **Monitoring**.
2. On the left, expand **EVENTS** > **Fraud Protection Service** > **Configuration**, and then click **Alert Transform Rules**.
3. Click the **Import** button.
   A popup screen opens.
4. Click **Choose File**, and then choose a CVS file to import.
5. Select a target account.
6. Click **Import**.
   The imported alert transform rule is applied to the types of alerts the account is configured to receive.

Modify alert forwarding rules

Before you can perform this task, you must be logged in as Admin, and if you plan to use a proxy to forward custom alerts, you must have configured a proxy server that your Data Collection Device cluster can access.

You can add, clone, or remove alert forwarding rules. You can forward alerts to a web service, an email address, a sys-log, or to a custom WebService location.

1. At the top of the screen, click **Monitoring**.
2. On the left, expand **EVENTS** > **Fraud Protection Service** > **Configuration**, and then click **Alert Forwarding Rules**.
3. On the Alert Forwarding Rules screen. select an action as appropriate:
   - To view details for a forwarding rule, click an alert name.
   - To clone an alert forward rule, select the check box for an alert and click **Clone**.
   - To remove an alert forward rule, select the check box for an alert and click **Delete**.
   - To add an alert forwarding rule, click **Create**.
4. On the New Alert Forwarding Rules screen, fill in the settings as needed:
   a) For **Forwarding Rule Name**, type a name for the alert rule.
   b) For **Description**, type a description of the alert rule.
   c) For **Status**, select the **Enabled** check box to forward alerts.
5. On the left, click **Alerts Matching**, and fill in the settings as needed:
   a) For **Alert Severity Equal OR Greater Than**, select the alert severity level from the list.
   b) For **Alert Categories**, move an alert category from the **Available** list to the **Selected** list.
   c) For **Alert Status**, select a status for the alert, and move it from the **Available** list to the **Selected** list.
   d) To forward only alerts that include a user name, for **Username**, select **Must be Present**.
   Enabling this setting significantly reduces the volume of alerts that FPS forwards.
   e) For **Accounts**, use the default **All Accounts**, or select a specific fraud protection account and move it to the **Selected** column. The alert forwarding rule will then only act on the alerts that the account is set to receive.
   f) .
6. On the left, click **Notification Targets** and fill in as appropriate:
   a) Select the **Enabled** check box for the destination to which you want to forward alerts.

   Note: *Depending on which forwarding method you choose, you can use variables to define the content of the alerts that you forward.*

   - Select **WebService** to send alert notifications to the F5 Security Operations Center (SOC) dashboard through the cloud web service.
     - You must configure WebService Config in Fraud Protection Service before you can select this option.
     - When you select **Webservice**, the screen opens the WebService area where you can specify additional options and variables.
     - For additional detail on how to use the fields in the WebService area, refer to *WebService method forwarding detail*.
   - Select **Email** to send notifications to an email address.

- You must configure the DNS and SMTP server on your data collection devices to use this option.
- When you select **Email**, the screen opens the Email area where you can specify additional fields and variables.
- For additional detail on how to use the fields in the Email area, refer to *Email forwarding method detail*.

- Select **Syslog** to send alert notifications to a sys-log server.
  - When you select **Syslog**, the screen opens the Syslog area where you can specify additional fields and variables.
  - For additional detail on how to use the fields in the Syslog area, refer to *Syslog forwarding method detail*.
- Select **Custom** to send custom alert notifications to a third party web service.
  - When you select **Custom**, the screen opens the Custom area where you can specify additional fields and variables.
  - For additional detail on the Custom area, and how to use the fields in it, refer to *Custom forwarding method detail*.

7. Click **Save & Close**.

WebService forwarding method detail

When you use the WebService forwarding method, you use the web service tab to define how the alert is sent.

1. For **WebService**, select the web service to which you want the alert to be sent.
2. Specify the variables that you want to have included in the alert by using the arrow button to move them from the **Available** list to the **Selected** list.

   For a list of forwarding method variables that you can use, refer to *Supported Forwarding Method variables*.
3. Click **Save & Close**.

Email forwarding method detail

When you use the Email forwarding method, you use the Email tab to define how the alert is sent.

1. For **Sender Name**, the screen specifies the name of the email sender (F5 Fraud Protection Service).
2. For **Sender Email Address**, type the email address from which you want the alert notifications forwarded.
3. For **Email Recipient(s)**, type the email address to which you want the alert notifications forwarded.
4. To run a test of the email addresses you specified above, click **Test**.

   Important: *A successful test confirms only that the alert was successfully sent. You should confirm with the recipient that the test message is received.*
5. For **Email Subject**, you can either use the default parameters to specify the alert email subject, or create your own using the supported parameters.

   For a list of forwarding method variables that you can use, refer to *Supported Forwarding Method variables*.
6. For **Mail Template**, you can add or subtract from the default list of parameters.

   Parameters listed here are included in the forwarded alert.
7. When you finish configuring the alert sending method, click **Save & Close**.

Syslog forwarding method detail

When you use the Syslog forwarding method, you use the Syslog tab to define how the alert is sent.

1. For **Syslog Facility**, type the facility number to which you want the alert notifications to be forwarded.
2. For **Syslog Severity**, select the severity level that you want to be appended to all forwarded alert notifications.

   The severity level you select here is added to all forwarded alerts. This level is unrelated to the severity level number assigned independently to each alert.
3. For **Syslog Server**, type the IP address of the server to which you want the alerts to be forwarded.
4. For **Syslog Port**, type the port number to which you want the alerts to be forwarded.
5. For **Syslog Protocol**, select the protocol that the target syslog server uses to accept forwarded alerts.
6. To run a test of the specified settings, click **Test**.

   Important: *A successful test confirms only that the alert was successfully sent. You should confirm with the recipient that the test message is received.*
7. For **Syslog Template**, you can add or subtract from the default list of parameters.

   Parameters listed here are included in the forwarded alert. For a list of forwarding method variables that you can use, refer to *Supported Forwarding Method variables*.
8. When you finish configuring the alert sending method, click **Save & Close**.

Custom forwarding method detail

Before you can perform this task, if you plan to use a proxy to forward custom alerts, you must have configured a proxy server that your data collection device cluster can access.

When you are configuring an alert forwarding rule and select the Custom method, you use the Custom tab to define the details of how the alert is sent. This alert type specifies a number of parameters that the alert receiving entity has specified as requirements of the service they use to listen for forwarded alerts. You specify the values for these parameters so that the forwarded alerts satisfy the requirements of the alert receiving entity.

1. If the alert recipient uses a service that requires an alert token, select the check box for **Uses Token**.

   The screen displays additional settings.
   a) For **WS Token Timeout**, type the number of seconds that the alert recipient specifies for forwarded alert tokens.
   b) For **WS Token URL**, type the IP address that the alert recipient specifies for forwarded alert tokens.
   c) For **WS Token Method**, select the REST API method that the alert recipient specifies for forwarded alert tokens.
   d) For **WS Token Headers**, type the required request header information specified by the alert recipient for forwarded alert token headers.
   e) For **WS Token Request**, type the required request body information specified by the alert recipient for forwarded alert tokens.
   f) For **WS Token Response**, type the required request response information specified by the alert recipient for forwarded alert responses.
2. If you want the alert traffic for this custom rule to route through a proxy, select **Use Proxy**, and then select the proxy you want to use.
3. For **WS Alert URL**, type the IP address specified by the alert recipient for forwarded alert responses.

4. For **WS Alert Method**, select the REST API method that the alert recipient specifies for forwarded alerts.
5. To run a test of the specified settings, click **Test**.

   Important: *A successful test confirms only that the alert was successfully sent (or, if you specified a proxy, that the alert reached the proxy server). You should confirm with the recipient that the test message is received.*

6. For **WS Alert Headers**, type the required alert header information specified by the alert recipient for forwarded alert headers.
7. For **WS Alert Request**, type in the parameters that you want to be included in the forwarded alerts.

   Parameters listed here are included in the forwarded alert. For a list of forwarding method variables that you can use, refer to *Supported Forwarding Method variables*.
8. When you finish configuring the alert sending method, click **Save & Close**.

Supported forwarding method variables

There are a number of forwarding method variables that you can use when you create an alert rule.

Variable Name	Alert Field
Account ID	{accountid}
Account Name	{account}
Alert Date (dd.mm.yyyy hh:mm)	{date}
Alert Date (yyyy-mm-dd hh:mm:ss)	{datefull}
Alert Date (Unix Timestamp)	{unixdate}
Alert Domain	{domain}
Alert Name	{name}
Alert Severity	{severity}
Alert Query	{query}
Alert Recommendation	{recommendation}
Alert Status (Numeric)	{statusid}
Alert Status (Textual)	{status}
Alert Type	{type}
Alert URL	{url}
Alert GUID	{guid}
Alert Referer	{referer}
Alert Details	{details}
Application Cookies	{session_data}
Authentication Token (For CustomWS Notifications)	{token}
Client Host Name	{hostname}
Client IP	{ip}
Client Language	{language}
Client Proxy Host Name	{proxyname}

Variable Name	Alert Field
Client Proxy IP	{proxy}
Client Username	{user}
Client User Agent	{agent}
Client Country	{geoip_country}
Client City	{geoip_city}
Client Device ID	{device_id}
Client Device Parameters	{device_params}
Full Alert HTML Data	{ht_data}
MD5 of Full Alert HTML	{ht}
MD5 of Minimal Alert HTML	{min}
Minimal Alert HTML Data	{min_data}

Add a fraud protection account

You create Fraud Protection accounts in order to receive alerts related to alert identifiers that have been configured on the BIG-IP® system. You can then assign BIG-IQ® users to limit their view of alerts and rules.

Accounts are used to filter alerts, and to transform rules and forwarding rules based on the alert ID configured on the BIG-IP system. Each FPS account has an account ID, and all alerts have an account ID field. You can view only the alerts whose account ID field matches an FPS account ID to which your user login has been assigned access.

The account name you give is displayed in place of the alert ID. If you configure an account, set the default view for each user that you assign to the account. Alert transform rules and forwarding rules that have an account are applied to alerts with the matching alert ID. If no accounts are assigned, then all alerts are considered.

1. At the top of the screen, click **Monitoring**.
2. On the left, expand **EVENTS** > **Fraud Protection Service** > **Configuration**, and then click **WebService Configuration**.
3. Click **Create**.
   The New FPS WebService Configuration screen opens.
4. Fill in as appropriate:

Option	Description
WebService Name	Type a name for the account that you would like to send alerts to (for example, `MortgageDept`).
Description	Type a description of the account that you would like to send alerts to.
WebService URI	This value is always filled in by default. The only reason to change this is if you want to forward to another legacy dashboard.
Remote Account ID	Type the remote account ID provided to you by the SOC.
SOC User	Type the user name provided to you by the SOC By default, the administrator is selected to look at the account.

Option	Description
	Note: *To create a user, go to* ***System Management*** > ***User Management*** > ***Users*** *and click* ***Add****. Be sure to give the user a user role of Fraud Protection Manager or Fraud Protection View*
	.
SOC Password	Type the password provided to you by the SOC.
Proxy	To route the alert traffic for this web service through a proxy, select **Use Proxy**, and then select the proxy you want to use.
Test SOC Connection	To test the SOC connection, click the Test button to confirm that your settings are correct.
	Important: *A successful test confirms only that a test alert was successfully sent (or, if you specified a proxy, that the alert reached the proxy server). You should confirm with the recipient that the test message is received.*

5. Click **Save & Close**.

You now have a fraud protection account that can manage the alerts that you specify.

Managing BIG-IQ Fraud Protection Service

Fraud Protection Service overview

BIG-IQ® Fraud Protection Service (FPS) sends alerts to users whenever they are victims of malware or phishing attacks. BIG-IQ filters all alerts into different types and displays them for you to monitor. FPS has the ability to create rules to modify alerts, rules for forwarding alerts, or download rules from the Security Operations Center (SOC). Types of alerts include:

Uninspected Alerts

This list contains all alert types that have a status of new.

Monitored Alerts

This list contains all monitored alert types.

Note: *If you have configured fraud protection accounts, then you can view only the alerts that have been specified for your account to view.*

Phishing Alerts

Phishing alerts include phishing user, copied pages, and user defined phishing. These alerts are created when a phishing victim enters user credentials onto a phishing web site, or when a phishing site has been detected by JavaScript. The user name that appears in the alert is the user name that is entered into the phishing site.

Malware Alerts

Malware alerts are separated into generic malware, targeted malware, external scripts, page modification, and user defined malware. The Malware Detection component thus enables the organization to take the necessary steps to mitigate the risks of the attack in real time. This component helps the organization to keep track of its affected users and reveal malicious money transaction attempts.

Suspicious Transactions

Suspicious Transactions include browser automation, remote access tools, transaction modification, and user defined. Suspicious transactions prevent automatic requests to the application's server by confirming that the request was made by a human and not issued automatically. Automatic requests can be issued by a Trojan horse attack injecting a malicious JavaScript code to the user's browser in order to perform an automatic money transfer to the attacker's account, or by random bots attempting to automatically scrape data from the application automation.

Suspicious Logins

Suspicious logins include stolen credentials and user inspection. These alerts provide protection against Trojan horse attacks, providing an encryption for the information at the application layer on the client side. This ensures that the information that is exposed to the Trojan horse attack will be encrypted. The encryption is conducted on the client side, using a public key generated by the web server and provided uniquely per session. When the encrypted information is received by the web server, it is decrypted using a private key that is kept on the server side.

Mobile

Mobile alerts integrate with the applications of financial service providers, improving protection against the aforementioned threats and provides alerts received on possible attacks. Mobile alerts neutralizes local threats found on customers’ mobile devices, without altering the user experience.

These alerts are created when the system detects an infected mobile device. Alert types that are included in this category are Mobile Malware, Mobile Man-in-the-middle (MITM), Mobile Security, and User Defined. Prevents phishing, Trojan horse attacks, and pharming attacks on mobile devices in real time, through detection, prevention, and application-level encryption.

Validation Errors

Validation error alerts are created when the expected cookie is missing or corrupted. Validation errors include transaction errors, encryption errors, missing components, and mobile errors.

Unfiltered Alerts

Unfiltered alerts are unfiltered views of all alerts except those that have the status of Ignore.

Saved Filters

Saved filters is a list of custom filters that you create and save. These are unique to each user. Saved filters are helpful if you would like to create your own view of alerts. If you are trying to track down a specific type of attack, you can save a unique filter to repeatedly check on a specific type of alert. The BIG-IQ® Fraud Protection Service provides a rich set of querying features which allow you to quickly and efficiently locate alerts that you are interested in.

FPS Alerts overview

There are a number of things you can do to specify the response to different kinds of alert types.

Each alert type has its own user interface, but the controls used to edit the rules that govern the response to these alerts are very similar.

Most alert types are organized into groups. On any list screen, you can click the little black triangle to expand the list.

- To access the Filter Alerts screen, click the **Filter** button at the top left of the screen. On the Filter Alerts screen you can view the existing query that defines the current alert rule. You can specify additional detail to further refine the query or create a new custom query.
- To refresh the list of alerts on the screen, click **Refresh**.
- To create a rule based on an alert, select the check box of the alert you want to use as the basis for the rule, and click **Create Rule**.
- To filter the list of alerts so that only alerts generated during one session are displayed, select the check box of the alert you are interested in, and click **Filter Related**.
- To export one or more alerts files to a CSV file that you can edit or inspect, click **More**, and then select **Export**.
- To change the status for an alert, select the check box for that alert, click **More**, and then select **Change Status**.

Note: *If all the check boxes are selected in a list, you can choose to either change the status for all of the alerts that are in view, or change the status for all of the alerts that match the query.*

- To remove an alert, select the check box for that alert, click **More**, and then select **Delete**.

Note: *If all the check boxes are selected in a list, you can choose to either remove all of the alerts that are in view, or remove all of the alerts that match the query.*

When you select a single alert, two changes take place:

- A **Filter Related** button becomes active. Click this button to view only alerts that have the same session global unique identifier (GUID) as the selected alert.
- A preview pane opens to show you details about the selected alert.

To use the Filter field in the right corner:

1. From the **Filter** control, select the type of match (**Contains**, or **Exact**) that you want to use.
2. In the **Filter** field, type the filter criteria you want to use, and press Enter.
3. A **Filtered by** field displays the alert criteria you applied, and the screen displays only alerts that match that criteria.
4. To see the rest of the alerts again, click the **X** to clear your filtered by alert criteria.

To display additional information about a specific alert, select the check box that corresponds to it. A preview pane opens.

When you select a single alert, a preview pane opens to show you details about the selected alert. The tabs that display depend on what data is available for the selected alert.

Details	This tab displays details about the URL that triggered the alert. • **Alert URL**: The URL of the site that was in use when the alert was sent. • **Alert Status**: The current status of the alert. • **Alert Severity**: The severity of the alert. By default, new alerts have a 50% severity, unless the alert matches an existing rule. • **Referrer**: The URL of the site that was visited just before the Alert URL was visited. • **User Agent**: User browser type and operating system. • **Language**: User browser and operating system language. • **Domain**: The name of the domain that triggered the alert. • **User**: The name of the dashboard user who performed an action that triggered the alert. • **Alert Details**: The display varies depending on the type of alert. • **Device ID**: The ID of the device that triggered the alert. • **Matched URL**: The portion of the URL that matched and triggered the alert.
HTML	This tab is visible only if the alert includes these details. It shows you the raw HTML that was included in the alert.
Data	This tab is visible only if the alert includes these details. It shows you the raw HTML and other data that was extracted for further diagnosis of the alert condition. If the alert type is External Sources or Trojan Validator, this tab displays the malware detection alerts. If the alert type is External Sources, the alert type is 6 and the alert component is 5 and the value contains the forbidden added HTML element and its contents in escaped base64 format. If the alert type is Trojan Validator, the alert type is 6 and the alert component is 3. The value contains the bait signatures in escaped base64 format.
About	This tab gives a brief summary of details about the alert type.
Advanced	This tab displays the exact query that was sent in the alert. This information can be used to debug alerts and understand the cause of the alert. It is helpful for the Security Operations Center (SOC).

Add an advanced query filter

Before you can perform this task, you must be logged in as Admin.

BIG-IQ® Fraud Protection Service provides a rich set of querying features that allow you to quickly and efficiently locate the alerts that you are interested in.

When you select the **Filter** button from an alerts screen, or when you select add/edit from the Saved Filters screen, you see a dialog box that allows you to specify what alerts you want to filter for.

The screen provides the most common filters in list and text boxes, but you can specify additional filters. The filters that display initially depend on the type of alert you are configuring.

1. At the top of the screen, click **Monitoring**.
2. On the left, expand **EVENTS** > **Fraud Protection Service**, and then click **Alerts**.
3. On the left, select the type of alert for which you want to specify advanced filter alerts.
   The Filter Alerts screen opens.
4. To add filter details, click the **Filter** button.
   The Filter Alerts popup screen opens.
5. Complete the Filter Alerts screen:
   a) For **Filter Name**, if you want to save this query for future use, type a name for this set of query details.
   b) For **Category**, select one or more categories to specify the type of alert.
   c) For **Date**, you can specify **last 2 weeks**, **last month**, **last three months**, **last six months**, or select a custom date range. If you only specify a start date, BIG-IQ selects all alerts from the start date to the current date.
   d) For **Alert Severity**, type the minimum and maximum severity of the alerts that you want to match.
   If the maximum is not entered, the default is 100.
   e) For **Status**, if you choose one of the options, only alerts of that status are shown.
   If multiple status are needed, then specify them in the **Additional Query Parameter** field (near the bottom of the screen).
   f) For **Location**, select the geographic location on which you want to filter.
   g) For **User**, type the name of the user that triggered the alert.
   You can use a wildcard `*`. For example `p*` matches all users whose name starts with the letter P.
   h) For **Domain**, type the domain of the site that was in use when the alert was sent.
   You can use a wildcard `*`. For example `p*` matches all host domains whose name starts with the letter P.
   You can also type the domain of the phishing site or the host of the site that was detected.
   i) For **Client IP**, type the IP address of the victim of the alert in which you are interested.
   j) For **Alert URL**, type the source URL that caused the alert.
   k) For **Guid**, type the unique identifier for the set of alerts that make up one session.
   To find the guid, select the alert, and then click the **Advanced** tab. Under Query Parameters, look for **fpm_guid**.
   l) For **Additional Query Parameters**, if what you want cannot be specified with the quick selections, you can use the query language.
   The format for these query parameters is: `key1: value1 key2: value2 (key3:value3 OR key4)`. **OR** is implied if it is not supplied.

   Important: *The query string syntax is parsed into a series of terms and operators. A term can be a single word or a phrase. Note that phrases must be surrounded by double quotes. In general the query string syntax observes the Lucene query syntax. The following characters are reserved and cannot be used in a query:*

```
+ - = && || > < ! ( ) { } [ ] ^ " ~ * ? : \ /
```

   For example: `(alertType:6 OR alertType:8) language:*us`

   For a list of advanced query parameters refer to *Advanced Query Parameter Syntax*.
6. Click **Save**.

Additional Query Parameters

If what you want can not be specified with the quick selections, you can use the query language. Available query parameters are listed here.

Parameter Name	What it means
category	The type of alert. Select one or more categories. If none are selected, the search will apply to all categories.
alertUrl	Type the source URL that caused the alert.
alertType	A specific type of alert within a category.
device	A specific variation within a type of alert.
component	A specific variation within a type of alert.
domain	Type the domain of the site that was in use when the alert was sent. You can also type the domain of the phishing site, or the host of the site that was detected.
clientIp	Type the IP address of the victim of the alert that you are interested in.
details	This parameter can contain many different values depending on the type of alert.
device	The device ID of the machine generating the alert (typically a mobile device).
alertId	A unique ID configured on the BIG-IP® device for each virtual IP address.
severity	Specifies the ID of the customer in the dashboard. When configuring a mobile security anti-fraud profile, you must ensure that the value you assign here for **Alert Identifier** is the same value used for VMobile's customer parameter in the init iOS method and Android constructor.
status	The status assigned by the SOC.
userAgent	The user browser type and operating system.
continent	The continent code.
country	The country code.
region	The region code.
language	User browser and OS language.
referer	The URL of the site that was visited just before the alert URL was visited.
uri	The URI to which the client requested to go.
user	Type the name of the user that triggered the alert.
guid	Type the unique identifier for the set of alerts that make up one session.
rule	As set by the user in the rule.
alertDetails	As set by the user in the rule.
recommendation	As set by the user in the rule.
date	You can specify **last 2 weeks**, **last month**, **last three months**, **last six months** or select a custom date range. If you only specify a start date, BIG-IQ® selects all alerts from the start date to the current date.
cookie	Cookie information associated with this alert.
dateType	Type the number of days back from which to start the query.

Create and save a custom filter

Before you can perform this task, you must be logged in as Admin.

You can create and save custom filters. This process is very similar to creating an advanced query filter, except you start with no default set of filters.

1. At the top of the screen, click **Monitoring**.
2. On the left, expand **EVENTS** > **Fraud Protection Service**, and then click **Alerts**.
3. Click **Saved Filters**.
   The Saved Filters screen opens.
4. Click **Create** to create a new filter.
   The New Saved Filter screen opens.
5. In the **Filter Name** field, type a name for the alert filter.
6. For **Category**, select the type of alert from the list.
7. For the **Date**, select from the options in the list.

   The options are, **Last 2 weeks**, **Last month**, **Last three months**, **Last six months**, or a **Custom** date range. If you only specify a start date, the system selects all alerts from the start date to the current date.
8. For **Alert Severity**, select the severity level of the alert. The **From** and **To** fields include numbers ranging from 1 to 100.
9. For **Status**, select the status from the list. You can pick one of the options, and only alerts of that status are shown. If you need more than one status, you can specify that in the **Additional Query parameter** field.
10. For **Location**, select the location from the list.
11. For **User**, type the user name.
12. In the **Domain** field, type the domain.

    The system only matches on exact match, and is case sensitive.
13. In the **Client IP** field, type the client IP address.
14. In the **Alert URL** field, type the alert URL.
15. In the **Guid** field, type the unique identifier.
16. If what you want can't be specified with the quick selections, you can use the query language in the **Additional Query Parameter** setting. or example:

    This is the format: `key1: value1 key2: value2 (key3:value3 OR key4)`. For example:

```
(alertType:6 OR alertType:8)
                                after Feb 02 2015 07:56:26 before Feb 10 2015 23:56:26
                                host:versafe.com alertId:ddd
                                severityGE:2 severityLE:94
                                status:new rule:rule1
```

17. Click **Save & Close**

You have now created and saved alert filters.

Change an alert status

Before you can perform this task, you must be logged in as Admin.

You can change the status of alerts in Fraud Protection Service. An alert status change is performed by an admin, security manager, or FPS manager to indicate that an alert has been inspected, and what the status of the alert is.

1. At the top of the screen, click **Monitoring**.
2. On the left, expand **EVENTS** > **Fraud Protection Service**, and then click **Alerts**.
3. Click **Unfiltered Alerts**.
4. Select the check box of the alert type for which you want to change the status.
5. Click the **More** button, and then select **Change Status**.
6. Under **Select the new status to set on alerts**, select the new status from the list.

Option	Description
New	The SOC team has not yet handled this item.
Open	The SOC team is currently handling this item.
Handle	The SOC team has finished handling this item.
Monitor	The SOC team has monitored this item.
Close	The SOC team has closed this item.
Ignore	The SOC team is familiar with the alert and has decided that it is not malicious (the alert is a false positive). Ignored alerts can be seen only when using filters.
Official	The SOC team has determined that this specific URL is legitimate.

7. Click **Change Selected**.
   Changing alert statuses displays while your request is processes.
8. Click **Close** when the alert status change completes.

Remove an alert

Before you can perform this task, you must be logged in as Admin.

You can delete the alerts that you have created in FPS.

1. At the top of the screen, click **Monitoring**.
2. On the left, expand **EVENTS** > **Fraud Protection Service**, and then click **Alerts**.
3. On the left, select the alert type that you want to delete.
4. Select the specific alert you want to delete, then click the **More** button, and select **Remove**.

Note: *If the header check box is selected, when you click* ***Remove*** *you are prompted to select whether you want to remove all of the alerts that are currently selected (only 50 to 75 at a time are selected at a time due to memory constraints), or all the alerts that match the query.*

The specified alerts are deleted.

Export an alert

Before you can perform this task, you must be logged in as Admin.

You can export the alerts that you have created in FPS.

1. At the top of the screen, click **Monitoring**.
2. On the left, expand **EVENTS** > **Fraud Protection Service**, and then click **Alerts**.

3. On the left, select the alert type that you want to export.
4. Select the alert you wish to export, then click the **More** button, and select **Export**.

The specified alerts are exported to a `.csv` file in your Downloads folder.

Legal Notices

Legal notices

Publication Date

This document was published on July 6, 2017.

Publication Number

MAN-0619-03

Copyright

Trademarks

For a current list of F5 trademarks and service marks, see *http://www.f5.com/about/guidelines-policies/trademarks*.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at: *https://f5.com/about-us/policies/patents*.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Index