Deploying the Shape SAFE iApp Template in the F5® BIG-IP® System

Shape SAFE iApp Template Version 1.0.0

October 27, 2020, Document Version 1.0.0

Table of Contents

Objective

This document is for F5 technical support staff specializing in deployment of Shape AI Fraud Engine (SAFE), to enable use of the security features of the BIG-IP together with SAFE.

Prerequisites

Before deploying or upgrading an iApp in the F5® BIG-IP® system, you should ensure the following:

1. Your BIG-IP version is 12.1.0 or later, with the LTM Module provisioned and licensed.
2. You have backed up the BIG-IP configuration as described here: Backing up your BIG-IP system configuration.
3. Your virtual server must have an HTTP profile and default pool attached to it.

Deploying the Shape SAFE iApp Template in the BIG-IP System

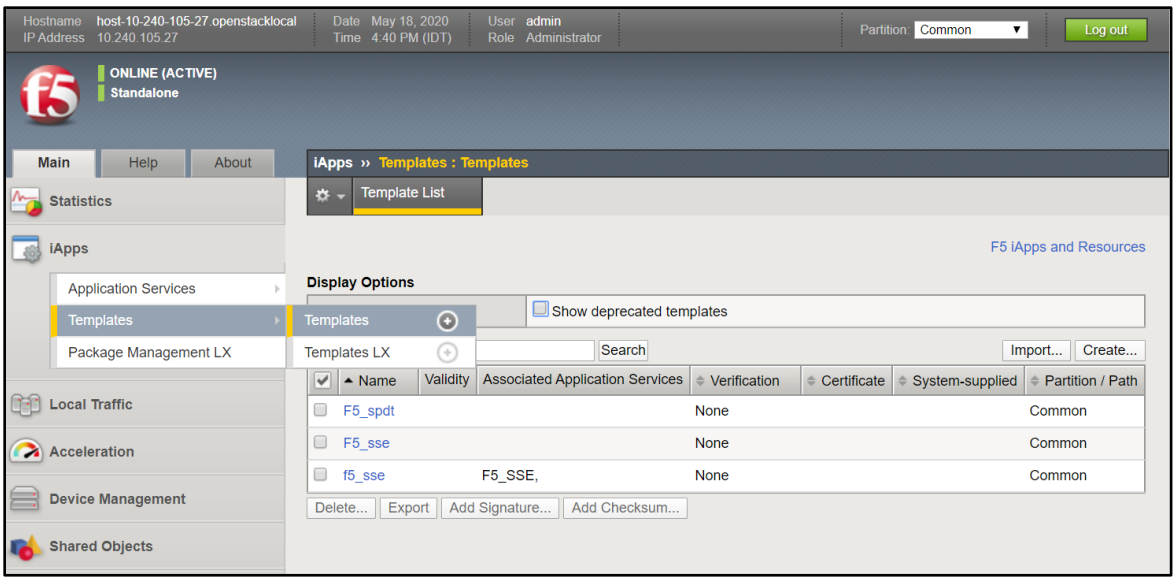
You deploy an iApp in the BIG-IP in two stages:

1. Import the Shape SAFE iApp Template that you received from F5 to the BIG-IP.
2. Create the iApp in the BIG-IP, based on the imported template.

The steps for performing these two stages are described below.

Import the Shape SAFE iApp template to the BIG-IP

1. In the Main tab in the BIG-IP, go to **iApps>Templates>Templates**.

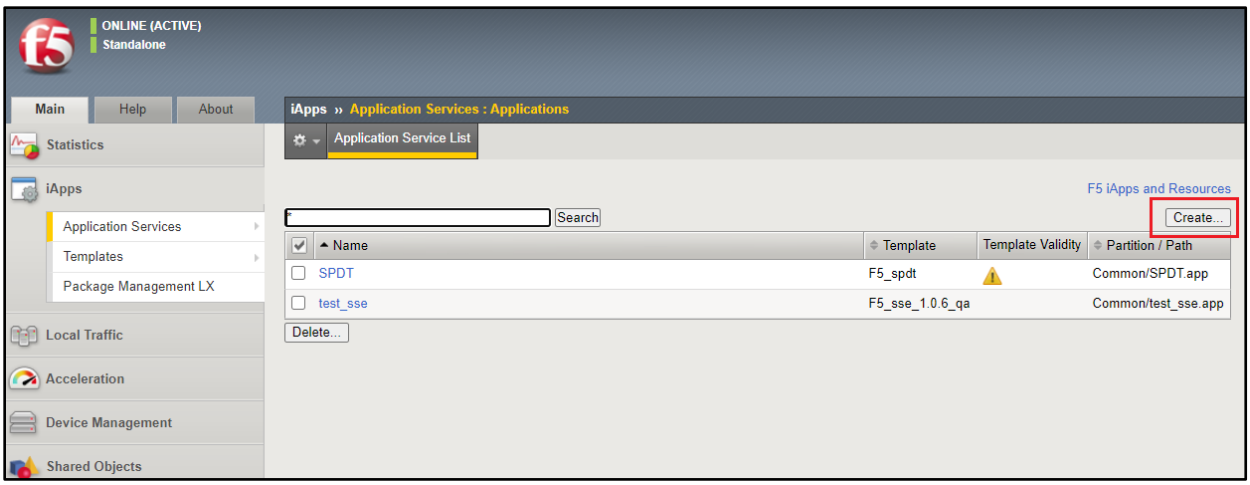


2. Click **Import**.
3. Click Choose File.
4. Select the Shape SAFE iApp template provided to you from F5.
5. Click the check box next to Overwrite Existing Templates.
6. Click **Upload**.

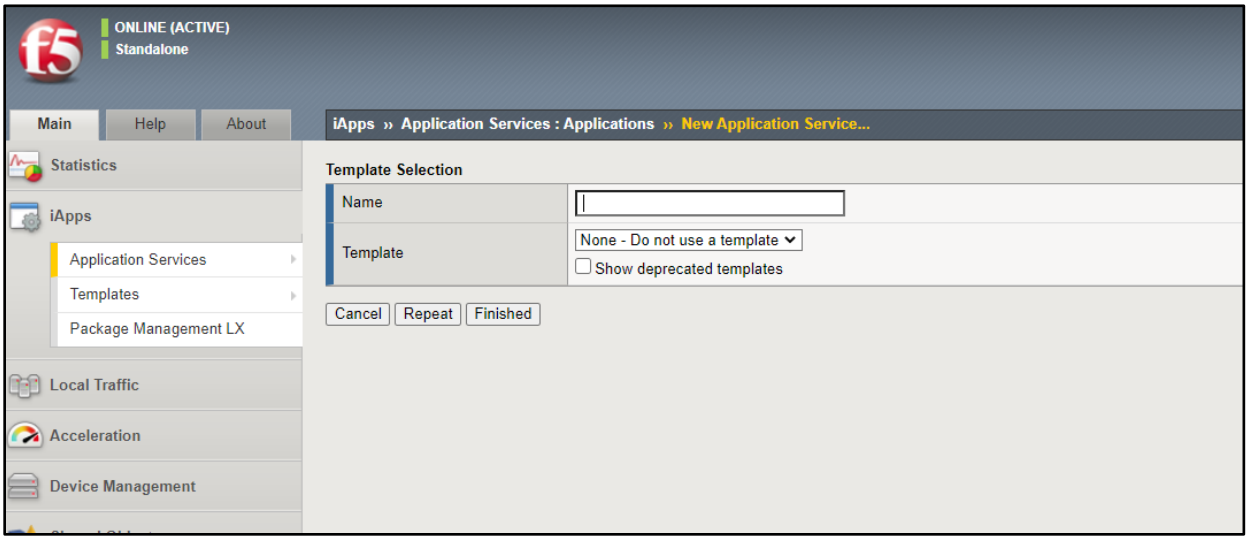
   The Shape SAFE iApp template is now displayed in the list of templates.

Create the iApp in the BIG-IP

1. In the Main tab in the BIG-IP, go to iApps>Application Services>Applications.
2. Click **Create**.



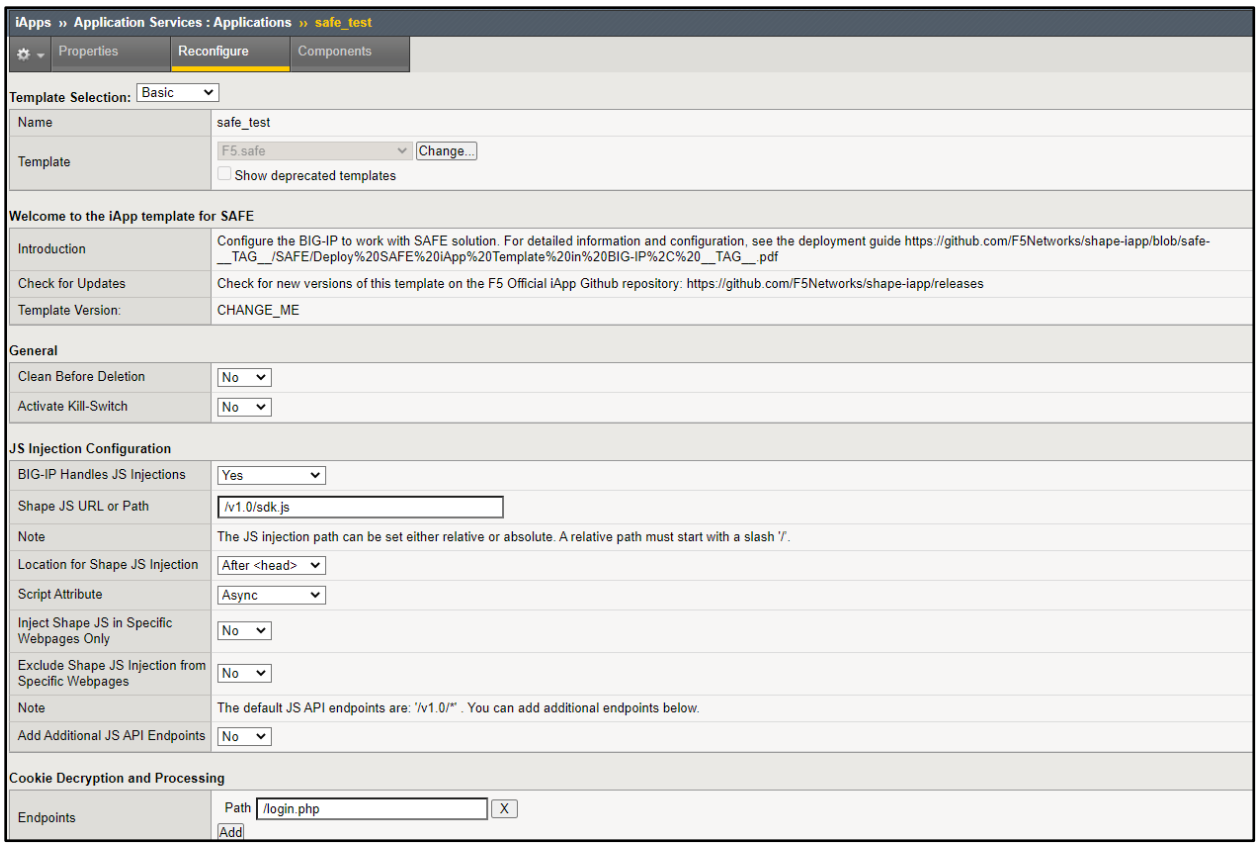
The New Application Service screen appears.



3. Assign a name to the iApp.

4. From the Template list, select the imported Shape SAFE iApp template.

   The Shape SAFE iApp template configuration settings appear.



5. In the JS Injection Configuration section:

   - BIG-IP Handles JS Injections: When Yes, BIG-IP handles JS injections. When No, the customer is responsible for deciding where to inject JS on the HTML code of the application's web pages.

   - Shape JS URL or Path: Enter the path you received from F5 support for the Shape JS injection.

     The Shape JS injection path can be set either relative or absolute. A relative path must start with a slash '/'. Use the following table to determine whether you should use a relative or absolute path.

Who handles JS injections?	Is JS obtained via BIG-IP?	Set **BIG-IP Handles JS Injections** to…	Shape JS URL or Path is…
BIG-IP	Yes	Yes	Relative path or customer domain absolute path
BIG-IP	No	Yes	Absolute path
Origin (application server)	Yes	No	Relative path or customer domain absolute path
Origin (application server)	No	No	Empty

- Location for Shape JS Injection: From the drop-down list, select a location in the HTML code of your webpage for the Shape JS Injection.

  Note: This setting is not displayed if BIG-IP Handles JS Injections = **No**.

- Script Attribute: Choose an attribute that is added at the end of the injected Shape JavaScript, either Async, Sync or Defer. This attribute determines how the JavaScript is loaded and executed.

- Inject Shape JS in Specific Webpages Only: Select **Yes** to inject the Shape JS in specific web pages of your web application. Select **No** to inject the Shape JS in all web pages of your web application.

  Note: This setting is not displayed if BIG-IP Handles JS Injections = **No**.

  - JS Injection Paths: If **Inject Shape JS in specific webpages only** = Yes, enter here the paths of the webpages in your application to receive the Shape JS injections.

- Exclude Shape JS injection from specific webpages: Select **Yes** to exclude the Shape JS injection from specific web pages in your web application.

  Note: This setting is not displayed if BIG-IP Handles JS Injections = **No**.

  - JS Excluded Paths: If you set **Exclude Shape JS injection from specific webpages** = Yes, enter here the paths of the web pages in your application that the Shape JS injections should be excluded from.

- Add Additional JS API Endpoints: If the Shape JavaScript is updated with a new endpoint(s) for Telemetry post requests, enter the endpoint(s) provided to you from F5 support here.

    - JS API Endpoints: If Add Additional JS API Endpoints=Yes, enter the endpoint(s) here.

6. In the Cookie Decryption and Processing section:

    - Endpoints: Enter here the paths to the web pages on which you want to decrypt and process cookies.

      Note: Endpoints are not case sensitive. Regardless of whether you use upper- or lower-case letters, all letters are set to lower-case.

      If you configured at least one endpoint here, you must assign values for Cookie Name, Encryption Key, and Header Name to Add for Cookie Decryption and Processing to work.

    - Cookie Name: Enter the cookie name you received from F5 support for the fraud recommendation cookie.

    - Encryption Key: Enter the encryption key you received from F5 support for the fraud recommendation cookie. The key must be base64 encoded.

    - Header Name to Add: Enter the header name you received from F5 support for the fraud recommendation header.

7. In the Pool Configuration section:

    - Traffic Routing Methodology: Select whether you want the iApp pool to be routed according to the Active/Active method or the Active/Passive method.

      In the Active/Active method, HTTP requests are sent based on a Round Robin method where requests are distributed evenly amongst the pool members.

      In the Active/Passive method, requests are also sent based on a Round Robin method, but only to active pool members. Active members are determined according to priority, where a lower number indicates higher priority. Active members have the same high priority. Those members continue to receive requests until all pool members become inactive. At this point, the active pool members will be the members with the next highest priority.

- Cookie Persistence for Shape Protection Pool: Select **Enable** if, after initial load-balancing, you want HTTP requests of the same session always sent to the same pool member in the Shape Protection Pool. Select **Disable** if you want the BIG-IP to perform standard load balancing.

- Shape Protection Pool: Add here the IP or FQDN for every pool member of the SAFE cluster. If you chose the Active/Passive routing method, you also need to assign a priority group number for the pool member, where a lower number means higher priority.

- Add HTTP Health Check: Choose whether to perform the HTTP Health Check on the entire pool. The HTTP Health Check is performed in intervals of 5 seconds. If you activate the health check, the following related settings are displayed:

    - Liveness Path: The path to the site where the health check will be performed on the entire pool.

    - Port: The port on which the health check is performed.

    - Response Code: Enter the code that will indicate a successful health check result in the response from the site that was checked.

8. In the Virtual Server Configuration section:

    - Application's Virtual Server(s) to Protect: Select your web application's virtual server(s).

      Note:

        - Selecting at least one virtual server is mandatory. Your iApp will not run if it is not assigned to at least one virtual server.

        - The virtual server(s) you select here must have an HTTP profile attached to it. If you select a virtual server that does not have an HTTP profile attached to it, you will not be able to complete iApp configuration.

        - Every virtual server you select here must have a default pool attached to it.

        - If you choose more than one virtual server here, they must all be the same type, either all HTTP or all HTTPS. To use virtual servers of different types, create an iApp for each type.

9. In the Advanced Features section:

   - Rewrite XFF Header with Connecting IP: Select **Yes** to add an XFF header to requests.

     Note: If an HTTP profile attached to one of the web application's virtual servers has an XFF header added to it and Rewrite XFF header with connecting IP = Yes, requests will show duplicate client IPs in the XFF headers. To avoid this situation, either remove the XFF header from the HTTP profile (see here for more details) or set Rewrite XFF header with connecting IP = No.

   - Choose a Parent Server-Side SSL Profile for Shape Pool: If you want to use an SSL profile(s) that is different from what the application pool uses, select it here.

     Note:

     - This feature cannot be used if you have 2 or more virtual servers configured for your iApp.

     - If the virtual server of your iApp does not have a server SSL profile attached to it, you must select an SSL profile here.

   - Encrypting Virtual Server IP: A default IP is assigned. If you have a virtual server already configured to this IP, assign a different IP here.

   - Server Name: The Server Name Indication (SNI) for pool members.

   - Enable Debug: Select **Yes** to enable debug logs.

10. Click **Finished**.

Disabling Strict Updates

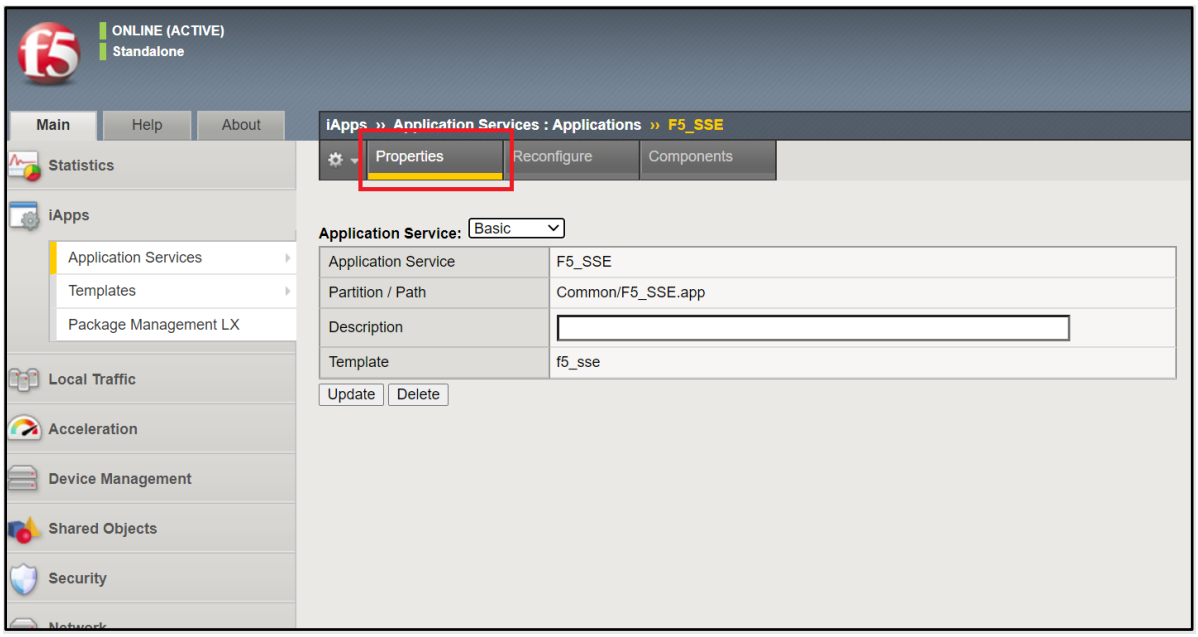
After you initially create the iApp in the BIG-IP, by default the iApp is created so that you cannot make any configuration changes to the components of the iApp, such as iRules, pool members, and pool nodes.

You can change this default setting so that you can make changes to the iApp's components as follows:

1. In the Main tab in the BIG-IP, go to **iApps>Application Services>Applications**.

2. In the iApp list, click on the iApp.

3. Click on the **Properties** tab.



4. At Application Service, select **Advanced**.

5. For Strict Updates, remove the check in the check box.

6. Click **Update**.

How to upgrade an iApp with a new template

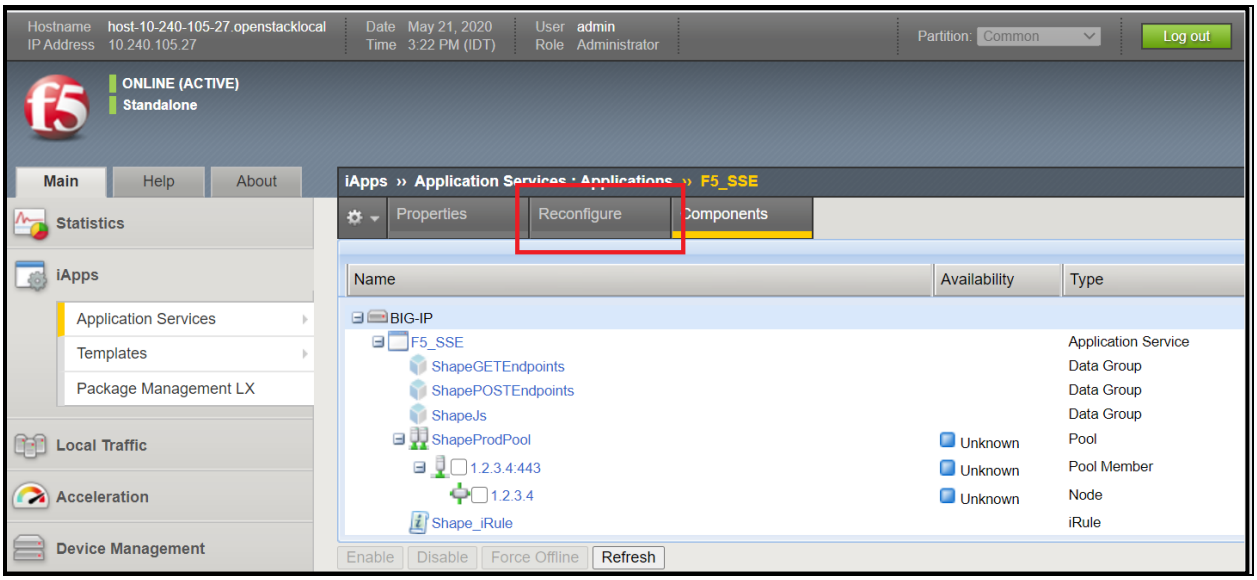
If you have an existing iApp and want to upgrade it with a new Shape SAFE iApp template, follow these instructions:

1. Import the new Shape SAFE iApp template to the BIG-IP, as explained in *Import the Shape SAFE iApp template* to the BIG-IP.

2. In the Main tab in the BIG-IP, go to **iApps>Application Services>Applications**.

3. In the iApp list, click on the iApp that you want to upgrade.

4. Click on the **Reconfigure** tab (see below).



5. Click **Change**, next to the Template setting.

6. From the drop-down template list, select the new imported template.

7. Configure the iApp according to the instructions in *Create the iApp in the BIG-IP*.

8. Click **Finished**.

How to change run-time priority for iRules

When you create the iApp, an iRule is automatically created on every virtual server protected by the iApp. If the virtual server has other iRules running on it that are not related to SAFE configuration, by default the SAFE iRule will run last, after all other iRules. You can change the run-time priority of the SAFE iRule so that it does not run last (or even runs first) in the following manner:

1. Go to **Local Traffic>Virtual Servers>Virtual Server List**.

2. Click on the virtual server where you want to change iRule priority.

   The Virtual Server Properties screen appears.

3. Click the **Resources** tab at the top.

4. In the iRules section, click **Manage**.

   A list of the enabled iRules and available iRules appears. In the enabled list, the order in which the iRules are listed is the run-time order. The iRule at the top of the list runs first,

the one after it runs second, and so on. If you have never changed run-time priorities before, the SAFE iRule is at the bottom of the list.

5. Click on the SAFE iRule and then click **Up** to move the iRule to the location you want in the list.

6. Click **Finished**.

How to disable an iApp

You can disable an iApp so that it is not currently active, but not permanently deleted. When disabling an iApp, its configuration is maintained and when you re-activate it all configuration settings are intact. When the iApp is disabled, HTTP requests are sent to the web application's server directly without any intervention from SAFE.

To disable an iApp:

1. In the Main tab in the BIG-IP, go to **iApps>Application Services>Applications**.

2. In the iApp list, click on the iApp that you want to disable.

3. Click on the **Reconfigure** tab.

4. In the General section, at Activate Kill-Switch select **Yes**.

5. Click **Finished**.

How to delete an iApp

To delete an iApp:

1. In the Main tab in the BIG-IP, go to **iApps>Application Services>Applications**.

2. In the iApp list, click on the iApp that you want to delete.

3. Click on the **Reconfigure** tab.

4. In the General section, at Clean Before Deletion select **Yes**.

5. Click **Finished**.

6. Go to **iApps>Application Services>Applications**.

7. In the list of iApps, select the check box next to iApp you are deleting.

8. Click **Delete**.

9. In the **Confirm** Delete screen, click **Delete** again.

   Note: If an HTML profile was attached to the virtual server prior to creating the iApp, you need to re-attach it after deleting the iApp.

Troubleshooting

1. If you receive the following error message when you click **Finish** to complete iApp configuration:

   01071912:3: HTTP_REQUEST event in rule (/Common/target_ssl_vip) requires an associated HTTP or FASTHTTP profile on the virtual-server.

   This is because you have selected a virtual server(s) that does not have an HTTP profile attached to it.

   To fix this problem, do the following:

   a. In the Main tab in the BIG-IP, go to Local Traffic>Virtual Servers>Virtual Server List.

   b. From the list of virtual servers, select the virtual server that you want your iApp to run on.

   c. In the Configuration section, for HTTP Profile (Client), select **http**.

   d. Click **Update**.

   e. Return to the iApp configuration, select your virtual server, and complete iApp configuration.

2. If you receive the following error message when you click **Finish** to complete iApp configuration:

   01071912:3: SSL::disable in rule (/Common/shape-iapp-test_Shape_iRule__Common_shop.f5se.com-http-vs) requires an associated SERVERSSL or CLIENTSSL or PERSIST profile on the virtual-server (/Common/shop.f5se.com-http-vs).

   This is because you have selected both HTTP and HTTPS virtual servers for your iApp. To fix this, you must select virtual servers of the same type, either HTTP or HTTPS.

3. If you use a FQDN in Shape protection pool and receive the following error message when you perform **Clean before deletion**:

01070110:3: Node address '/Common/_auto_34.95.74.240' is referenced by a member of pool '/Common/sse_ShapeProdPool'.

You need to delete the node mentioned in the error message. Go to **Local Traffic>Nodes>Node List**, delete the node from the list, and then perform **Clean Before Deletion** again.

4. If you see duplicate IPs in the XFF header, this is because the XFF injection is enabled in both the HTTP profile and in the iApp. To disable the injection in the HTTP profile, do the following:

    a. In the Main tab in the BIG-IP, go to Local Traffic>Profiles>Services>HTTP.

    b. Select the HTTP profile that you use for your web application.

    c. At Insert X-Forwarded-For choose **Disabled**.

    d. Click **Update**.

    You can also fix this issue by setting Rewrite XFF header with Connecting IP = No.

5. If you receive the following error message when you click **Finish** to complete iApp configuration:

    01070333:3: Virtual Server /Common/<IAPP_NAME>_ssl_vs illegally shares destination address, source address, service port, ip-protocol, and vlan with Virtual Server /Common/<IAPP_NAME>_ssl_vs.

    You need to change the Encrypting Virtual Server IP.

Known Issues

1. **GUI limitation for settings with multiple entries:** There is a GUI limitation for the following settings that allow multiple entries:

    - JS Injection path when Inject Shape JS in Specific Webpages Only=**Yes**
    - JS Excluded path when Exclude Shape JS Injection from Specific Webpages=**Yes**.
    - Endpoints
    - Shape Protection Pool

    For all the settings listed above, if you delete an entry that is not at the bottom of the list you must click **Finished** before adding a new entry.

Legal Notices

Publication Number

MAN-0801-00

Copyright

Trademarks

Patents