



Foglight® 7.1.0

Integration with SAML 2.0 in PingFederate



© 2023 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (<https://www.quest.com>) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. All other trademarks and registered trademarks are property of their respective owners.

Legend



WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death



CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.



IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Contents

Foglight and SAML 2.0 Integration in PingFederate	4
Before you begin.....	5
Step 1: Configuring the SP Connection	6
Step 2: Configuring Browser SSO	7
Step 3: Configuring Assertion Creation.....	8
Step 4: Configuring Protocol Settings	12
Step 5: Configuring Credentials.....	15
Step 6: Setting up SAML in Foglight	18
About us.....	23

Foglight and SAML 2.0 Integration in PingFederate

Starting with release 5.9.3, Foglight® Management Server supports Active Directory Federation Services (ADFS) 2.0 and PingFederate 8.x (and later) using the Security Assertion Markup Language (SAML) 2.0 protocol. Follow the below steps in sequence to completely integrate SAML SSO with the Foglight Management Server on the PingFederate server.

i **NOTE:** PingFederate supports both http protocol and https protocol. Foglight SAML login on PingFederate could be using either IP address or the host name. For detailed configurations about IP or host name logon, refer to Before you begin.

- Before you begin
- Step 1: Configuring the SP Connection
- Step 2: Configuring Browser SSO
- Step 3: Configuring Assertion Creation
- Step 4: Configuring Protocol Settings
- Step 5: Configuring Credentials
- Step 6: Setting up SAML in Foglight

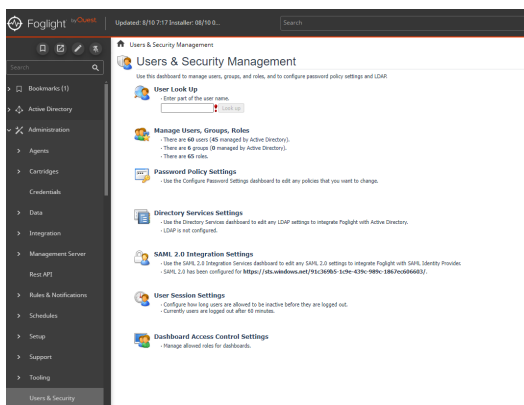
Before you begin

i NOTE:

- If you are about to use SAML IP login, make sure to run the following command:
`-Dquest.saml.hostname=<foglight-server-ip>` to start up your Foglight Management Server.
- When logging into your Foglight Management Server, make sure to keep using the same approach as what you configured during the SAML integrations. For example, if you set up the HTTPS SAML login using the IP address, you must log into your Management Server with `https://<foglight-server-ip>:<foglight-server-port>`.

You need to enable SAML 2.0 SSO Configuration in your Foglight Management Server prior to setting up the SAML integration. Follow the steps below to enable SAML 2.0 SSO Configuration:

- 1 Log into the Foglight Management Server as a Security Administrator.
- 2 Under **Dashboards**, click **Administration > Users & Security**, and then click **SAML 2.0 Integration Settings**. The *SAML 2.0 SSO Configuration* dashboard appears.
- 3 Click **Enable**.

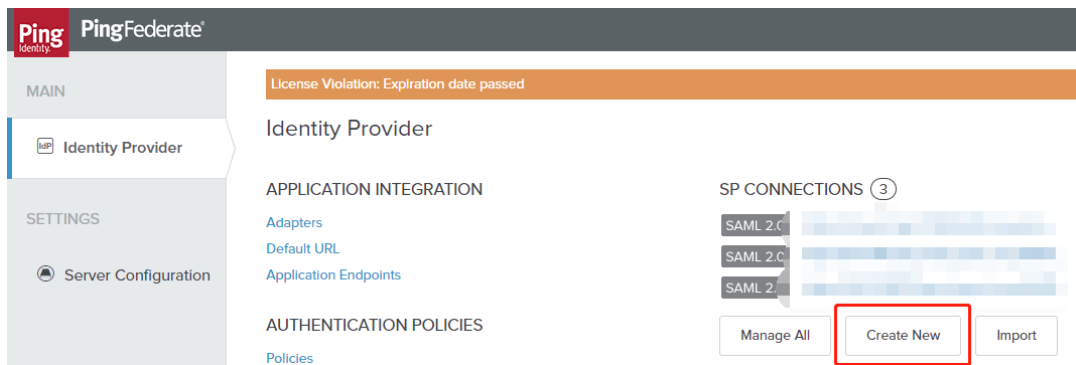


- 4 Download the metadata file that is to be imported to the PingFederate server later. Foglight supports both HTTP and HTTPS login:
 - For HTTP login: Get the metafile from the Foglight server URL:
 - IP login: http://<foglight_server-ip>:<port>/console/saml2/metadata.xml
 - Host name login: http://<foglight_server-host-name>:<port>/console/saml2/metadata.xml
 - For HTTPS login: Get the metafile from the Foglight server URL:
 - IP login: https://<foglight_server-ip>:<port>/console/saml2/metadata.xml
 - Host name login: https://<foglight_server-host-name>:<port>/console/saml2/metadata.xml

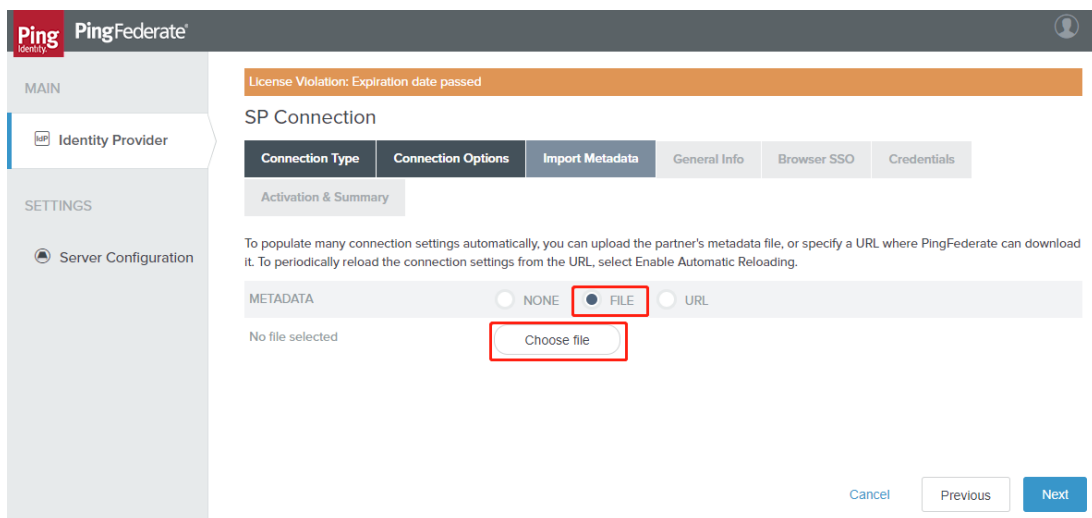
Step 1: Configuring the SP Connection

To configure the Service Provider (SP) connection:

- 1 Sign in PingFederate as an administrator.
- 2 Click **Identity Provider** and navigate to **Identity Provider** configurations.
- 3 Under **SP CONNECTIONS**, click **Create New**.



- 4 On the **Connection Type** tab, select the **BROWSER SSO PROFILES** connection template and click **Next**.
- 5 On the **Connection Options** tab, select **BROWSER SSO** and click **Next**.
- 6 On the **Import Metadata** tab, select **FILE** as the type of importing metadata, and then click **Choose file** to select the Foglight SSO metadata file. Click **Next**.



- 7 On the **Metadata Summary** tab, review the information and click **Next**.
- 8 On the **General Info** tab, ensure that the **PARTNER'S ENTITY ID**, **CONNECTION NAME**, and **BASE URL** fields pre-populate based on the metadata, and then click **Next**.

PingFederate

License Violation: Expiration date passed

SP Connection

Connection Type | Connection Options | Import Metadata | Metadata Summary | General Info | Browser SSO

Credentials | Activation & Summary

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.

PARTNER'S ENTITY ID (CONNECTION ID)

CONNECTION NAME

VIRTUAL SERVER IDS

BASE URL

Step 2: Configuring Browser SSO

To configure the browser SSO:

- 1 On the **Browser SSO** tab, click **Configure Browser SSO**.

PingFederate

License Violation: Expiration date passed

SP Connection

Connection Type | Connection Options | Import Metadata | Metadata Summary | General Info | Browser SSO

Credentials | Activation & Summary

This task provides connection-endpoint and other configuration information enabling secure browser-based SSO, to resources at your partner's site. Click the button below to create or revise this configuration.

BROWSER SSO CONFIGURATION

- 2 On the **SAML Profiles** tab, select all of the options and click **Next**.

License Violation: Expiration date passed

SP Connection | Browser SSO

SAML Profiles | Assertion Lifetime | Assertion Creation | Protocol Settings | Summary

A SAML Profile defines what kind of messages may be exchanged between an Identity Provider and a Service Provider, and how the messages are transported (bindings). As an IdP, you configure this information for your SP connection.

Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles
<input checked="" type="checkbox"/> IDP-INITIATED SSO	<input checked="" type="checkbox"/> IDP-INITIATED SLO
<input checked="" type="checkbox"/> SP-INITIATED SSO	<input checked="" type="checkbox"/> SP-INITIATED SLO

Cancel Save Draft Next

- 3 On **Assertion Lifetime** tab, enter your desired assertion validity time (default is 5) and click **Next**.

Step 3: Configuring Assertion Creation

To configure assertion creation:

- 1 On the **Assertion Creation** tab, click **Configure Assertion Creation**.

License Violation: Expiration date passed

SP Connection | Browser SSO

SAML Profiles | **Assertion Lifetime** | **Assertion Creation** | Protocol Settings | Summary

This task provides the configuration for creating SAML assertions to enable SSO access to resources at your SP partner's site.

Assertion Configuration	
IDENTITY MAPPING	Standard
ATTRIBUTE CONTRACT	SAML_SUBJECT
ADAPTER INSTANCES	0
AUTHENTICATION POLICY MAPPINGS	0

Configure Assertion Creation

Cancel Save Draft Previous Next

- 2 On the **Identity Mapping** tab, choose the **STANDARD** option and click **Next**.
- 3 On the **Attribute Contract** tab, select the **Subject Name Format** for the **SAM_SUBJECT** and extend the contract as below, and then click **Next**.

PingFederate

License Violation: Expiration date passed

SP Connection | Browser SSO | Assertion Creation

Identity Mapping | **Attribute Contract** | Authentication Source Mapping | Summary

An Attribute Contract is a set of user attributes that this server will send in the assertion.

Attribute Contract	Subject Name Format
SAML_SUBJECT	urn:oasis:names:tc:SAML:1:namelid-format:unspecified

Extend the Contract	Attribute Name Format	Action
mail	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit Delete
SAML_AUTHN_CTX	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit Delete
SAML_NAME_FORMAT	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit Delete
uid	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit Delete
user_principal	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit Delete

<input type="text"/>	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Add
----------------------	---	-----

Cancel Save Draft Previous Next

- 4 On the **Authentication Source Mapping** tab, click **Map New Adapter Instance**.

PingFederate

License Violation: Expiration date passed

SP Connection | Browser SSO | Assertion Creation

Identity Mapping | Attribute Contract | **Authentication Source Mapping** | Summary

PingFederate uses IdP adapters, partner IdPs or Authentication Policies to authenticate users to your SP. Users may be authenticated by one of several different adapters or authentication policy contracts, so map an adapter instance for each IDM system or a authentication policy contract for each policy.

Adapter Instance Name	Virtual Server IDs	Action
Authentication Policy Contract Name	Virtual Server IDs	Action

Map New Adapter Instance Map New Authentication Policy

Cancel Save Draft Previous Next

- 5 Select an **Adapter Instance** and click **Next**. The adapter must include the user's username.

License Violation: Expiration date passed

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

Adapter Instance Mapping Method Attribute Contract Fulfillment Issuance Criteria Summary

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.

ADAPTER INSTANCE HTML Form IdP Adapter

Adapter Contract

displayName

email

mail

policy.action

uid

user_principal

username

☐ OVERRIDE INSTANCE SETTINGS

Manage Adapter Instances

Cancel Save Draft Next

- On the **Mapping Method** tab, select **USE ONLY THE ADAPTER CONTRACT VALUES IN THE SAML ASSERTION** and click **Next**.

License Violation: Expiration date passed

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

Adapter Instance Mapping Method Attribute Contract Fulfillment Issuance Criteria Summary

You can choose to fulfill the Attribute Contract with your partner using either the values provided by the "HTML Form IdP Adapter" adapter, or you can use these values plus additional attributes retrieved from local data stores.

Adapter Contract

displayName

email

mail

policy.action

uid

user_principal

username

☐ RETRIEVE ADDITIONAL ATTRIBUTES FROM MULTIPLE DATA STORES USING ONE MAPPING

☐ RETRIEVE ADDITIONAL ATTRIBUTES FROM A DATA STORE - INCLUDES OPTIONS TO USE ALTERNATE DATA STORES AND/OR A FAILSAFE MAPPING

☒ USE ONLY THE ADAPTER CONTRACT VALUES IN THE SAML ASSERTION

Cancel Save Draft Previous Next

- On the **Attribute Contract Fulfillment** tab, fulfill your **Attribute Contract** as below and click **Next**.

Attribute Contract	Source	Value
SAML_AUTHN_CTX	Text	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
SAML_NAME_FORMAT	Text	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

PingFederate

License Violation: Expiration date passed

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

Adapter Instance | Mapping Method | Attribute Contract Fulfillment | Issuance Criteria | Summary

Fulfill your Attribute Contract with values from the authentication adapter or with dynamic text values.

Attribute Contract	Source	Value	Actions
SAML_AUTHN_CTX	Text	urn:oasis:names:tc:SAM	None available
SAML_NAME_FORMAT	Text	urn:oasis:names:tc:SAM	None available
SAML_SUBJECT	Adapter	username	None available
mail	Adapter	mail	None available
uid	Adapter	uid	None available
user_principal	Adapter	user_principal	None available

Cancel Save Draft Previous Next

8 On the **Issuance Criteria** tab, leave the default values as is and click **Next**.

9 On the **Summary** tab, verify adapter mapping configurations and click **Done**.

PingFederate

License Violation: Expiration date passed

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

Adapter Instance | Mapping Method | Attribute Contract Fulfillment | Issuance Criteria | Summary

Click a heading link to edit a configuration setting.

Adapter Instance

Selected adapter HTML Form IdP Adapter

Mapping Method

Adapter HTML Form IdP Adapter

Mapping Method Use only the Adapter Contract values in the mapping

Attribute Contract Fulfillment

uid	uid (Adapter)
mail	mail (Adapter)
SAML_AUTHN_CTX	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport (Text)
user_principal	user_principal (Adapter)
SAML_SUBJECT	username (Adapter)
SAML_NAME_FORMAT	urn:oasis:names:tc:SAML:1:nameid-format:unspecified (Text)

Issuance Criteria

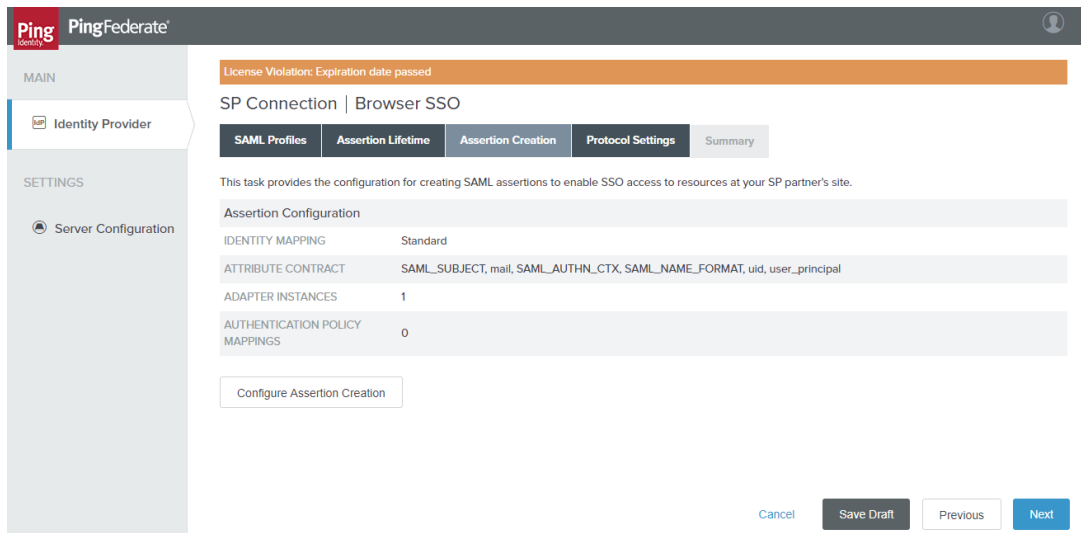
Criterion	(None)
-----------	--------

Cancel Save Draft Previous Done

10 On the **Authentication Source Mapping** tab, click **Next**.

11 On the **Summary** tab, click **Done**.

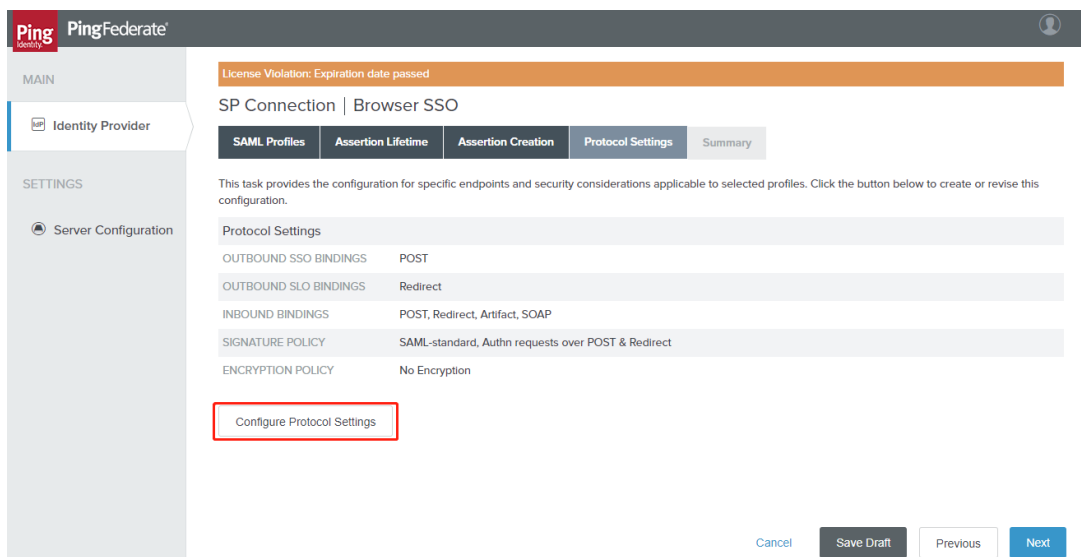
12 On the **Assertion Creation** tab, click **Next**.



Step 4: Configuring Protocol Settings

To configure protocol settings:

- 1 On the **Protocol Settings** tab, click **Configure Protocol Settings**.



- 2 On the **Assertion Consumer Service URL** tab, ensure the **Binding** and **Endpoint URL** are set as below and click **Next**.

PingFederate'

License Violation: Expiration date passed

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL | **SLO Service URLs** | 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	1	POST	/console/saml2/saml_assertion_consumer	Edit Delete
<input type="checkbox"/>	<input type="text"/>	- SELECT -	<input type="text"/>	Add

Cancel Save Draft Next

- 3 On the **SLO Service URLs** tab, ensure the **Binding** and **Endpoint URL** are set as below and click **Next**.

PingFederate'

License Violation: Expiration date passed

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL | **SLO Service URLs** | Allowable SAML Bindings | Artifact Resolver Locations | Signature Policy

Encryption Policy | Summary

As the IdP, you may send SAML logout messages to the SP's Single Logout Service. Depending on the situation, the SP may request that messages be sent to one of several URLs, via different bindings. Please provide the endpoints that you would like to use.

Binding	Endpoint URL	Response URL	Action
Redirect	/console/saml2/slo		Edit Delete
- SELECT -	<input type="text"/>	<input type="text"/>	Add

Cancel Save Draft Previous Next

- 4 On the **Allowable SAML Bindings** tab, select **POST** and **REDIRECT** and click **Next**.

PingFederate'

License Violation: Expiration date passed

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL | SLO Service URLs | **Allowable SAML Bindings** | Signature Policy | Encryption Policy | Summary

When the SP sends messages, what SAML bindings do you want to allow?

☐ ARTIFACT

☒ POST

☒ REDIRECT

☐ SOAP

Cancel Save Draft Previous Next

- 5 On the **Signature Policy** tab, select the **REQUIRE AUTHN REQUESTS TO BE SIGNED WHEN RECEIVED VIA THE POST OR REDIRECT BINDINGS** option and click **Next**.

PingFederate

License Violation: Expiration date passed

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL | SLO Service URLs | Allowable SAML Bindings | **Signature Policy** | Encryption Policy | Summary

Additional guarantees of authenticity may be agreed upon between you and your partner. For SP-initiated SSO, you can choose to require signed authentication requests sent via the POST or redirect bindings. You can also choose to sign assertions sent to this partner, regardless of the binding used.

☒ REQUIRE AUTHN REQUESTS TO BE SIGNED WHEN RECEIVED VIA THE POST OR REDIRECT BINDINGS

☐ ALWAYS SIGN THE SAML ASSERTION

Cancel Save Draft Previous Next

- On the **Encryption Policy** tab, select the **NONE** option and click **Next**.

PingFederate

License Violation: Expiration date passed

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL | SLO Service URLs | Allowable SAML Bindings | Signature Policy | **Encryption Policy** | Summary

Additional guarantees of privacy may be used between you and your partner. Specify an encryption policy for the exchange of SAML messages.

☒ NONE

☐ THE ENTIRE ASSERTION

☐ ONE OR MORE ATTRIBUTES

☐ SAML_SUBJECT

☐ MAIL

☐ SAML_AUTHN_CTX

☐ SAML_NAME_FORMAT

☐ UID

☐ USER_PRINCIPAL

Cancel Save Draft Previous Next

- On the **Summary** tab, verify the summary and click **Done**.

PingFederate

License Violation: Expiration date passed

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL | SLO Service URLs | Allowable SAML Bindings | Signature Policy | Encryption Policy | Summary

Summary information for your Protocol Settings configuration. Click a heading link to edit a configuration setting.

Protocol Settings

Assertion Consumer Service URL

Endpoint URL: /console/saml2/saml_assertion_consumer (POST)

SLO Service URLs

Endpoint URL: /console/saml2/slo (Redirect)

Allowable SAML Bindings

Artifact	false
POST	true
Redirect	true
SOAP	false

Signature Policy

Require digitally signed AuthN requests	true
Always sign the SAML Assertion	false

Encryption Policy

Status	Inactive
--------	----------

Cancel Save Draft Previous Done

- 8 On the **Protocol Settings** tab, click **Next**.
- 9 On the **Browser SSO Summary** tab, click **Done**.
- 10 On the **Browser SSO** tab, click **Next**.

PingFederate

License Violation: Expiration date passed

SP Connection

Connection Type | Connection Options | Import Metadata | Metadata Summary | General Info | Browser SSO | Credentials

Activation & Summary

This task provides connection-endpoint and other configuration information enabling secure browser-based SSO, to resources at your partner's site. Click the button below to create or revise this configuration.

BROWSER SSO CONFIGURATION

Configure Browser SSO

Cancel Save Draft Previous Next

Step 5: Configuring Credentials

To configure credentials:

- 1 On the **Credentials** tab, click **Configure Credentials**.

PingFederate

License Violation: Expiration date passed

SP Connection

Connection Type | Connection Options | Import Metadata | Metadata Summary | General Info | Browser SSO | Credentials

Activation & Summary

For each credential shown here, configure the necessary settings.

Credential Requirement	
DIGITAL SIGNATURE	Not Configured
SIGNATURE VERIFICATION SETTINGS	Unanchored Certificate (Primary CN=Foglight, Secondary Not Configured)

Configure Credentials

Cancel Save Draft Previous Next

- 2 On the **Digital Signature Settings** tab, select the Signing Certificate to use the SSO service and click **Next**.

PingFederate

License Violation: Expiration date passed

SP Connection | Credentials

Digital Signature Settings | Signature Verification Settings | Summary

You may need to digitally sign SAML messages or security tokens to protect against tampering. Please select a key/certificate to use from the list below.

SIGNING CERTIFICATE 0t62:D7:1B:C4:A7 (cn=SSO)

☐ INCLUDE THE CERTIFICATE IN THE SIGNATURE <KEYINFO> ELEMENT.

SIGNING ALGORITHM RSA SHA256

Manage Certificates

Cancel Save Draft Next Done

- 3 On the **Signature Verification Settings** tab, click **Manage Signature Verification Settings**.

PingFederate

License Violation: Expiration date passed

SP Connection | Credentials

Digital Signature Settings | Signature Verification Settings | Summary

Incoming SAML messages or security tokens may be digitally signed. This configuration task provides options for verifying signatures.

Manage Signature Verification Settings

Cancel Save Draft Previous Next Done

- 4 On the **Trust Model** tab, select the **UNANCHORED** option and click **Next**.

PingFederate

License Violation: Expiration date passed

SP Connection | Credentials | Signature Verification

Trust Model | Signature Verification Certificate | Summary

Select the Trust Model to be used for verifying digital signatures received from this partner.

☐ ANCHORED The verification certificate must be signed by a Trusted CA and included in the incoming message.

☒ UNANCHORED The verification certificate is self-signed, or you wish to trust a specific certificate.

Cancel Save Draft Next

- 5 On the **Signature Verification Certificate** tab, select the Foglight certificate that should have been imported, and then click **Next**.

PingFederate

License Violation: Expiration date passed

SP Connection | Credentials | Signature Verification

Trust Model | Signature Verification Certificate | Summary

Please select the certificate(s) to use when verifying these digital signatures. When multiple certificates are chosen, each certificate is tried from the top of the list down until the signature is verified.

PRIMARY 8B:30:CD:B9:6A:CF:34:B5 (cn=Foglight) ▼

SECONDARY - SELECT - ▼

Manage Certificates

Cancel Save Draft Previous Next

- 6 On the **Summary** tab, click **Done**.
- 7 On the **Signature Verification Settings** tab, click **Next**.
- 8 On the **Credentials Summary** tab, click **Done**.
- 9 On the **Credentials** tab, click **Next**.

PingFederate

License Violation: Expiration date passed

SP Connection

Connection Type | Connection Options | Import Metadata | Metadata Summary | General Info | Browser SSO | Credentials

Activation & Summary

For each credential shown here, configure the necessary settings.

Credential Requirement

DIGITAL SIGNATURE	CN=SSO
SIGNATURE VERIFICATION SETTINGS	Unanchored Certificate (Primary CN=Foglight, Secondary Not Configured)

Configure Credentials

Cancel Save Draft Previous Next

- 10 On the **Activation & Summary** tab, choose the **ACTIVE** option for the Connection Status. Verify the configurations and click **Save**.

License Violation: Expiration date passed

SP Connection

Connection Type	Connection Options	Import Metadata	Metadata Summary	General Info	Browser SSO	Credentials
Activation & Summary						
Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.						
Connection Status		<input checked="" type="radio"/> ACTIVE <input type="radio"/> INACTIVE				
SSO Application Endpoint		https://10.30.155.30:9031/idp/startSSO.ping?PartnerSpId=http%3A%2F%2FQCQGQ6Q52.prod.quest.corp%3A8080%2Fconsole%2Fsaml2%2Fmetadata.xml				
Summary						
SP Connection						
Connection Type						
Connection Role		SP				
Browser SSO Profiles		true				
Protocol		SAML 2.0				
Connection Template		No Template				
WS-Trust STS		false				
Outbound Provisioning		false				
Connection Options						

Step 6: Setting up SAML in Foglight

To set up SAML in the Foglight Management Server:

- 1 Log into the Foglight Management Server as a Security Administrator.
- 2 Under **Dashboards**, click **Administration > Users & Security > SAML 2.0 SSO**. The *SAML 2.0 SSO Configuration* dashboard appears.
- 3 Click **Edit Settings** and configure the SAML settings as below. You could get the actual values from the PingFederate server.
 - a *Identity Provider Entity ID*: You could get this value from PingFederate's **Server Settings**.

Respond to Get Requests false

Generate Traps false

Account Management

User Administrator | UserAdmin,Admin,CryptoAdmin

Password Change Notification false

Roles & Protocols

Enable OAuth 2.0 Authorization Server false

IdP SAML 2.0 Support true

Enable IdP Discovery false

Federation Info

My Base URL <https://10.30.155.30:9031>

SAML 2.0 Entity ID pingserver

- b *Login URL*: You could get this value from the SP Connection that you have configured on the PingFederate server.

PingFederate

License Violation: Expiration date passed

SP Connection

Connection Type | Connection Options | Metadata URL | General Info | Browser SSO | Credentials | Activation & Summary

Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

Connection Status: ☒ ACTIVE ☐ INACTIVE

SSO Application Endpoint <https://10.30.155.30:9031/ldp/startSSO.ping?PartnerSpId=http%3A%2F%2FQCGQ6Q52.prod.quest.corp%3A8080%2Fconsole%2Fsam2%2Fmetadata.xml>

Summary

SP Connection

Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template

- c *Logout URL*: The value is https://<pingfederate_server>:<port>/ldp/SLO.sam2. You could get the logout common postfix from PingFederate's **Protocol Endpoints**.

PingFederate

License Violation: Expiration date passed

Identity Provider

APPLICATION INTEGRATION

[Adapters](#)
[Default URL](#)
[Application Endpoints](#)

AUTHENTICATION POLICIES

[Policies](#)
[Selectors](#)
[Policy Contracts](#)
[Sessions](#)

LOCAL IDENTITY

[Identity Profiles](#)

FEDERATION INFO

[Protocol Endpoints](#)

SP AFFILIATIONS 0

[Manage All](#) [Create New](#)

SP CONNECTIONS 4

SAML 2.0	http://QCGQ6Q52.prod.quest.corp:8080/...
SAML 2.0	https://zhuvn-fog-2708:8443/console/s...
SAML 2.0	http://Q6Y7WD3X.prod.quest.corp:8080/...
SAML 2.0	https://Q6Y7WD3X.prod.quest.corp:8443/...

[Manage All](#) [Create New](#) [Import](#)

- d *Attribute Key*: This is used to identity the attribute key of the assertion response. Take the below SAML 2.0 assertion response for example:

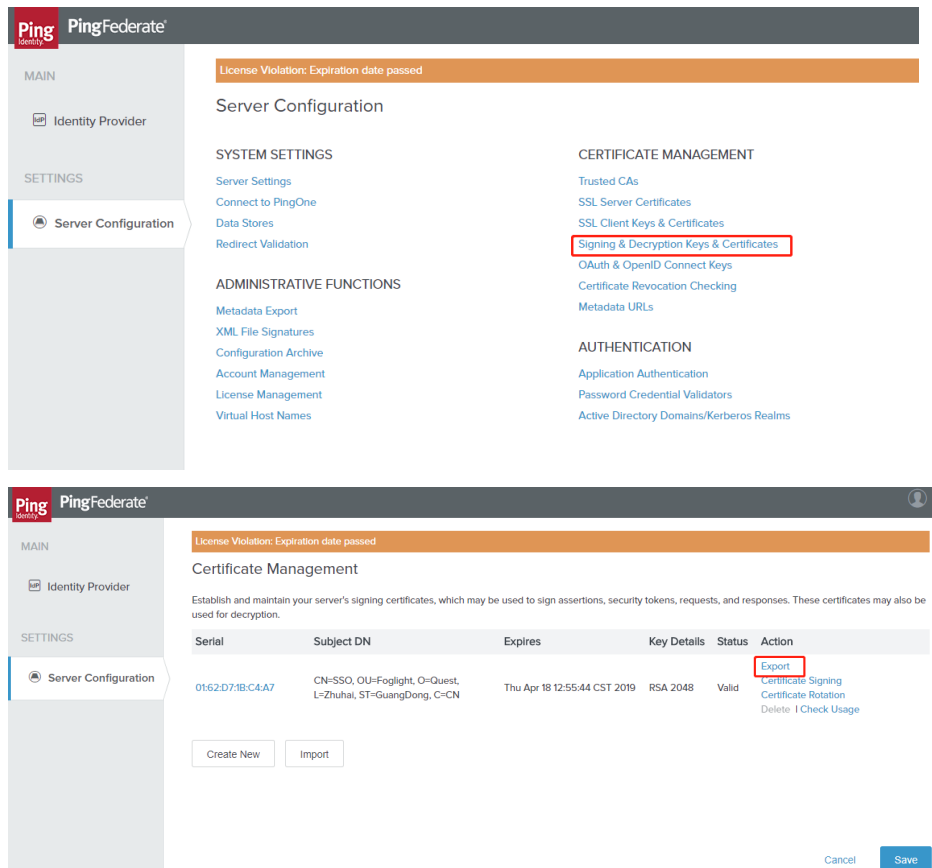
```

<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  <saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
  <saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema"
    <saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer><ds:Signature xmlns:ds="http://www.w3.org/2000/09/
    <ds:SignedInfo><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="#pf8495b10f-2a17-5411-3a19-33bf6852f431"><ds:Transforms><ds:Transform Algorithm="http://www.w3
  <ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIICajCCAdOgAwIBAgIBADANBgkqhkiG9w0BAQ0FADBSMQswCQYDVQQGEwJ1czETMBEGA1UI
  <saml:Subject>
    <saml:NameID SPNameQualifier="http://sp.example.com/demo1/metadata.php" Format="urn:oasis:names:tc:SAML:2.0:na
    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml:SubjectConfirmationData NotOnOrAfter="2024-01-18T06:21:48Z" Recipient="http://sp.example.com/demo1/indi
    </saml:SubjectConfirmation>
  </saml:Subject>
  <saml:Conditions NotBefore="2014-07-17T01:01:18Z" NotOnOrAfter="2024-01-18T06:21:48Z">
    <saml:AudienceRestriction>
      <saml:Audience>http://sp.example.com/demo1/metadata.php</saml:Audience>
    </saml:AudienceRestriction>
  </saml:Conditions>
  <saml:AuthnStatement AuthnInstant="2014-07-17T01:01:48Z" SessionNotOnOrAfter="2024-07-17T09:01:48Z" SessionIndex:
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
  <saml:AttributeStatement>
    <saml:Attribute Name="uid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
      <saml:AttributeValue xsi:type="xs:string">test</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="mail" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
      <saml:AttributeValue xsi:type="xs:string">test@example.com</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="eduPersonAffiliation" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
      <saml:AttributeValue xsi:type="xs:string">users</saml:AttributeValue>
      <saml:AttributeValue xsi:type="xs:string">examplerole1</saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>

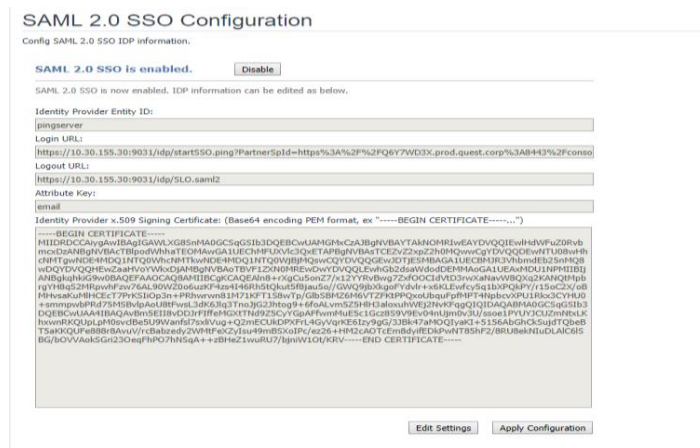
```

In the **saml:AttributeStatement** element, there are three **saml:Attribute** elements. Both **uid** and **mail** can be used to identify a user. In this sample response, either **uid** or **mail** can be used as the *Attribute Key*. Generally the IDP Server administrator knows details about this information. The Foglight Management Server tries to use several common keys, such as uid, email, mail, sAMAccountName and etc. Therefore if you are a Foglight administrator and have questions about this *Attribute Key*, reach out to your IDP server's administrator for detailed information.

- e *Identity Provider x.509 Signing Certificate*: You could get this value from PingFederate's **Signing & Decryption Keys & Certificates**.



The following shows an example of SAML 2.0 SSO Configuration in PingFederate.



- 4 Click **Apply Configuration** to save the configuration.

Then configurations of integrating SAML 2.0 SSO with the Foglight Management Server in PingFederate are completed.

Config SAML 2.0 SSO IDP information.

SAML 2.0 SSO is now enabled. IDP information can be edited as below.

Identity Provider Entity ID:

pingserver

Login URL:
<https://10.30.155.30:9031/idp/startSSO.ping?PartnerSpId=http%3A%2F%2FQCGQ6Q52.prod.quest.corp%3A8080%2Fconsole>

Logout URL:

<https://10.30.155.30:9031/idp/SLO.saml2>

Attribute Key:

Identity Provider x.509 Signing Certificate: (Base64 encoding PEM format, ex "-----BEGIN CERTIFICATE-----")

[illegible]

Cancel

Apply Configuration

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece – you – to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at <https://support.quest.com>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- [Submit and manage a Service Request](#)
- [View Knowledge Base articles](#)
- [Sign up for product notifications](#)
- [Download software and technical documentation](#)
- [View how-to-videos](#)
- [Engage in community discussions](#)
- [Chat with support engineers online](#)
- [View services to assist you with your product.](#)