The F5 and Okta Solution for High Security SSO

July 2017
Introduction

When an organization needs high security but has a low risk tolerance, it may wish to keep all aspects of user authentication on the premises. Okta and F5® BIG-IP® Access Policy Manager® (APM) may be configured to meet this requirement and provide the flexibility and power of the Okta cloud in combination with secure traffic management and on-premises, single sign-on (SSO) authentication provided by F5 BIG-IP products.

The Integrated Solution

F5 BIG-IP APM serves as the SAML identity provider (IdP). Okta serves as a SAML service provider to BIG-IP APM but plays the role of SAML IdP to cloud applications. (See Figure 1.)

This topology provides the following key features:

- BIG-IP APM handles authentication of users behind the firewall. More importantly, user credentials stay on-premises at all times. As shown in Figure 1 above, credentials are stored in the directory services, which can be any corporate Active Directory or LDAP.
- A simple integration bridges Okta as a SAML service provider for BIG-IP APM.
Okta provides pre-integrated solutions to over 5,000 applications through the Okta Application Network for SSO.

The user experience can be easily configured to achieve a UI flow that is BIG-IP APM centric or Okta centric, depending on your needs.

Prerequisites

The configuration procedures here assume that you have:

- A physical or virtual BIG-IP platform with BIG-IP APM licensed.
- An Okta org with SSO.
- One or more applications (service providers) capable of SAML authentication.
- An available IP/port for BIG-IP APM (for example, TCP/443 for HTTPS).
- A DNS entry pointing to an IP address hosted on or directed via NAT to BIG-IP APM.
- A corresponding SSL certificate if you will be using HTTPS.

Configuration

Note: This document does not cover the setup steps required to configure downstream applications such as Salesforce, Office 365, or Box but will refer to them as examples.

Set up BIG-IP APM to be a SAML IdP

This setup includes creating a self-signed certificate, exporting it to save it locally, and configuring the SAML local IdP services.

Create a self-signed certificate for signing SAML assertions

RECOMMENDED DEPLOYMENT PRACTICES
The F5 and Okta Solution for High Security SSO

Figure 2: Starting the process of creating a self-signed certificate

2. Click **Create**.

3. Enter a **Name** that is appropriate and unique.

4. For **Issuer**, select **Self**.

5. For **Key Type**, select **RSA**.

6. For **Key Size**, select **2048**.

7. Provide relevant and suitable values for the remaining configuration fields as desired. (See Figure 3.)
RECOMMENDED DEPLOYMENT PRACTICES
The F5 and Okta Solution for High Security SSO

8. Click **Finished**. The new certificate appears (see Figure 4), and you are now ready to export the certificate using the next procedure.

**Export the self-signed certificate**

1. After creating a self-signed SSL certificate, click the **Name** of the newly created certificate in the **SSL Certificate List**.

2. When the certificate properties display, click **Export**....
**RECOMMENDED DEPLOYMENT PRACTICES**

The F5 and Okta Solution for High Security SSO

---

### Figure 5: Preparing to export the certificate

<table>
<thead>
<tr>
<th>General Properties</th>
<th>Certificate Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Public Key Type</td>
</tr>
<tr>
<td>F5 as IdP Signing Certificate.crt</td>
<td>RSA</td>
</tr>
<tr>
<td>Partition / Path</td>
<td>Public Key Size</td>
</tr>
<tr>
<td>Common</td>
<td>2048 bits</td>
</tr>
<tr>
<td>Certificate Subject(s)</td>
<td>Expires</td>
</tr>
<tr>
<td>F5 BIG-IP APM as IdP, Your Company</td>
<td>May 29 2027 21:18:41 GMT</td>
</tr>
<tr>
<td></td>
<td>Version</td>
</tr>
<tr>
<td></td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Serial Number</td>
</tr>
<tr>
<td></td>
<td>233932721</td>
</tr>
<tr>
<td>Subject</td>
<td>Common Name</td>
</tr>
<tr>
<td></td>
<td>F5 BIG-IP APM as IdP</td>
</tr>
<tr>
<td>Organization</td>
<td>Your Company</td>
</tr>
<tr>
<td>Division</td>
<td>Authentication</td>
</tr>
<tr>
<td>Locality</td>
<td>Seattle</td>
</tr>
<tr>
<td>State Or Province</td>
<td>Washington</td>
</tr>
<tr>
<td>Country</td>
<td>US</td>
</tr>
</tbody>
</table>

**Issuer**

Self

**Email**

**Subject Alternative Name**

---

#### Certificate Export

<table>
<thead>
<tr>
<th>Certificate Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>AwEAAATANBgkqhkiG9w0BAQsFAAOCAQEAAB1gX5A2L1HKKIIAsWeABhY3X1mE6QZuCS7UyuJUP6g6QcPfo6hBcLzrM066Ew17d6IrM59tYBS9v9cZcR3JnEeXHc9b1HkygH12Qh1Jl9Ly4vZvQ3ivioVRE+iTIPwz61zrF2VAzgKCSOJzmCxBc86fLevP3vexo2eL0bcfDfJAI1I7pxU901I2ZhiJ8R.</td>
</tr>
</tbody>
</table>

**Certificate File**

Download F5_as_IdP_Signing_Certificate.crt

---


---

4. Make note of the saved file location for use later when adding an identity provider in the procedure called **Set up Okta org to accept BIG-IP APM as an IdP**.
Configure SAML local IdP services

1. In the BIG-IP APM configuration utility, navigate to Access > Federation > SAML Identity Provider > Local IdP Services.
2. Click Create in the Local IdP Services section.
3. Under General Settings, create an IdP service. Start by entering an IdP Service Name, using a descriptive and unique name for the IdP service on BIG-IP APM.

![General settings for the IdP service](image)

4. Enter an IdP Entity ID, which should be created so that it will be a globally unique identifier for the BIG-IP APM system as it will be processed by downstream service providers. Generally, this is accomplished by configuring the IdP Entity ID as if it were a URI. This is a good practice, but it should not be confused as a valid/accessible web resource. We suggest <scheme>://<hostname:port>/<IdP Service Name>. For example:
   - https://tmf5.oktaprise.com:8443/F5_Big-IP_APM_as_IdP
   - https://host.domain.tld/IdP_Service_Name
5. Select a Scheme value and enter a Host name appropriate for your configuration. The Scheme and Host values are used to populate endpoint values in the metadata. These values must align with the scheme and hostname that will be associated with the virtual server (inclusive of port if not the default port associated with the scheme—80 for HTTP and 443 for HTTPS—for the values in the metadata to be valid. Scheme and host values can be updated after initial creation.
6. Optionally, enter a Description of this service.
7. Select the desired Log Level.
8. Click SAML Profiles, and select Web Browser SSO. Make sure that no other options under SAML Profiles are selected.
RECOMMENDED DEPLOYMENT PRACTICES
The F5 and Okta Solution for High Security SSO

Figure 8: SAML settings for the IdP service

9. Click **Endpoint Settings**, and ensure that no value is selected under **Artifact Resolution Service**.

Figure 9: Endpoint settings for the IdP service

10. Click **Assertion Settings**. Under **Assertion Subject Type**, select **Unspecified**.

Figure 10: Assertion settings for the IdP service

11. Select an **Assertion Subject Value**, which must align with an Okta account username or email. Okta supports transformation of the subject value using the **Okta Expression Language (OEL)**, which can append a domain name to a bare/unqualified username. This step relates to your configuration of the **Authentication Settings** in the later procedure called **Set up Okta org to use BIG-IP APM as an IdP**.

   - **Local Auth**
     - %{session.logon.last.username}
   - **AD Auth**
     - %{session.ad.last.attr.userPrincipalName}
     - %{session.ad.last.attr.sAMAccountName}
12. For Authentication Context Class Reference, select

13. Enter an Assertion Validity of 600.

14. Ensure that Encryption of Subject is not selected.

15. (Optional.) Click SAML Attributes. In this sample configuration, there is no need for additional attributes in the assertion. If you wanted to perform just-in-time (JIT) user provisioning from SAML assertions in the subordinate Okta org, you would need to add the required attributes from the authoritative source here. Otherwise, you can skip this step.

   Figure 11: SAML attributes, which in this scenario are used only if you want to perform JIT user provisioning from SAML assertions

16. Click Security Settings and select the Signing Key and Signing Certificate you created previously.

   Figure 12: Security settings

17. Click OK. The newly created local IdP service will display in the list.

   Figure 13: The new local IdP service
Set up the Okta org to accept BIG-IP APM as an IdP

This procedure adds an identity provider in the Okta org.

1. From the Okta Admin Console, navigate to Security > Identity Providers, and click Add Identity Provider.

2. Under General Settings, enter a unique and descriptive Name for this identity provider.

![Figure 14A: Adding an identity provider](image)

3. Under Authentication Settings, select an IdP Username that takes into consideration the values you provided in the SAML assertion settings when you Configure SAML local IdP services earlier. The example shown in Figure 14B appends a static value to the name provided, turning username into `username@oktaprise.com: idpuser.subjectNameld + "@oktaprise.com"`. 
4. If required, for Filter, select Only allow usernames that match defined RegEx Pattern. (No filter is required in the example in Figure 14B.)

5. For Match against, select a value to match your environment based on the value being delivered in the SAML assertion. The objective is to accurately and unambiguously identify the user in the Okta org based on the value delivered in the assertion. The solution is currently configurable to match against Okta Username, Email, or both. The example in Figure 14B matches against Okta Username.

6. When no match is found, you can elect to perform JIT user provisioning or redirect the user to the Okta sign-in page (as in Figure 14B). Select the option you prefer. Note that if you select Create new user, additional options will be presented for you to configure.

7. Scroll down as needed to the SAML Protocol Settings.

8. Enter the IdP Issuer URI based on the IdP Entity ID you created when configuring BIG-IP APM. For example, enter <https://tmf5.oktaprise.com:8443/F5_Big-IP_APM_as_IdP>. See Figure 16.
9. Enter the **IdP Single Sign-On URL** based on the **IdP Name Settings Host** you created when configuring BIG-IP APM, using this format: `<scheme>://<hostname:port>/saml/idp/profile/redirectpost/sso`. For example, enter `<https://tmf5.oktaprise.com:8443/saml/idp/profile/redirectpost/sso>`. See Figure 16.

10. For **IdP Signature Certificate**, click **Browse files...**, navigate to the **self-signing certificate file you created previously**, and select it.

11. Click **Show Advanced Settings** and select the following advanced settings. Refer to Figure 17.

   - **Request Binding**: Select **HTTP POST**.
   - **Request Signature**: Select **Sign SAML Authentication Requests**.
   - **Request Signature Algorithm**: Select **SHA-256**.
   - **Response Signature Verification**: Select **Response or Assertion**.
   - **Response Signature Algorithm**: Select **SHA-256**.

13. Select **Trust-specific** for **Okta Assertion Consumer Service URL**.

14. For **Max Clock Skew**, select **2 Minutes**.

15. Click **Add Identity Provider**, click **Download metadata**, and save the metadata.xml file locally. Make note of the file location, which you will use in a subsequent procedure.

---

**Figure 17: Advanced SAML protocol settings**

**Figure 18: Downloading the metadata**
Set up BIG-IP APM with SAML SP connectors

This configuration involves creating a service provider connector and binding it to the IdP service.

Configure a SAML external SP connector

1. In the BIG-IP APM configuration utility, navigate to Access > Federation > SAML Identity Provider > External SP Connectors.
2. Click Create and click From Metadata.
3. Click Browse and select the metadata file you saved in the previous procedure.
4. Enter a unique Service Provider Name.
5. Leave Select Signing Certificate blank, since the metadata provided by Okta isn’t signed, and click OK.
6. Select the newly created external SP connector and click Edit.
7. Under General Settings, the SP Entity ID will be populated from the metadata and align with the value of the Audience URI as configured for the Okta identity provider. Enter a Description if desired (optional).
8. Click **Endpoint Settings**, leave **Relay State** blank, and under **Assertion Consumer Service(s)**, click **Add**.

9. Create an **Assertion Consumer Service** with the following properties:
   - **Index**: 0
   - **Default**: Selected
   - The **Location URL** will be populated from the metadata to align with the value for the **Assertion Consumer Service URL** used in the Okta IdP configuration and in the format:
     <https://mattegantest.oktapreview.com/sso/saml2/0oa9jbf10zd6RCQeT0h7>
RECOMMENDED DEPLOYMENT PRACTICES
The F5 and Okta Solution for High Security SSO

- Binding: POST

10. Click Update.

11. Click Security Settings and select Require Signed Authentication Request.

![Connector security settings](image)

Figure 22: Connector security settings

12. The Signing Certificate will be populated from the metadata import as from Okta. Select Response must be signed and Assertion must be signed.

13. For Signing Algorithm, select RSA-SHA256.

14. Leave Assertion must be encrypted unselected.

15. Click SLO Service Settings. We recommend leaving all settings here at their defaults, which means confirming that Single Logout Service Settings and Single Logout Response URL are blank.
RECOMMENDED DEPLOYMENT PRACTICES
The F5 and Okta Solution for High Security SSO

Figure 23: SLO service settings

16. Click **OK**.

**Bind the SP connector to the IdP service**

1. In the BIG-IP APM configuration utility, navigate to **Access > Federation > SAML Identity Provider > Local IdP Services**.

2. Select the IdP service you configured in the procedure called Configure SAML local IdP services—make sure its check box is selected—and click **Bind/Unbind SP Connectors**.

Figure 24: Binding the connector to the service

3. Select the **SP Connection Name** you configured in the previous procedure, and click **OK**.
Set up BIG-IP APM with a SAML SSO portal

This configuration involves creating a webtop, a SAML resource to publish the IdP entry on that webtop, a portal access profile and policy, and a virtual server for the IdP service and webtop.

Create a full webtop

1. In the BIG-IP APM configuration utility, navigate to Access > Webtops > Webtop Lists and click Create.

   
   ![Figure 25: Creating the webtop](image)

   2. Enter a distinct Name and select Full for the Type.

   3. Click Finished.

Create a SAML resource to publish the IdP entry on the webtop

1. In the BIG-IP APM configuration utility, navigate to Access > Federation > SAML Resources and click Create.
RECOMMENDED DEPLOYMENT PRACTICES
The F5 and Okta Solution for High Security SSO

Create an access profile for the SAML SSO portal

1. In the BIG-IP configuration utility, navigate to Access > Profiles/Policies > Access Profiles (Per-Session Policies) and click Create.

2. Under General Properties, enter a Name and select the appropriate Profile Type and Profile Scope. (See Figure 27.)

3. Leave other settings at their default values.
4. Under **Language Settings**, add **English (en)** (or the language your users will be using) as an **Accepted Language**, make it the default, and click **Finished**.

**Edit the access policy for the access profile**

1. In the BIG-IP configuration utility, navigate to **Access > Profiles/Policies > Access Profiles (Per-Session Policies)**.

2. Select the access profile you just created and click **Edit** in the **Per-Session Policy** field to open the visual policy editor.

![Figure 28: Editing the access policy in the visual policy editor](image)

3. Bypass the **Logon Page** default and replace **LocalDB Auth** (which is for demonstration purposes only) with appropriate values such as **AD Auth**. For example, select a valid **LocalDB Instance** that you can populate.

4. Click **Advanced Resource Assign**, add an expression for **LocalDB Auth Has Passed**, and assign the previously created webtop and SAML resource. (See Figure 29.)

![Figure 29: Editing the properties for the Advanced Resource Assign part of the policy](image)

5. Change the result of the fallback branch for **Advanced Resource Assign** to **Allow**.
Create a virtual server for the IdP service and webtop

1. In the BIG-IP configuration utility, navigate to Local Traffic > Virtual Servers : Virtual Server List and click Create.

2. Under General Properties, enter a unique Name for the virtual server.

3. For Type, select Standard.

4. For Source Address, enter 0.0.0.0/0 or a suitable range for your purposes.

5. For Destination Address/Mask, enter the address aligned with the hostname (or address) you used in previous configuration steps.

6. For Service Port, enter an available port that aligns with the port specified or implied in previous configuration.

7. For State, select Enabled.

8. Under Configuration: (Basic), ensure the following configuration values are selected:
   - Protocol: TCP
   - HTTP Profile: http
   - Source Address Translation: None

9. For SSL Profile (Client), select the SSL client profile associated with the certificate that aligns with the hostname.
10. Under **Content Rewrite**, select **None** as the **Rewrite Profile** and **None** as the **HTML Profile**.

11. Under **Access Policy**, select the **Access Profile** you configured previously.
RECOMMENDED DEPLOYMENT PRACTICES
The F5 and Okta Solution for High Security SSO

12. For **Acceleration**, select **Basic**, then confirm that all other settings are **None**.

13. For **Resources**, confirm that all settings are blank or **None**, then click **Finished**.
Set up SaaS provisioning with Okta

In addition to SSO, the Okta Application Network supports account provisioning for many popular SaaS applications.

The easiest way to enable provisioning and user onboarding in Okta is to set up directory integration between Okta and your directory services. This integration does not synchronize the directory credentials to Okta, but it does allow you to customize the list of attributes being synchronized into Okta, which can then be used for downstream account provisioning through Universal Directory and attribute mapping done between Okta and the applications.

Learn more about this integration, including directory integration and Universal Directory, attribute mapping, application provisioning, groups and group membership, and group-based provisioning.