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

Shape SSE API iApp Template Version 1.0.1

September 22, 2020

Document Version 1.0.0

Table of Contents

Objective

This document is for F5 technical support staff specializing in SSE API deployment, to enable use of the security features of the BIG-IP together with the SSE.

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 SSE API iApp Template in the BIG-IP System

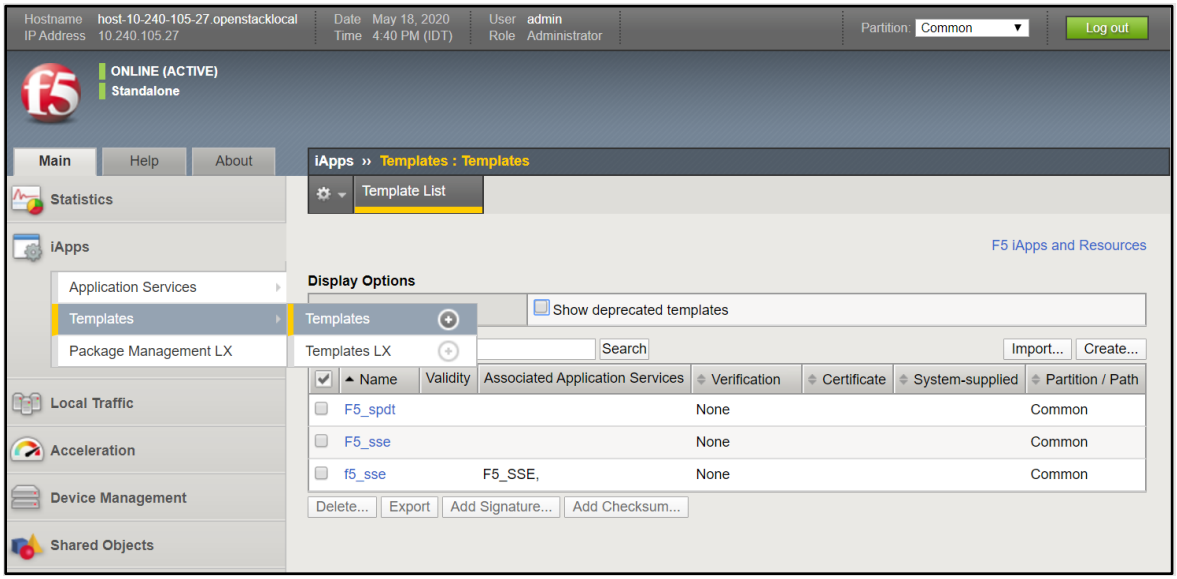
You deploy an iApp in the BIG-IP in two stages:

1. Import the Shape SSE API 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 SSE API iApp template to the BIG-IP

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



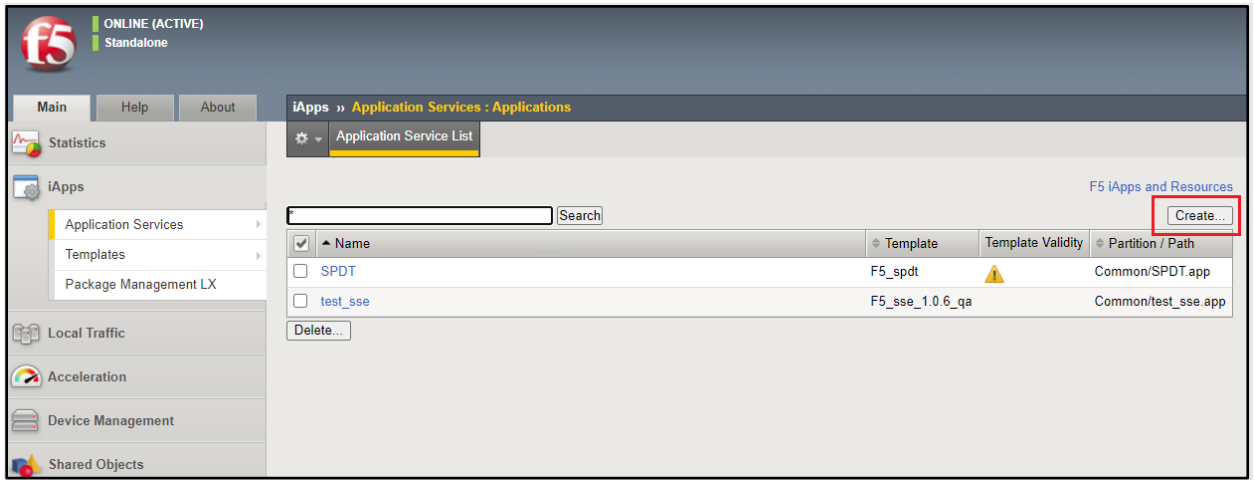
2. Click **Import**.

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

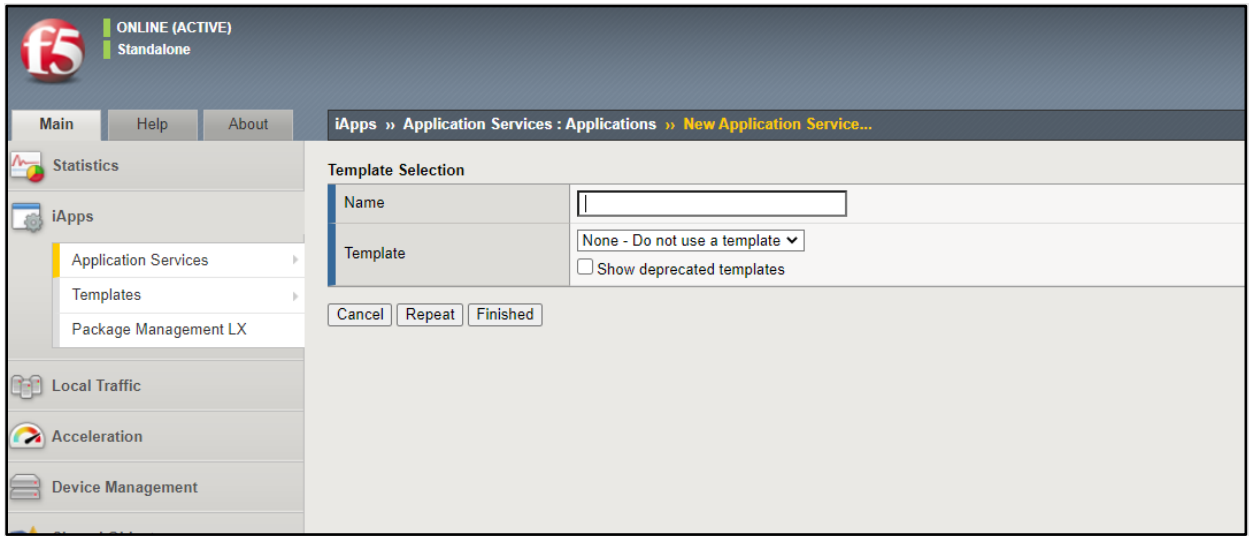
   The Shape SSE API iApp template is now displayed in the list of templates.

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**.

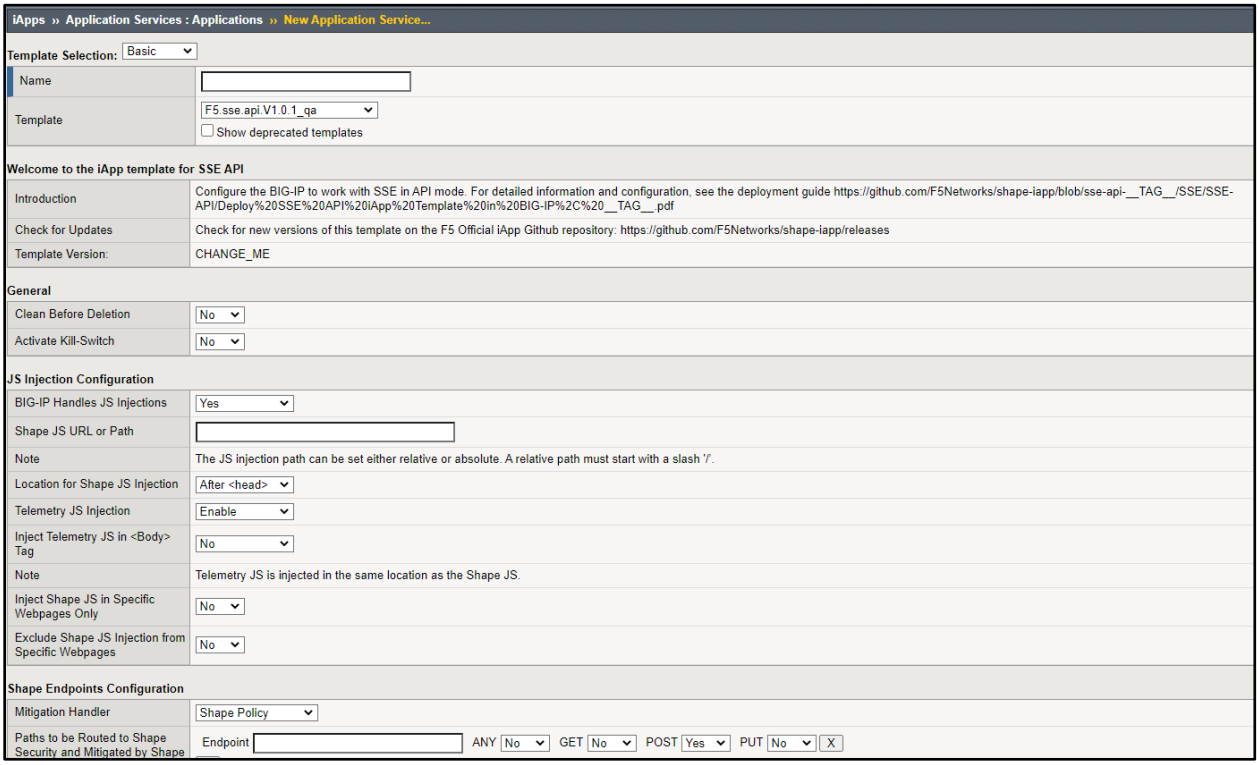


   The New Application Service screen appears.



3. Assign a name to the iApp.
4. From the Template list, select the template that you imported.

The Shape SSE API 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 his 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**.

- Telemetry JS injection: When enabled, the BIG-IP injects Telemetry JS in the HTML code of your webpage.

  Note: When this setting is disabled, the client request may be blocked by Shape Policy.

- Inject Telemetry JS in <Body> tag: Select **Yes** to inject the Telemetry JS in the <body> tag in the HTML code of your webpage.

  Note:

  - If **No** is selected, the Telemetry JS is injected in the same location as the Shape JS.
  - This setting is not displayed if Telemetry JS Injection is disabled.

- Inject Shape JS in Specific Webpages Only: Select **Yes** if you want to inject the Shape JS (and Telemetry JS if enabled) in specific web pages of your web application. Select **No** to inject the Shape JS (and Telemetry JS if enabled) 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 you set **Inject Shape JS in specific webpages only** = Yes, enter here the paths of the webpages in your application to receive the Shape JS (and Telemetry JS if enabled) injections.

- Exclude Shape JS Injection from Specific Webpages: Select **Yes** if you want to exclude the Shape JS injection (and Telemetry JS if enabled) 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 where the Shape JS (and Telemetry JS if enabled) injections should be excluded.

6. In the Shape Endpoints Configuration section:

- Mitigation Handler: Choose whether you want the iApp or Shape Policy to handle mitigation of malicious HTTP requests.
- Paths to be routed to Shape Security: Use these settings to configure which pages on the website will be protected by SSE.
  - Endpoint: Enter here the path to the web page you want to be protected by SSE. For example, **/login**.

    Note: The path must be lowercase letters only and start with '/'.
  - ANY: Set this to Yes if you want the path to be protected with any type of method. Set it to No if you want to limit protection to only a certain method(s).
  - GET: Set this to Yes if you want the path protected when it has a GET method.
  - POST: Set this to Yes if you want the path protected when it has a POST method.
  - PUT: Set this to Yes if you want the path protected when it has a PUT method.

    Note: You must set at least one of the methods above (or ANY) to **Yes**. HTTP requests will not be routed if nothing is set to **Yes**.
  - Mitigation Action: If you choose iApp for the Mitigation handler, choose from one of the following mitigation actions you want the iApp to take if a malicious HTTP request is detected on the endpoint:
    - **Continue:** Allow the HTTP request to continue to the web page.
    - **Redirect:** Redirect the HTTP request to a different web page that you define.

- **Block:** Block the HTTP request from accessing the web page.
- **Drop:** Drop the HTTP request.

Note: Mitigation Actions are displayed only if you set Mitigation Handler to iApp.

- Add: Click to add another path.

7. In the Define Mitigation Actions section:

- Redirect Path: Enter here the path where you want the HTTP request redirected. The path you enter can be either relative or absolute. If absolute, it must contain the protocol, either http or https. If relative, it must start with '/'.

  Entering Redirect Path is mandatory if you select **Shape Policy** for the Mitigation Handler. If you select **iApp** for the Mitigation Handler, it is mandatory only if you assigned **Redirect** as the Mitigation Action for at least one endpoint.

- Block Data: Select the Response Code that will appear on the blocking page and enter the HTML code you want for the Response Body in the blocking page.

  Note: The size of the Response Body should not exceed 30 KB.

  Entering Block Data is mandatory if you select **Shape Policy** for the Mitigation Handler. If you select **iApp** for the Mitigation Handler, it is mandatory only if you assigned **Block** as the Mitigation Action for at least one endpoint.

- Bot Header Name to Origin (optional): Add here a header name that indicates the HTTP request is considered malicious but allowed to continue to the web page. This setting is optional, if empty no header is added to the request.

  Note: This setting appears only if you select **iApp** for the Mitigation Handler.

8. In the Allow Criteria section:

- Allow IP addresses: Enter here IP addresses that do not need to be checked by the SSE.
- Allow Headers: Enter here the names and values for headers in the HTTP requests that does not need to be checked by the SSE.

9. 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 SSE 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.

10. In the API Request Settings section:
    - For API Hostname, API Key, and Telemetry Header Prefix: Enter the values for these settings provided to you by F5 Support.
    - Timeout Value for API Response: Set the length of time (in milliseconds) that the BIG-IP should wait to receive a response from the SSE after the BIG-IP sends the API request to the SSE. If the BIG-IP does not receive a response from the SSE after this time period, the BIG-IP sends the original API request back to the original server.
11. 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, it is not possible to have a virtual sever with a client SSL profile attached to it and another virtual server without a client SSL profile. Either all virtual severs must have client SSL profiles attached or none of them can have client SSL profiles attached. If you want to use a combination of virtual servers, some with the client SSL profile and some without, create one iApp for virtual servers with the client SSL profile and another one for virtual servers without the client SSL profile.
- For every virtual server you select here, if prior to creating the iApp the virtual server did not have a persistence profile attached to it and you enable Cookie Persistence for Shape Protection Pool, when deleting the iApp the persistence profile must be removed manually from the virtual server.

12. In the Advanced Features section:

- Enable TLS fingerprint: Select **Yes** to send API requests to the SSE with a TLS fingerprint.
- 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, remove the XFF header from the HTTP profile (see here for more details).
- Add Server-Side SSL Profile for Shape Pool: If you want to use a server-side 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.

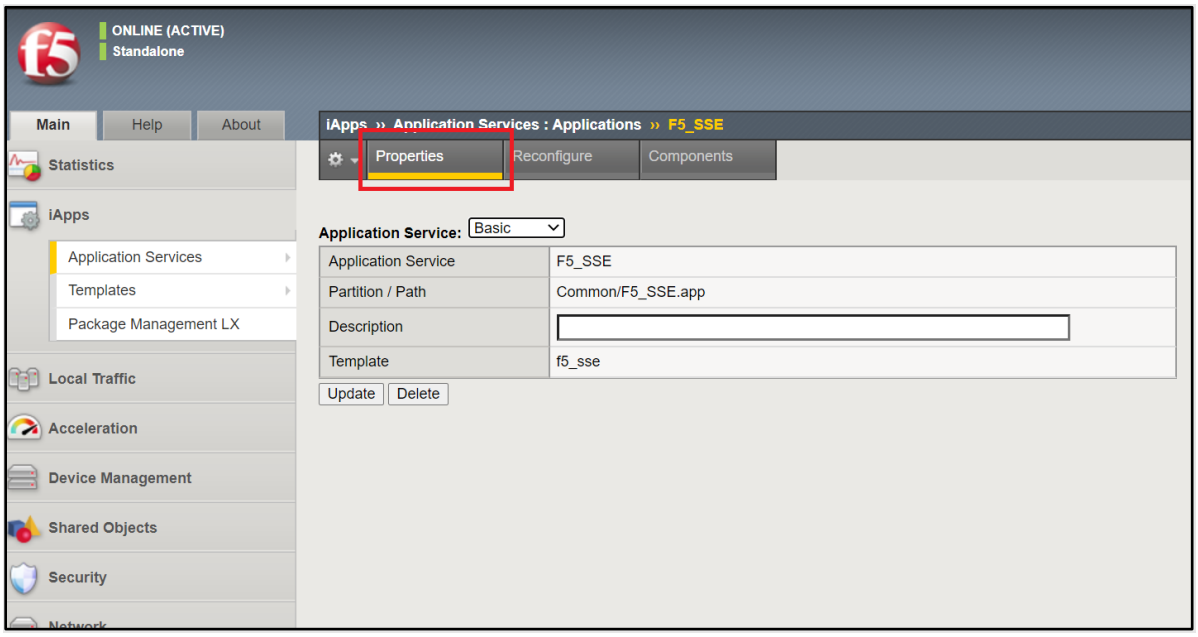
13. Click **Finished**.

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.

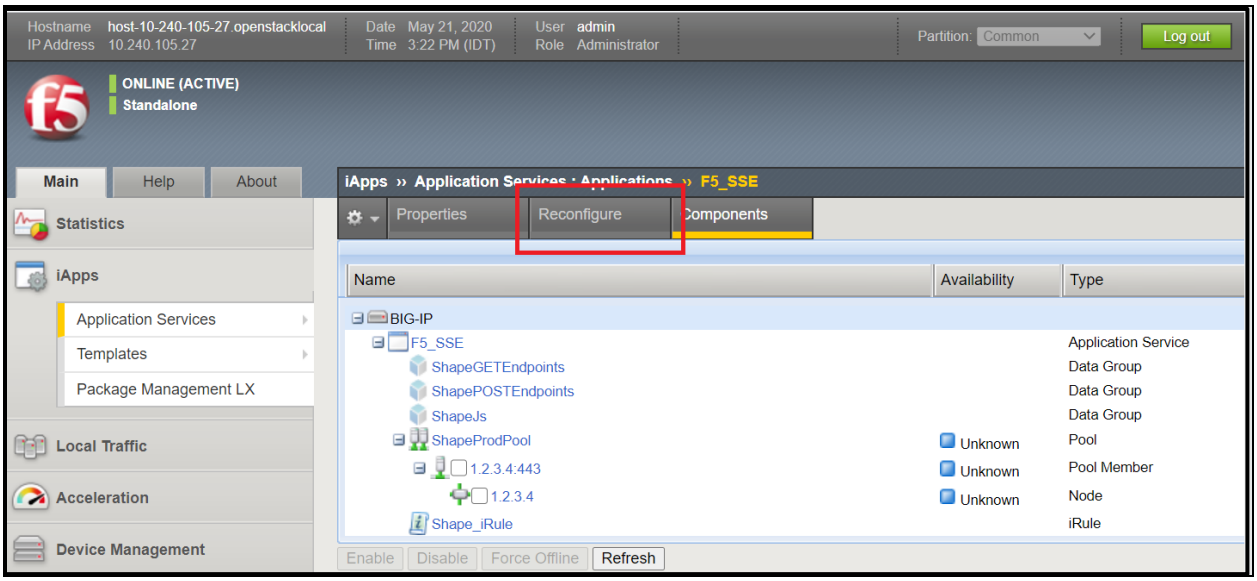


4. At Application Service, select **Advanced**.
5. For Strict Updates, remove the check in the check box.
6. Click **Update**.

How to upgrade an iApp with a new template

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

1. Import the new template to the BIG-IP, as explained in *Import the Shape SSE API 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 SSE configuration, by default the SSE iRule will run last, after all other iRules. You can change the run-time priority of the SSE 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 SSE iRule is at the bottom of the list.

5. Click on the SSE 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 the SSE.

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, prior to creating the iApp, an HTML profile was attached to one or more virtual servers protected by the iApp, you need to re-attach it to the virtual server after deleting the iApp.
   - For every virtual server protected by the iApp, if prior to creating the iApp the virtual server did not have a persistence profile attached to it and you enable Cookie Persistence for Shape Protection Pool, when deleting the iApp the persistence profile must be removed manually from the virtual server.

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**.

5. If you use a FQDN in Shape Protection Pool, and then try to replace that with one of the FQDN's resolved IPs, you might get one of the following errors:

   01071c39:3: Modify of ephemeral pool member (pool /Common/SAFE_ShapeProdPool member /Common/216.239.32.21) is not permitted.

   or:

   0107003a:3: Pool member node (/Common/216.239.34.21) and existing node (/Common/_auto_216.239.34.21) cannot use the same IP Address (216.239.34.21).

   You can resolve the error as follows:

   a. Remove the FQDN from the Shape Protection Pool table.

   b. Click **Finish**.

   c. Click **Reconfigure**.

   d. Add the desired IP to the Shape Protection Pool table.

   e. Click **Finish**.

Known Issues

1. For Shape Endpoints Configuration, if at least one method or ANY is not selected, the endpoint path will not receive SSE protection. When completing iApp configuration (i.e., you click **Finished** to complete configuration), there is no system validation to determine whether at least one method or ANY was selected and no error message will appear if a method or ANY is not selected.
2. **GUI limitation for settings with multiple entries:** There is a GUI limitation for the following settings that allow multiple entries:
    - JS Injection Paths (when Inject Shape JS in Specific Webpages Only = Yes)
    - JS Excluded Paths (when Exclude Shape JS injection from specific webpages = Yes).
    - Paths to be Routed to Shape Security (in Shape Endpoints Configuration)
    - Allow IP Addresses
    - Allow Headers
    - 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-0799-01

Copyright

Trademarks

Patents