Prerequisites

Before deploying or upgrading an SSE iApp in the BIG-IP, 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 attached to it.

How to deploy an SSE iApp in the BIG-IP

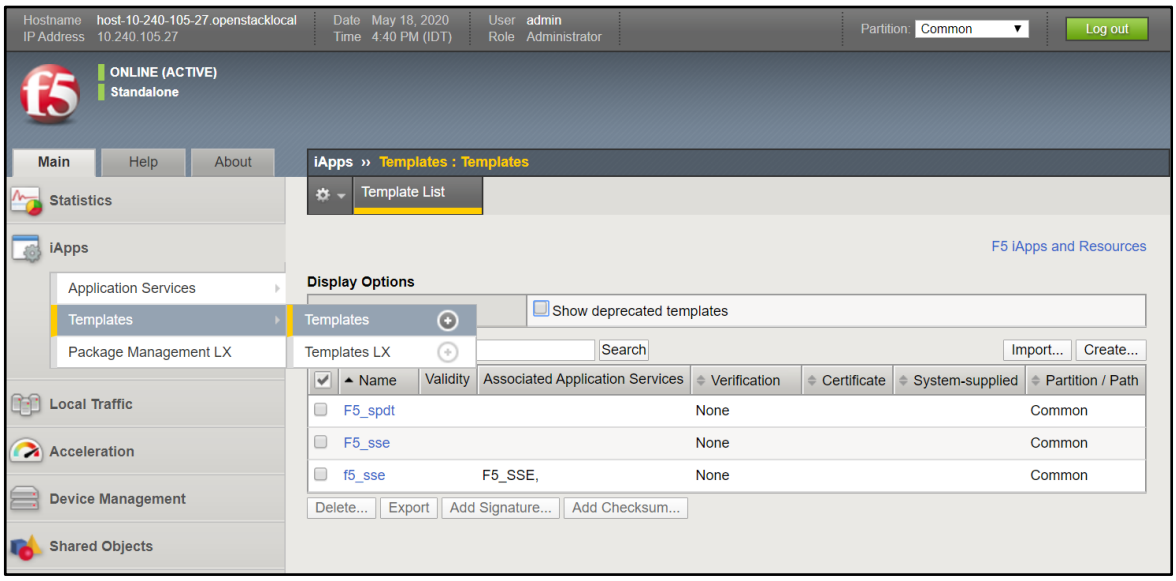
You deploy an SSE iApp in the BIG-IP in two stages:

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 template you imported.

The steps for performing these two stages are described below.

Import the template to the BIG-IP

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



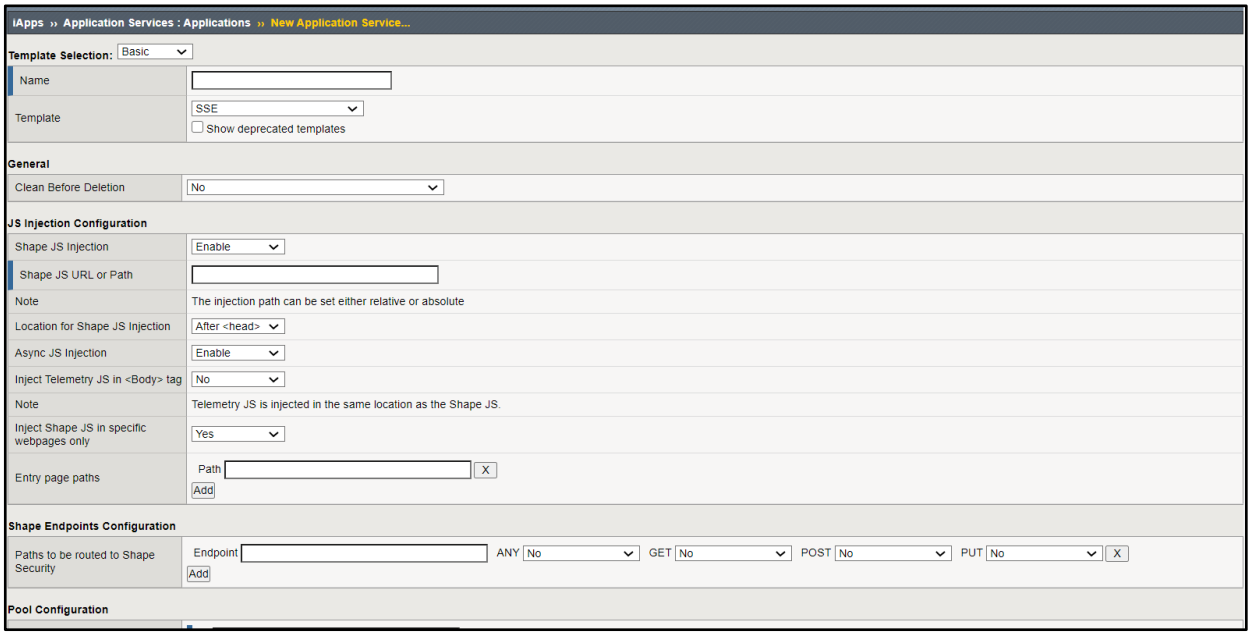
2. Click **Import**.
3. Click **Choose File**.
4. Select the template file provided to you from F5.
5. Click the check box next to Overwrite Existing Templates.
6. Click **Upload**.

The F5 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.
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 webpages 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 sites will be protected by SSE.
        - Endpoint: Enter here the path to the site you want to be protected by SSE.

          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 (i.e., GET, POST, or PUT). 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.
        - 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 request 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 sent to the highest priority group members and those members continue to receive requests until all group members become inactive. At this point, requests are then sent to the next highest priority group members.
    - 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.
    - Add HTTP Health Check: Choose whether to perform the HTTP Health Check on pool members. The HTTP Health Check is performed in intervals of 5 seconds. If you activate the health check, the following settings related settings are displayed:

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

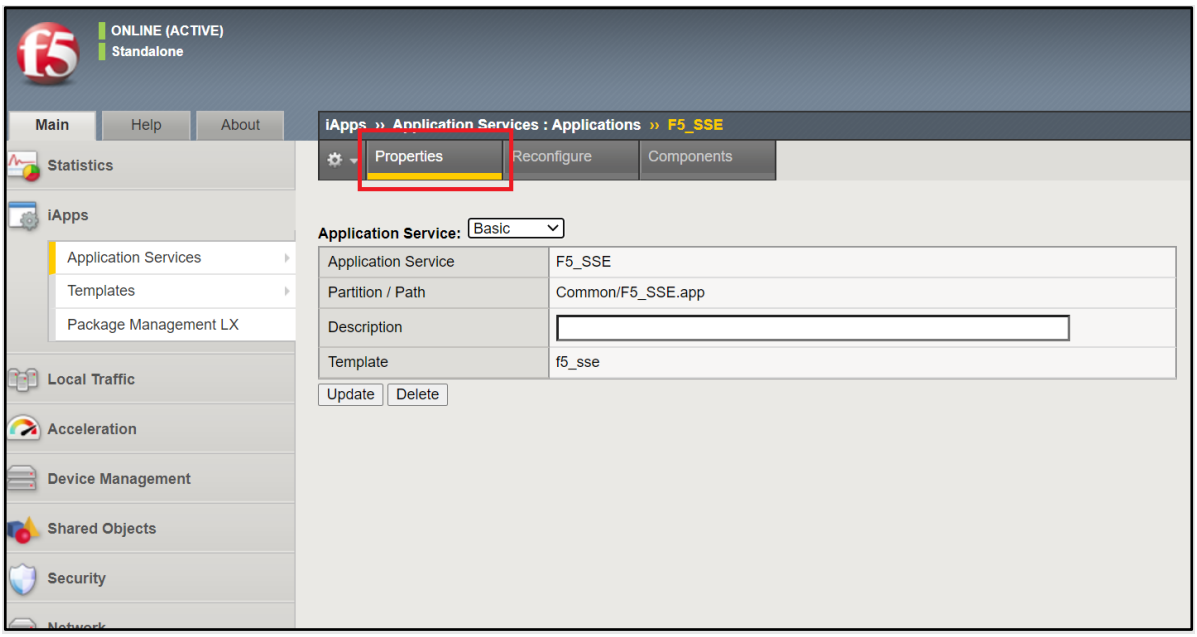
8. In the Virtual Server Configuration section:
   - Application's virtual server(s) to protect: Select the virtual server(s) that your iApp runs on.
9. In the Advanced Features section:
   - Rewrite XFF header with Connecting IP: Select **Yes** to add an XFF header to requests.
   - Add different server SSL profile for Shape pool: If you want to a use SSL profile(s) that are different from what the application pool uses, select them 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.

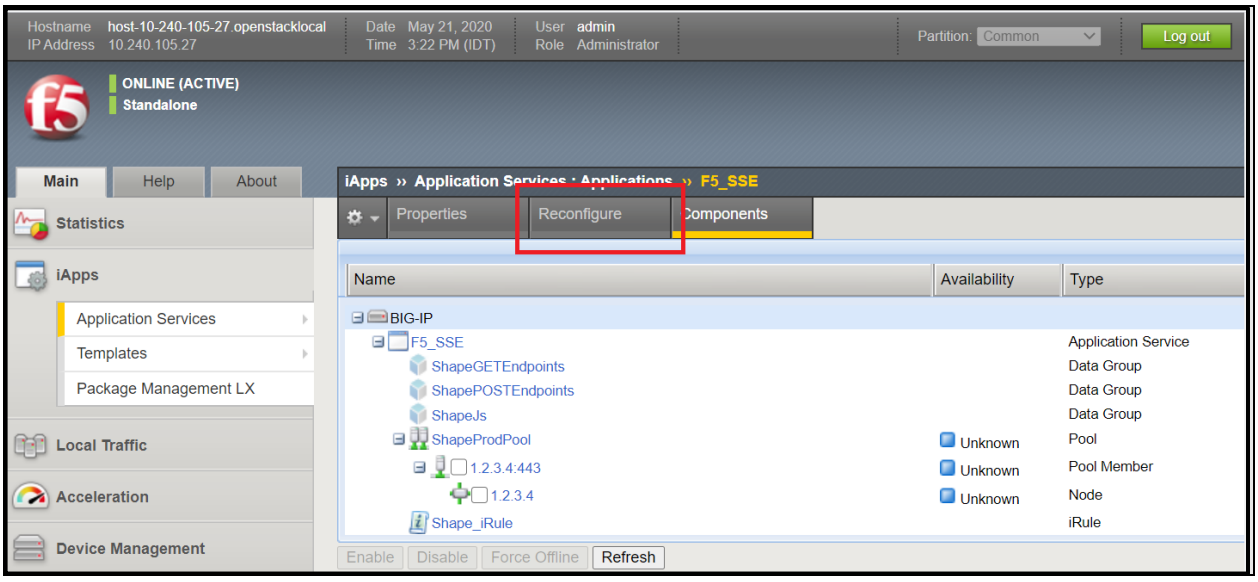


4. At Application Service, select **Advanced**.
5. For Strict Updates, remove the check in the check box.
6. Click **Update**.

How to upgrade an iApp with a new template

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

1. Import the new template to the BIG-IP, as explained in *Import the 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 template that you imported.
7. Configure the iApp according to the instructions in *Create the iApp in the BIG-IP*.
8. Click **Finished**.

How to delete an SSE iApp

To delete an SSE 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 upgrade.
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.