

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

SSE iApp Template Version 1.0.0

July 16, 2020, Document Version 1.0.0



## Table of Contents

Prerequisites .....	1
Deploying the SSE iApp Template in the BIG-IP System .....	1
Import the SSE iApp template to the BIG-IP .....	1
Create the iApp in the BIG-IP .....	2
Disabling Strict Updates .....	6
How to upgrade an iApp with a new template .....	6
How to delete an iApp .....	7
Troubleshooting .....	8
Known Issues .....	9
Legal Notices .....	10

## 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 SSE iApp Template in the BIG-IP System

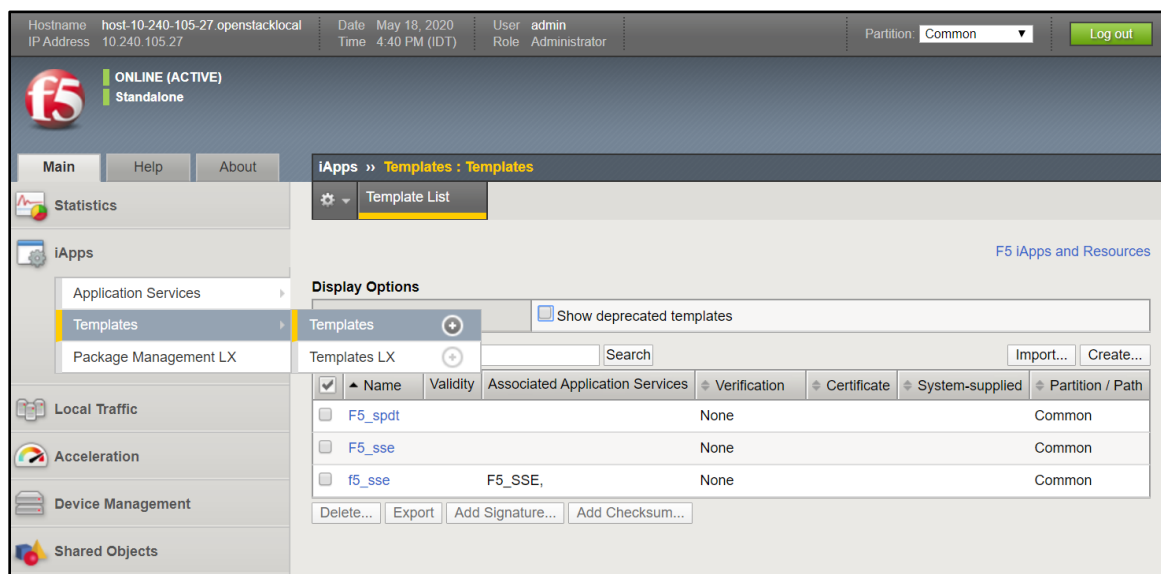
You deploy an iApp in the BIG-IP in two stages:

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

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

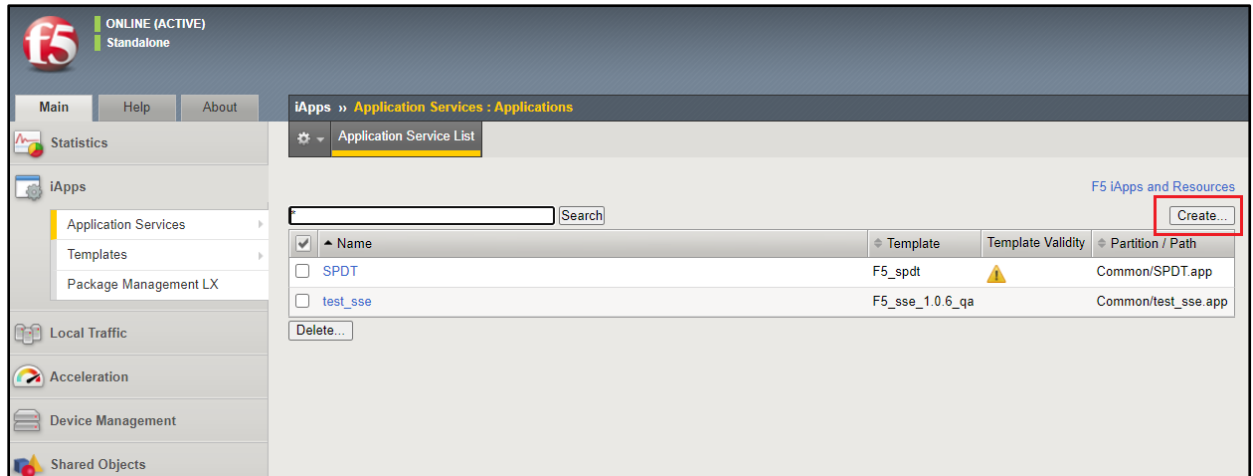


2. Click **Import**.
3. Click Choose File.
4. Select the SSE iApp template (version 1.0.0) provided to you from F5.
5. Click the check box next to Overwrite Existing Templates.
6. Click **Upload**.

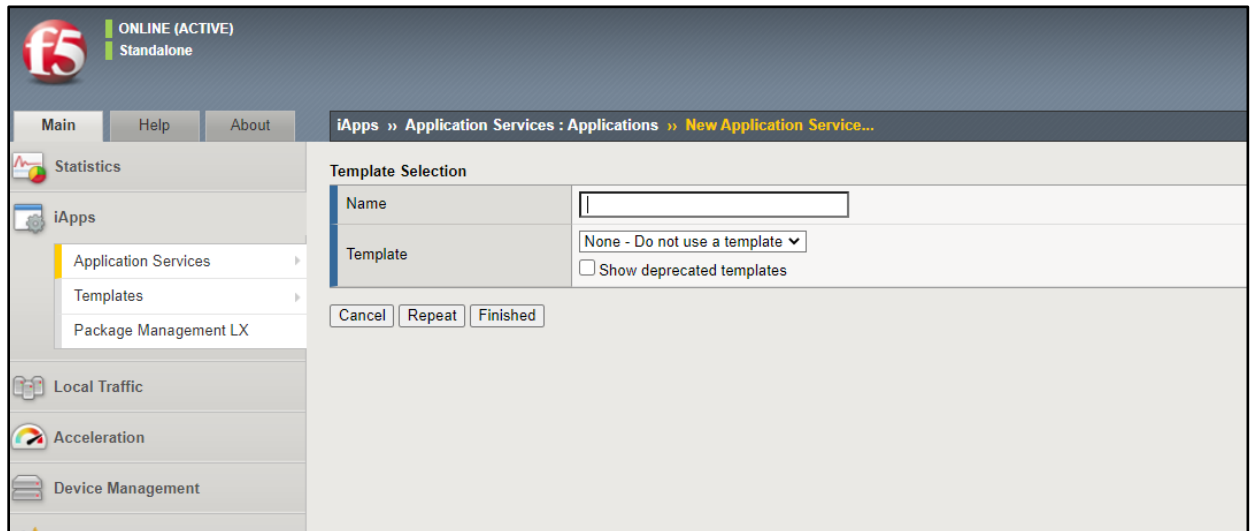
The SSE iApp template is now displayed in the list of templates.

## 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 SSE iApp template.

The SSE iApp template configuration settings appear.

IApps » Application Services : Applications » New Application Service...

Template Selection: Basic

Name:

Template: SSE

**General**

Clean Before Deletion: No

**JS Injection Configuration**

Shape JS Injection: Enable

Shape JS URL or Path:

Note: The injection path can be set either relative or absolute

Location for Shape JS Injection: After <head>

Async JS Injection: Enable

Inject Telemetry JS in <Body> tag: No

Note: Telemetry JS is injected in the same location as the Shape JS.

Inject Shape JS in specific webpages only: Yes

Entry page paths: Path

**Shape Endpoints Configuration**

Paths to be routed to Shape Security: Endpoint  ANY No GET No POST No PUT No

**Pool Configuration**

5. In the JS Injection Configuration section:

- Shape JS Injection: Enabled by default. If this setting is disabled, the Shape Security Solution cannot be implemented on your iApp.
- Shape JS URL or Path: Enter the path you received from F5 support for the Shape JS injection.
- 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.
- Async JS Injection: When enabled, the BIG-IP injects Async JS in the HTML code of your webpage.
- Inject Telemetry JS in <Body> tag: Select Yes to inject the Async JS in the <body> tag in the HTML code of your webpage.

**Note:** If No is selected, the Async JS is injected in the same location as the Shape JS.

- Inject Shape JS in specific webpages only: Select **Yes** if you want to inject the Shape JS (and Async JS if enabled) in specific webpages of your web application. Select **No** to inject the Shape JS (and Async JS if enabled) in all web pages of your web application.
- Entry Page 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 Async JS if enabled) injections.

6. In the Shape Endpoints Configuration section:

- **Paths to be routed to Shape Security:** Use these settings to configure which pages in 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**.

- **Add:** Click to add another path.

#### 7. In the Pool Configuration section:

- **Shape outbound IPs:** Enter here the IPs of the SSE cluster that are used to send requests to the BIG-IP. These IPs should be provided to you from F5 support.

**Note:** Enter here only valid IPs or IPs with a subnet range. If you enter an invalid IP, an error message will appear in the BIG-IP when you click **Finished**.

- **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.

- **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.

8. In the Virtual Server Configuration section:

- Application's virtual server(s) to protect: Select the virtual server(s) that your iApp runs on.

**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. If you want 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.
- Add different server 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.

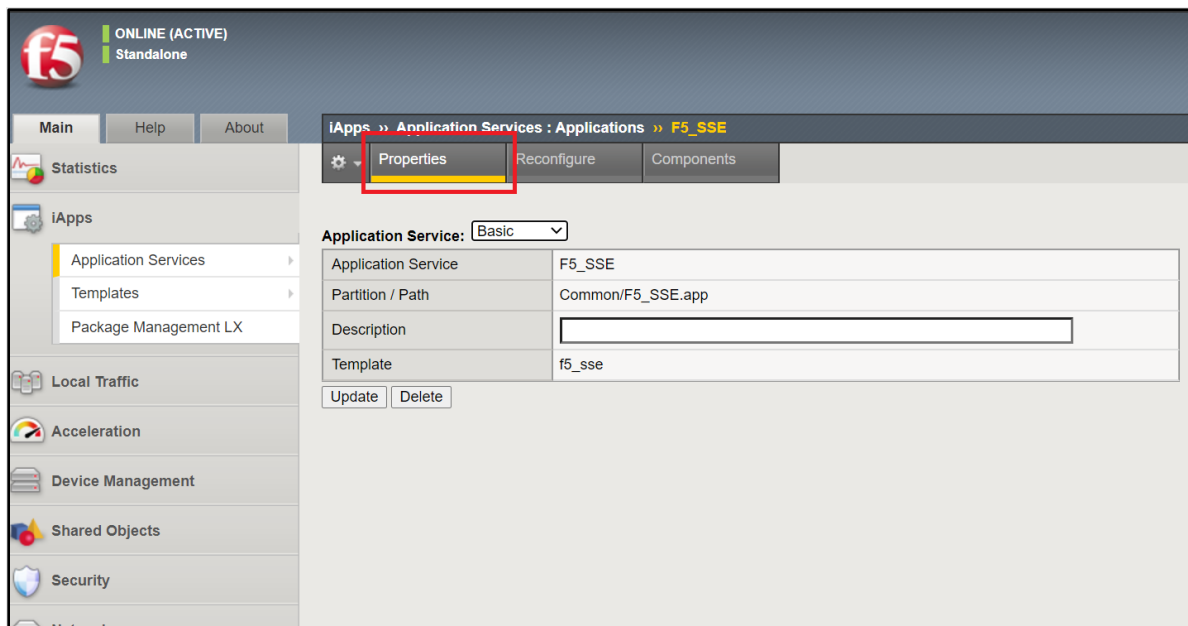
10. Click **Finished**.

## 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**.

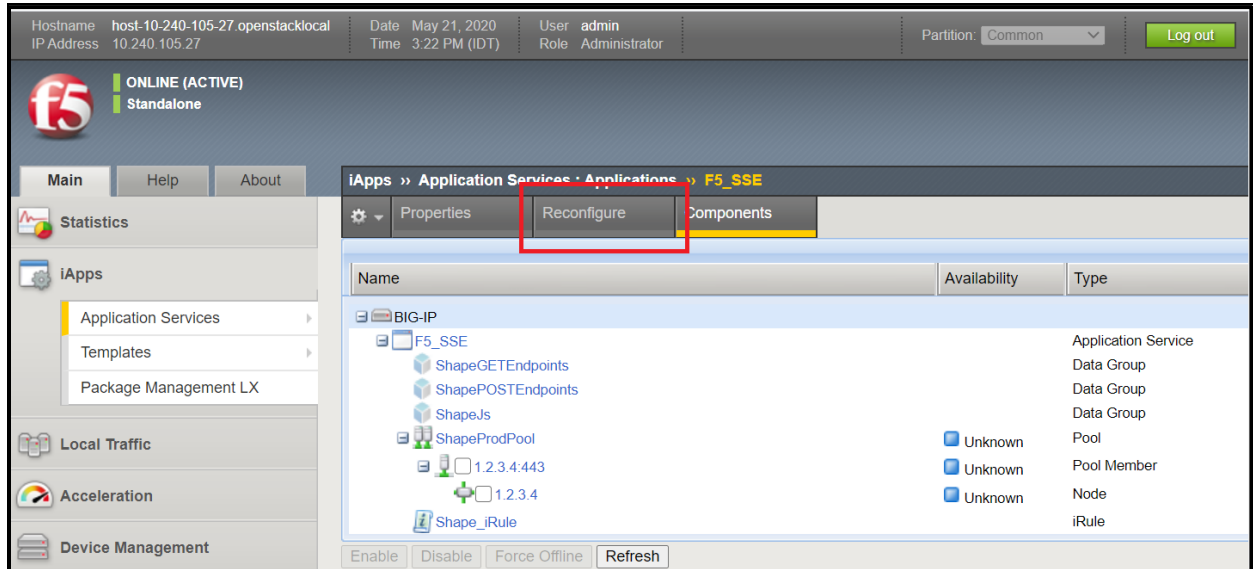
## How to upgrade an iApp with a new template

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

1. Import the new SSE iApp template to the BIG-IP, as explained in [Import the SSE 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 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.

## Known Issues

### 1. Known issues regarding 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.
- If you delete an endpoint that is not at the bottom of the list, you must click **Finished** before adding a new endpoint.

### 2. If you are using a custom persistence cookie, refer to this article:

<https://support.f5.com/csp/article/K9815> to avoid a situation where the BIG-IP system overwrites the custom persistence cookie.

## Legal Notices

### **Publication Number**

MAN-0798-00

### **Copyright**

Copyright © 2020, F5 Networks, Inc. All rights reserved.

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>