



DEPLOYMENT GUIDE

The F5 BIG-IP and Ping Identity Integrated Solution for Secure Access Management



February 2017

Contents

Contents.....	2
Introduction	3
Prerequisites	3
Use Case 1: Horizontal Scaling and Offloading PingAccess Agent Functionality to the BIG-IP Platform	5
Create local traffic pools of PingAccess nodes on the BIG-IP system.....	6
Create a PingAccess agent properties file.....	7
Upload PingAccess agent properties to BIG-IP APM	8
Create a PingAccess profile for BIG-IP APM authentication	9
Add the PingAccess profile to the virtual server	10
Verification.....	10
Use Case 2: SAML Single Sign-On	11
Create a PingFederate IdP adapter.....	12
Create an SP connection for BIG-IP APM.....	13
Export the metadata file from PingFederate	17
Configure SAML SP and IdP on the BIG-IP system.....	17
Configure BIG-IP access policy to authenticate with the PingFederate IdP	19
Add the access profile to the virtual server	20
Verification.....	21
Appendix	22
Statistics	22
BIG-IP APM reports.....	22
Passing SAML attributes to a back-end web application.....	22
Troubleshooting PingAccess and PingFederate	23

Introduction

The F5 and Ping Identity joint solution helps customers take advantage of the benefits of single sign-on (SSO) and federated identity in cloud computing environments. Used in conjunction with F5® BIG-IP® Access Policy Manager® (APM), the PingFederate cloud identity management (IdM) software extends the benefits of F5 access and security capabilities to federated environments. As a result, organizations can achieve stronger security while enjoying the benefits of cloud computing.

The highly scalable joint solution provides seamless access for internal and external users anywhere, anytime, from any device. Using trusted, standards-based identity protocols (including SAML, OpenID, WS-Federation, and OAuth), the solution enables employees, customers, partners, or consumers to access multiple resources using their existing network credentials. The solution also eases IT administration and helps to reduce costs because it provides consolidated user access control across both cloud and on-premises resources. It also speeds the roll-out of cloud and mobile applications because user accounts are automatically added to cloud-based applications.

This guide addresses deployment of the joint solution for two common use cases:

- Horizontal scaling and offloading of PingAccess agent functionality to an F5 BIG-IP platform
- SAML single sign-on implementation

Prerequisites

Deploying the joint solution requires provisioning the following F5 products or software modules:

- **F5 BIG-IP® Local Traffic Manager™ (LTM)** for intelligent traffic management as well as advanced application security, acceleration, optimization, and load balancing.
- **F5 BIG-IP APM** for policy enforcement to secure web access.

The following PingIdentity products are also needed to deploy the joint solution:

- **PingAccess® server** for access policy management to web application and application programming interfaces (APIs).
- **PingFederate® server** for secure single sign-on, API security and provisioning for web users.

Optionally, customers can consider:

- **F5 BIG-IP® Application Security Manager™ (ASM)** to deploy web application firewall (WAF) services for application protection.
- **F5 BIG-IP® Advanced Firewall Manager™ (AFM)** for protection from aggressive volumetric DDoS attacks.

DEPLOYMENT GUIDE

F5 and Ping Identity Secure Access Management

The following implementation steps must be completed before you proceed with the configuration tasks described in this guide:

1. The F5 BIG-IP platform must be installed with F5 TMOS® version 13.0 or higher.
2. BIG-IP LTM and BIG-IP APM modules must be licensed and provisioned on the BIG-IP system.
3. The web application to be protected must be published and deployed on the BIG-IP system. Refer to the guidance available at <https://www.f5.com/pdf/deployment-guides/iapp-http-dg.pdf>.
4. The PingAccess solution must be installed with the administrative console and runtime engine nodes defined. Refer to the guidance at https://docs.pingidentity.com/category/product_docs.
5. The PingFederate solution must be installed and integrated with PingAccess.
6. Network reachability must exist between the BIG-IP system, PingAccess, and PingFederate.

Use Case 1: Horizontal Scaling and Offloading PingAccess Agent Functionality to the BIG-IP Platform

The BIG-IP system provides flexible, high-availability scaling by distributing application access requests to many PingAccess nodes, depending on resource constraints and availability. This enables true horizontal scaling.

By default, TMOS software version 13.0 and higher ships with PingAccess agent/gateway protocol support. This support enables the BIG-IP platform to serve as the policy enforcement point (PEP), intercepting requests to the protected resources on the web server and evaluating the applicable access control policies. These policies are evaluated either by accessing a locally cached policy decision or by querying PingAccess.

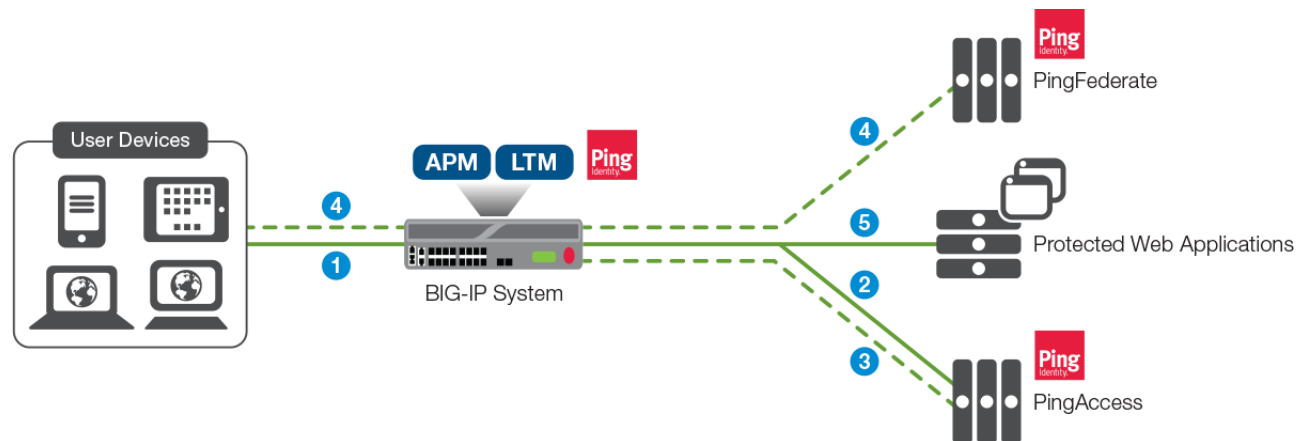


Figure 1: The F5 BIG-IP system deployed as a policy enforcement point for secure web access.

In this deployment, a user request flows to a protected resource in this manner:

1. The client requests a protected resource on the web server. If the user is already authenticated, this request is handled per step 5 below.
2. Using the built-in PingAccess agent functionality, BIG-IP APM requests a decision from the PingAccess policy server.
3. PingAccess checks the URL policy and determines that the requested resource is protected. It then responds to BIG-IP APM indicating that the user should be redirected to PingFederate for authentication.
4. BIG-IP APM redirects the user to PingFederate. After successful authentication, the user is redirected to BIG-IP APM with a PingFederate token.
5. BIG-IP APM passes the PingFederate token to PingAccess, which validates the PingFederate response and provides BIG-IP APM with the decision to allow or deny access to the resource. (This decision comes with an expiration and will be cached in BIG-IP APM, which enforces the decision until its expiration.)

When the decision is to allow access (or when a previous decision that has not yet expired is in the cache), the user is directed to the resource.

Solution configuration for this deployment includes:

- Configuring a load balancing pool of PingAccess nodes.
- Creating PingAccess agent properties on PingAccess.
- Importing those properties into the BIG-IP system.
- Configuring a PingAccess profile.
- Associating the access profile to the virtual server.

Create local traffic pools of PingAccess nodes on the BIG-IP system

Configure a pool of PingAccess nodes that serve requests from the BIG-IP system, which acts as a policy enforcement point in place of a PingAccess agent.

1. On the main tab of the BIG-IP system management interface, click **Local Traffic > Pools**.
2. When the **Pool List** screen opens, click **Create**.
3. When the **New Pool** screen opens, in the **Name** field, type a unique name for the pool.
4. In the **Health Monitors** section, select **tcp**. Or select an HTTP or HTTPS type of health monitor if you configure one to use this custom send string:

```
GET /pa/heartbeat.ping\r\n.
```

5. In the **Resources** section, under **New Members**, add PingAccess nodes that serve requests from the same agent. Do this by either typing an IP address in the **Address** field or selecting a preexisting node address from the **Node List**. Then, in the **Service Port** field, type the port number. (The default port number for PingAccess node is 3030.) Finally, click **Add**.
6. **Click Finished**. The new pool appears in the pool list.

The screenshot displays the 'Basic' configuration tab for a PingAccess pool. The 'Name' field is 'PingAccessPool' and the 'Description' is 'Loadbalancing pool of PingAccess nodes'. Under 'Health Monitors', the 'Active' list contains '/Common/Ping' and the 'Available' list contains '/Common/gateway_icmp', 'http', 'http_head_f5', and 'https'. In the 'Resources' section, the 'Load Balancing Method' is 'Round Robin' and 'Priority Group Activation' is 'Disabled'. The 'New Members' section shows three radio buttons: 'New Node' (selected), 'New FQDN Node', and 'Node List'. Below these, the 'Node Name' is '192.168.16.213' (Optional), 'Address' is '192.168.16.213', and 'Service Port' is '3030'. An 'Add' button is present, and a text box below it contains the string 'R:1 P:0 C:0 192.168.16.212 192.168.16.212 :3030'. At the bottom are 'Edit' and 'Delete' buttons. The footer contains 'Cancel', 'Repeat', and 'Finished' buttons.

Figure 2: A load balancing pool of PingAccess nodes

If the deployment consists of multiple PingFederate servers, you can create a similar pool and an associated virtual server on the BIG-IP system to load balance the requests. You should use this virtual server IP and port number to connect to PingFederate pool.

Create a PingAccess agent properties file

Create PingAccess agent and generate-properties files for the BIG-IP system to manage authorizations before allowing client requests to access the protected resources.

1. Log in to the PingAccess web UI. On the main tab, click **Agents**.
2. In the list of existing agents, click **Add Agent**.
3. On the **New Agent** page, specify a **Name** and enter the **PingAccess Hostname** and **Port**.

Note. The BIG-IP system does not consume the PingAccess host and port number information in the properties file, as the system is already aware of the PingAccess nodes and the ports of the members in its local load balancing pool.

4. Click **Save & Download** to generate the PingAccess properties file. You will import the saved PingAccess properties file into BIG-IP system in the next procedure.

The screenshot shows the 'New Agent' configuration page in the PingAccess interface. The left sidebar contains a 'MAIN' section with links to Applications, Sites, Agents (highlighted), and Policies, and a 'SETTINGS' section with links to Access and Networking. The main content area has the following fields:

- NAME:** A text input field containing 'BIGIP'.
- DESCRIPTION:** A text input field containing 'Agent Properties'.
- PINGACCESS HOST:** A text input field containing '192.168.16.212' and a port dropdown menu set to '3030'.
- FAILOVER HOST:** A text input field with a question mark icon.

At the bottom right, there is a blue 'Save & Download' button. The footer of the sidebar shows copyright information: 'Copyright © 2003-2017 Ping Identity Corporation. All rights reserved.'

Figure 3: Agent configuration on PingAccess

Upload PingAccess agent properties to BIG-IP APM

To upload the agent properties file exported from PingIdentity server (in [the last procedure](#)) into BIG-IP APM, follow these steps:

1. On the main tab of the BIG-IP management interface, navigate to **Access > Federation > PingAccess > Agent Properties** and click **Create**.
2. When the new screen opens, type a unique **Name**.
3. In the Configuration area for **Properties File**, click **Browse**.
4. Navigate to and select the agent properties file you downloaded from PingAccess server. Click **Open**.
5. If BIG-IP APM detects a valid SSL certificate in the properties file, an **Import SSL Certificate** check box displays. (See Figure 4.) If so, select it, and the SSL certificate loads from the PingAccess server.

Note: When importing the SSL certificate, the BIG-IP system can automatically detect and create the server **SSL profile** and specify the SSL certificate in the **Trusted Certificate Authorities** field.

If no check box displays, indicating that the BIG-IP system did not detect an SSL certificate to import, you will need to download the SSL certificate manually from the PingAccess server, import it to the BIG-IP system, and configure a server SSL profile to use it.

6. Click **Finished**.

General Properties	
Name	PingAccessAgent
Configuration	
Properties File	C:\BIGIP_agent.propertie Browse...
Import SSL Certificate	<input checked="" type="checkbox"/> Enable
Cancel Repeat Finished	

Figure 4: Importing the PingAccess agent properties file into BIG-IP APM

Create a PingAccess profile for BIG-IP APM authentication

Next, configure a profile on the BIG-IP system that specifies the PingAccess agent properties and PingAccess pool name for integration with APM

1. In the main tab of the BIG-IP management interface, click **Access > Federation > PingAccess > Profiles** and click **Create**.
2. When the new screen opens, type a unique **Name**.
3. Under **Configuration**, select a **Properties File** from the list, or click **+** to upload a PingAccess agent properties file before you make a selection.
4. Select the **Pool Name** of the pool of PingAccess nodes that you configured earlier, or click **+** to create a new pool.
5. By default, the **Use HTTPS** setting is selected (enabled). If you use this default, select the **Server SSL Profile** that is configured with the PingAccess server SSL certificate as the trusted certificate authority. If BIG-IP APM imported the server SSL certificate from the PingAccess agent properties file, the profile name will match the properties file name.

General Properties	
Name	PingAccessProfile
Configuration	
Properties File	+ /Common/PingAccessAgent ▼
Pool Name	+ /Common/PingAccessPool ▼
Use HTTPS	<input checked="" type="checkbox"/> Enabled
Server SSL Profile	/Common/PingAccessAgent ▼
Cancel Repeat Finished	

Figure 5: PingAccess profile configuration on the BIG-IP system

Add the PingAccess profile to the virtual server

The PingAccess profile must be associated with the virtual server of the web application for BIG-IP APM to apply the profile to incoming traffic. In addition, if an access policy is configured for this access profile, you must run it.

1. First, before you assign the PingAccess profile, ensure the virtual server is configured with a **tcp** and **http** profile.
2. Then, on the main tab of the BIG-IP management interface, click **Local Traffic > Virtual Servers**.
3. When the **Virtual Server List** appears, click the name of the virtual server.
4. Scroll down to the **Access Policy** section. Select the correct **PingAccess Profile**.
5. Click **Update** to save.

General Properties	
Name	PingAccessProfile

Configuration	
Properties File	+ /Common/PingAccessAgent ▼
Pool Name	+ /Common/PingAccessPool ▼
Use HTTPS	<input checked="" type="checkbox"/> Enabled
Server SSL Profile	/Common/PingAccessAgent ▼

Cancel Repeat Finished

Figure 6: Associating the PingAccess profile with the virtual server

Verification

The joint solution can be verified by accessing the protected resources on the web server. If you are deploying into a test environment in which you do not already have an application protected behind the BIG-IP system, you can deploy and use the pre-packaged [PingAccess Quickstart Application](#).

Refer to the [Appendix](#) of this document for troubleshooting aids.

Use Case 2: SAML Single Sign-On

The joint solution that uses the BIG-IP system as a SAML service provider (SP) and PingFederate as a SAML identity provider (IdP) delivers best-of-breed SAML single sign-on (SSO) with full legacy, on-premises and off-premises support in virtual desktop infrastructure (VDI), SSL VPN, or web access management (WAM) environments.

Figure 7 illustrates one such SAML SSO integration use case for WAM in which the BIG-IP system also acts as a reverse proxy for publishing apps beyond the firewall, where they can be accessed through PingFederate.

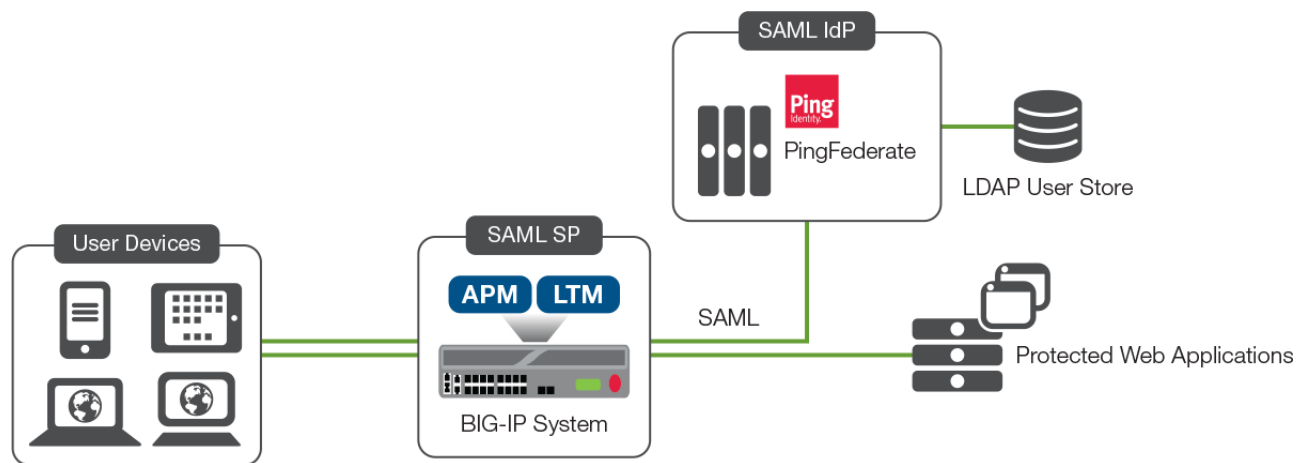


Figure 7: SAML SSO integration with the BIG-IP system and PingFederate

SAML SSO integration entails:

- The use of BIG-IP APM as the SP and PingFederate as the IdP. A SAML trust is built between the BIG-IP system and PingFederate.
- Users can be defined locally within PingFederate. In most cases, an on-premises Active Directory and/or LDAP is the source of identities and is integrated with PingFederate.
- The target web resources are protected behind the BIG-IP system. If the web servers are Windows-based, the customer may have an option to set up Kerberos-based SSO.
- SAML assertions from PingFederate are consumed by the BIG-IP system, which appropriately translates those assertions for the downstream application based on the application's authentication scheme.

Deployment configuration for this solution includes:

- Configuring a PingFederate IdP adapter.
- Creating a PingFederate SP connection, on PingFederate, for the BIG-IP system.
- Configuring BIG-IP APM as a SAML SP.
- Configuring PingFederate as a SAML IdP, leveraging the metadata file.
- Creating a SAML policy and associating it with the virtual server on the BIG-IP system.

Create a PingFederate IdP adapter

The configuration steps below assume that a password credential validator is configured on PingFederate. Refer to [PingFederate documentation](#) to understand and configure a password credential validator before proceeding with the next steps. (In the sample configuration below, an LDAP user store has been added as the password credential validator.)

1. Log in to the PingFederate web UI. From the main tab, navigate to **IdP Configuration > Adapters**.
2. Under **Manage IdP Adapter Instances**, click **Create New Instance**.
3. On the **Type** tab, enter an **Instance Name** and **Instance ID**. The ID may not contain spaces or underscores.
4. Select **HTML Form IdP Adapter** as the **TYPE**, and then click **Next**.

Manage IdP Adapter Instances | Create Adapter Instance

Type | IdP Adapter | Extended Contract | Adapter Attributes | Adapter Contract Mapping | Summary

Enter an Adapter Instance Name and Id, select the Adapter Type, and a parent if applicable. The Adapter Type is limited to the adapters currently installed on your server.

INSTANCE NAME

INSTANCE ID

TYPE [Visit Pingidentity.com for additional types](#)

PARENT INSTANCE

Figure 8: Creating a new IdP adapter instance

5. On the **IdP Adapter** tab, click **Add a new row to 'Credential Validators'** to define a credential-authentication mechanism instance for the adapter.
6. Select a password **Credential Validator** and click **Update**.
7. Scroll down and click **Next**.

Manage IdP Adapter Instances | Create Adapter Instance

Type	IdP Adapter	Extended Contract	Adapter Attributes	Adapter Contract Mapping	Summary
Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.					
CREDENTIAL VALIDATORS (A list of Password Credential Validators to be used for authentication.)					
PASSWORD CREDENTIAL VALIDATOR INSTANCE					Action
<div>LDAPUserStore</div>					<div>Update</div> <div>Cancel</div>
Add a new row to 'Credential Validators'					

Figure 9: Adding credential validators to the IdP adapter

- On the **Extended Contract** tab, click **Next**.
- On the **Adapter Attributes** tab, select the username checkbox under **Pseudonym** (and, optionally, other attributes, if available), and then click **Next**.
- On the **Adapter Contract Mapping** tab, click **Next**.
- Review the **Summary** and click **Done**.

Create an SP connection for BIG-IP APM

Create a PingFederate SP connection for BIG-IP APM.

- On the PingFederate management console, navigate to **IdP Configuration > SP Connections** and click **Create New**.
- On the **Connection Type** tab, click **Next**.
- On the **Connection Options** tab, click **Next**.
- On the **Import Metadata** tab, click **Next**.
- On the **General Info** tab, enter the BIG-IP system's **Entity ID** and **Connection Name**. Scroll down and click **Save**. (Alternatively in step-4, you can import the metadata file below containing the entity ID and connection name after configuring the [SP Service below](#).)

SP Connection

Connection Type	Connection Options	Import Metadata	General Info	Browser SSO	Credentials	Activation & Summary
<p>This information identifies your partner's unique connection identifier (Connection ID). Connection Name represents the plain-language identifier for this connection. Optionally, you can specify multiple virtual server IDs for your own server to use when communicating with this partner. If set, these virtual server IDs will be used in place of the unique protocol identifier configured for your server in Server Settings. The Base URL may be used to simplify configuration of partner endpoints.</p>						
PARTNER'S ENTITY ID (CONNECTION ID)		<input type="text" value="https://democorp.net/sp"/>				
CONNECTION NAME		<input type="text" value="BIG-IP-SP"/>				
VIRTUAL SERVER IDS		<input type="text"/> <input type="button" value="Add"/>				
BASE URL		<input type="text" value="https://democorp.net"/>				

Figure 10: BIG-IP APM SP service

6. On the **Browser SSO** tab, click **Configure Browser SSO**.

SP Connection | Browser SSO

- Under **SAML Profiles**, choose **SP-Initiated SSO**, and click **Next**.
- Under **Assertion Lifetime**, click **Next**.
- Under **Assertion Creation**, click **Configure Assertion Creation**.

SP Connection | Browser SSO | Assertion Creation

- Under **Identity Mapping**, choose the **STANDARD** option, then click **Next**.
- Under **Attribute Contract**, the default contract: **SAML_SUBJECT** identifies the user in the SAML assertions. Optionally, you can choose to extend the contract to include custom user attributes in the assertions. Click **Next**.
- Under **Authentication Source Mapping**, click **Map New Adapter Instance**.

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

- Under **Adapter Instance**, select the adapter instance (see Figure 11), and click **Next**.

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

Adapter Instance	Mapping Method	Attribute Contract Fulfillment	Issuance Criteria	Summary
<p>Select an IdP adapter instance that may be used to authenticate users for this partner. Attributes returned by the adapter instance you choose (the Adapter Contract) may be used to fulfill the Attribute Contract with your partner.</p>				
ADAPTER INSTANCE	<input type="text" value="HtmlFormIdpAdapter"/>			

Figure 11: Adapter instance binding

- H. Under **Mapping Method**, choose the second option to retrieve additional attributes from the data store, and click **Next**.
- I. Under **Attribute Sources & User Lookup**, click on **Add Attribute Source**.

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping | Source & User Lookup

- i. Under **Data Store**, specify the **Attribute Source Description** and select the **Active Data Store** (see Figure 12), and then click **Next**.

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping | Attribute Sources & User Lookup

Data Store	LDAP Directory Search	LDAP Filter	Attribute Contract Fulfillment	Summary
This server uses local data stores to retrieve supplemental attributes to be sent in an assertion. Specify an Attribute Source name that will distinguish this user lookup for the selected data store.				
ATTRIBUTE SOURCE DESCRIPTION	DataStore			
ACTIVE DATA STORE	192.168.16.111:17389			
DATA STORE TYPE	LDAP			

Figure 12: Selecting the LDAP data store

- ii. Under **LDAP Directory Search**, enter the **BASE DN** and click **Next**.
- iii. Under **LDAP Filter**, enter **sAMAccountName=\${username}**, and click **Next**.
- iv. Under **Attribute Contract Fulfillment**, select the **Attribute Contract** and **Value** to be used in assertions (see Figure 13), and then click **Next**.

SP Connections | SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping | Attribute Sources & User Lookup

Data Store	LDAP Directory Search	LDAP Filter	Attribute Contract Fulfillment	Summary
Fulfill your Attribute Contract with values from the authentication adapter, dynamic text values, or from a data store lookup.				
Attribute Contract	Source	Value	Actions	
SAML_SUBJECT	Adapter	username	None available	

Figure 13: Specifying the attribute contract and value used in SAML assertions

- v. Review the **Summary** and click **Done**.

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

- J. When the **Attribute Sources & User Lookup** page (from step I above) reappears, click **Next**.

- K. Under **FailSafe Attribute Source**, click **Next**.
- L. Under **Attribute Contract Fulfilment**, select the **Attribute Contract source** and **value**, click **Next**.
- M. Review the **Summary** and click **Done**.

SP Connection | Browser SSO | Assertion Creation

- N. When the **Authentication Source Mapping** page (from step F above) reappears, click **Next**.
- O. Review the **Summary** and click **Done**.

SP Connection | Browser SSO

- P. When the **Assertion Creation** page (from step C above) reappears, click **Next**.
- Q. In the **Protocol Settings** section, click **Configure Protocol Settings**.

SP Connection | Browser SSO | Protocol Settings

- R. Enter the **Assertion Consumer Service URL** for SAML assertions (see Figure 14) and click **Next**.

SP Connections | SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL Allowable SAML Bindings Artifact Resolver Locations Signature Policy Encryption Policy

Summary

As the IdP, you send SAML assertions to the SP's Assertion Consumer Service. The SP may request that the SAML assertion be sent to one of several URLs, via different bindings. Please provide the possible assertion consumer URLs below and select one to be the default.

Default	Index	Binding	Endpoint URL	Action
default	0	POST	https://www.democorp.net/saml/sp/profile/post/acs	Edit Delete

Figure 14: Specifying the assertion consumer service URL

- S. In the **Allowable SAML Bindings** section, select the **POST** and **Redirect** options and deselect all others. Then click **Next**.
- T. Under **Signature Policy**, click **Next**.
- U. Under **Encryption Policy**, click **Next**.
- V. Review the configuration **Summary** and click **Done**.

SP Connection | Browser SSO

- W. When the **Protocols Settings** section (from step Q above) reappears, click **Next**.
- X. Review the **Summary** and click **Next**.

SP Connection

7. When the **Browser SSO** tab (from step 6 above) reappears, click **Next**.
8. Under **Credentials**, click **Configure credentials**.

SP Connection | Browser SSO

- A. Under **Digital Signature Setting**, select the signing certificate and click **Next**.
- B. Review the **Summary** and click **Next**.

SP Connection

9. When the **Credentials** page (from Step 8 above) reappears, click **Next**.
10. Under **Activation & Summary** choose **Connection Status: Active**, validate the rest of the configuration, and click **Save**.

Export the metadata file from PingFederate

Export the metadata file to import into BIG-IP APM.

1. On the PingFederate management console, navigate to **Server Configuration > Administrative Functions > Metadata Export**.
2. If the server has been configured for multiple roles (IdP and SP), select the option **I am the Identity Provider (IdP)**, and then click **Next**. Otherwise, proceed to Step 3.
3. Under **Metadata mode**, select **Select Information to Include in Metadata Manually**, and click **Next**.
4. Under **Protocol**, click **Next**.
5. Under **Attribute Contract**, click **Next**.
6. Under **Signing Key**, select the certificate previously configured on the connection profile. Click **Next**.
7. Under **XML encryption certificate**, click **Next**.
8. Choose your desired option to enforce encryption, and click **Next**.
9. Review the **Summary** and click **Export**.
10. Save the metadata file generated, and then click **Done**.

Configure SAML SP and IdP on the BIG-IP system

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

1. On the main tab of the BIG-IP management interface, navigate to **Access > Federation > SAML Service Provider > Local SP Services**.

- When the **Local SP Services** page appears, click **Create**.
- Enter a unique **Name** for the SAML SP service and the **Entity ID**. Then click **OK**.

Create New SAML SP Service

General Settings | Endpoint Settings | Security Settings | Authentication Context | Advanced Settings

Name*: BIGIP-SP

Entity ID*: http://democorp.net/sp

SP Name Settings

Scheme : https Host :

Description :

Relay State :

OK Cancel

Figure 15: Creating SAML SP Service

- Select the radio button of the SAML SP service you just created. Scroll down and select **Bind/Unbind IdP Connectors**.
- In the resulting pop-up window, Click on **Create New IdP Connector** and **From Metadata**.
- When the **Create New SAML IdP Connector** popup window appears, click **Browse** and select the metadata.xml file you exported from PingFederate.
- Enter an **Identity Provider Name**, then **Select Signing Certificate** (or confirm the certificate is displayed), and click **OK**. A PingFederate IdP connector will be created and its signing certificate imported.

Create New SAML IdP Connector

Select File*: metadata.xml Browse

Identity Provider Name*: PingFederate

Select Signing Certificate : Select a value...

OK Cancel

Figure 16: Creating SAML IdP connector

- Click **Add New Row**. Select the configured PingFederate IdP as the **SAML IdP Connector**, select `#{session.server.landinguri}` as the **Matching Source**, and select `/*` as the **Matching Value**. These choices instruct the BIG-IP system to use the PingFederate IdP for all requests on this web application. This URI can be adjusted based on specific folders or other **Matching Source** parameters.

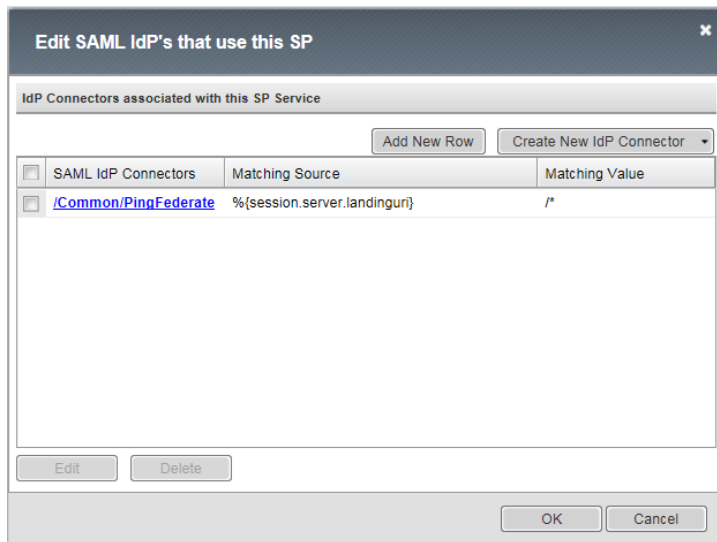


Figure 17: SAML IdP connector binding to SP

- Click **OK** to complete the SAML IdP and SP configuration.

Configure BIG-IP access policy to authenticate with the PingFederate IdP

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

- From the main tab of the BIG-IP management interface, navigate to **Access > Access Profiles/Policies**.
- When the **Access Profiles** page appears, click **Create**.
- Choose **All** for **Profile type**, and choose **Virtual Server** as the **Profile scope**.
- Scroll down and select the languages you want to support. Move them to the **Accepted Languages** box.
- Click **Finished**. The **Access Profiles** list will appear.
- Under **Access Policy**, click **Edit** for the access profile you just created to launch the visual policy editor. The visual policy editor opens the access policy in a separate window.
- Click **+** anywhere in the access policy to add a new action item. The **Add Item** window opens and lists predefined actions grouped by purpose (such as General Purpose, Authentication, and so on).
- In the **Authentication** grouping, select **SAML Auth** and click **Add Item**. The **SAML Auth Properties**

window opens.

9. Under **SAML Authentication SP**, select the SAML [SP service](#) you created from the **AAA Server** list, and then click **Save**. The **Access Policy** window opens.
10. Add any additional actions you require to complete the policy.
11. Change the **Successful** rule outcome from **Deny** to **Allow** and click **Save**.

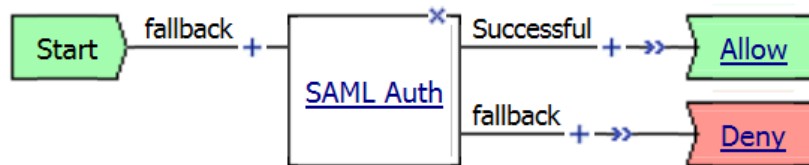


Figure 18: The visual policy editor's display of a simple access policy to authenticate users against the PingFederate SAML IdP

12. Click **Apply Access Policy** (at the top of the window) to activate your changes to this access policy and apply it.
13. Click **Close** to close the visual policy editor.

Add the access profile to the virtual server

Associate the access profile with the virtual server of the web application so that BIG-IP APM can apply the policy to incoming traffic.

1. From the main tab of the BIG-IP management interface, click **Local Traffic > Virtual Servers**.
2. When the **Virtual Server List** page appears, click the name of the virtual server.
3. On the Virtual server **Properties** page, scroll down to the **Access Policy** section and select the **Access Profile** you created.

Access Policy	
Access Profile	SAMLPolicy ▼
Connectivity Profile	+ None ▼
Per-Request Policy	None ▼
VDI Profile	None ▼
Application Tunnels (Java & Per-App VPN)	<input type="checkbox"/> Enabled
OAM Support	<input type="checkbox"/> Enabled
PingAccess Profile	None ▼

Figure 19: Associating the SAML access policy with the virtual server

4. Click **Update** to save and associate the access policy with the virtual server.

Verification

When you've completed configuration, test the SAML SSO integration.

1. Open the browser on the client and access the web application via *<virtual server IP Address: Port No>*.
2. The BIG-IP system will redirect the request to PingFederate for user authentication. A sign-on window displays.

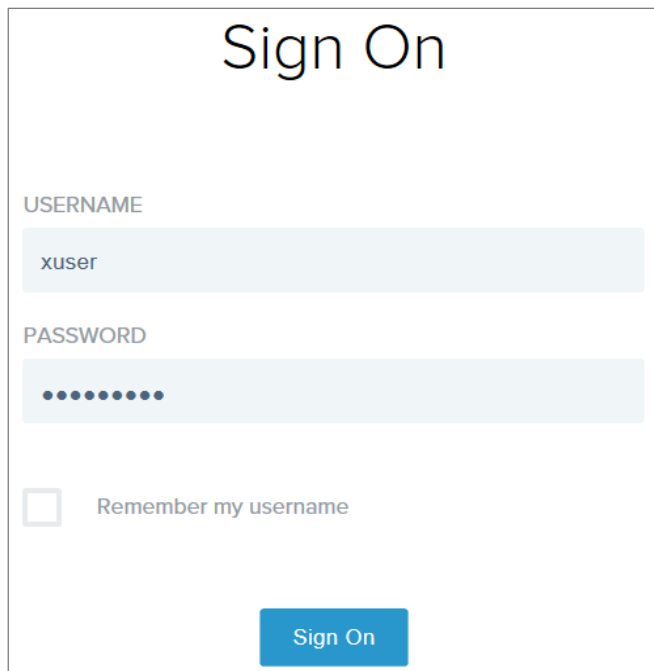


Figure 20: Redirected PingFederate login page

3. Enter the user credentials and click **Sign On**.
4. After successful authentication against the user store, the user will be directed to the protected resources on the web server.

Appendix

Once configuration is complete, the following resources may be useful in troubleshooting and other management activities.

Statistics

Log in to the BIG-IP system's command line interface and enter the following commands to understand the agent connections to PingAccess server and obtain statistics, which may aid in troubleshooting.

```
tmctl ping_access_agent_main_stats
tmctl profile_pingaccess_stat
```

BIG-IP APM reports

On the main menu of the BIG-IP management interface, navigate to **Access > Overview > Active Sessions** for a report that can help you to understand the transaction trace, which may aid in troubleshooting SAML SSO problems.

Session ID	Variables	User	Client IP	Start Time	Expiration	Bytes In	Bytes Out	Session Type	Profile Name
09cfc17e	View	n/a	192.168.16.10	2017-02-09 23:09:38	2017-02-09 23:14:45	473	1884	n/a	/Common/SAMLPolicy

Figure 21: F5 BIG-IP APM reports

Passing SAML attributes to a back-end web application

In a Kerberos SSO environment, F5 iRules® can be used to extract the SAML attributes of interest from the incoming assertion and pass them as HTTP headers to the back-end web application. (This is completely optional.)

Before you create the iRule on BIG-IP system, it is important to configure PingFederate to include the interesting/custom attributes and their values in the SAML assertions.

1. Log in to the BIG-IP management interface. From the main tab, navigate to **Local Traffic > iRules > iRules List**.
2. When the **iRule List** page appears, click **Create**.
3. Specify a **Name** for the iRule and copy and paste (or enter) the following iRule into the **Definition** window.

```

when RULE_INIT {
  set static::debug 0
}
when ACCESS_ACL_ALLOWED {
  set PINGUser [ACCESS::session data get "session.saml.last.identity"]
  if { $static::debug } { log local0. "id is $PINGUser" }
  if { ![HTTP::header exists "PING_USER"]} { {
    HTTP::header insert "PING_USER" $PINGUser
  }

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

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

```

4. Click **Finished**.
5. Next, associate the iRule with the virtual server. To do so, from the main tab, click **Local Traffic > Virtual Servers**.
6. When the **Virtual Server List** page opens, Click the virtual server.
7. Click the **Resources** tab.
8. Under **iRules**, click **Manage** and add the iRule you created above to the **Enabled** list.
9. Click **Finished**.

Troubleshooting PingAccess and PingFederate

Refer to the troubleshooting sections of the [PingAccess](#) and [PingFederate](#) administrator guides to understand the debugging and logging options for PingFederate and PingAccess. Generic network and HTTP header tracing tools found in popular browsers can also be used to troubleshoot interactions between the solution components.