BIG-IP® DataSafe™ Configuration

Version 13.1

Table of Contents

Adding BIG-IP DataSafe to the BIG-IP System

Overview: Adding BIG-IP DataSafe to the BIG-IP system

F5® Networks security provides BIG-IP® DataSafe™, which protects users from Trojan attacks by encrypting data at the application layer on the client-side. Encryption is performed 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. Users can view alerts on potential encryption attacks in the Data Protection log in the BIG-IP system or in a remote Syslog Server if you choose to configure one for receiving alerts.

In order to use BIG-IP DataSafe in the BIG-IP system, you need to provision Fraud Protection Service (FPS) for BIG-IP DataSafe, create a BIG-IP DataSafe profile, create a virtual server, and associate the profile with that virtual server.

Note: *In most cases, the virtual server that you will create for your profile will be an SSL virtual server.*

Task Summary

Provisioning Fraud Protection Service for BIG-IP DataSafe using the Configuration utility
Provisioning Fraud Protection Service for BIG-IP DataSafe using tmsh
Creating a node for a remote syslog server
Creating a pool for a remote syslog server
Creating a web application server node
Creating a web application pool
Creating a remote high-speed log destination
Creating a log publisher
Creating an initial BIG-IP DataSafe profile
Creating a custom HTTP profile
Creating a virtual server
Associating a profile with a virtual server

Provisioning Fraud Protection Service for BIG-IP DataSafe using the Configuration utility

You must provision Fraud Protection Service (FPS) for BIG-IP DataSafe before performing any of the other tasks for adding BIG-IP DataSafe to the BIG-IP System. You can provision FPS either from the Configuration utility in the BIG-IP system, or from the Traffic Management shell (tmsh). The following steps explain how to provision FPS from the Configuration utility in the BIG-IP system.

1. On the Main tab, click **System** > **Resource Provisioning**.
2. Go to the Fraud Protection Service (FPS) row in the list of modules, and in the Provisioning column select the check box and choose one of the following from the drop-down:
   - **Dedicated:** Specifies that the system allocates all CPU, memory, and disk resources to one module. When you select this option, the system sets all other modules to None (Disabled).

- **Nominal:** Specifies that, when first enabled, a module gets the least amount of resources required. Then, after all modules are enabled, the module gets additional resources from the portion of remaining resources.
- **Minimum:** Specifies that when the module is enabled, it gets the least amount of resources required. No additional resources are ever allocated to the module.

3. Click **Submit**.

Provisioning Fraud Protection Service for BIG-IP DataSafe using tmsh

You must provision Fraud Protection Service (FPS) for BIG-IP DataSafe before performing any of the other tasks for adding BIG-IP DataSafe to the BIG-IP System. You can provision FPS either from the Configuration utility in the BIG-IP system, or from the Traffic Management shell (tmsh). The following steps explain how to provision FPS from tmsh.

1. Open the TMOS Shell (`tmsh`).
2. View the current provisioning of the system by typing `list sys provision` in the command line. The system displays the provision configuration. In this example, the system has nominal provisioning for LTM® and the other modules are unprovisioned.

```
sys provision afm { }
sys provision am { }
sys provision apm { }
sys provision asm { }
sys provision avr { }
sys provision dos { }
sys provision fps { }
sys provision gtm { }
sys provision ilx { }
sys provision lc { }
sys provision ltm {
    level nominal
}
sys provision pem { }
sys provision sslo { }
sys provision swg { }
sys provision urldb { }
```

3. Modify provisioning for the FPS module by typing `modify sys provision fps <level_type>` in the command line, where *`<level_type>`* is one of the following:

   - `dedicated`: Specifies that the system allocates all CPU, memory, and disk resources to one module. When you select this option, the system sets all other modules to None (Disabled).
   - `nominal`: Specifies that, when first enabled, a module gets the least amount of resources required. Then, after all modules are enabled, the module gets additional resources from the portion of remaining resources.
   - `minimum`: Specifies that when the module is enabled, it gets the least amount of resources required. No additional resources are ever allocated to the module.

   For example, to set FPS provisioning to nominal, type `modify sys provision fps level nominal`
   The system displays the provision configuration. In this example, the system now has nominal provisioning for FPS.

```
sys provision afm { }
sys provision am { }
sys provision apm { }
sys provision asm { }
sys provision avr { }
sys provision dos { }
sys provision fps {
    level nominal
}
sys provision gtm { }
sys provision ilx { }
sys provision lc { }
sys provision ltm {
    level nominal
}
sys provision pem { }
sys provision sslo { }
sys provision swg { }
sys provision urldb { }
```

4. Save the changes to the stored configuration by typing `save sys config` in the command line.
5. Verify the current provisioning of the system by typing `list sys provision` in the command line..

Creating a node for a remote syslog server

Before creating a node for a remote syslog server, you must first provision FPS for BIG-IP DataSafe.

Creating a node for a remote syslog server only necessary if you want alerts sent to a remote syslog server. If you don't want alerts sent to a remote syslog server, skip this section.

Note: *An alternate way to create a node is to create a pool member. When you create a pool member, the BIG-IP® system automatically creates the corresponding node. For example, if you create pool member* `10.10.20.30:80`*, the system automatically creates a node with the address* `10.10.20.30`*.*

1. On the Main tab, expand **Local Traffic**, and click **Nodes**.
   The Node List screen opens.
2. Click the **Create** button.
   The New Node screen opens.
3. In the **Name** field, type a descriptive label for the node.

   Names are case-sensitive.
4. In the **Address** field, types the IP address of the remote Syslog server.
5. Click **Finished**.
   The screen refreshes, and the new node appears in the node list.

Creating a pool for a remote syslog server

Before creating a pool for a remote syslog server, you should create a node for the remote syslog server.

Creating a pool for a remote syslog server only necessary if you want alerts sent to a remote syslog server. If you don't want alerts sent to a remote syslog server, skip this section.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. At the **New Members** setting, select **Node List**.
5. In the **Address** field, select the IP address of the remote Syslog server.
6. In the **Service Port** field, select **HTTP** or **HTTPS** from the list.
7. Click **Add**.

8. Click **Finished**.

The new pool appears in the Pools list.

Creating a web application server node

Before creating a web application server node, you must first provision FPS for BIG-IP DataSafe.

Local traffic pools use nodes as resources for load balancing. A *node* is an IP address that represents a server resource, which hosts applications.

Note:

- If you plan to add your BIG-IP® DataSafe™ profile to an existing virtual server (i.e., you are not going to create a new virtual server for your profile), you do not need to create a new web application node.
- An alternate way to create a node is to create a pool member. When you create a pool member, the BIG-IP® system automatically creates the corresponding node. For example, if you create pool member `10.10.20.30:80`, the system automatically creates a node with the address `10.10.20.30`.

1. On the Main tab, expand **Local Traffic**, and click **Nodes**.
   The Node List screen opens.
2. Click the **Create** button.
   The New Node screen opens.
3. In the **Name** field, type a descriptive label for the node.

   Names are case-sensitive.
4. In the **Address** field, type the IP address of the web application server.
5. Click **Finished**.
   The screen refreshes, and the new node appears in the node list.

Creating a web application pool

Before creating a web application server pool, you must first create a web application server node.

You can create a pool of servers that you can group together to receive and process traffic.

Note:

- If you plan to add your BIG-IP® DataSafe™ profile to an existing virtual server (i.e., you are not going to create a new virtual server for your profile), you do not need to create a new web application pool.
- Repeat the following steps for each desired pool.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the web application pool.
4. Using the **New Members** setting, add each resource that you want to include in the pool:
   a) Select **Node List**.
   b) For the **Address** option, select the IP address of the web application server.
   c) For the **Service Port** option, select **HTTP** or **HTTPS** from the list.
   d) Click **Add**.
5. Click **Finished**.

The new pool appears in the Pools list.

Creating a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one remote syslog server pool exists on the BIG-IP® system.

Create a log destination of the **Remote Syslog** type if you want to have alerts sent to a remote syslog server. If you don't want alerts sent to a remote syslog server, skip this section.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.
5. From the **Pool Name** list, select the remote syslog server pool that you defined previously.
6. From the **Protocol** list, select the TCP protocol.
7. Click **Finished**.

Creating a log publisher

Create a log publisher to specify where the BIG-IP system sends alert messages.

Note: *If you want alerts sent to a remote syslog server, you need to create two log publishers, one for the local syslog server and one for the remote syslog server.*

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. For the **Destinations** setting, select **local-syslog** from the **Available** list, and click **<<** to move the destination to the **Selected** list.
5. Click **Finished**.
   The list of Log Publishers appears, showing the Log Publisher you just created.
6. If you want to have alerts sent to a remote syslog server, repeat steps 2-5, and at step 4 select the log destination that you created previously from the **Available** list.

Creating an initial BIG-IP DataSafe profile

Overview: Creating an initial profile

Typically, when you create your initial profile, you will want to:

- Set general properties for the profile in the Profile Properties screen
- Define URLs to be included in the profile
- Set one of the URLs to be a login page
- Configure a post-login URL (in certain situations)

Therefore, the instructions for creating an initial profile are presented according to these four stages.

Configuring general properties for a BIG-IP DataSafe profile

Configure general properties for a BIG-IP® DataSafe™ profile to ensure proper encryption of data on your web site.

1. On the Main tab, click **Security** > **Data Protection** > **DataSafe Profiles**.
   The DataSafe Profiles screen opens.
2. Click **Create**.
   The Create New DataSafe Profile screen opens.
3. Select the **Customize All** check box.
4. In the **Profile Name** field, type a unique name for the profile.
5. From the **Parent Profile** list, choose which parent profile you want to base your profile on.

   Note:

   - All undefined properties in the profile you are creating will be inherited from the parent profile. And any future changes to those properties in the parent profile will be automatically inherited by the profile you are creating.
   - URL properties are not inherited.

6. If you previously created a Log Publisher for a remote Syslog server, select it from the **Log Publisher** list.
7. From the **Local Syslog Publisher** list, select the Log Publisher that you previously created for the local Syslog server.
8. If your web application is case-sensitive to URLs, do the following:
   a) Click **Advanced** in the General Settings section.
   The Advanced settings appear.
   b) For the **URLs are case sensitive** setting, select the **Enabled** check box.

   Note:

   - You should enable this setting only if your web application is case-sensitive to URLs.
   - This setting cannot be changed after initial creation of your profile and does not affect parameters in the profile.

9. Click **Create**.
   The BIG-IP DataSafe profile has been created.

After creating your the profile, you should define the URLs that you want to include in your profile.

Defining URLs in the profile

Define URLs in your BIG-IP® DataSafe™ profile to ensure proper protection of your web site.

1. On the Main tab, click **Security** > **Data Protection** > **DataSafe Profiles**.
   The DataSafe Profiles screen opens.
2. From the list of profiles, select the profile on which you want to define a URL.
   The DataSafe Profile Properties screen opens.
3. In the DataSafe Configuration area, click **URL List**.
   The URL List opens.
4. Click the **Add** button.
   The Create New URL screen opens.
5. In the **URL Path** field, choose one of the following types for the URL path:

   - **Explicit**: Assign a specific URL path.
   - **Wildcard**: Assign a wildcard expression URL. Any URL that matches the wildcard expression is considered legal and will receive protection. For example, typing the wildcard expression `*` specifies that any URL is allowed.

a) If you chose **Explicit**, type the URL path.

b) If you chose **Wildcard**, type the wildcard expression URL and if you want it to include a query string, select the **Include Query String** check box.

The syntax for wildcard entities is based on shell-style wildcard characters. This following table lists the wildcard characters that you can use so that the entity name matches multiple objects.

Wildcard character	Matches
*	All characters
?	Any single character
[abcde]	Exactly one of the characters listed
[!abcde]	Any character not listed
[a-e]	Exactly one character in the range
[!a-e]	Any character not in the range

***Note:** Wildcards do not match regular expressions. Do not use a regular expression as a wildcard.*

6. Click **Advanced**.
7. If you want the BIG-IP DataSafe JavaScript to be injected on the web page of the URL, select the **Enabled** check box for **Inject Main JavaScript** (selected by default).

***Note: Inject Main JavaScript** can be disabled for web pages that do not require encryption protection and only receive data from a protected page.*

8. If you want to change the default location where the BIG-IP DataSafe Main JavaScript is injected in the URL's web page, at **Location of Main JavaScript Injection**, do the following:
   - Select a position for the Main JavaScript (either before or after the tag you define).
   - In the **Tag** field, type the tag for determining where the Main JavaScript is placed.
9. Click **Create** to save your initial URL settings.

Set a URL to be a login page

Set a URL in your profile to be a login page if you want to encrypt data on a login page in your web site.

1. On the Main tab, click **Security** > **Data Protection** > **DataSafe Profiles**.
   The DataSafe Profiles screen opens.
2. From the list of profiles, select the relevant profile.
   The DataSafe Profile Properties screen opens.
3. In the DataSafe Configuration area, click **URL List**.
   The URL List opens.
4. Click the URL that you want to set as the login page, or click **Add** if you want to create a new URL to be a login page.
   The URL Properties screen (or Create New URL screen) opens.
5. In the URL Configuration area, select **Parameters**.
6. Type a parameter name in the text field and click the **Add** button.
   The parameter name is added to the list of parameters in the table.
7. In the parameter row in the table, select **Identify as Username**.
8. Under URL Configuration select **Login Page Properties**.

***Note:** Configuring the **Login Page Properties** is not required but recommended because a login cannot be verified as successful unless at least one of the criteria in the **Login Page Properties** is configured.*

9. For the **URL is Login Page** setting, select the **Yes** check box.
   The Login Page Properties appear.

   ***Note:** You must configure at least one of the Login Page Properties. If you configure more than one Login Page Property, then all the criteria for all properties must be fulfilled for the BIG-IP system to consider the login successful.*

10. In the **A string that should appear in the response body** field, type a string that should appear in the successful response to the login URL.
11. In the **A string that should NOT appear in the response body** field, type a string that should not appear in the successful response to the login URL.
12. In the **Expected HTTP response status code** field, select **Specify** and type the HTTP response status code that the server must return to the user upon successful login, or select **None**.

    ***Note:** If you select **None**, HTTP response code is not used to determine a successful login.*

13. In the **Expected response header** field, type a header name that the successful response to the login URL must match.
14. In the **Expected cookie name** field, type a cookie name that the successful response to the login URL must include.
15. Click Save.
    The Login Page and Parameter settings are saved.

If the form action in the http request from the login page URL does not refer to the login page URL, you need to also configure a post-login URL.

Configuring a post-login URL

You need to configure a post-login URL only if the login page sends the login request to a URL that is different from the login URL. (For example, the login page URL is `/login.jsp`, but it sends the user name and password to `/validate.jsp`).

Configure a post-login URL to ensure that the BIG-IP® system can retrieve the user name and decrypt the password.

1. On the Main tab, click **Security** > **Data Protection** > **DataSafe Profiles**.
   The DataSafe Profiles screen opens.
2. From the list of profiles, select the relevant profile.
   The DataSafe Profile Properties screen opens.
3. In the DataSafe Configuration area, click **URL List**.
   The URL List opens.
4. Select the check box next to the login URL.
5. Click the **Clone** button.
   The Clone URL pop-up screen opens.
6. In the **URL Path** field, type the URL that is referred to in the form action of the HTTP request.
7. Optional: In the **Description** field, type a description for the URL.
8. If you don't want to encrypt data on the web page of the URL that you are cloning, disable the **Inject JavaScript** setting.
9. Click the **Clone** button in the Clone URL pop-up screen.

***Note:** A cloned URL inherits all properties from the original URL, including parameters. However, once the cloned URL is created, there is no further dependency, and any future changes made in the original URL are not inherited by the cloned URL.*

Creating a custom HTTP profile

This procedure should be performed only if SNAT or Auto Map is used for Source Address Translation in the virtual server.

An HTTP profile defines the way that you want the BIG-IP®system to manage HTTP traffic.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Services** > **HTTP**.
   The HTTP profile list screen opens.
2. Click **Create**.
   The New HTTP Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. Select the **Custom** check box.
5. In the **Insert X-Forwarded-For** field, select **Enabled**.
6. Click **Finished**.

The custom HTTP profile now appears in the HTTP profile list screen.

Creating a virtual server

You can create a virtual server on the BIG-IP® system, where clients send application requests. The virtual server manages the network resources for the web application that you are securing with a security policy.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address/Mask** field, type an address, as appropriate for your network.

   The supported format is address/prefix, where the prefix length is in bits. For example, an IPv4 address/prefix is `10.0.0.1` or `10.0.0.0/24`, and an IPv6 address/prefix is `ffe1::0020/64` or `2001:ed8:77b5:2:10:10:100:42/64`. When you use an IPv4 address without specifying a prefix, the BIG-IP® system automatically uses a `/32` prefix.
5. In the **Service Port** field, type `80`, or select **HTTP** from the list.
6. From the **HTTP Profile** list:
   a) If you previously created an HTTP profile, then select the profile you created.
   b) Otherwise, select **http**.
7. From the **Source Address Translation** list, select the appropriate translation.
8. From the **Default Pool** list, select the pool that is configured for the application server.
9. Click **Finished**.

Associating a profile with a virtual server

In order to complete the process of adding BIG-IP® DataSafe™ to a virtual server, you need to associate the profile with the virtual server.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, from the Security menu, choose Policies.
4. From the **Anti-Fraud Profile** list, select **Enabled**, and then from the **Profile** list, select the profile you created previously.
5. Click **Update** to save the changes.

General Configuration Options for BIG-IP DataSafe Profiles and URLs

Configuring advanced general settings on a profile

Configure advanced general settings on BIG-IP® DataSafe™profiles if you want to change the default settings that the BIG-IP® system assigns to profiles.

1. On the Main tab, click **Security** > **Data Protection** > **DataSafe Profiles**.
   The DataSafe Profiles screen opens.
2. From the list of profiles, select the relevant profile.
   The DataSafe Profile Properties screen opens.
3. In the General Settings area of the DataSafeProfile Properties screen, click **Advanced**.
   The Advanced settings appear.
4. In the **Alert Path** field, use the automatically generated path, or define your own path.

   Note: *If you define your own path, ensure that the path is not used by any other field in the profile and that it is not an already existing URL.*

5. In the **Suggested Username Header** field, use the default header or type a header that will be added to AJAX requests when the BIG-IP system detects an AJAX login attempt, which is common for Single Page Applications.

   With this header, the BIG-IP system can detect the username that was used for the login. The client sends this header only for URLs in the profile that have a parameter set as Identify as Username.
6. For the **JavaScript Directory** field, use the automatically generated path, or define your own.

   This path specifies the location of the main BIG-IP DataSafe JavaScript. This path does not include the actual file name of the JavaScript.

   Note: *This path should be changed only if your application is already using a directory with the same path as the automatically assigned default path.*

7. For the **JavaScript Configuration Directory** field, use the automatically generated path, or define your own path that specifies the location of the BIG-IP DataSafe JavaScript containing profile configuration settings.

   This path specifies the location of the configuration JavaScript. This path does not include the actual file name of the JavaScript.

   Note: *This path should be changed only if your application is already using a directory with the same path as the automatically assigned default path.*

8. For the **JavaScript Removal Location** field, use the automatically generated path, or define your own path that specifies the location of the image file name that the system uses for detecting a JavaScript removal attack.
9. For **JavaScript Grace Threshold**, change the default value if you want to raise or lower the maximum amount of time (in seconds) permitted between when a protected web page is loaded and its injected JavaScript activates.
10. Leave the **Additional function to be run before JavaScript load** field blank unless instructed otherwise by F5®.

11. For the **Prevent duplicate alerts from Client Side** setting, select the **Enabled** check box to prevent the client from sending an alert with information that is identical to an alert previously sent by the client during the past 24 hours.
12. Click **Save**.
    The BIG-IP system saves the changes that you made to the advanced settings.

Enable an iRule to handle logins and alerts

Enabling iRules® to handle logins and alerts is only relevant if you have written an iRule to handle the `ANTIFRAUD_ALERT` event, or the `ANTIFRAUD_LOGIN` event and the iRule is associated with the same virtual server as your profile.

Enable an iRule to handle logins and alerts if you want to use an iRule to disable alerts or record login events.

1. On the Main tab, click **Security** > **Data Protection** > **DataSafe Profiles**.
   The DataSafe Profiles screen opens.
2. From the list of profiles, select the relevant profile.
   The DataSafe Profile Properties screen opens.
3. In the General Settings area of the DataSafeProfile Properties screen, click **Advanced**.
   The Advanced settings appear.
4. In the **Trigger iRule Events** setting, select the **Enabled** check box.
5. Click **Save**.
   iRules are now enabled to handle logins and alerts.

iRule events

iRules® can subscribe to the `ANTIFRAUD_ALERT` event and the `ANTIFRAUD_LOGIN` event in BIG-IP® DataSafe™

iRule event	Description
`ANTIFRAUD_ALERT`	Occurs when alerts are sent to the BIG-IP® system.
`ANTIFRAUD_LOGIN`	Occurs when a user successfully logs in to the profile. Or if login validation is not configured, this event can occur if just the user name is identified.

iRule Examples

The following example shows how an iRule uses the `ANTIFRAUD_ALERT` event to log all available information about an alert that was sent by the BIG-IP system to the location `/var/log/ltm`.

```
when ANTIFRAUD_ALERT{
  log local0. "=========Anti-Fraud Alert========="
  log local0. "Alert Identifier: [ANTIFRAUD::alert_id]"
  log local0. "Alert Type: [ANTIFRAUD::alert_type]"
  log local0. "Alert Component: [ANTIFRAUD::alert_component]"
  log local0. "Alert Details: [ANTIFRAUD::alert_details]"
  log local0. "Alert GUID: [ANTIFRAUD::alert_guid]"
  log local0. "Alert Device ID: [ANTIFRAUD::alert_device_id]"
  log local0. "Alert License ID: [ANTIFRAUD::alert_license_id]"
  log local0. "Alert Score: [ANTIFRAUD::alert_score]"
  log local0. "Alert Transaction Data: [ANTIFRAUD::alert_transaction_data]"
  log local0. "Alert Username: [ANTIFRAUD::alert_username]"
  log local0. "Alert HTTP Referrer: [ANTIFRAUD::alert_http_referrer]"
  log local0. "Alert Additional Info: [ANTIFRAUD::alert_additional_info]"
  log local0. "Alert Forbidden Added Element: [ANTIFRAUD::alert_forbidden_added_element]"
  log local0. "Alert Bait Signatures: [ANTIFRAUD::alert_bait_signatures]"
  log local0. "Alert HTML: [ANTIFRAUD::alert_html]"
}
```

The following example shows how an iRule uses the `ANTIFRAUD_ALERT` event to disable a specific alert according to its type.

```
when ANTIFRAUD_ALERT{
if {[ANTIFRAUD::alert_type] eq "components_validation"}{
  log local0. "Alert Type is components validation"
  ANTIFRAUD::disable_alert
  log local0. "Disabled Alert"
  }
}
```

The following example shows how an iRule uses the `ANTIFRAUD_LOGIN` event with its commands.

```
when ANTIFRAUD_LOGIN{
  log local0. "=========Anti-Fraud Login========="
  # read mode
  log local0. "Username: [ANTIFRAUD::username]"
  log local0. "GUID: [ANTIFRAUD::guid]"

  # write mode
  ANTIFRAUD::username "other_user"
}
```

Values for iRule commands

The following values can be used in iRule commands:

Value	Description
alert_id	For example, d4.
alert_type	The type of alert.
alert_component	An error type that is determined according to the alert_type.
alert_details	Additional information regarding the alert.
alert_device_id	Persistent browser identifier.
alert_license_id	crc32 of the license id in hex.
alert_transaction_data	Key-value list of all parameters marked to be attached.
alert_username	When this command is used without any additional arguments, this is the name of the user who triggered the alert. It is possible to use additional arguments to override the current user name (write mode), as shown in the `ANTIFRAUD_LOGIN` example above.
alert_http_referrer	The URL of the site that was visited just before the Alert URL was visited.
alert_additional_info	Shows additional information about the alert, such as the `parameter values too long` error message.
disable_alert	Disables the current alert.

For more information about iRules, go to F5® Networks DevCentral™ (`https://devcentral.f5.com/irules`).

Configuring URL parameters

Configure URL parameters to protect sensitive URL parameter values. For example, if you have a `password` parameter sent by GET and you want to encrypt its value, assign the **Encrypt** attribute (for Application Layer Encryption) and the **GET** method.

Note: *When a protected web page (an INJECTION page) passes data to another web page (an ACTION page), for example via a submit form, both web pages must have the exact same parameter configurations. Otherwise, appropriate alerts may not be sent.*

1. On the Main tab, click **Security** > **Data Protection** > **DataSafe Profiles**.
   The DataSafe Profiles screen opens.
2. From the list of profiles, select the relevant profile.
   The DataSafe Profile Properties screen opens.
3. In the DataSafe Configuration area, click **URL List**.
   The URL List opens.
4. Click the URL on which you want to configure parameters.
   The URL Properties screen opens.
5. In the URL Configuration area, select **Parameters**.
6. Type a parameter name in the text box and click the **Add** button.
   The parameter name is added to the list of parameters in the table.
7. In the parameter row in the table, select parameter attributes as follows:
   - **Identify as Username**: When enabled, the system considers this parameter a username. Only one parameter per URL can have this attribute.

     Note: *If you did not set **URL is Login Page=Yes** and you set a parameter to be a user name here, a warning sign appears under this column on the parameter row indicating that the user name is identified without access validation unless the URL is a Login Page.*
   - **Encrypt** : When enabled, the system encrypts the parameter's **value** attribute.
   - **Substitute Value**: When enabled, the system substitutes the parameter's value with a random value in the web application while the form is being filled. This option is available only after the **Encrypt** setting is enabled, unless you are using a custom encryption function.

     Note: *If you assign this attribute to a password parameter, the web browser's autocomplete feature for passwords does not work on this parameter.*
   - **Obfuscate**: When enabled, the system encrypts the parameter's **name** attribute. This attribute cannot be assigned to a parameter if **Application Layer Encryption** is not enabled.
   - **Method**: Select the method of request from where parameter data is received (POST or GET).
8. Repeat steps 6 and 7 for each parameter you want on the URL.
9. Click **Save** to save URL parameter settings.

Cloning a profile

If you want to create a new profile with settings identical to an existing profile, you can clone the profile. Unlike parent-child profiles, the cloned profile is not dependent on the original one, and any changes made to the original profile after cloning are not inherited by the previously cloned profile.

Note: *A cloned profile inherits all properties from the original profile, including all URL properties.*

1. On the Main tab, click **Security** > **Data Protection** > **DataSafe Profiles**.
   The DataSafe Profiles screen opens.
2. Select the check box next to the profile that you want clone.
3. Click the **Clone** button.
   The Clone Profile pop-up screen opens.
4. In the Clone Profile pop-up screen, assign a profile name and (optionally) a description.
5. Click **Clone**.
   The cloned profile is created and appears in the list of profiles in the DataSafe Profiles screen.

Cloning a URL

You can clone a URL if you want to create a new URL with identical settings to an existing URL.

1. On the Main tab, click **Security** > **Data Protection** > **DataSafe Profiles**.
   The DataSafe Profiles screen opens.
2. From the list of profiles, select the profile with the URL you want to clone.
   The DataSafe Profile Properties screen opens.
3. In the DataSafe Configuration area, click **URL List**.
   The URL List opens.
4. Select the check box next to the URL that you want clone.
5. Click the **Clone** button.
   The Clone URL pop-up screen opens.
6. In the Clone URL pop-up screen, assign a URL path and (optionally) a description.
7. If you don't want to encrypt data on the web page of the URL that you are cloning, disable the **Inject JavaScript** setting.
8. Click the **Clone** button in the Clone URL pop-up screen.

   Note: *A cloned URL inherits all properties from the original URL, including parameters. However, once the cloned URL is created, there is no further dependency, and any future changes made in the original URL are not inherited by the cloned URL.*

Encrypting Data on the Application Level

Overview: Encrypting Data on the Application Level

Application Layer Encryption verifies whether the user was trying to use a fabricated password, validates the client-side password, encrypts credentials in real-time upon submission, and protects against in-browser key loggers by generating fake keyboard events. DataSafe™ allows you to configure data encryption on the application level, so that sensitive data entered (input) by a user on the client-side is protected against attempted fraud attacks that occur in the web application.

Task Summary

Encrypting data as it leaves the web browser

Encrypt data as it leaves the web browser if you want to protect data that was entered by the user as it leaves the web browser.

1. On the Main tab, click **Security** > **Data Protection** > **DataSafe Profiles**.
   The DataSafe Profiles screen opens.
2. From the list of profiles, select the relevant profile.
   The DataSafe Profile Properties screen opens.
3. In the DataSafe Configuration area, click **URL List**.
   The URL List opens.
4. Select the URL on which you want to encrypt data.
   The URL Properties screen appears.
5. In URL Configuration area, select **Application Layer Encryption**.
   The Application Layer Encryption settings are displayed.
6. Ensure that the **Enabled** check box for **Application Layer Encryption** is selected.
7. If you want to use a custom encryption algorithm on URL parameters (instead of the BIG-IP® default encryption function), in the **Custom Encryption Function** field, type your custom encryption function.

   Note: *If you use a custom encryption function, you can not enable* ***Real-Time Encryption*** *on this URL. Real-Time Encryption encrypts passwords as the user types them.*

   The custom encryption function encrypts all URL parameters where **Encrypt** is disabled and **Substitute Value** is enabled on the parameter.
8. In the URL Configuration area, select **Parameters**.
9. Type a parameter name in the text field and click the **Add** button.
   The parameter name is added to the list of parameters in the table.
10. In the parameter row in the table, do the following:

- Select the **Encrypt** check box.
- If the parameter is for a password field and you want to use substitute values when the user inputs the password, select the **Substitute Value** check box.

  Note: *If you assign the* ***Substitute Value*** *attribute to a password parameter, the web browser's auto-complete feature for passwords does not work on this parameter.*

Important: *If you want a custom encryption function to be applied to this parameter, do not select the check boxes for both* ***Encrypt*** *and* ***Substitute Value*** *on the parameter. If you do this, the custom encryption function will not be applied to this parameter.*

11. Repeat steps 9 and 10 for every URL parameter you want the system to encrypt.
12. Click **Save**.
    The URL configuration settings are saved.

If the form action in the http request from the URL you created above does not refer to the URL you created above, you need to also configure a URL for decrypted data.

Applying AJAX Encryption on a URL

You can apply AJAX encryption on a URL if the web page of your URL sends AJAX data and you want it to be encrypted.

1. On the Main tab, click **Security** > **Data Protection** > **DataSafe Profiles**.
   The DataSafe Profiles screen opens.
2. From the list of profiles, select the relevant profile.
   The DataSafe Profile Properties screen opens.
3. In the DataSafe Configuration area, click **URL List**.
   The URL List opens.
4. Select the URL on which you want to apply AJAX encryption.
   The URL Properties screen appears.
5. In URL Configuration area, select **Application Layer Encryption**.
   The Application Layer Encryption settings are displayed.
6. Select the **Enabled** check box for the **Full AJAX Encryption** setting.
7. If your URL uses JSON format for submitting data, do the following:
   a) On the left, under URL Configuration, select **Parameters**.
   b) Type a parameter name or ID in the text field and click **Add**.
   The parameter name or ID is added to the list of parameters in the table.
   c) In the parameter row in the table, select both the **Encrypt** check box and the **Substitute Value** check box.
   d) In the **AJAX Mapping** text box, type a mapping key for the parameter that is sent from the client to the server.

   For example, if you have a single page application form with an input field **name** or **ID** called **A** and you want to send it in the **B** key in the JSON file, type `B` in this text box.

   Note: *If the input field* ***name*** *or* ***ID*** *in the HTML of your web page has the same* ***name*** *or* ***ID*** *as the key of the JSON file, you do not need to type a mapping key in this text box.*

8. Click **Save**.
   The URL configuration settings are saved.

Configuring a URL for decrypting data

You need to configure a separate URL for decrypted data only if the form action in the HTTP request from the client does not refer to the URL from which the request is being sent.

Configure a URL for decrypted data to ensure that your server can read and verify encrypted data that was sent from the client.

1. On the Main tab, click **Security** > **Data Protection** > **DataSafe Profiles**.
   The DataSafe Profiles screen opens.
2. From the list of profiles, select the relevant profile.
   The DataSafe Profile Properties screen opens.
3. In the DataSafe Configuration area, click **URL List**.
   The URL List opens.
4. Select the check box next to the URL where the client sends encrypted data.
5. Click the **Clone** button.
   The Clone URL pop-up screen opens.
6. In the **URL Path** field, type the URL that is referred to in the form action of the HTTP request.
7. Optional: In the **Description** field, type a description for the URL.
8. If you don't want to encrypt data on the web page of the URL that you are cloning, disable the **Inject JavaScript** setting.
9. Click the **Clone** button in the Clone URL pop-up screen.

Note: *A cloned URL inherits all properties from the original URL, including parameters. However, once the cloned URL is created, there is no further dependency, and any future changes made in the original URL are not inherited by the cloned URL.*

Configuring HTML field obfuscation

Before configuring HTML field obfuscation, **Application Layer Encryption** must be enabled on the URL.

Configure HTML field obfuscation if you want the BIG-IP® system to encrypt the `name` attribute of all defined HTML `<input>` fields, and then decrypt them back to the original `name` on the BIG-IP system.

1. On the Main tab, click **Security** > **Data Protection** > **DataSafe Profiles**.
   The DataSafe Profiles screen opens.
2. From the list of profiles, select the relevant profile.
   The DataSafe Profile Properties screen opens.
3. In the DataSafe Configuration area, click **URL List**.
   The URL List opens.
4. Select the URL on which you want to configure HTML field obfuscation.
   The URL Properties screen appears.
5. In URL Configuration area, select **Application Layer Encryption**.
   The Application Layer Encryption settings are displayed.
6. Select the **Enabled** check box for the **HTML Field Obfuscation** setting.
   The **Add Decoy Inputs** and **Remove Element IDs** fields are displayed.
7. Select the **Enabled** check box for the **Add Decoy Inputs** setting if you want the system to randomly, and continuously, generate and remove decoy `<input>` fields that are added to the web page.

   Enabling **Add Decoy Inputs** makes it harder for an attacker to identify sensitive information with either JavaScript or a proxy.

8. Select the **Enabled** check box for the **Remove Element IDs** setting if you want the system to remove the ID attribute from URL parameters that have the **Obfuscate** property.
9. In the URL Configuration area, select **Parameters**.
10. Type a parameter name in the text field and click the **Add** button.
    The parameter name is added to the list of parameters in the table.
11. In the parameter row within the table, select **Obfuscate**.
12. Repeat steps 10 and 11 for every URL parameter you want the system to obfuscate.
13. Click **Save**.
    The URL configuration settings are saved.

Removing JavaScript event listeners from URL parameters

Before you can remove JavaScript event listeners from URL parameters, Application Layer Encryption must be enabled on the URL.

You can remove JavaScript event listeners from URL parameters to protect sensitive data in URL parameters from being obtained by potential attackers.

Note: *Some web applications add non-malicious event listeners that improve functionality. If you choose to activate removal of event listeners on URL parameters, this will remove all event listeners, including non-malicious ones added by the web application. You should take this into account before deciding to activate removal of event listeners.*

1. On the Main tab, click **Security** > **Data Protection** > **DataSafe Profiles**.
   The DataSafe Profiles screen opens.
2. From the list of profiles, select the relevant profile.
   The DataSafe Profile Properties screen opens.
3. In the DataSafe Configuration area, click **URL List**.
   The URL List opens.
4. Select the URL on which you want to remove JavaScript event listeners.
   The URL Properties screen opens.
5. In URL Configuration area, select **Application Layer Encryption**.
   The Application Layer Encryption settings are displayed.
6. Select the **Enabled** check box for the **Remove Event Listeners** setting.
7. In the URL Configuration area, select **Parameters**.
8. Type a parameter name in the text field and click the **Add** button.
   The parameter name is added to the list of parameters in the table.
9. In the parameter row within the table, select **Obfuscate** or **Substitute Value**.

   Note: *If you assign the* ***Substitute Value*** *attribute to a password parameter, the web browser's auto-complete feature for passwords does not work on this parameter.*
10. Repeat steps 8 and 9 for every URL parameter on which you want to remove JavaScript event listeners.
11. Click **Save**.
    The URL configuration settings are saved.

Configuring advanced encryption on a URL

Before configuring advanced encryption on a URL, **Application Layer Encryption** must be enabled on the URL.

Configure advanced encryption on a URL if you want to apply on your URL the advanced encryption methods provided by BIG-IP® DataSafe™.

1. On the Main tab, click **Security** > **Data Protection** > **DataSafe Profiles**.
   The DataSafe Profiles screen opens.
2. From the list of profiles, select the relevant profile.
   The DataSafe Profile Properties screen opens.
3. In the DataSafe Configuration area, click **URL List**.
   The URL List opens.
4. Select the URL on which you want to apply advanced encryption methods.
   The URL Properties screen appears.
5. In URL Configuration area, select **Application Layer Encryption**.
   The Application Layer Encryption settings are displayed.
6. Select the **Enabled** check box for the **Identify Stolen Credentials** setting.

   When this setting is enabled, the system examines whether the user is trying to use a password that was stolen from a parameter where **Substitute Value** is enabled.
7. Select the **Enabled** check box for the **Hide Password Revealer Icon** setting.

   When this setting is enabled, the system hides the password revealer icon on a web page, for browsers that use a password revealer icon (for example, Internet Explorer versions 10 and later).

   Note: *If you are using **JavaScript Function for Substitute Values** or **Custom Encryption Function**, you must enable **Hide Password Revealer Icon**. Otherwise, the user will see the actual substitute value if the user clicks the Password Revealer icon in the browser.*
8. Select the **Enabled** check box for the **Keylogger Protection** setting.

   When this setting is enabled, the system protects against in-browser key loggers.
9. Select the **Enabled** check box for the **Real-Time Encryption** setting.

   Real-Time Encryption encrypts input field parameters as the user types them.

   Note:

   - The **Real-Time Encryption** setting does not appear if you don't have at least one parameter on your URL with the Encrypt property.
   - Real-Time Encryption cannot be enabled on the URL if you are also using a custom encryption function.
10. If you do not want to use the default BIG-IP DataSafe JavaScript function for assigning substitute values for HTML password input fields and prefer to use your own JavaScript function, in the **JavaScript Function for Substitute Values** field, type your JavaScript function.

    The JavaScript function you type here must return substitute values for all passwords input field parameters where **Substitute Value** is enabled on the parameter. If you leave this field blank, the default BIG-IP DataSafe JavaScript function is used.
11. Click **Save**.
    The URL configuration settings are saved.

JavaScript Engine Updates

Overview: Updating the JavaScript engine

The BIG-IP® system provides an option for updating the JavaScript engine, which improves client-side functionality and enhances protection of your BIG-IP® DataSafe™ profile. In the Engine Updates screen you can choose to download and install an engine update from the Update server when it is available, or perform a manual installation of an engine update from an update file you receive from F5.

Once daily, the BIG-IP system determines if engine updates are available from the Update server. If so, the system notifies you in the status area of the screen.

***Note:** If you are working with a group of BIG-IP systems that are in a trust domain and an update is performed on one of the BIG-IP systems in that group, all the other systems in that group are simultaneously updated as well.*

Updating the JavaScript engine

Updating the JavaScript engine enables the BIG-IP® system to discover new types of generic malware.

1. On the Main tab, click **Security** > **Security Updates** > **Data Protection** > **Engine Update**.
2. Choose one of the following delivery modes:
   - Select **Automatic** if you want to download and install an engine update from the Update server if it is available.
   - Select **Manual** if you want to perform an engine update from an update file you receive from F5.

   If you set Delivery Mode to **Manual**, the **Upload File** setting appears.

   a) If you set Delivery Mode to **Manual**, at the **Upload File** field click the browse button to upload the engine update file you received from F5® support.

   ***Note:** Setting Delivery Mode to **Manual** is a temporary setting and only valid as long as you are in the update screen. When you leave the update screen, Delivery Mode reverts back to **Automatic**.*
3. If you received a notification that updates are available or have uploaded an engine update file that you received from F5 support, click the **Install Updates** button to install the update.

   ***Note:** The engine update takes from 2-4 hours to take effect.*
4. In addition to the notice that is displayed if the daily update check determines that an update is available, you can also check for available updates by clicking the **Check for Engine Updates** button.

   The **Check for Engine Updates** button is useful in the case where a new update has become available after the daily check was performed. If you click this button and an update is available, you will receive a notification.

Alert Logs

Viewing the alert log

You can view the alert log to see detailed information on possible or actual attacks on your encrypted data.

1. On the Main tab, click **System** > **Logs** > **Data Protection**.
   The Data Protection log appears. The Data Protection log displays the following alert information:
   - **Timestamp:** The date and time when the system logged the alert information.
   - **Host:** The name of the host that logged the alert information.
   - **Client IP:** The IP address of the victim of the alert.
   - **Event URL:** The URL of the site that was in use when the alert was sent.
   - **User Name:** The name of the client-side user who performed the action that triggered the alert.
   - **Event Type:** The type of the alert, which will be one of the following:
     - **VCRYPT:** Server-side Encryption Error alerts. These alerts are created when the BIG-IP system detects an error in the Application Layer Encryption component.
     - **AJAX_VCRYPT:** Encryption Alerts for the Full AJAX payload. These alerts are created when the BIG-IP system detects an encryption or decryption error in the full AJAX payload.
     - **JS_VCRYPT:** Client-side Encryption Error Alerts. These alerts are created when the BIG-IP DataSafe JavaScript detects an error in the Application Layer Encryption component.
     - **COMPONENTS_VALIDATION:** Server-side Missing Components Alerts. These alerts are created when the BIG-IP system detects missing BIG-IP DataSafe components on a protected web page.
     - **JS_MISSING_COMPONENTS:** Client-side Missing Components Alerts. These alerts are created when the BIG-IP DataSafe JavaScript detects missing BIG-IP DataSafe components on a protected web page.
   - **Component:** The alert sub-type.
2. To view additional information on an alert, click the **More Details** link in the far-right column.
   Clicking this link displays the following additional information on an alert:
   - **Defined Value:** This is used only in Encryption Staging Mode, when Component = VCRYPT_STAGING_MODE_FAILED. The parameter name is displayed along with the type of problem, which will be either MISMATCH or MISSING.
   - **Resolved Value:** This is used only in Encryption Staging Mode, when Component = VCRYPT_STAGING_MODE_FAILED. The parameter name is displayed along with the type of problem, which will be either MISMATCH or MISSING.
   - **Details:** The information displayed here varies depending on the alert type.
   - **Additional Info:** The information displayed here varies depending on the alert type.
   - **URL Name:** The URL of the site from where the alert was sent, as configured in the BIG-IP. This can differ from the Event URL, for example if a wildcard URL was configured in the BIG-IP.
   - **Client IP Geolocation:** The geographic location of the client IP.
   - **Transaction ID:** An HTTP transaction ID generated by AVR for the Risk Engine.
   - **Guid:** An internal ID generated by BIG-IP DataSafe for identifying the user whose action generated the alert.
   - **User Agent:** The user's browser type and operating system.
   - **HTTP Referrer:** The URL of the web page that was visited just before the Alert URL was visited.

Legal Notices

Legal notices

Publication Date

This document was published on June 21, 2018.

Publication Number

MAN-0681-00

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

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.

Index