Contents

Introduction ........................................................................................................................................... 3

Publishing SAMPLE Web Application VIA F5 BIG-IP ................................................................. 5

Configuring Okta as SAML 2.0 Identity Provider for F5 BIG-IP ................................................. 9

Configuring F5 BIG-IP as SAML 2.0 Service Provider for Okta .............................................. 15
  Configure SAML SP Service .................................................................................................................. 15
  Configure SAML IdP Connector and Bind SAML SP Service to SAML IdP Connector ............... 18
  Configure an F5 BIG-IP Access Policy to Authenticate with Okta SAML IdP ....................... 22
  Adding the access profile to the virtual server ................................................................................... 28

Testing the F5 BIG-IP + Okta Integration ...................................................................................... 32

Appendix ............................................................................................................................................... 34
  TROUBLESHOOTING .......................................................................................................................... Error! Bookmark not defined.
  Additional References .......................................................................................................................... 34
  Sample F5 BIG-IP Virtual Lab Setup with VMWare ................................................................. 35
**Introduction**

F5® BIG-IP® Local Traffic Manager™ (BIG-IP LTM®) and F5 BIG-IP Access Policy Manager® (BIG-IP APM®) provide extended capabilities in conjunction with Okta identity management platform. The integration in this document allows Okta to support applications with header-based authentication, kerberos-based authentication. In addition, F5 BIG-IP also can act as a reverse proxy for publishing on-premise apps beyond the firewall where they can be accessed through Okta.

The diagram above illustrates the basic integration between the two products.

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

2) Between Okta an F5 BIG-IP, a SAML trust is built where F5 BIG-IP acts as a SAML Service Provider.

3) The target applications are protected behind F5 BIG-IP. This document covers applications that are either protected by header-based authentication or Kerberos.

4) SAML assertion from Okta is consumed by F5 BIG-IP which then “translates” the assertion appropriately for the downstream application based on their authentication scheme.
This combined solution provides best-of-breed Identity as a Service (IDaaS) deployment with full legacy and on-premise app support that is easy to deploy and configured through Okta. It also helps lower TCO by removing the need to maintain traditional on-prem identity solutions for on-premise apps.

The following table illustrates the use cases when considering using Okta and F5 BIG-IP together.

<table>
<thead>
<tr>
<th>Authentication Mechanism</th>
<th>Okta</th>
<th>F5 BIG-IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. SAML</td>
<td>Acts as SAML Identity Provider</td>
<td>-</td>
</tr>
<tr>
<td>2. WS-Fed</td>
<td>Acts as WS-Fed Identity Provider</td>
<td>-</td>
</tr>
<tr>
<td>3. Login Page only (username/pwd)</td>
<td>Okta’s Secure Web Authentication providing form-post capability through browser plug-in</td>
<td>-</td>
</tr>
<tr>
<td>4. Header-based</td>
<td>Acts as identity provider</td>
<td>Receives SAML from Okta – generates header(s) for downstream app</td>
</tr>
<tr>
<td>6. Reverse-Proxy to access on-prem application from outside the firewall</td>
<td>Acts as identity provider if only authenticated users are allowed</td>
<td>Acts as reverse proxy</td>
</tr>
</tbody>
</table>

This document will go through the following:

- Publish a sample ASP.NET IIS web application via F5 BIG-IP
- Configure Okta as SAML 2.0 IdP for F5 BIG-IP
- Configure F5 BIG-IP as SAML 2.0 SP for Okta
- Testing the SSO integration

The instructions provided here should work for F5 BIG-IP version 11.* and up. You can apply this to any production or lab edition of the product.

For an example of how to set up F5 BIG-IP environment, the Appendix presents a basic set of instructions around a VMWare example.
Publishing SAMPLE Web Application VIA F5 BIG-IP

We assume that you have an existing F5 BIG-IP setup where you can test the Okta integration.

If you are new to F5 BIG-IP, please refer to the F5 Support Site for download, setup and general information around F5 BIG-IP (https://support.f5.com/kb/en-us/products/big-ip_apm.html).

The instructions below assumes a Microsoft Windows Server environment with IIS enabled.

1. It is recommended to configure F5 BIG-IP to proxy requests to the test webserver by creating an iApp. Click iApp -> Application Services -> 'Create'
2. Provide a Name for this application and choose f5.microsoft_iis as the Template (use http template for generic webservers). Also provide the Virtual Server IP-Address on the external interface (e.g., 12.12.1.12)
3. Scroll down on the same page and under Server Pool, Load Balancing section, provide the IP-address of the test web server and port it is listening on (e.g., 11.11.1.11 and 80). Also provide an FQDN for the web server hostname (e.g., www.democorp.co) and click ‘Finish’
4. F5 BIG-IP will show the status of this application
5. To test the connection, launch a browser on the host machine and point it to the external IP-address chosen in the previous screen (e.g., 12.12.1.12 and it should render the backend webserver page).

6. It is recommended to put a hosts file entry to point a test hostname (e.g., www.democorp.co) to this backend app IP-address (e.g., 12.12.1.12). Also, place a file headers.aspx in the root of the webserver’s folder with the following line to display all headers:

```html
<%@ Page Language="C#" Trace="true" %>
```
7. The page in previous step will be used to verify Okta integration in the next section
Configuring Okta as SAML 2.0 Identity Provider for F5 BIG-IP

1. Under “Applications” – choose “Add Application” option and click on “Create New App”.

2. Create a new SAML 2.0 App in Okta and provide it a name and optionally choose a logo.

3. In SAML Settings, provide the Single Sign On URL (should be: <https://external-f5-hostname/saml/sp/profile/acs>), Audience URI (SP Entity ID).

Note that F5 BIG-IP versions prior to 11.5.0 (not included) only supports SHA1 as Signature Algorithm. So it has to be set to RSA-SHA1. F5 BIG-IP version 11.5.0 and above supports RSA-SHA256. It is strongly recommended that you upgrade to a version that supports RSA-SHA256.
4. Scroll down on the same page and provide custom attributes to be passed in the SAML assertion to the ASP.NET application
5. Click ‘Finish’ on the next screen
Create SAML Integration

3. Help Okta Support understand how you configured this application

Are you a customer or partner?
- I'm an Okta customer adding an internal app
- I'm a software vendor, I'd like to integrate my app with Okta

The optional questions below assist Okta Support in understanding your app integration.

App type
- This is an internal app that we have created

Previous Finish

6. This app can now be assigned to authorized users or groups. Additional security options like App Sign On policy to provide MFA and granular control can be applied as well.
7. Click on the ‘Sign On’ tab in the app and then click on then ‘Identity Provider metadata’ link to save the SAML metadata.xml that will be imported in F5 BIG-IP
8. Okta SAML Identity Provider setup is complete.
Configuring F5 BIG-IP as SAML 2.0 Service Provider for Okta

Configure SAML SP Service

Configure a SAML SP service for F5 BIG-IP Access Policy Manager to provide AAA authentication, requesting authentication and receiving assertions from a SAML IdP.

1. On the Main tab, click Access Policy > SAML > BIG-IP as SP. The BIG-IP as SP screen opens and displays a list of local SP services

2. In the Name field, type a unique name for the SAML SP service. In the Entity ID field, provide the Audience URI that was provided in Okta SAML configuration
Create New SAML SP Service

General Settings

Security Settings

Name*: BIGIPSP

Entity ID*: http://www.democorp.co/sp

Description:

Relay State:

OK  Cancel
3. Click ‘OK’
Configure SAML IdP Connector and Bind SAML SP Service to SAML IdP Connector

Configure Okta as SAML IdP connector in F5 BIG-IP so that Access Policy Manager (as a SAML service provider) can send authentication requests to Okta IdP, relying on it to authenticate users and to provide access to resources behind APM.

1. On the Main tab, click Access Policy > SAML > BIG-IP as SP. The BIG-IP as SP screen opens and displays a list of local SP services. Select ‘BIGIPSP’ SAML SP service from the list.

2. Click ‘Bind/Unbind IdP Connectors’. Then click ‘Create New IdP Connector’ and ‘From Metadata’
3. Browse to metadata.xml download from Okta and enter an ‘Identity Provider Name’ and click ‘OK’
4. This will create an Okta IdP Connector and also import its signing certificate
5. Click ‘Add New Row’. Choose OktaldP as the SAML IdP Connect, Matching Source as: 
   %{session.server.landinguri} and Matching Value as /*. It tells F5 BIG-IP to use OktaldP for all requests
   on this webserver. This URI can be adjusted based on specific folders or other Matching Source
   parameters. Click ‘OK’
6. SAML IdP and SP setup is complete.
Configure an F5 BIG-IP Access Policy to Authenticate with Okta SAML IdP

With the F5 BIG-IP system as a SAML service provider, configure an F5 BIG-IP access policy to direct users to Okta SAML IdP for authentication.


2. Provide the policy a name. In non-HTTPS test environment, make sure the “Secure” cookie option is deselected. Other custom values for timeouts and session can be optionally provided. Choose a Language and click ‘Finished’
3. After the policy has been created, click on ‘Edit...’ under the ‘Access Policy’ column

4. The F5 BIG-IP APM visual policy editor opens the access policy in a separate screen displaying the default policy
5. Click on the ‘+’ icon between Start and Deny nodes and on the pop-up window, choose ‘SAML Auth’
6. On the next screen, under ‘Properties’, choose a name for the auth method and in AAA Server dropdown, select the previously configured BIG-IP SP. Click ‘Save’
7. The access policy looks like the following. Note that F5 BIG-IP APM is a very powerful tool and additional processing including fetching attributes from other AD/LDAP sources for insertion and additional backend authorization can be performed.

An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the Add Macro button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with Device Wizards. On the main navigation pane, expand Templates and Wizards, and click Device Wizards, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the Configuration Guide for BIG-IP Access Policy Manager for more on creating and editing an access policy.

Please see the Online Help for more Visual Policy Editor basics.
8. Click ‘Apply Access Policy’. Then click ‘Close’
9. To put the access policy into effect, you must attach it to the virtual server that was created for the test ASP.NET IIS web app
Adding the access profile to the virtual server

Associate the access profile with the virtual server so that F5 BIG-IP APM can apply the profile to incoming traffic and run the previously defined access policy.


2. Click on the virtual server. Then scroll all the way to the bottom to the ‘Access Policy’ section. Select the previously defined ‘Access Profile’ and click ‘Update’.

3. Next create an F5 BIG-IP iRule® to extract the custom SAML attributes from the incoming assertion and pass them as HTTP headers to the backend test ASP.NET IIS application. Click ‘Create’.
4. Paste the F5 BIG-IP iRule text below into the Definition window

```plaintext
when RULE_INIT {
    set static::debug 0
}

when ACCESS_ACL_ALLOWED {
    set oktaUser [ACCESS::session data get "session.saml.last.identity"]
    if { }{ log local0. "id is $oktaUser"
    if { ![HTTP::header exists "OKTA_USER"] } {
        HTTP::header insert "OKTA_USER" $oktaUser
    }

    set oktaFirstName [ACCESS::session data get "session.saml.last.attr.name.FirstName"]
    if { }{ log local0. "id is $oktaFirstName"
    if { ![HTTP::header exists "OKTA_FIRSTNAME"] } {
        HTTP::header insert "OKTA_FIRSTNAME" $oktaFirstName
    }

    set oktaLastName [ACCESS::session data get "session.saml.last.attr.name.LastName"]
    if { }{ log local0. "id is $oktaLastName"
    if { ![HTTP::header exists "OKTA_LASTNAME"] } {
```
HTTP::header insert "OKTA_LASTNAME" $oktaLastName 
)

set oktaCity [ACCESS::session data get "session.saml.last.attr.name.City"]
if { $static::debug } { log local0. "id is $oktaCity" } 
if { ![HTTP::header exists "OKTA_CITY"] } {
   HTTP::header insert "OKTA_CITY" $oktaCity 

5. Next, apply this F5 BIG-IP iRule to the Virtual Server

![Virtual Server List]

6. Click 'Edit' under Resources column

![Virtual Server Configuration]

7. Click 'Manage' under iRules

8. Add OktaIRule that previously created to the Enabled list and click Finished
Okta & F5 Integration Guide for Web Access Management with F5 BIG-IP

Resource Management

IRule

<table>
<thead>
<tr>
<th>Enabled</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>/Common</td>
<td></td>
</tr>
<tr>
<td>OktaRule</td>
<td></td>
</tr>
<tr>
<td>&lt;</td>
<td></td>
</tr>
<tr>
<td>&gt;&gt;</td>
<td></td>
</tr>
<tr>
<td>sys_auth_krbdelegatel</td>
<td></td>
</tr>
<tr>
<td>sys_auth_ssl_cc ldap</td>
<td></td>
</tr>
<tr>
<td>sys_auth_ssl_crlidp</td>
<td></td>
</tr>
<tr>
<td>sys_auth_ssl_ocsp</td>
<td></td>
</tr>
</tbody>
</table>

Up | Down

Cancel | Finished
Testing the F5 BIG-IP + Okta Integration

Follow the steps below to test the integration:

1. Go to the published application URL [http://www.democorp.co/headers.aspx](http://www.democorp.co/headers.aspx)
2. F5 BIG-IP should redirect the request to Okta for authentication. Enter credentials

3. Complete the MFA challenge
4. Should be redirected to the published application web page

<table>
<thead>
<tr>
<th>HTTP_Cache_Control</th>
<th>max-age=0</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP_Connection</td>
<td>keep-alive</td>
</tr>
<tr>
<td>HTTP_Accept</td>
<td>text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/*;q=0.8</td>
</tr>
<tr>
<td>HTTP_Accept_Language</td>
<td>en-US,en;q=0.8</td>
</tr>
<tr>
<td>HTTP_Cookie</td>
<td>BIGipServerSSOWebApp.app~SSOWebApp_pool=184617739,20480.0000</td>
</tr>
<tr>
<td>HTTP_Host</td>
<td><a href="http://www.democorp.co">www.democorp.co</a></td>
</tr>
<tr>
<td>HTTP_User_Agent</td>
<td>Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36</td>
</tr>
<tr>
<td>HTTP_Upgrade_Insecure_Requests</td>
<td>1</td>
</tr>
<tr>
<td>HTTP_DNT</td>
<td>1</td>
</tr>
<tr>
<td>HTTP_OKTA_USER</td>
<td><a href="mailto:gary.ward@democorp.com">gary.ward@democorp.com</a></td>
</tr>
<tr>
<td>HTTP_OKTA_FIRSTNAME</td>
<td>Ward</td>
</tr>
<tr>
<td>HTTP_OKTA_LASTNAME</td>
<td>Seattle</td>
</tr>
</tbody>
</table>

5. Note the HTTP_OKTA_* headers indicating successful extraction of SAML headers
Appendix

Reports and Logs

F5 BIG-IP APM Reports -> All Sessions report and Okta System Log can provide traces of transactions that can aid in troubleshooting

For more on Okta System Log – please refer to Okta documentation here – (https://support.okta.com/help/articles/Knowledge_Article/27605453-Using-the-Okta-Reports-Page)

Additional References

Okta Company website – https://www.okta.com

Okta Customer Support – https://support.okta.com

Okta Documentation - https://support.okta.com/help/documentation
Sample F5 BIG-IP Virtual Lab Setup with VMWare

The following outlines the steps to create a basic setup of an F5 BIG-IP environment using VMWare.

NOTE: This should only be used as a sample guidance. To set up a production environment, please refer to the F5 BIG-IP documentation listed above.

1. F5 BIG-IP should be setup with three network interfaces:
   i. Management (10.10.1.1)
   ii. Internal (11.11.1.1)
   iii. External (12.12.1.1)

   It is recommended that VMWare is setup with three custom host-only networks as shown below:

2. There should be an IIS or Apache webserver to test backend application with the suggested IP-address: 11.11.1.11

3. Open the downloaded image file in VMWare Workstation and deploy it using default options, then start the F5 BIG-IP VM
4. Switch to VM console and on login prompt, enter `root` as username and `default` as password

5. Enter `ifconfig -a | more` to find the DHCP assigned IP-address to this VM. For example, `inet addr: 192.168.1.149` is the IP-address below:

```
eth0 Link encap:Ethernet HWaddr 00:0C:29:0E:2C:FB
inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe6a:2cbf/64 Scope:link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1321 errors:0 dropped:0 overruns:0 frame:0
TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:106996 (104.4 KIB) TX bytes:1086 (1.0 KIB)
```

6. Launch a browser on the host machine and enter the `https://IP-address` obtained in the previous step, For example: `https://192.168.1.149`

7. A certificate warning will be issued by the browser. This is normal, click proceed to the login page:

![BIG-IP Configuration Utility](image)

```
Welcome to the BIG-IP Configuration Utility.
Log in with your username and password using the fields on the left.
```

8. Enter `admin` as username and `admin` as password and click ‘Log in’

9. Click ‘Next’ in the Setup Utility section:
10. Click ‘Activate’ under License

11. Enter Registration Key received via email and click ‘Next’
12. Click ‘Accept’ after reviewing the license agreement

13. After license activation, in the Resource Provisioning screen, select Access Policy (APM) and make sure Local Traffic (LTM) is also selected. Then click ‘Next’
14. In the Platform screen, enter the static IP address for Management Port and a Host Name for the F5 BIG-IP. Also choose passwords for Root and Admin accounts.
15. The system should redirect to the new Management address and port. Log in with the new Admin password. Click ‘Next’ to configure the Network.

16. Unselect Config Sync options and click ‘Next’ as they are not needed for this lab

17. Configure the Internal Network
18. Configure the External Network
19. Base setup is complete at this point.