

**IMPORTANT:** This guide has been archived. While the content in this guide is still valid for the products and version listed in the document, it is no longer being updated and may refer to F5 or 3rd party products or versions that have reached end-of-life or end-of-support. See <https://support.f5.com/csp/article/K11163> for more information.



## Configuring the BIG-IP APM as a SAML 2.0 Identity Provider for Common SaaS Applications

Welcome to the F5® deployment guide for configuring the BIG-IP® Access Policy Manager (APM) to act as a SAML Identity Provider for commonly used Software as a Service (SaaS) applications. This document contains guidance on configuring the BIG-IP® APM as an IdP for to perform Single Sign-On for the following SaaS applications: Office 365, Salesforce, Workday, Amazon Web Services, Concur, Service Now, Jive, Wombat, Zendesk, Webex, Box, and Google Apps.

### Products and applicable versions

Product	Version
BIG-IP APM	11.6 - 12.1
iApp Template Version <sup>1</sup>	f5.saas_idp.v.1.0.1rc2
Deployment Guide version	1.3 (see <i>Document Revision History on page 26</i> )
Last updated	01-31-2019

**Important:** Make sure you are using the most recent version of this deployment guide, available at <http://f5.com/pdf/deployment-guides/saml-idp-saas-dg.pdf>.

If you are looking for older versions of this or other deployment guides, check the Deployment Guide Archive tab at: <https://f5.com/solutions/deployment-guides/archive-608>

To provide feedback on this deployment guide or other F5 solution documents, contact us at [solutionsfeedback@f5.com](mailto:solutionsfeedback@f5.com)

# Contents

About SAML	3
Prerequisites and configuration notes	3
<b>Configuration example</b>	<b>4</b>
Choosing a BIG-IP APM Access Policy option in Advanced mode	4
<b>Configuring F5 BIG-IP to act as a SAML 2.0 Identity Provider</b>	<b>5</b>
Configuring DNS and NTP settings on the BIG-IP system	5
Generating or importing certificates	6
<b>Configuring the BIG-IP iApp template for SaaS applications</b>	<b>7</b>
Advanced options	8
Template options	8
SaaS Applications	8
BIG-IP APM Configuration	10
BIG-IP IdP Virtual Server	13
IDP Encryption Certificate and Key	15
iRules	15
Finished	15
<b>Appendix: Manual Configuration table</b>	<b>16</b>
Creating the SP initiated and/or IdP Initiated configuration	18
Editing the Access Policy using the VPE	20
<b>Troubleshooting</b>	<b>23</b>
<b>Document Revision History</b>	<b>26</b>

## About SAML

Security Assertion Markup Language (SAML) defines a common XML framework for creating, requesting, and exchanging authentication and authorization data among entities known as Identity Providers (IdPs) and Service Providers (SPs). This exchange enables single sign-on among such entities.

- IdP is a system or administrative domain that asserts information about a subject. The information that an IdP asserts pertains to authentication, attributes, and authorization. An assertion is a claim that an IdP makes about a subject.
- Service Provider is a system or administrative domain that relies on information provided by an IdP. Based on an assertion from an IdP, a service provider grants or denies access to protected services.

In simple terms, an IdP is a claims producer and a service provider is a claims consumer. An IdP produces assertions about users, attesting to their identities. Service providers consume and validate assertions before providing access to resources.

This deployment guide discusses configuration steps to setup the BIG IP APM as SAML IdP for following SaaS applications. The guide is organized to match the admin's workflow (admin only needs to perform the prerequisites and BIG IP APM base system configuration one time and then add in each SaaS application by configuring the SAML related parameters as required).

Salesforce	Workday	Amazon Web Services (AWS)
Concur	Service Now	Jive
Wombat	Zendesk	WebEx
Box	Google Apps	Office 365

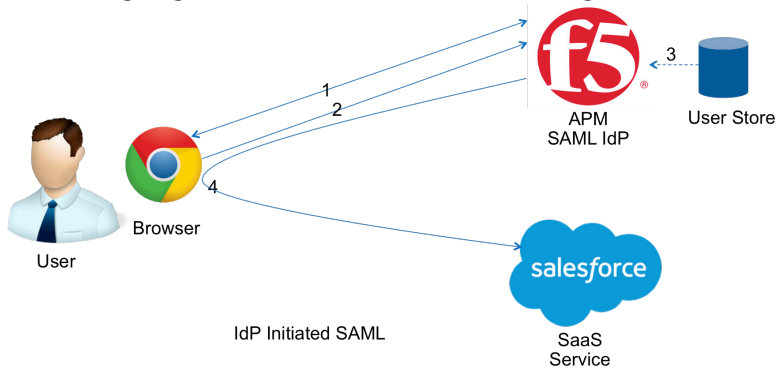
## Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- ▶ This guide assumes the person configuring this implementation is (or is working with) the administrator of their respective SaaS Application tenant to configure the SAML Service Provider (SP) functionality. Below are pointers to available vendor SAML SP configuration. You can reach out to the other vendors for their SAML SP configuration documentation.
  - » **Salesforce SP Configuration:**  
[https://help.salesforce.com/apex/HTViewHelpDoc?id=sso\\_saml.htm](https://help.salesforce.com/apex/HTViewHelpDoc?id=sso_saml.htm)
  - » **Amazon Web Services SP Configuration**  
<http://docs.aws.amazon.com/IAM/latest/UserGuide/identity-providers-saml.html>
  - » **Service-Now SAML Configuration**  
[http://wiki.servicenow.com/index.php?title=SAML\\_2.0\\_Setup](http://wiki.servicenow.com/index.php?title=SAML_2.0_Setup)
  - » **Jive SP Configuration**  
[https://docs.jivesoftware.com/jive/6.0/community\\_admin/index.jsp?topic=/com.jivesoftware.help.sbs.online\\_6.0/admin/ConfiguringSSOwithSAML.html](https://docs.jivesoftware.com/jive/6.0/community_admin/index.jsp?topic=/com.jivesoftware.help.sbs.online_6.0/admin/ConfiguringSSOwithSAML.html)
  - » **Zendesk SP Configuration**  
<https://support.zendesk.com/hc/en-us/articles/203663676-Using-SAML-for-single-sign-on-Plus-and-Enterprise->
  - » **Box SP Configuration**  
<https://community.box.com/t5/For-Admins/Single-Sign-On-SSO-with-Box-For-Administrators/ta-p/1263>
  - » **Google Apps SP Configuration**  
<https://support.google.com/a/answer/60224?hl=en>
- ▶ For this guide, the BIG-IP system **must** be running version 11.6 or later. This configuration does not apply to previous versions.
- ▶ You must have the APM module fully licensed and provisioned. You must have the LTM module provisioned, even if it is not licensed. You can ignore the provisioning warning when LTM is not licensed.
- ▶ We assume you have already obtained the appropriate SSL certificate(s) and key(s), and they are installed on the BIG-IP system. See *Generating or importing certificates on page 6* for specific information.
- ▶ If you are using a SaaS application other than Office 365, you must manually create an SP Connector for each application you intend to use. See *Creating the SP initiated and/or IdP Initiated configuration on page 18* for specific guidance on configuring these objects.

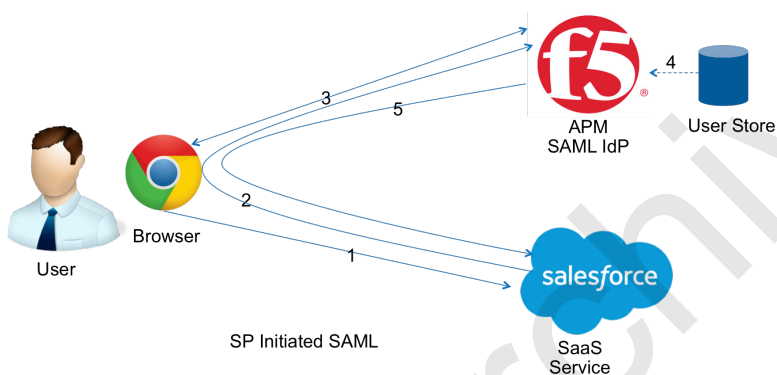
## Configuration example

The following diagrams show the traffic flow for this configuration. In these examples, we use Salesforce as our SaaS application.



IdP Initiated SAML

1. User logs on to the F5 APM IdP and is directed to the Webtop.
2. User selects a Salesforce service from the Webtop.
3. F5 APM may retrieve attributes from the user data store to pass on with the SaaS service provider.
4. APM directs the requests to the SaaS service with the SAML assertion and optional attributes via the user browser.



SP Initiated SAML

1. User accesses the Salesforce SaaS service.
2. Salesforce redirects the user back to the F5 APM SAML IdP with SAML request via users browser.
3. F5 APM prompts the user to logon with the relevant credentials.
4. At this time F5 APM may retrieve attributes from the user data store to pass on with the SaaS service provider.
5. APM then sends a SAML response to Salesforce with the authentication information and optional attributes via the user browser for allowing access to the service.

### Choosing a BIG-IP APM Access Policy option in Advanced mode

One of the key components of this configuration is the BIG-IP APM Access Policy. The Access Policy is an object that contains the criteria for granting access to various servers, applications, and other resources on your network. If you select the Basic configuration mode in the iApp template, the system creates the recommended Access Policy for you.

If you select the Advanced configuration mode, you have the option of either selecting an existing APM Access Policy, or having the iApp create one for you. What makes this iApp template unique is the ability for the iApp to create the recommended Access Policy for you, but not associate the Access Policy with the iApp configuration. The iApp effectively creates a copy of the recommended Access Policy which is not a part of the Application Service (an Application Service contains all items created by the iApp, and protects the configuration from modification unless the Strict Updates feature is disabled). This feature allows you to customize the Access Policy after you submit the template without having to disable Strict Updates. It also allows you to re-enter the iApp template and make other modifications without overwriting any customization you made to the Access Policy. After customizing the Access Policy outside the iApp, you then re-enter the template and select the policy you just customized from the list of available policies.

If you do not need to customize the Access Policy, you can simply allow the iApp to create the standard policy without selecting the option of not associating it with the application service. For more information, see *BIG-IP APM Configuration on page 10*.

## Configuring F5 BIG-IP to act as a SAML 2.0 Identity Provider

The first task in federating user identify with a SaaS application is to setup your BIG-IP APM to act as the SAML Identify Provider. You need to complete the following tasks:


1. Configuring the DNS and NTP settings on the BIG-IP system, on this page.
2. Generate a self-signed certificate or import a certificate/key combination to the BIG-IP system that is used to sign the IdP SAML assertions. See [Generating or importing certificate used to sign your SAML Assertion](#) on page 5.
3. Import the SSL certificate and key that will be used by your IdP Virtual Server. See [Importing a valid SSL certificate for authentication](#) on page 5.
4. Configure the BIG IP system as SAML IDP based on the information below.


### Configuring DNS and NTP settings on the BIG-IP system

To use BIG-IP APM, you must configure DNS and NTP settings on the BIG-IP system before beginning the configuration.

#### Configuring the DNS settings

In this section, you configure the DNS settings on the BIG-IP system to point to a DNS server that can resolve your Active Directory server or servers. In many cases, this IP address will be that of your Active Directory servers themselves.

 **Note:** *DNS lookups go out over one of the interfaces configured on the BIG-IP system, not the management interface. The management interface has its own, separate DNS settings.*

 **Important** *The BIG-IP system must have a self IP address in the same local subnet and VLAN as the DNS server, or a route to the DNS server if located on a different subnet. The route configuration is found on the Main tab by expanding **Network** and then clicking **Routes**. For specific instructions on configuring a route on the BIG-IP system, see the online help or the product documentation.*

#### To configure DNS settings

1. On the Main tab, expand **System**, and then click **Configuration**.
2. On the Menu bar, from the **Device** menu, click **DNS**.
3. In the **DNS Lookup Server List** row, complete the following:
  - a. In the **Address** box, type the IP address of a DNS server that can resolve the Active Directory server.
  - b. Click the **Add** button.
4. Click **Update**.

#### Configuring the NTP settings

The next task is to configure the NTP settings on the BIG-IP system for authentication to work properly.

#### To configure NTP settings

1. On the Main tab, expand **System**, and then click **Configuration**.
2. On the Menu bar, from the **Device** menu, click **NTP**.
3. In the **Address** box, type the fully-qualified domain name (or the IP address) of the time server that you want to add to the Address List.
4. Click the **Add** button.
5. Click **Update**.

To verify the NTP setting configuration, you can use the **ntpq** utility. From the command line, run **ntpq -np**.

See <http://support.f5.com/kb/en-us/solutions/public/10000/200/sol10240.html> for more information on this command.

## Generating or importing certificates

The next task is to import (or generate a self-signed) certificates on to the BIG-IP system. This configuration requires two different certificates, one that is used to sign your SAML assertion, and the other used by your external users to connect to your IdP service.

### Generating or importing certificate used to sign your SAML Assertion

Before you begin configuring the BIG-IP system, you need to make sure that you either create or import the certificate that will be used to sign your assertions to the BIG-IP device. That certificate can be either a self-signed certificate generated by the BIG-IP system, or you can import any certificate on the BIG-IP system for this purpose. The only restriction is that a wildcard certificate cannot be used to sign SAML assertions for some SaaS applications (for example, Salesforce does not allow wildcard certificates).

To generate or import a certificate, go to **System > File Management > SSL Certificate List**. If you are using a certificate from a third-party CA, click **Import**. If you want the BIG-IP system to generate a self-signed certificate, click **Create**.

### Importing a valid SSL certificate for authentication

You also need to import a valid SSL certificate onto the BIG-IP system that is trusted by all browsers, as it will be used by your external users to connect to your IdP service and authenticate themselves to the SaaS application cloud.

To import a certificate, go to **System > File Management > SSL Certificate List**, and then click **Import**. From the **Import Type** list, select the appropriate value, such as Certificate. Repeat for the key if necessary.

Archived

## Configuring the BIG-IP iApp template for SaaS applications

Use the following guidance to help configure the BIG-IP system as a SAML 2.0 Identity Provider for Common SaaS Applications using the BIG-IP iApp template.

### Downloading and importing the iApp

The first task is to download the iApp template and import it onto the BIG-IP system. Ensure you download the file with the latest version number.

#### To download and import the iApp

1. Open a browser and go to: [downloads.f5.com](https://downloads.f5.com).
2. Click **Find a Download**, and then in the BIG-IP F5 Product Family section, click **iApp-Templates**.
3. Extract (unzip) the **f5.saas\_idp.v<latest version>** file. For this release, it is in the **RELEASE\_CANDIDATES** directory.
4. Log on to the BIG-IP system web-based Configuration utility.
5. On the Main tab, expand **iApp**, and then click **Templates**.
6. Click the **Import** button on the right side of the screen.
7. Select the **Overwrite Existing Templates** check box.
8. Click the **Choose File** button, and then browse to the location you saved the iApp file.
9. Click the **Upload** button. The iApp is now available for use. If you are configuring the BIG-IP system manually, see *Appendix: Manual Configuration table on page 16*.

### Getting started with the iApp template

To begin the iApp Template, use the following procedure.

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApp**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a unique name.
5. From the **Template** list, select **f5.saas\_idp.v1.0.1rc1** (or a newer version if applicable). The View iApp template opens.

## Advanced options

If you select **Advanced** from the **Template Selection** list, you see Sync and Failover options for the application. This feature, new to v11, is a part of the Device Management configuration. This functionality extends the existing High Availability infrastructure and allows for clustering, granular control of configuration synchronization and granular control of failover. For more information on Device Management, see the Online Help or product documentation.

### 1. **Device Group**

To select a specific Device Group, clear the **Device Group** check box and then select the appropriate Device Group from the list.

### 2. **Traffic Group**

To select a specific Traffic Group, clear the **Traffic Group** check box and then select the appropriate Traffic Group from the list.

## Template options

This section of the template asks about your View and BIG-IP implementation.

### 1. **Do you want to see inline help?**

Select whether you want to see informational and help messages inline throughout the template. If you are unsure, we recommend leaving the default, **Show inline help text**. Important and critical notes are always shown, no matter which selection you make.

- **Yes, show inline help**

This selection causes inline help to be shown for most questions in the template.

- **No, do not show inline help**

If you are familiar with this iApp or with the BIG-IP system in general, you can select this option to hide the inline help text.

### 2. **Which configuration mode do you want to use?**

Select whether you want to use F5 recommended settings, or have more granular, advanced options appear in the iApp.

- **Basic - Use F5's recommended settings**

In basic configuration mode, options like load balancing method, parent profiles, and settings are all set automatically. The F5 recommended settings come as a result of extensive testing with VMware View, so if you are unsure, choose Basic.

- **Advanced - Configure advanced options**

In advanced configuration mode, you have more control over individual settings and objects, such as the ability to select an existing APM authentication profile and specific tcp optimizations. You can also choose to attach iRules you have previously created to the application service. This option provides more flexibility for advanced users.

In this template, one of the benefits of Advanced mode is the ability for the iApp to create an Access Policy but not associate it with the iApp Application Service. See *Choosing a BIG-IP APM Access Policy option in Advanced mode on page 4* for more details.

Advanced options in the template are marked with the Advanced icon: **Advanced**. If you are using Basic/F5 recommended settings, you can skip the questions with this icon.

## SaaS Applications

This section of the template asks you about the SaaS application(s) for which you are deploying this template.

### 1. **Which SaaS application (and SP Connector) are you using?**

Select the SaaS application for which you are deploying this iApp template. You must specify the SaaS application, the SP Connector, and Display Name for each application you choose as described below. If you created a custom SAML BIG-IP as IdP object, you can select it from the list. You must still select the SP Connector and Display name for any custom objects you select.

**i Important** *For all of the SaaS applications other than Microsoft Office 365, you must have an existing, manually-created SP Connector. See [Creating the SP initiated and/or IdP Initiated configuration on page 18](#) for instructions if you have not yet created one.*

- **Application**

From the list, select either a new federation relationship for the SaaS application you are using, or select a custom object you manually created outside the iApp template (**Access Policy > SAML > BIG-IP as IdP**).



- **SP**

From the list, select the SP Connector you created for your application. Again, if you have not created one, see *Creating the SP initiated and/or IdP Initiated configuration on page 18* for all applications except Office 365.

- **Display Name**

Type the name for the application you want displayed to users after successful authentication. This name (and associated icon) will be the link users click to launch the application.

- **IdP Initiated?**

Choose whether the connections for the application you selected are initiated by the service provider only, or both an IdP and service provider.

- a. **No, SP only**

Select this option if connections for the application you choose are only service provider initiated. In this case, IdP initiated connections are not allowed.

- b. **Yes, IdP and SP**

Select this option if the connections can be initiated both by an IdP and a service provider.

If you want to include more SaaS applications, click **Add** and repeat this step.

## 2. **Did you select Amazon Web Services as an SaaS application?**

Choose whether or not Amazon Web Services (AWS) is one of the SaaS applications you selected in question #1. The system needs to know if you are deploying the iApp for AWS because AWS requires SAML attributes that are specific to your AWS account.

- **No, I did not select AWS as an SaaS application**

Select this option if you did not select Amazon Web Services as one of the SaaS applications for which you are deploying this template. If you did select AWS, but select No from this list, the template will display an error and will not complete.

- **Yes, I selected AWS as an SaaS application**

Select this option if you selected Amazon Web Services as one of the SaaS applications in question #1. You must answer the following questions.

- a. **What is your Amazon Web Services account number?**

Because AWS requires SAML attributes that are specific to your AWS account, the system needs to know your AWS account number. Note that the actual SAML assertion passed over the wire will be encrypted. Type your account number in this field.

- b. **What is your AWS Identity Provider Name?**

Type your AWS identity Provider name.

## 3. **Are attributes required for any SAML resources?**

Choose whether any of the SAML resources require attributes.

- **No, my SAML resource(s) do not require attributes**

Select this option if your SAML resources do not require attributes. Continue with the next section.

- **Yes, my SAML resource(s) require attributes**

Select this option if your SAML resources require attributes. You must add the attributes in the questions that appear.

- a. **Which attributes (for each SaaS application requiring SAML resources) do you want to use?**

Some SaaS applications, like AWS, require Identity Provider attributes. Use this section to add the attributes for each SaaS application that requires them.

Using AWS as an example, there are two SAML attributes that are required for AWS SAML assertions. The first is used to identify the Username that is associated with the session, and the second identifies the AWS Security Role that should be assigned to the session.

The first attribute uses the name: **https://aws.amazon.com/SAML/Attributes/Role** and a value of: **arn:aws:iam::[Account #]:role/{session.samlresource.aws.role},arn:aws:iam::[Account #]:saml-provider/[IdP Name]**. In this case, you must change the [Account #] and [IdP Name] flags with the information from your AWS environment. This attribute maps the session to the specified specific role and account number.

The Second attribute uses the Name: **https://aws.amazon.com/SAML/Attributes/RoleSessionName** and a value of **{session.logon.last.logonname}**. This attribute is used to identify the username for the session.

- **Display Name**  
The Display Name MUST match the display name used in SaaS application selection at the start of this section. The attributes you specify are added to the application tied to the Display Name.
- **Attribute Name**  
In the Attribute Name field, specify the attribute name.
- **Attribute Value**  
In the Attribute Value field, specify the attribute value.

## BIG-IP APM Configuration

This section of the template asks about the APM configuration, including how the iApp should create the Access Policy.

### 1. ***Should the iApp create a new Access Policy or use an existing one?*** Advanced

This advanced question determines the Access Policy used by the system. As described in *Choosing a BIG-IP APM Access Policy option in Advanced mode on page 4*, the iApp can either create a new Access Policy that is associated with the iApp application service, create a copy of the Access Policy that is not associated with the iApp service (which allows easier customization), or you can choose an existing Access Policy that you have customized.

- **Create a new APM Access policy**  
Select this option if you want the iApp template to create the recommended Access Policy. In this scenario, the Access Policy is associated with the iApp Application Service (which is typical for nearly all iApp templates). If you want to customize this Access Policy, you would have to disable the Strict Updates feature. If you require customization after running the iApp, we strongly recommend you use the next option instead.
- **Create a new APM Access policy, but don't associate it with the iApp configuration**  
Select this option if you want the iApp to create the recommended Access Policy, but not include it with the iApp configuration. In this case, the template names the newly created Access Policy *<name you gave the iApp>\_copy1*, and does not associate the policy with the Application Service (an Application Service contains all items created by the iApp, and protects the configuration from modification unless the Strict Updates feature is disabled).  
  
This option enables you to customize the Access Policy created by the template without disabling Strict Updates. All other objects created by the iApp are still protected while Strict Updates is enabled and cannot be modified outside the iApp template.  
  
If you re-enter the iApp to modify any of the iApp settings, you must select the newly customized policy from this list to continue using the Access Policy with this deployment. Otherwise, if you leave this same option when re-configuring the iApp, the iApp creates another copy (*\_copy2*, then *\_copy3*, and so on) each time you submit the template, and the newest copy is associated with the virtual server created by the template.  
  
It is outside the scope of this document to provide guidance on Access Policy customization. See the BIG-IP APM documentation ([https://support.f5.com/kb/en-us/products/big-ip\\_apm.html](https://support.f5.com/kb/en-us/products/big-ip_apm.html)) for your version.
- **Select an existing Access Policy**  
If you have an existing Access Policy you created for this implementation, or if you have customized the iApp produced by the template using the *Create a new APM policy, but don't associate it with the iApp configuration* described in the previous bullet, select it from the list.

### 2. ***How is your EntityID formatted?***

*This question only appears if you are using BIG-IP version 12.0 or later. If using an earlier version, continue with #3.*

Choose whether your EntityID is formatted as a URL or a URN. If you select URN, additional questions appear (#4 and #5) asking for the host name and scheme of your IdP deployment.

### 3. ***What EntityID do you want to use for your SaaS applications?***

Type the EntityID for your SaaS applications. The EntityID is a required configuration setting, and is used by the SAML Service Provider (SP) to properly identify and match the SAML assertion coming from the BIG-IP system. The format of the IdP Entity ID should be the URL to the federation service URL that users will use to authenticate themselves to the BIG-IP system. For example, if our Entity ID is <https://login.example.com/idp/f5/>, the host name of the federation service is login.example.com. The URI part of the Entity ID, [/idp/f5/](https://login.example.com/idp/f5/), simply helps build a unique IdP identifier string for the SAML assertion for this particular IdP instance.

#### 4. **What is the hostname of your IdP deployment?**

*This question only appears if you are using BIG-IP version 12.0 or later, and if you selected your EntityID is a URN. If using an earlier version or if you selected your EntityID is a URL, continue with #6.*

Because you selected your EntityID is a URN, the system needs to know the hostname for the IdP implementation to use in the BIG-IP APM SSO Configuration object. Type the hostname of your IdP deployment.

#### 5. **What is the IdP scheme?**

*This question only appears if you are using BIG-IP version 12.0 or later, and if you selected your EntityID is a URN. If using an earlier version or if you selected your EntityID is a URL, continue with #6.*

Because you selected your EntityID is a URN, the system needs to know whether your IdP deployment scheme is HTTP or HTTPS. This setting is also used in the SSO Configuration object for BIG-IP APM. Select the appropriate value from the list.

- **HTTPS**  
Select HTTPS if the IdP scheme uses HTTPS in your environment.
- **HTTP**  
Select HTTP if the IdP scheme uses HTTP in your environment.

#### 6. **Should the iApp create a new AAA server or use an existing one?**

The AAA Server contains the authentication mechanism for the BIG-IP APM Access Policy.

Select whether you want the template to create a new BIG-IP APM AAA Server object, or if you have already created an AAA object for this implementation on the BIG-IP system. We recommend letting the iApp template create a new AAA server unless you have specific requirements that necessitate a custom AAA Server.

- **Select an existing AAA Server**  
If you have already created an AAA Server object for this deployment, select it from the list. If you want to create your own AAA Server but have not already done so, you must exit the template and create the object before it is available in the list. Continue with *BIG-IP IdP Virtual Server on page 13*.
- **Create a new AAA Server**  
Select this option (the default) to have the template create a new Active Directory AAA Server object for this environment.
  - a. **Which Active Directory server IP address in your domain can this BIG-IP system contact?**  
Type both the FQDN and IP address of all Active Directory servers in your domain that this BIG-IP system can contact. Make sure this BIG-IP system and the Active Directory servers have routes to one another and that firewalls allow traffic between the two. Click **Add** to include additional servers.
  - b. **What is the FQDN of the Active Directory implementation for your SaaS application users?**  
Type the Active Directory domain name for your implementation in FQDN (fully qualified domain name) format. This is the FQDN for the whole domain, and not the FQDN for a specific host.
  - c. **Does your Active Directory domain allow anonymous binding?**  
Select whether anonymous binding is allowed in your Active Directory environment.
    - **Yes, anonymous binding is allowed**  
Select this option if anonymous binding is allowed. No further information is required for this question.
    - **No, credentials are required for binding**  
If credentials are required for binding, you must specify an Active Directory user name and password.
      - a. **Which Active Directory user with administrative permissions do you want to use?**  
Type a user name with administrative permissions.
      - b. **What is the password for that user?**  
Type the associated password.  
*These credentials are stored in plaintext on your BIG-IP system.*
  - d. **How do you want to handle health monitoring for this pool?**  
Specify whether you want the template to create a new LDAP monitor or a new ICMP monitor, or if you select an existing monitor. For more accurate monitoring, we recommend using an LDAP monitor.

- **Select an existing monitor for the Active Directory pool**

Select this option if you have already created a health monitor (only monitors with a **Type** of LDAP or External can be used) for the Active Directory pool that will be created by the template. If you want to create a health monitor, but have not already done so, you must exit the template and create the object before it becomes available from the list.

The iApp allows you to select monitors that are a part of another iApp Application Service. If you select a monitor that is a part of another Application Service, be aware that any changes you make to the monitor in the other Application Service will apply to this Application Service as well.

- a. Which monitor do you want to use?

From the list, select the LDAP or External monitor you created to perform health checks for the Active Directory pool created by the template. Only monitors that have a Type value of LDAP or External appear in this list. Continue with the next section.

- **Use a simple ICMP monitor for the Active Directory pool**

Select this option if you only want a simple ICMP monitor for the Active Directory pool. This monitor sends a ping to the servers and marks the server UP if the ping is successful. Continue with the next section.

- **Create a new LDAP monitor for the Active Directory pool**

Select this option if you want the template to create a new LDAP monitor for the Active Directory pool. You must answer the following questions:

- a. Which Active Directory user name should the monitor use?

Specify an Active Directory user name for the monitor to use when attempting to log on as a part of the health check. This should be a user account created specifically for this health monitor, and *must* be set to never expire.

- b. What is the associated password?

Specify the password associated with the Active Directory user name.

- c. What is the LDAP tree for this user account?

Specify the LDAP tree for the user account. As noted in the inline help, ADSI editor, a tool for Active Directory LDAP administration, is useful for determining the correct LDAP tree value. For example, if the user name is 'user1' which is in the organizational unit 'F5 Users' and is in the domain 'f5.example.com', the LDAP tree would be: ou=F5 Users, dc=f5, dc=example, dc=com.

- d. Does your Active Directory domain require a secure protocol for communication?

Specify whether your Active Directory implementation requires SSL or TLS for communication, or does not require a secure protocol. This determines the port the health monitor uses.

- **No, a secure protocol is not required**

Select this option if your Active Directory domain does not require a secure protocol.

- **Yes, SSL communication is required**

Select this option if your Active Directory domain requires SSL communication. The health check uses port 636 as the Alias Service Port.

- **Yes, TLS communication is required**

Select this option if your Active Directory domain requires TLS communication. The health check uses port 389 as the Alias Service Port.

- e. How many seconds between Active Directory health checks?

Specify how many seconds the system should use as the health check Interval for the Active Directory servers. We recommend the default of 10 seconds.

- f. Which port is used for Active Directory communication?

Specify the port being used by your Active Directory deployment. The default port displayed here is determined by your answer to the secure protocol question. When using the TLS security protocol, or no security, the default port 389. The default port used when using the SSL security protocol is 636.

- g. Which APM logging profile do you want to use?

*This question only appears if you are using BIG-IP version 12.0 or later*

BIG-IP version 12.0 allows you to attach a logging profile to your BIG-IP APM configuration. If you created an APM logging profile for this configuration, you can select it from the list. The default profile is named **default-log-setting**. For more information on APM logging, see the BIG-IP APM documentation for v12.0 and later.

- **Do not specify a logging profile for the APM profile**

Select this option if you do not want to use an APM logging profile at this time. You can always re-enter the template at a later date to choose a logging profile. Continue with the next section.

- **Select an existing APM logging profile from the list**  
If you already created a BIG-IP APM logging profile, or want to use the default profile (**default-log-setting**), select it from the list.

## BIG-IP IdP Virtual Server

This section gathers information about your IdP environment that will be used in the BIG-IP virtual server.

### 1. **What is the IP address clients will use to access the BIG-IP IdP Service?**

Type the IP address you want to use for the BIG-IP virtual server. Clients will resolve the FQDN of the Identity Provider to this IP address.

### 2. **What port do you want to use for the virtual server?**

Type the port number you want to use for the BIG-IP virtual server IP address you specified in the previous question. The default port is 443 (HTTPS).

### 3. **Do you want to redirect inbound HTTP traffic to HTTPS?** **Advanced**

*This question does **not** appear in BIG-IP version 12.0 and later; if using 12.0 or later continue with #4.*

Select whether you want the BIG-IP system to automatically redirect HTTP traffic to the HTTPS virtual server. This is useful when users forget to use HTTPS when attempting to connect to the environment.

- **Redirect HTTP to HTTPS**

Select this option to redirect HTTP traffic to HTTPS. If you select this option (the default), the BIG-IP system creates an HTTP virtual server and attaches a very small redirect iRule to ensure users get to the correct location.

- a. **From which port should traffic be redirected?**

Type the port number for the traffic that you want to redirect to HTTPS. The most common is port 80 (the default).

- **Do not redirect HTTP to HTTPS**

Select this option if you do not want to enable the automatic redirect.

### 4. **Do you want to restrict client traffic to specific VLANs?** **Advanced**

The BIG-IP system allows you to restrict client traffic to specific VLANs that are present on the system. This can provide an additional layer of security, as you can allow or deny traffic from the VLANs you choose. By default, all VLANs configured on the system are enabled. If you select to enable or disable traffic on specific VLANs, you must specify the VLANs in the next question. The VLAN objects must already be configured on this BIG-IP system before you can select them.

- **Enable traffic on all VLANs and Tunnels**

Choose this option to allow traffic from all VLANs and Tunnels. If you select this option, the question asking about VLANs disappears. Continue with the next question.

- **Yes, enable traffic only on the VLANs I specify**

Choose this option to restrict client traffic to specific VLANs that you choose in the following question. The system will accept client traffic from these VLANs, and deny traffic from all other VLANs on the system.

- a. **On which VLANs should traffic be enabled or disabled?**

Use this section to specify the VLANs that accept client traffic. By default, all VLANs on the BIG-IP system appear in the Selected box, so click the VLANs and then use the Move buttons to adjust list membership.


**Note:** *If you choose to allow traffic from certain VLANs, when additional VLANs are added to the BIG-IP system at a later time, this iApp configuration will deny traffic from these VLANs by default. To accept traffic from these VLANs, you must re-enter the template and add the VLAN(s).*

- **Yes, disable traffic only on the VLANs I specify**

Choose this option to deny client traffic from the specific VLANs that you choose in the following question. The system will refuse client traffic from these VLANs, and accept traffic from all other VLANs on the system.

- a. **On which VLANs should traffic be enabled or disabled?**

Use this section to specify the VLANs that should not accept client traffic. By default, all VLANs on the BIG-IP system appear in the Selected box, so it is critical in this case that you click the VLANs and then use the Move button (>>) to adjust list membership.

 **Warning** *If you choose to disable certain VLANs, you must move at least one VLAN to the Options list. Otherwise, the system will deny traffic from all VLANs on the box, and the configuration, although valid, will not pass any traffic.*

5. ***Will clients be connecting to this BIG-IP virtual server primarily over a LAN or a WAN?*** **Advanced**

Select whether most clients are connecting over a WAN or LAN. The iApp uses your selection to determine the default TCP optimization settings in the next question.

- **Most clients connect over a WAN**  
Select this option if most of your clients are coming into the environment over a Wide Area Network.
- **Most clients connect over a LAN**  
Select this option if most your clients are coming into the environment over a Local Area Network.

6. ***How do you want to optimize client-side connections?*** **Advanced**

The client-side TCP profile optimizes the communication between the BIG-IP system and the client by controlling the behavior of the traffic which results in higher transfer rates, improved connection reliability and increased bandwidth efficiency.

Unless you have requirements for configuring specific TCP optimization settings, we recommend allowing the iApp to create a new profile. Creating a custom profile is not a part of this template; see **Local Traffic >> Profiles : Protocol : TCP** to create a TCP profile. To select any new profiles you create, you need to restart or reconfigure this template.

- **Create the appropriate tcp-optimized profile (recommended)**  
Select this option to have the system create the recommended TCP profile. The parent profile (either WAN or LAN optimized) is determined by your selection to the "What type of network connects clients to the BIG-IP system" question.
- **Select the TCP profile you created from the list**  
If you created a custom TCP profile for this implementation, select it from the list.

7. ***Which HTTP profile do you want to use?*** **Advanced**

The HTTP profile contains settings for instructing the BIG-IP system how to handle HTTP traffic. Choose whether you want the iApp to create a new HTTP profile or if you have previously created an HTTP profile for this deployment.

Unless you have requirements for configuring specific HTTP settings, we recommend allowing the iApp to create a new profile. To select a profile from the list, it must already be present on the BIG-IP system. Creating a custom profile is not a part of this template; see **Local Traffic >> Profiles : Services : HTTP** to create a HTTP profile. To select any new profiles you create, you need to restart or reconfigure this template.

- **Select an existing HTTP profile from the list**  
If you already created an HTTP profile for this implementation, select it from the list.
- **Create a new HTTP profile (recommended)**  
Select this option for the iApp to create a new HTTP profile.

8. ***Do you want to create a new client SSL profile or use an existing one?***


*This question only appears if you selected Advanced configuration mode, however if you selected Basic mode, the Certificate and Key questions (a and b) under "Create a new Client SSL profile" appear.*

The iApp can create a new Client SSL profile, or if you have created a Client SSL profile which contains the appropriate SSL certificate and key for your implementation, you can select it from the list.

Unless you have requirements for configuring specific Client SSL settings, we recommend allowing the iApp to create a new profile. To select a profile from the list, it must already be present on the BIG-IP system. Creating a custom profile is not a part of this template; see **Local Traffic > Profiles > SSL > Client** to create a Client SSL profile. To select any new profiles you create, you need to restart or reconfigure this template.

- **Select the Client SSL profile you created from the list**  
If you manually created a Client SSL profile that includes the appropriate certificate and key, select it from the list.
- **Create a new Client SSL profile**  
Select this option if you want the iApp to create a new Client SSL profile.
  - a. ***Which certificate do you want this BIG-IP system to use for client authentication?***  
Select the SSL certificate you imported onto the BIG-IP system for client authentication.

If you have not yet imported a certificate, you can leave the default selections and reconfigure this iApp after obtaining the certificates. Using the default certificate and key results in an incomplete configuration which is not secure until you import and assign a trusted certificate and key that are valid for all fully qualified domain names used to access the application.

 **Warning** *The default certificate and key on the BIG-IP system is not secure and should never be used in production environments. The trusted certificate must be valid for all fully qualified domain names used to access the application. For more information on importing certificates and keys, see the BIG-IP documentation.*

b. What is the associated private key?

Select the SSL private key associated with the certificate you selected above.

c. Do you need to use an intermediate certificate?

Select whether you need to use an intermediate certificate in this implementation. Immediate certificates are intended to create a chain of trust between the CA that signed the certificate and the CA that is already trusted by the recipient of the certificate. This allows the recipient to verify the validity of the certificates presented, even when the signing CA is unknown. See <http://support.f5.com/kb/en-us/solutions/public/13000/300/sol13302.html> for help creating an intermediate certificate chain.

- **Do not use an intermediate certificate**  
Select this option if you do not require an intermediate certificate for this deployment. Continue with the next section.
- **Select the certificate you imported from the list**  
If you imported an intermediate certificate onto the BIG-IP system for this implementation, select it from the list.

## IDP Encryption Certificate and Key

This section gathers information about your SaaS application IdP environment that will be used in the BIG-IP virtual server.

1. Which certificate do you want to use to encrypt your SAML Assertion?

Select the name of the certificate you imported to use to encrypt your SAML Assertion. The certificate must be present on the BIG-IP system in order to select it. To select any new certificates and keys you import, you must restart or reconfigure this template.

 **Important** *The certificate can be either self-signed certificate generated by the BIG-IP system, or you can import a certificate for this purpose. The only restriction is you cannot use a wildcard certificate to sign SAML assertions to the SaaS application.*

2. What is the associated private key?

Select the SSL private key associated with the certificate you selected.


## iRules

In this section, you can add custom iRules to the deployment. This entire section is available only if you selected Advanced mode.

iRules are a scripting language that allows an administrator to instruct the system to intercept, inspect, transform, direct and track inbound or outbound application traffic. An iRule contains the set of instructions the system uses to process data flowing through it, either in the header or payload of a packet.

1. Do you want to add any custom iRules to the configuration? **Advanced**

Select if have preexisting iRules you want to add to your implementation.

 **Warning** *While iRules can provide additional functionality not present in the iApp, improper use or misconfiguration of an iRule can result in unwanted application behavior and poor performance of your BIG-IP system. We recommended you verify the impact of an iRule prior to deployment in a production environment.*

If you do not want to add any iRules to the configuration, continue with the following section.

If you have iRules you want to attach to the virtual server the iApp creates for your servers, from the **Options** box, click the name of the applicable iRule(s) and then click the Add (<<) button to move them to the **Selected** box.

## Finished

Review the answers to your questions. When you are satisfied, click the **Finished** button. The BIG-IP system creates the relevant objects.

## Appendix: Manual Configuration table

The BIG-IP system configuration for SAML consists of two parts: a one time setup, and a per SaaS application setup.

The table contains a list of configuration objects along with any non-default settings you should configure as a part of this deployment. Settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects and descriptions of how each step related back to overall configuration, refer BIG IP SAML Configuration is available at [https://support.f5.com/kb/en-us/products/big-ip\\_apm.html](https://support.f5.com/kb/en-us/products/big-ip_apm.html) > select your BIG IP version > click BIG-IP Access Policy Manager: Authentication and Single Sign-On.

**Configure the objects in this table no matter which SaaS application you are using.**

Profiles ( <i>Local Traffic &gt; Profiles</i> )		
<b>HTTP</b> ( <i>Profiles &gt; Services</i> )	Name	Type a unique name
	Parent Profile	<b>http</b>
	Insert X-Forwarded-For	<b>Enabled</b>
<b>TCP</b> ( <i>Profiles &gt; Protocol</i> )	Name	Type a unique name
	Parent Profile	<b>tcp-wan-optimized</b> or <b>tcp-lan-optimized</b> depending on where most clients are located
	Idle Timeout	<b>1800</b>
<b>Client SSL<sup>3</sup></b> ( <i>Profiles &gt; SSL</i> )	Name	Type a unique name
	Parent Profile	<b>clientssl</b>
	Certificate and Key	Select the Certificate and Key you imported from the associated list
	Chain	If applicable, select the Chain certificate you imported
<b>Health Monitors<sup>1</sup></b> ( <i>Local Traffic &gt; Monitors</i> )		<b>Note:</b> Only necessary if creating a pool of Active Directory servers. Choose <u>either</u> an ICMP or LDAP monitor.
<b>Simple ICMP Monitor</b>		
<b>Name</b>	Type a unique name.	
<b>Type</b>	<b>Gateway ICMP</b>	
<b>LDAP Monitor</b>		
<b>Configuration</b>	Select <b>Advanced</b> from the Configuration list (if necessary)	
<b>Name</b>	Type a unique name, such as AD_LDAP_monitor	
<b>Type</b>	<b>LDAP</b>	
<b>Interval</b>	<b>10</b> (recommended)	
<b>Timeout</b>	<b>31</b> (recommended)	
<b>User Name</b>	Type a user name with administrative permissions	
<b>Password</b>	Type the associated password	
<b>Base</b>	Specify your LDAP base tree. For example, CN=SharePoint Users,DC=example,DC=com	
<b>Filter</b>	Specify the filter. We type <b>cn=user1</b> , using the example above: user1 in OU group "SharePoint Users" and domain "example.com"	
<b>Security</b>	Select a Security option (either <b>None</b> , <b>SSL</b> , or <b>TLS</b> )	
<b>Chase Referrals</b>	<b>Yes</b>	
<b>Alias Address</b>	<b>*All Addresses</b>	
<b>Alias Address Port</b>	<b>389</b> (for None or TLS) or <b>686</b> (for SSL)	
<b>AAA Servers</b> ( <i>Access Policy--&gt;AAA Servers</i> )		
<b>If you are using a single Active Directory Server</b>		
<b>Name</b>	Type a unique name.	
<b>Type</b>	<b>Active Directory</b>	
<b>Domain Controller</b>	Type the IP address or FQDN name of an Active Directory Domain Controller	
<b>Domain Name</b>	Type the Active Directory domain name	
<b>Admin Name<sup>2</sup></b>	Type the AD user name with administrative permissions (optional)	
<b>Admin Password<sup>2</sup></b>	Type the associated password (optional). Type it again in the Verify Password box	

<sup>1</sup> Only necessary if using a pool of Active Directory servers

<sup>2</sup> Optional; Admin Name and Password are only required if anonymous binding to Active Directory is not allowed in your environment



<b>If you are using a pool of Active Directory Servers</b>	
<b>Name</b>	Type a unique name.
<b>Type</b>	<b>Active Directory</b>
<b>Domain Name</b>	Type the FQDN of the Windows Domain name
<b>Server Connection</b>	Click <b>Use Pool</b> if necessary.
<b>Domain Controller Pool Name</b>	Type a unique name
<b>Domain Controllers</b>	<b>IP Address:</b> Type the IP address of the first domain controller <b>Hostname:</b> Type the FQDN of the domain controller Click <b>Add</b> . Repeat for each domain controller in this configuration.
<b>Server Pool Monitor</b>	Select the monitor you created above.
<b>Admin Name<sup>2</sup></b>	Type the Administrator name
<b>Admin Password<sup>2</sup></b>	Type the associated password
<b>Connectivity Profile (Access Policy &gt; Secure Connectivity)</b>	
<b>Name</b>	Type a unique name
<b>Parent Profile</b>	<b>connectivity</b>
<b>Access Profile (Access Policy &gt; Access Profiles)</b>	
<b>Name</b>	Type a unique name.
<b>SSO Configuration</b>	Select the appropriate SSO Configuration you created.
<b>Languages</b>	Move the appropriate language(s) to the <b>Accepted</b> box.
<b>Access Policy (Access Policy &gt; Access Profiles &gt; Edit)</b>	
<b>Edit</b>	After completing all of the configuration objects, including those on the following pages, edit the Access Profile you just created using the guidance in <i>Editing the Access Policy using the VPE on page 20</i> .
<b>iRules (Local Traffic &gt; iRules) <b>Important:</b> Only necessary if your SaaS application is Office 365.</b>	
<b>Name</b>	Type a unique name.
<b>Definition</b>	Copy and paste the following code into the Definition field, omitting the line numbers.
	<pre> 1  when ACCESS_POLICY_AGENT_EVENT { 2      if {[ACCESS::policy agent_id] eq "encode"} { 3          set tmpVar [binary format H* [substr "[ACCESS::session data get session.ad.last.attr.objectGUID]" 2]] 4          ACCESS::session data set session.ad.last.attr.objectGUIDencoded [b64encode \$tmpVar] 5      } 6  }</pre>
<b>Virtual Servers (Local Traffic &gt; Virtual Servers)</b>	
<b>HTTP</b>	<i>(This virtual is only necessary if you want to redirect users from HTTP to HTTPS and if SAML services are configured with redirect binding.)</i>
<b>Name</b>	Type a unique name.
<b>Address</b>	Type the IP Address for the virtual server
<b>Service Port</b>	<b>80</b>
<b>iRule</b>	Enable the built-in <b>_sys_https_redirect</b> iRule
<b>HTTPS</b>	
<b>Name</b>	Type a unique name.
<b>Address</b>	Type the IP Address for the virtual server
<b>Service Port</b>	<b>443</b>
<b>Protocol Profile (client)</b>	Select the WAN optimized TCP profile you created above
<b>HTTP Profile</b>	Select the HTTP profile you created above
<b>SSL Profile (Client)</b>	Select the Client SSL profile you created above
<b>Access Profile</b>	Select the Access Profile you created
<b>Connectivity Profile</b>	Select the Connectivity profile you created above
<b>iRule</b>	If your SaaS application is Office 365 only, enable the iRule you created

After you have created all of the objects on this table, continue with the following page.

## Creating the SP initiated and/or IdP Initiated configuration

The following IdP SAML configuration consists of two subsections, depending on the whether you need SSO Portal (IdP and SP Initiated) or No SSO Portal (SP Initiated) SAML configuration:

1. **SSO Portal (IdP and SP Initiated)** – In this configuration, the user either authenticates to the IdP and then selects the SaaS application from SSO portal (IdP Initiated) or goes to the SaaS application and then gets redirected to the IdP for authentication (SP Initiated). In this case, you must complete both the IdP setup and external SP connector completed per SaaS application.
2. **No SSO Portal (SP Initiated)** – In this configuration, the user goes to the SaaS application and the SaaS SP redirects the user to the IdP for authentication (no SSO portal). For this configuration, the following IdP Setup Configuration should only be performed once, and the external SP connector configuration needs to be repeated for each SaaS application. (Note – the IdP setup configuration is only done once as in this case all the SP's share the same IdP configuration parameters.)

IdP Configuration (Access Policy > SAML > BIG-IP as IdP)	
<b>IdP Service Name</b>	Type a unique name.
<b>IdP Entity ID</b>	Type your Entity ID. See SaaS application table in <i>Configuring the IdP and SP connector settings for different web applications on page 19</i>
<b>IdP Name Settings</b>	<i>BIG-IP v12 only: If the Entity ID you typed above is a URN (like <code>idp:example.com:my_idp_name</code>):</i> You must configure the Name Settings: <b>Scheme:</b> Select either <b>https</b> or <b>http</b> as appropriate <b>Host:</b> Type the Host name of your IdP implementation.
<b>SAML Profiles</b>	Select Web Browser SSO profile. (Note: The SAML Profiles tab was introduced in 12.0)
<b>Assertion Settings</b>	In the left pane of the Create New IdP Service box, click Assertion Settings. Assertion Subject Type: Type the Subject Type, Refer the SaaS application in the table below for details. Assertion Subject Value: Type your Subject Value, Refer the SaaS application in the table below for details.
<b>SAML Attributes</b>	In the left pane of the Create New IdP Service box, click SAML Attributes. Name: Type your SAML Attribute Name. Value: Type your SAML Attribute Value, Refer the SaaS application in the table below for details
<b>Security Settings</b>	In the left pane of the Create New IdP Service box, click Security Settings. Assertion Signing Key: Select the appropriate Key Public Certificate: Select the appropriate Certificate
External SP Connector (Access Policy > SAML > BIG-IP as IdP > External SP Connectors (on the menu bar) > Create	
<b>Note:</b> <i>We strongly recommend you configure these options using the Import Metadata option (Create &gt; From Metadata, and then specify the File and Service Provider Name). Only use the following guidance if the metadata is not available.</i>	
<b>Service Provider Name</b>	Type a unique name.
<b>SP Entity ID</b>	Type your Entity ID. See SaaS application table in <i>Configuring the IdP and SP connector settings for different web applications on page 19</i>
<b>Endpoint Settings</b>	<i>In the left pane of the Create New SAML SP Connector box, click Endpoint Settings.</i> Relay State: None Assertion Consumer Service (click Add): Location URL: Type the URL. Refer the SaaS application in the table below for details. Binding: POST Index: 0 Default: Checked (Note – index and default fields have been added in BIG-IP v12.0)
<b>Security Settings</b>	<i>In the left pane of the Create New SAML SP Connector box, click Security Settings.</i> <b>Require Signed Authentication Request:</b> Refer value in the SaaS application in the table below. In the Response sent to SP by this device section <b>Response must be signed:</b> Refer value in the SaaS application in the table below. <b>Signing Algorithm:</b> RSA-SHA1 <b>Assertion must be signed:</b> Refer value in the SaaS application in the table below.
Bind/Unbind SP Connectors (Access Policy > SAML > BIG-IP as IdP)	
On the BIG-IP as IdP page, check the box to the right of the SAML IdP you created, and then click the <b>Bind/Unbind SP Connectors</b> button. Select the External SP Connector you just created, and then click the <b>OK</b> button to complete the binding.	
SAML Resource (Access Policy > SAML > SAML Resources)	
<b>Name</b>	Type a unique name.
<b>Publish on Webtop</b>	<b>Enabled</b>
<b>SSO Configuration</b>	Select the SSO Configuration you just created
Webtop (Access Policy > Webtops)	
<b>Note:</b> <i>The Webtop should only be configured once for ALL SaaS applications (not one per SaaS application).</i>	
<b>Name</b>	Type a unique name
<b>Type</b>	<b>Full</b>

## Configuring the IdP and SP connector settings for different web applications

These tables describe the IdP and SP connector configuration for different web applications to be used with the preceding tables.

➔ **Note:** The EntityID mentioned in the following table is a required configuration setting used by the Service Provider (SP) to identify and match the SAML assertion coming from the BIG-IP system. The format of the IdP Entity ID should be the URL that users use to authenticate themselves to the BIG-IP system. For example, if the Entity ID is `https://login.example.com/idp/saml/idpm` the federation service host name is `login.example.com`.

IdP Service Configuration				
SaaS Application	IdP Entity ID1	Subject-type	Subject-value	SAML Attribute
Salesforce	https://[BIG IP IdP virtual server DNS URL]/saml/idp	Entity	<code>%{session.samlresource.last.emailaddr}</code> <sup>1,2</sup>	Blank
Workday		Entity	<code>%{session.ad.last.attr.sAMAccountName}</code>	Blank
Amazon Web Services		Unspecified	<code>%{session.ad.last.attr.sAMAccountName}</code>	See below <sup>3</sup>
Concur		email-address	<code>%{session.samlresource.last.emailaddr}</code> <sup>1</sup>	Blank
Service-Now		Entity	<code>%{session.ad.last.attr.sAMAccountName}</code>	Blank
Jive		Unspecified	<code>%{session.ad.last.attr.sAMAccountName}</code>	See below <sup>4</sup>
Wombat		email-address	<code>%{session.ad.last.attr.mail}</code>	Blank
Zendesk		email-address	<code>%{session.samlresource.last.emailaddr}</code> <sup>1</sup>	Blank
Webex		Unspecified	<code>%{session.ad.last.attr.mail}</code>	Blank
Box		email-address	<code>%{session.ad.last.attr.mail}</code>	Blank
Google Apps		Unspecified	<code>%{session.ad.last.attr.mail}</code>	Blank

<sup>1</sup> Use session variable `session.samlresource.last.emailaddr` to ensure the case sensitivity of the email address for this configuration. (With `session.ad.last.attr.mail` the case sensitivity will not be valid for thiS SaaS application). Use the variable assign VPE object with TCL command - `session.samlresource.last.emailaddr = return [string tolower [mcget {session.ad.last.attr.mail}]]`

<sup>2</sup> Salesforce – Recommendation is to use email address as the subject value for Salesforce IdP setup. (Avoid using Federated ID as it can lead to issues.)

<sup>3</sup> AWS – Add the following two name-value pairs. The Role ARN can be found in the IAM Management Console in the Roles section.

Name	Value
<code>https://aws.amazon.com/SAML/Attributes/RoleSessionName</code>	<code>%{session.ad.last.attr.sAMAccountName}</code>
<code>https://aws.amazon.com/SAML/Attributes/Role</code>	<code>arn:aws:iam::[Account Code]:role/%{session.samlresource.role.cloud275},arn:aws:iam::[Account Code]:saml-provider/[Site Code]</code>

<sup>4</sup> Jive – Add the following three name-value pairs

Name	Value
Mail	<code>%{session.ad.last.attr.mail}</code>
Sn	<code>%{session.ad.last.attr.sn}</code>
givenName	<code>%{session.ad.last.attr.givenName}</code>

Continue with the SP Connector Configuration table on the following page

SP Connector Configuration				
SP Entity ID	Sign request	Sign response	Sign Assertion	Assertion Consumer Service URL
https://saml.salesforce.com <sup>1</sup>	Blank	Check	Blank	https://test.salesforce.com/?saml=[Site Code] <sup>2</sup>
http://www.workday.com/implementation/urn:amazon:webservices		Blank	Check	https://wd5.myworkday.com/[Environment Code]/login-saml.flex <sup>2</sup>
https://www.concursolutions.com/SAMLRedirector/ClientSAMLLogin.aspx		Check	Blank	https://signin.aws.amazon.com/saml
https://[Site Code].service-now.com <sup>2</sup>		Check	Blank	https://www.concursolutions.com/SAMLRedirector/ClientSAMLLogin.aspx
https://hive.[Site Code].com <sup>2,3</sup>		Check	Blank	https://[Site Code].service-now.com/navpage.do <sup>2</sup>
https://sso.wombatsecurity.com/shibboleth		Check	Blank	https://hive.[Site Code].com/saml/sso <sup>2</sup>
https://[Site Code].zendesk.com <sup>2</sup>		Check	Blank	https://sso.wombatsecurity.com/Shibboleth.sso/SAML2/POST
http://www.webex.com		Check	Blank	https://[Site Code].zendesk.com/access/saml <sup>2</sup>
box.net <sup>4</sup>		Check	Check	https://[Site Code].webex.com/dispatcher/SAML2AuthService?siteurl=[Site Code] <sup>2</sup>
google.com/a/[GoogleAppsDomain Name]		Blank	Check	https://sso.services.box.net/sp/ACS.saml2
		Check	Blank	https://www.google.com/a/yourGoogleAppDomainName/acs

<sup>1</sup> For SP initiated SAML, the SP Entity ID must match the domain value as described in the Salesforce documentation - [https://developer.salesforce.com/page/Single\\_Sign-On\\_with\\_Force.com\\_and\\_Microsoft\\_Active\\_Directory\\_Federation\\_Services#My\\_Domain](https://developer.salesforce.com/page/Single_Sign-On_with_Force.com_and_Microsoft_Active_Directory_Federation_Services#My_Domain)

<sup>2</sup> Site Code, Environment Code and Department Code are values negotiated with the SaaS application provider during service registration.

<sup>3</sup> The host name part of the URL can be configured as applicable, e.g.: host name is "hive" here. (Jive is deployed on-premise service).

<sup>4</sup> The Single Logout Request URL for box.net is <https://sso.services.box.net/sp/SLO.ssaml2>.

## Editing the Access Policy using the VPE

The next step is to edit the Access Policy for the SaaS application on the APM using the Visual Policy Editor (VPE). The VPE is a powerful visual scripting language that offers virtually unlimited options in configuring an Access Policy.

### To edit the Access Policy

- On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
- Locate the Access Profile you created, and then, in the Access Policy column, click **Edit**. The VPE opens in a new window.
- Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.
- Click the **Logon Page** option button, and then click the **Add Item** button.
  - Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.
  - Click **Save**.
- Click the **+** symbol on the between **Logon Page** and **Deny**.
- On the Authentication tab, click **AD Auth** option button, and then click the **Add Item** button.
  - From the **Server** list, select the AAA server you configured in the table above.
  - Click **Finished** and then click **Save**. You now see a Successful and Fallback path from AD Auth.
- On the Successful path between **AD Auth** and **Deny**, click the **+** symbol.
- On the Authentication tab, click the **AD Query** option button, and then click **Add Item**.
  - From the **Server** list, select the AAA server you created.
  - In the **Search Filter** box, type **samAccountName=%{session.logon.last.username}**
  - Click the Branch Rules tab and then click the delete (x) button next to the default branch rule to remove it.
  - Click **Add Branch Rule**.
  - In the **Name** box, type **Successful**.
  - Click the **change** link.
  - Click the **Add Expression** button.

- h. From the **Agent Sel** list, select **AD Query**.
- i. From the Condition list, select AD Query Passed, and then click the **Add Expression** button.
- j. Click **Finished** and then click **Save**.

9. On the Successful path between **AD Query** and **Deny**, click the **+** symbol.

**10. These steps are only required if your SaaS Application is Office 365:**

- a. On the General Purpose tab, click the **iRule Event** option button, and then click **Add Item**.
- b. In the **ID** field, type **encode**.
- c. Click **Save**.

**11. This step is only required for IdP-initiated SAML; not required for SP initiated:**

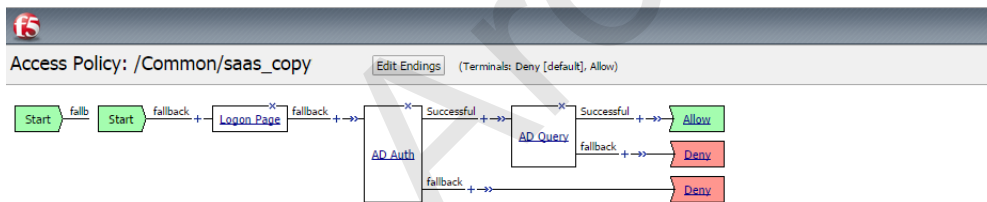
On the Successful path between **AD Query** (or **iRule Event**) and **Deny**, click the **+** symbol.

- a. On the Assignment tab, click the **Advanced Resource Assign** option button, and then click **Add Item**.
- b. Click **Add new entry**.
- c. Click the **Add/Delete** link on the new entry.
- d. Click **SAML** tab.
- e. Check the box for the SAML SSO Configuration you created using the table.
- f. Click the **Webtop** tab.
- g. Click the option button for the Webtop profile you created using the table.
- h. Click **Update**, and then click the **Save** button.

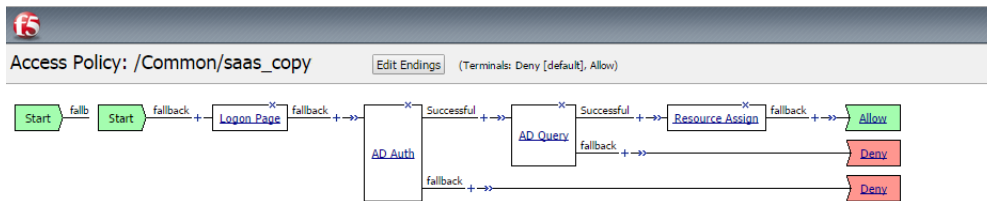
12. On the path between **Advanced Resource Assign** (or **AD Query** or **iRule Event**) and **Deny**, click the **Deny** box, click **Allow**, and then click **Save**.

13. Click the yellow Apply Access Policy link in the upper left part of the window, and then click the **Close** button on the upper right.

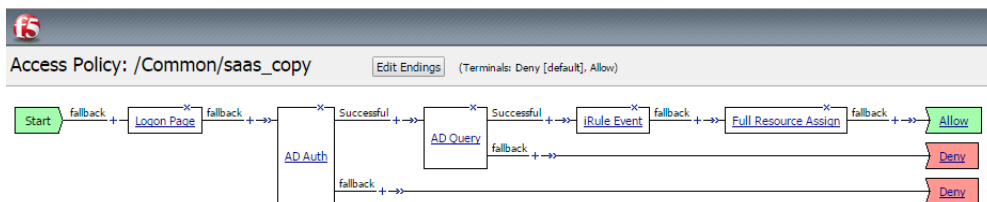
When complete, your VPE should look similar to the following example if you did not configure the iRule event or Resource Assign.



If you did configure the Resource Assign event but not the iRule event, your VPE should look similar to the following



If you configured both the Resource Assign and the iRule event, your VPE should look similar to the following:



---

## Testing the newly Configured Federated Setup

To test your newly-configured federated domain, open a web browser and go to Assertion Consumer service URL listed in table above (for example for AWS go to <https://signin.aws.amazon.com/saml>). You should be redirected to your federation URL on your BIG-IP APM and see the login page.

Type your Active Directory credentials, and then the BIG-IP system should issue a SAML Assertion to the SaaS application. If the assertion was properly accepted, the user sees their SaaS application account. If they are not provisioned with a SaaS application, they will see an error message informing them of that.

Archived

## Troubleshooting

We strongly recommend you configure the external SP connector part of the IdP setup by importing metadata from the SP. If you have to configure the external SP connector manually, ensure all the URLs are valid and are not missing any required forward slashes (/).

If you choose to transition from SP initiated (no SSO portal) to SSO portal implementation you need to unbind multiple SP connectors from the single IdP and follow the steps mentioned in the SSO portal section (*Creating the SP initiated and/or IdP Initiated configuration on page 18*) for setting up the configuration.

To debug other issues, we recommend collecting a SAML trace and BIG-IP log information by using the following tools

1. Collect HTTP traces using anyone of the below mentioned tools
  - » Firefox SAML Tracer Plugin
  - » HTTP Watch
  - » Fiddler2

For example refer to the following example of SAML trace with reference fields that can be verified to debug SAML issues. The value of the fields highlighted below should match the value defined in the Per SaaS Application SAML Configuration Table and settings required by the SP.

```
<saml2p:Response ID="_af0cc54316a8c9baaf3ace3575f317775fd135"
  IssueInstant="2015-08-20T18:38:54Z"
  Destination=https://www.concursolutions.com/SAMLRedirector/ClientSAMLLogin.aspx <-SAML destination on where the request should be sent
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
  Version="2.0"
  >
<saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://trust.XYZ.com/saml/idp </saml2:Issuer> <- SAML IdP Entity ID
<saml2p:Status>
<saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</saml2p:Status>
<saml2:Assertion Version="2.0"
  ID="_03b3f64db7f1b81a2e11e290414033c3349ab2"
  IssueInstant="2015-08-20T18:38:54Z"
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
  >
<saml2:Issuer>https://trust.XYZ.com/saml/idp </saml2:Issuer> <- SAML IdP Entity ID
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <ds:Reference URI="#_03b3f64db7f1b81a2e11e290414033c3349ab2">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
              PrefixList="xs"
            />
          </ds:Transforms>
        </ds:Reference>
      </ds:SignedInfo>
    </ds:Signature>
  </saml2:Assertion>
</saml2p:Response>
```

```

        </ds:Transform>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    <ds:DigestValue>BkkCgMZGroGBug3JrF/2w02ZMgc=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
    <ds:SignatureValue>OmsIEr/1dnAJ0TJBxPSgZs627d/SanKCtr30nGOMck23vseS96VuoJUA4+SAqcLIyeH0pF+M0Mfvn3oJESdIbxqF0icpXB4z62wTFS/OJU
way8KT50tqkUo+tf3Vx1EJNgByZz0uSpdbv/Vn06kvc4U0u3dotjhjTFT6sTC8qjJSIr10BnYmy6F1DCtYSLuc3MU1sSxU0aW0J4XkEAVtwf0FRFDKR2Yb4xuj4sd0mc3TFH6jPn/
sZ0QExr6DAL/AcRX3LiEV9sdH5nfgreYFpkqoSMMcg1e+YKqB/NRoHFU0H3/4+1kker1ZA+IA/sZcIAuvvJ7I6Gz6XE+59WM5g==</ds:SignatureValue>
    <ds:KeyInfo>
        <ds:X509Data>
            <ds:X509Certificate>MIIGDCCBVygAwIBAgITcwAARuT+LC57ZUoJbgAAAABG5DANBgkqhkiG9w0BAQUF
ADBNMRMwEQYKCZImiZPyLGBGRYDY29tMRUwEwYKCCZImiZPyLGBGRYFRjVOZXQx
<snipped for brevity>...
1QvyZC1sTPYDg3XVUUC9LKRyuuOnhDwA</ds:X509Certificate>
        </ds:X509Data>
    </ds:KeyInfo>
</ds:Signature>
<saml2:Subject>
    <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">User@XYZ.com </saml2:NameID> <- SAML subject
    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml2:SubjectConfirmationData NotOnOrAfter="2015-08-20T18:48:54Z"
            Recipient="https://www.concursolutions.com/SAMLRedirector/ClientSAMLLogin.aspx"
            />
    </saml2:SubjectConfirmation>
</saml2:Subject>
<saml2:Conditions NotBefore="2015-08-20T18:38:54Z"
    NotOnOrAfter="2015-08-20T18:48:54Z"
    >
    <saml2:AudienceRestriction>
        <saml2:Audience>https://www.concursolutions.com/SAMLRedirector/ClientSAMLLogin.aspx </saml2:Audience> <-SAML_SP_Entity-ID
    </saml2:AudienceRestriction>
</saml2:Conditions>
<saml2:AuthnStatement AuthnInstant="2015-08-20T18:38:54Z"
    SessionIndex="_03b3f64db7f1b81a2e11e290414033c3349ab2"
    >
    <saml2:AuthnContext>
        <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
</saml2:AuthnStatement>
</saml2:Assertion>
</saml2p:Response>

```



2. Collect BIG-IP debug logs by enabling them using anyone of the following methods
  - a. In BIG-IP as IdP tab > IdP Setup > Select Log level as "Debug"
  - b. For pre 12.0 - Goto TMSH CLI and modify sys db log.sso.level value to debug (IdP and SP) .
  - c.

For post 12.0 – Go to **Access Policy > Event Logs > Log Settings >** and then select the log setting associated with the Access Profile. Click the **Edit > Access System Logs**, and then from the **SSO list**, select **Debug**.

;If you need to contact F5 support for any issues, collect the following information and the SAML trace and debug logs are mentioned above. The data should be collected from the beginning of the transaction (eg: user goes to the SP/IdP) to the end (when the issue is observed).

1. QKView (post enabling debug logging)
2. Details of the virtual server configuration, APM profile and configured SAML object in BIG IP IdP.
3. Details of any third party application used in the setup.

Archived

## Document Revision History

Version	Description	Date
1.0	New guide	01-26-2016
1.1	Substantially updated the guide for the improved release candidate version of the iApp (f5.saas_idp.v.1.0.0rc1).	04-20-2016
1.2	Updated the guide for the official release candidate version of the iApp (f5.saas_idp.v.1.0.1rc1) on downloads.f5.com.	06-16-2016
1.3	Updated the guide for the official release candidate version of the iApp (f5.saas_idp.v.1.0.1rc2) on downloads.f5.com which includes the following changes:  - Corrected an issue that caused TCL iApps using client-ssl profiles to break when the iApp was reconfigured. This issue only affected iApps running on BIG-IP 14.1.	01-31-2019

Archived

**F5 Networks, Inc.** 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 [www.f5.com](http://www.f5.com)

F5 Networks, Inc.  
Corporate Headquarters  
[info@f5.com](mailto:info@f5.com)

F5 Networks  
Asia-Pacific  
[apacinfo@f5.com](mailto:apacinfo@f5.com)

F5 Networks Ltd.  
Europe/Middle-East/Africa  
[emeainfo@f5.com](mailto:emeainfo@f5.com)

F5 Networks  
Japan K.K.  
[f5j-info@f5.com](mailto:f5j-info@f5.com)

