RECOMMENDED DEPLOYMENT PRACTICES

The F5 and Okta Solution for Web Access Management with Multifactor Authentication

November 2017
## Contents

**Contents** .......................................................................................................................... 2

**Introduction** .................................................................................................................... 3

**The Integrated Solution** .................................................................................................. 4
  Okta multifactor authentication .......................................................................................... 5
  Prerequisites ....................................................................................................................... 6

**Deployment Procedures** ................................................................................................ 6
  Publish a sample web application via the BIG-IP system ................................................ 6
  Configure Okta as the SAML 2.0 identity provider ......................................................... 9
    Additional app configuration ............................................................................................ 11
  Configure MFA factor types in Okta ............................................................................... 14
  Manage MFA policies ........................................................................................................ 16
    Create an MFA policy ....................................................................................................... 16
    Add a policy rule ............................................................................................................. 16
    Softlock .......................................................................................................................... 17
  Configure BIG-IP APM as the SAML 2.0 service provider .............................................. 18
    Configure the SAML SP service .................................................................................... 18
    Create a SAML IdP connector and bind it to the SAML SP service ............................... 21
    Configure a BIG-IP access policy to authenticate with the Okta SAML IdP ............... 24
    Add the access profile to the virtual server ................................................................. 30

**Testing the BIG-IP APM and Okta Integration** ............................................................... 31
  Reports and logs ............................................................................................................... 32

**Appendix** ..................................................................................................................... 32
  Configuring mobile devices for use with Okta MFA ....................................................... 32
    Set up Okta Verify on a mobile device .......................................................................... 32
    Reconfigure an Okta Verify account .......................................................................... 34
    Configure voice call authentication ............................................................................ 34
    Reset and reconfigure voice call authentication ........................................................ 35
  Extract attributes from the Okta SAML assertion (example) ......................................... 35
    Create an iRules script ............................................................................................... 35
    Apply the new iRule to the virtual server .................................................................. 37
  Additional Resources ..................................................................................................... 38
Introduction

Despite recent advances in security and identity management, controlling and managing access to applications through the web—whether by onsite employees, remote employees or contractors, customers, partners, or the public—is as difficult as ever. IT teams are challenged to control access based on granular characteristics such as user role while still providing fast authentication and, preferably, unified access with single sign-on (SSO) capabilities. The ability to audit access and recognize and stop attempts at unauthorized access are also critical in today’s security environment.

F5® BIG-IP® Local Traffic Manager™ (LTM) and F5 BIG-IP® Access Policy Manager® (APM) address these challenges, providing extended access management capabilities when used in conjunction with the Okta identity management platform. The integrated solution allows Okta to support applications with header-based and Kerberos-based authentication and multifactor authentication using a variety of factor types. In addition, the BIG-IP system can act as a reverse proxy for publishing on-premises applications beyond the firewall, where they can be accessed through Okta.

Figure 1: The basic integration between the F5 BIG-IP system and Okta
The Integrated Solution

In this integrated solution (shown in Figure 1 above):

- Okta is the identity provider. Users can be defined locally within Okta. In most cases, an on-premises Active Directory and/or LDAP is the source of identities and is integrated with Okta via Okta’s AD/LDAP agent.

- Between Okta and the F5 BIG-IP system, a SAML trust is built with the BIG-IP platform acting as a SAML service provider (SP).

- The target applications are protected behind the BIG-IP reverse proxy by header-based authentication or Kerberos authentication.

SAML assertion from Okta is consumed by the BIG-IP system, which then translates the assertion appropriately for the downstream application based on its authentication scheme.

This combined solution provides best-of-breed Identity as a Service (IDaaS) deployment with full legacy and on-premises app support that is easy to deploy and configure through Okta. It also helps lower total cost of ownership (TCO) by removing the need to maintain traditional on-premises identity solutions for on-premises apps.

A variety of use cases apply when Okta and the BIG-IP system are deployed together.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Authentication Mechanism</th>
<th>Okta Role</th>
<th>BIG-IP APM Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SAML</td>
<td>SAML identity provider</td>
<td>N/A (BIG-IP APM can also act as the IdP)</td>
</tr>
<tr>
<td>2</td>
<td>WS-Fed</td>
<td>WS-Fed Identity Provider</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>Login page only (username/password)</td>
<td>Okta’s Secure Web Authentication provides form-post capability through a browser plug-in</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>Header-based</td>
<td>Identity provider</td>
<td>Receive SAML from Okta; generate header(s) for downstream app</td>
</tr>
<tr>
<td>5</td>
<td>Kerberos</td>
<td>Identity provider</td>
<td>Receive SAML from Okta; obtain Kerberos ticket for downstream Kerberos-enabled app</td>
</tr>
<tr>
<td>6</td>
<td>Reverse-proxy to access on-premises applications from outside the firewall</td>
<td>Identity provider if only authenticated users are allowed</td>
<td>Reverse proxy</td>
</tr>
</tbody>
</table>

Deployment of the integrated solution involves:

- Publishing a sample ASP .NET IIS web application via the BIG-IP system.
- Configuring Okta as a SAML 2.0 IdP for the BIG-IP system.
- Configuring multifactor authentication (MFA)
RECOMMENDED DEPLOYMENT PRACTICES
The F5 and Okta Solution for Web Access Management

- Configuring the BIG-IP system as a SAML 2.0 SP for Okta.
- Testing the SSO integration.

Okta multifactor authentication

Okta's native multifactor authentication (MFA) method, Okta Verify, balances ease of use with security. However, sometimes circumstances dictate other choices. Feedback from hundreds of Okta customers exposed a number of scenarios where a third-party MFA provider was needed. For instance, some organizations have a pre-existing investment in a legacy MFA provider and may be wary of the cost and effort of changing the user experience. Others require the high-level assurance that hardware tokens can deliver for a subset of privileged users. Still others are in a state of transition—eager to adopt Okta Verify, but reluctant to migrate too abruptly from a previous provider.

Accordingly, organizations are not restricted to Okta Verify. Various third-party authentication methods are compatible and work seamlessly with the Okta identity platform and BIG-IP security, many involving one-time passwords (OTPs).

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Integration Type</th>
<th>Note</th>
<th>Supported Authentication Method(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>On-Premises MFA Agent</td>
<td>This type of integration relies on the Okta agent to facilitate communication between the Okta service and an on-premises RADIUS server.</td>
<td>OATH-OTP</td>
</tr>
<tr>
<td>Entrust</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symantec</td>
<td>Native</td>
<td>Symantec integrations are built upon provider APIs or WebSDKs. They vary in feature support because not all features are similarly accessible.</td>
<td>OTP</td>
</tr>
<tr>
<td>Duo Security</td>
<td>Native</td>
<td></td>
<td>OTP, Push, Voice</td>
</tr>
<tr>
<td>Google Authenticator</td>
<td>Native</td>
<td></td>
<td>OTP</td>
</tr>
<tr>
<td>YubiKey</td>
<td>Native</td>
<td></td>
<td>OTP, Push OTP</td>
</tr>
</tbody>
</table>

Okta can also support multiple factors simultaneously, allowing organizations to migrate between factors or support heterogeneous user environments.

**Note:** This document provides detailed guidance only for Okta MFA resources; other options are listed above for informational purposes only.
Prerequisites

The use cases and deployment procedures in this document apply for F5® TMOS® version 11.0 and above. They can be applied to any production or lab edition of the F5 products. Refer to AskF5 for additional information, including how to initially set up a BIG-IP environment and handle basic BIG-IP LTM and BIG-IP APM configuration.

For additional information about installing the Okta portion of the solution, refer to Okta documentation or customer support.

Deployment Procedures

These instructions assume that you have an existing BIG-IP system where you can test the Okta integration. If you are new to BIG-IP products, please refer to AskF5 for initial download, setup, and operating information.

Publish a sample web application via the BIG-IP system

These instructions assume a Microsoft Windows Server environment with IIS enabled.

1. Configure the BIG-IP system to proxy requests to the test web server using F5® iApps®. To create an appropriate iApp, open the BIG-IP interface and click iApp > Application Services > Applications > Create.

2. Provide a Name for this application and select f5.microsoft_iis as the Template (or use the http template for generic web servers).

![Figure 2: Creating an iApp](https://example.com/image.png)
3. Scroll down to the **Virtual Server and Pools** questions.

4. Enter the **Virtual Server IP Address** on the external interface (e.g., 12.12.1.12). See Figure 3.

5. Provide the IP address of the test web server and the port it is listening on (e.g., 11.11.1.11 and 80; see Figure 3).

6. Provide a fully qualified domain name (FQDN) for the web server hostname (e.g., www.democorp.co).

7. Click **Finish**. The BIG-IP interface will display the status of this application. (See Figure 4.)
RECOMMENDED DEPLOYMENT PRACTICES
The F5 and Okta Solution for Web Access Management

8. To test the connection, launch a browser on the host machine and point it to the external IP address previously chosen (e.g., 12.12.1.12). The browser should render the backend web server page.

9. We recommend putting an entry into your local hosts file to point a test hostname (e.g., www.democorp.co) to this backend app IP address (12.12.1.12 in the example).
10. We also recommend placing a file, headers.aspx, in the root of the web server's folder with the following line to display all headers:

```csharp
<%@ Page Language="C#" Trace="true" %>
```

Configure Okta as the SAML 2.0 identity provider

1. In the Okta interface, under Applications, click Add Application, and click Create New App.

![Figure 6: Adding an app in Okta](image)

2. Create a new SAML 2.0 app in Okta. Assign it a name and choose an optional logo if desired.
3. Under **SAML Settings**, enter the **Single Sign-On URL** (which should be `<https://external-f5-hostname/saml/sp/profile/acs>`) and the **Audience URI (SP Entity ID)**.

4. Set the **Signature Algorithm** to **RSA-SHA1**. TMOS versions 11.5.0 and above support RSA-SHA256. We strongly recommend that you upgrade to a TMOS version that supports RSA-SHA256.
5. Scroll down to provide custom attributes to be passed in the SAML assertion to the ASP .NET application.

6. Click Finish. The app can now be assigned to authorized users or groups or additional security applied.

Additional app configuration

1. To assign the app or apply additional security options, such as App Sign-On policy to provide MFA and granular control, click the Assignments or Sign On tabs in the app.
Figure 9: Assigning the app to specific groups

Figure 10: Configuring authentication
2. On the **Sign On** tab, under **View Setup Instructions** (which are contextual and specific for F5), click **Identity Provider metadata** (see Figure 11) to save the SAML metadata.xml that will be imported into the BIG-IP system and to complete Okta SAML Identity Provider setup.

![F5 BIG IP](image)

**Figure 11: Saving the XML metadata**
Configure MFA factor types in Okta

Multifactor authentication (MFA) provides an additional layer of security for enterprise applications. MFA can be configured at the organization level, the application level, or both. When both are configured, users are asked for the additional authentication factors when they sign into Okta and again when they sign into apps configured for app-level MFA. For information on application-level MFA, reference Okta's App Level MFA documentation.

Administrators can choose which types of authentication can be used for signing into Okta or a specific application. **Note:** *This document provides detailed guidance only for Okta MFA resources; other options are listed for informational purposes only.*

1. In the Okta interface, click the **Factor Type** tab and click **Edit**.
2. Select one or more of these acceptable factor types.
   - **Okta Verify:** To sign in, a user must start the Okta Verify app on their mobile device to generate a six-digit code they use to sign into the organization. This numerical code is generated using the industry standard time-based, one-time password algorithm. In addition, the first time users sign in after this factor is configured, they see that extra verification is required and must perform the setup steps noted in the Appendix of this document.
   - **Okta Verify with Push:** Okta Verify with Push authentication adds a level of convenience to the user's authentication process. Push notifications enable users to verify their identities with a single tap on their mobile device—without the need to type a passcode. This gives them direct access to their apps while retaining the same level of security. This feature is available for iPhone, Android, and Windows devices. For details on this option, see Okta Verify with Push Authentication in the Okta Help Center.
   - **Google Authenticator:** To sign in, users must start the Google Authenticator app on their mobile device to generate a six-digit code. This numerical code is generated using the industry standard time-based, one-time password algorithm. The allowable clock skew is two minutes. After five unsuccessful attempts, regardless of the time between the attempts, the user account is locked and must be reset by an administrator. The first time users sign in after this factor is configured, they see that extra verification is required and must perform setup steps on their mobile devices.
   - **SMS Authentication:** To sign in, users must enter a security token that has been sent to their mobile device. The first time users sign in after this factor is configured, they see that extra verification is required and must perform setup steps on their mobile devices.
   - **Voice Call Authentication:** To sign in, the user must enter a security token that is generated and sent via phone call to a mobile device or landline. Direct Inward Dial (DID) is not supported. In addition, this is an Okta Early Access feature; please contact Okta Support to enable it.
   - **Symantec VIP:** Symantec Validation and ID Protection Service (VIP) is a cloud-based authentication service that enables secure access to networks and applications. Available for free in the United States and Canada in both enterprise and SSO editions, this factor type enables the use of a VIP Manager tool to obtain a certificate for signing in.
RECOMMENDED DEPLOYMENT PRACTICES
The F5 and Okta Solution for Web Access Management

- **Okta On-Premises MFA**: Formerly known as the RSA SecurID agent, this factor type generates a numerical authentication code users enter to sign into the organization. To sign in, users must use an RSA hardware dongle device or soft token to generate the authentication code. The numbers are generated using a built-in clock and the card's factory-encoded random key. The agent acts as a RADIUS client and will communicate with your RADIUS-enabled on-premises MFA server, including RSA Authentication manager for RSA SecurIDs. For more details, see Configuring the On-Premises MFA Agent (including RSA SecurID) in the Okta Help Center.

- **Duo Security**: When signing in, users are prompted for additional verification. Users can then select the authentication type supported by their device. For details about this option, see Configuring Duo Security in the Okta Help Center.

- **YubiKey**: A YubiKey, produced by Yubico, is a USB-compatible multifactor authentication device that delivers a unique password every time it's activated by a user. Using their USB connector, users simply press on the YubiKey hard token to emit a new, one-time password (OTP), which they then use to securely log into their accounts. Security is assured, as all YubiKey validation occurs within the Okta Cloud, and Okta guarantees Okta-level quality of service and uptime for YubiKey authentication. Okta supports the following Yubico hardware devices:
  - YubiKey Edge and Edge-N (Nano), which both offer strong authentication using Yubico OTP with a tap of the device.
  - YubiKey-Neo, which offers both contact (USB) and contact-free (NFC, MIFARE) communication. YubiKey Neo supports OTP and smart card functionality.
  - Yubikey Neo-N (Nano), which offers strong authentication via Yubico OTP with the touch of a button.

For more details, see YubiKey in the Okta Help Center.

- **Security Question Authentication**: To sign in, users must enter the correct response to a security question they select from a list of possible questions.

- **Email Authentication**: Users receive an email message containing a code to enter during Okta sign-in. Note: Using email is not a best practice, and we do not recommend it. Email is a very insecure method of additional verification because email can be compromised by third parties, is not always transmitted over secure protocols, and can also be used, depending on the recovery flow, for primary credential recovery. Although we do offer email as a factor experience for convenience and to help our customers migrate from legacy identity platforms, we do not consider it a secure, modern method for secondary authentication. When you add it as a factor, you must explicitly accept the risk.

- **Windows Hello (Web Authentication)**: Users, who must be running the Microsoft Edge browser, sign in to Okta using Windows Hello. This is an Okta Early Access feature; to enable it, please contact Okta Support.

- **U2F security key (FIDO 1.0)**: Users enter a U2F compliant security key to sign into Okta. U2F is supported only for Chrome and Firefox browsers, and Firefox users must download an extension. This is
RECOMMENDED DEPLOYMENT PRACTICES
The F5 and Okta Solution for Web Access Management

an Okta Early Access feature. To enable it, please contact Okta Support.

3. When Okta configuration is completed, click Save.

Find mobile device configuration and use procedures for the Okta factor types in the Appendix.

Manage MFA policies

Use the Okta Multifactor Policies tab to create and enforce policies for your chosen MFA factor types. Policies can be applied to specific groups and automatically enforced for only users in those groups to determine the types of authentication challenges a given user receives. An MFA policy can be based on variables such as location, group definitions, and authentication type. It can also specify actions to take, such as allowing access or prompting for a challenge.

Note: If your organization does not require group-based factors, it is not necessary to create additional policies. In that case, simply retain the default policy.

Create an MFA policy

1. In the Okta interface, click the Multifactor Policies tab. The default policy displays as the policy applied when no other policy has been set. It reflects the factors previously chosen on the Factor Type tab.

2. Click Add Multifactor Policy.

3. Add Policy displays. Enter a descriptive Policy Name.

4. Describe the elements of the policy in the Policy Description.

5. Assign the policy to one or more groups by entering a predefined group. (Once you begin typing, group names will be suggested or auto-completed.)

6. The factor type(s) you set up on the Factor Type tab should appear as Effective Factors. For each, select whether the factor should be required, optional, or disabled for that group.

7. Click Create Policy to complete the process.

8. In the policy list, select any policy to display these additional management options:
   - Active: Click to activate or deactivate the selected policy. A deactivated policy will not be applied to any user, but you can reactivate it later.
   - Edit: Click to change properties or assignment of the selected policy.
   - Delete: Click to delete the selected policy. The default policy cannot be deleted, and a deleted policy cannot be recovered.

9. Change the order of any existing policies, except the default policy, by dragging the bar on the policy name to rearrange the list as desired.

Add a policy rule

Rules allow you to add conditions to your policy choices.

2. Enter a descriptive Rule Name.

3. Optionally, click Exclude Users to exclude individual users of a group from the rule (not the policy).

4. Under Enroll Multifactor, select from the following two options for the rule:
   - The user must enroll in the multifactor option during their initial sign-in to Okta.
   - The user can enroll when first challenged for an MFA option.

5. Once a policy rule has been created, select one or more users on which to apply the rule and enforce where the user will be challenged for authentication:
   - Anywhere: The user will be challenged when making connections within the network or outside of it.
   - On Network: The user is only challenged when making connections off the network.

   Manage configuration for the network by clicking Manage Configurations for Network to access gateway settings that enable the access choice. For details about this option, see Public Gateway IPs on the Okta Help Center.

6. Once you have created a rule, select it (in the list beneath Add Rule) to view its details, including excluded users and when an authentication factor will be prompted.

7. While selected, the following actions can be taken for the selected rule:
   - Active: Click to activate or deactivate the selected rule. If you deactivate a rule, it will not be applied to any user, but you can reactivate it later.
   - Expand: Click to view details (which also display when the rule name is selected with a click.)
   - Edit: Click to change the rule properties.
   - Delete: Click to delete the selected rule. A deleted rule cannot be recovered.

8. Rearrange or prioritize rules by dragging the rule name above or below other rules in the list.

Softlock

The Okta Softlock feature, available for password policies, is also available for delegated authentication. Active Directory (AD)-mastered and LDAP-mastered users can attempt a maximum number of MFA attempts, after which the Okta account will be locked. AD-mastered users can take advantage of the Okta self-service feature to unlock the account, but LDAP-mastered users require administrator action to unlock the Okta account.
Configure BIG-IP APM as the SAML 2.0 service provider

This configuration involves two stages: configuring the SP service and configuring connectors.

Configure the SAML SP service

Configure a SAML SP service for BIG-IP APM to provide AAA authentication by requesting authentication and receiving assertions from a SAML IdP.

1. On the Main tab of the BIG-IP interface, click Access > Federation > SAML Service Provider > Local SP Services. A list of local SP services is displayed. Click Create.

![Figure 12: Configuring the BIG-IP system as the service provider](image)

2. Under General Settings, enter a unique Name for the SAML SP service (e.g., BIGIPSP). For the Entity ID, enter the audience URI you set up during Okta SAML configuration. For Host, enter the FQDN or IP address for the BIG-IP virtual server established earlier in this process.
3. Click **Security Settings**. (There are no configuration changes to be made on the **Endpoint Settings** page.)
4. Under **Security Settings**, ensure that the proper key and certificate are chosen for your environment. Then click **Authentication Context**.


![Figure 15: Selecting the authentication context](image)

6. Click **Advanced Settings**. Click **Allow Name-Identifier Creation**.

Create a SAML IdP connector and bind it to the SAML SP service

BIG-IP APM (as a SAML service provider) can send authentication requests to the Okta IdP, relying on it to authenticate users and to provide access to resources behind BIG-IP APM.

1. On the Main tab of the BIG-IP interface, click Access > Federation > SAML Service Provider > Local SP Services. A list of local SP services is displayed.
2. Select the BIGIPSP (or whatever unique Name you gave the SAML SP service you created earlier).
Figure 17: Starting configuration of the connector

3. Click **Bind/Unbind IdP Connectors**.

4. Under **Create New IdP Connector**, select **From Metadata**.

Figure 18: Creating a new connector
5. Browse to select the metadata.xml download from Okta, enter an Identity Provider Name, and click OK.

![Selecting the downloaded XML file](image)

Figure 19: Selecting the downloaded XML file

6. Once an Okta IdP connector is created and its signing certificate is imported, click Add New Row.

7. Select OktaldP as the SAML IdP Connector, `<%{session.server.landinguri}>` as the Matching Source, and `/` as the Matching Value. This tells BIG-IP APM to use the OktaldP for all requests on this web server. This URI can be adjusted based on specific folders or other matching source parameters.
Configure a BIG-IP access policy to authenticate with the Okta SAML IdP

Once the BIG-IP system is set up as a SAML service provider, configure a BIG-IP access policy to direct users to the Okta SAML IdP for authentication.

1. On the **Main** tab of the BIG-IP interface, click **Access > Profiles/Policies > Access Profiles.**
2. Click **Create**.
3. Enter a policy **Name**, and for the **Profile Type**, select **All**.
4. Under **SSO Across Authentication Domains**, in a non-HTTPS test environment, make sure secure **Cookie Options** is **not** selected. (See Figure 22.)
5. (Optional). Enter custom values for timeouts and session as desired.
6. Choose a **Language** and click **Finished**.
### General Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>OktaSAMLPolicy</td>
</tr>
<tr>
<td>Parent Profile</td>
<td>access</td>
</tr>
<tr>
<td>Profile Type</td>
<td>All</td>
</tr>
<tr>
<td>Profile Scope</td>
<td>Profile</td>
</tr>
</tbody>
</table>

### Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inactivity Timeout</td>
<td>900 seconds</td>
</tr>
<tr>
<td>Access Policy Timeout</td>
<td>300 seconds</td>
</tr>
<tr>
<td>Maximum Session Timeout</td>
<td>604800 seconds</td>
</tr>
<tr>
<td>Minimum Authentication Failure Delay</td>
<td>2 seconds</td>
</tr>
<tr>
<td>Maximum Authentication Failure Delay</td>
<td>5 seconds</td>
</tr>
<tr>
<td>Max Concurrent Users</td>
<td>0</td>
</tr>
<tr>
<td>Max Sessions Per User</td>
<td>0</td>
</tr>
<tr>
<td>Max In Progress Sessions Per Client IP</td>
<td>128</td>
</tr>
<tr>
<td>Restrict to Single Client IP</td>
<td>No</td>
</tr>
<tr>
<td>Use HTTP Status 503 for Error Pages</td>
<td>No</td>
</tr>
</tbody>
</table>

### Configurations

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logout URI Include</td>
<td>Add</td>
</tr>
<tr>
<td>Logout URI Timeout</td>
<td>5 seconds</td>
</tr>
<tr>
<td>Microsoft Exchange</td>
<td>None</td>
</tr>
<tr>
<td>User Identification Method</td>
<td>HTTP</td>
</tr>
<tr>
<td>OAuth Profile</td>
<td>None</td>
</tr>
</tbody>
</table>

### SSO Across Authentication Domains (Single Domain mode)

<table>
<thead>
<tr>
<th>SSO Options</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Cookie</td>
<td></td>
</tr>
<tr>
<td>Cookie Options</td>
<td>Secure/Persistent</td>
</tr>
</tbody>
</table>

**Figure 22:** Ensure that no cookie options are selected in an HTTPS environment.

7. Once the policy has been created, click **Edit...** under **Access Policy**.
8. The BIG-IP APM visual policy editor opens to display the default access policy. Click the + between the **Start** and **Deny** nodes.

9. Under the **Authentication** tab, select **SAML Auth**.
RECOMMENDED DEPLOYMENT PRACTICES
The F5 and Okta Solution for Web Access Management

Figure 25: Selecting SAML authorization

10. On the next screen, under Properties, enter a Name for the authentication method.
11. For **AAA Server**, select the previously configured **BIGIPSP** (or the unique SP name you created previously).

12. Click **Save**. The visual policy editor displays the access policy as per Figure 27. Note that BIG-IP APM is a very powerful tool that can also perform additional processing, including fetching attributes from other AD/LDAP sources for insertion and additional backend authorization.
13. Click **Apply Access Policy**, then click **Close**.

To put the access policy into effect, you must attach it to the virtual server that you previously created for the test ASP.NET IIS web app, as shown in the next procedure.

**Add the access profile to the virtual server**

Associate the access profile with the virtual server so that BIG-IP APM can apply the profile to incoming traffic and run the previously defined access policy.

1. On the **Main** tab of the BIG-IP interface, click **Local Traffic > Virtual Servers > Virtual Server List**. The Virtual Server List displays.
2. Select the virtual server. Then scroll down. Under Access Policy, select the previously defined Access Profile and click Update.

<table>
<thead>
<tr>
<th>Access Policy</th>
<th>OktasAMLPolicy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity Profile</td>
<td>None</td>
</tr>
<tr>
<td>Per-Request Policy</td>
<td>None</td>
</tr>
<tr>
<td>VDI Profile</td>
<td>None</td>
</tr>
<tr>
<td>Application Tunnels (Java &amp; Per-App VPN)</td>
<td>Enabled</td>
</tr>
<tr>
<td>OAM Support</td>
<td>Enabled</td>
</tr>
<tr>
<td>PingAccess Profile</td>
<td>None</td>
</tr>
</tbody>
</table>

Figure 29: Assigning the access policy

Testing the BIG-IP APM and Okta Integration

Follow these steps to test the integration.

1. Go to the published application URL created earlier in these procedures.
2. The BIG-IP system should redirect the request to Okta for authentication. Enter your credentials.
3. Okta will pass the SAML assertion to the BIG-IP system and you should be granted access to the IIS web server that was setup earlier in these procedures.
Reports and logs

The All Sessions report (under Access > Overview > Access Reports) and Okta System Log can provide traces of transactions that can aid in troubleshooting.

Figure 31: The All Sessions report can aid troubleshooting.

Appendix

Configuring mobile devices for use with Okta MFA

Once a factor type has been configured in Okta and all other configuration has been completed and tested, configuration also needs to be completed between users’ mobile devices and their desktop or laptop. The configuration procedures vary slightly for each factor type. Note: This document provides detailed guidance only for Okta MFA resources, not for the third-party options available.

Set up Okta Verify on a mobile device

When the Okta Verify factor type is selected, each mobile device requires this setup procedure to be completed by the user between their mobile device and their desktop or laptop.

1. When loggin in to the organization on the desktop, click Setup.
2. Select the mobile device, follow the instructions to download and install the Okta Verify app, and then click Next.
3. Configure Okta Verify to link it to your Okta account. This can be accomplished by scanning a QR code or manually entering the code. (See Figure 32 and the alternative steps below.)

4. Once configuration is complete, use Okta Verify by opening the app and using the six-digit number that will be generated to authenticate when prompted.

**Option A: To scan a QR code**

- On your mobile device, start the Okta Verify app, tap **Account**, and then tap **Scan Code**.
- Scan the QR code on your computer screen using your phone camera. The passcode generator generates codes to use when prompted for extra verification.
- When authenticating and prompted for a passcode, enter the passcode generated. You have 30 seconds before the app generates a new one.
- The account is linked. Click **Next** in the Okta interface.

**Option B: To configure an account manually**

- On your mobile device, start the Okta Verify app, tap **Account**, and then tap **Enter Account**.
- Enter your Okta username (for example, ted@mycompany.com) in the **Okta Account** field.
- On your computer, click **Can’t scan the QR code** to get the secret key.

![Figure 32: Linking Okta Verify to the user’s account (for an iPhone. Other mobile OS screens are similar).](image-url)
RECOMMENDED DEPLOYMENT PRACTICES
The F5 and Okta Solution for Web Access Management

- Enter the displayed key in the **Secret Key** field on the app.
- Click **Save**. The account is linked. The passcode generator generates codes to use when prompted for extra verification. You have 30 seconds to enter the passcode before the app generates a new one.

### Reconfigure an Okta Verify account

A user can revoke an existing Okta Verify passcode and reconfigure the account at any time. This might be necessary if a phone is lost or stolen, for instance, or if the user has a new phone to link to the account.

1. Install the Okta mobile app on the phone, if it’s not already installed.
2. Sign in to the organization (for example, `mycompany.okta.com`).
3. Click the **Account** tab.
4. In the **Extra Verification** section, click **Setup** and follow the prompts to reconfigure the account.

### Configure voice call authentication

Note that Direct Inward Dial (DID) is not supported, and that this is an Early Access feature. To enable it, please contact Okta Support. Once this factor type is enabled and configured, the first time users sign in, they will see that extra verification is required and must perform the following steps.

1. On the mobile device, click **Setup** (beside **Voice Call**).
2. Enter the number for the mobile device or landline that should receive the authentication call. For landline business phones, an extension may be entered. (See Figure 33.)
3. Click **Call**.
4. The device displays **A Call is in progress...** Answer the call and enter the provided code into the **Enter code** field on the mobile device.
5. Click **Verify** and then **Done** (if needed).

![Figure 33: Voice call verification as displayed on the mobile device](image-url)
6. Verification is complete. To authenticate subsequently, users must click Call, answer the voice call to receive the required code, enter that code into the mobile device, and click Verify.

Reset and reconfigure voice call authentication

If a mobile device is lost or receives a new phone number, users can reset and reconfigure their voice call authentication by following these steps.

1. While logged in to the Okta home page, select Settings from the drop-down menu under the user name.
2. Click Edit Profile.
3. Scroll down to Extra Verification.
4. Click Reset. (See Figure 34.)

5. Enter the new phone number, then click Update. The account will be reconfigured.

Extract attributes from the Okta SAML assertion (example)

The following is an example for extracting attributes from within the SAML assertion. At this point only the user name will be extracted. You can configure Okta to include additional attributes in the SAML assertion, if required.

Create an iRules script

1. Create an F5® iRules® script to extract the custom SAML attributes from the incoming assertion and pass them as HTTP headers to the backend test ASP.NET IIS application.
RECOMMENDED DEPLOYMENT PRACTICES
The F5 and Okta Solution for Web Access Management

Figure 35: Creating an iRule

2. On the **Main** tab of the BIG-IP interface, click **Local Traffic > iRules > iRules List**.

3. Click **Create**.

4. Copy and paste the iRules text below into the **Definition** field. (See Figure 36.)

   ```
   when RULE_INIT {set static::debug 0}
   set oktaUser [ACCESS::session data get "session.saml.last.identity"]
   if { $static::debug } { log local0. "id is $oktaUser" }
   if { ![HTTP::header exists "OKTA_USER"] } [HTTP::header insert "OKTA_USER" "$oktaUser"]
   ```
RECOMMENDED DEPLOYMENT PRACTICES
The F5 and Okta Solution for Web Access Management

5. Click Finished.

Apply the new iRule to the virtual server

1. Apply the iRule you created to the virtual server by clicking Edit... under Resources.

2. On the Resources tab of the virtual server detail page, under iRules, click Manage.
RECOMMENDED DEPLOYMENT PRACTICES
The F5 and Okta Solution for Web Access Management

Figure 38: Applying the iRule to the virtual server

3. Add the Okta iRule that you previously created to the **Enabled** list, and click **Finished**.

Figure 39: Enabling the iRule

Additionally Resources

For additional information, including basic [BIG-IP LTM](https://docs.f5.com) and [BIG-IP APM](https://docs.f5.com) configuration, refer to [AskF5](https://docs.f5.com) or to Okta [documentation](https://docs.okta.com) or [customer support](https://docs.okta.com).