

# Content Collaboration: Single Sign-On Configuration Guide

## PingFederate

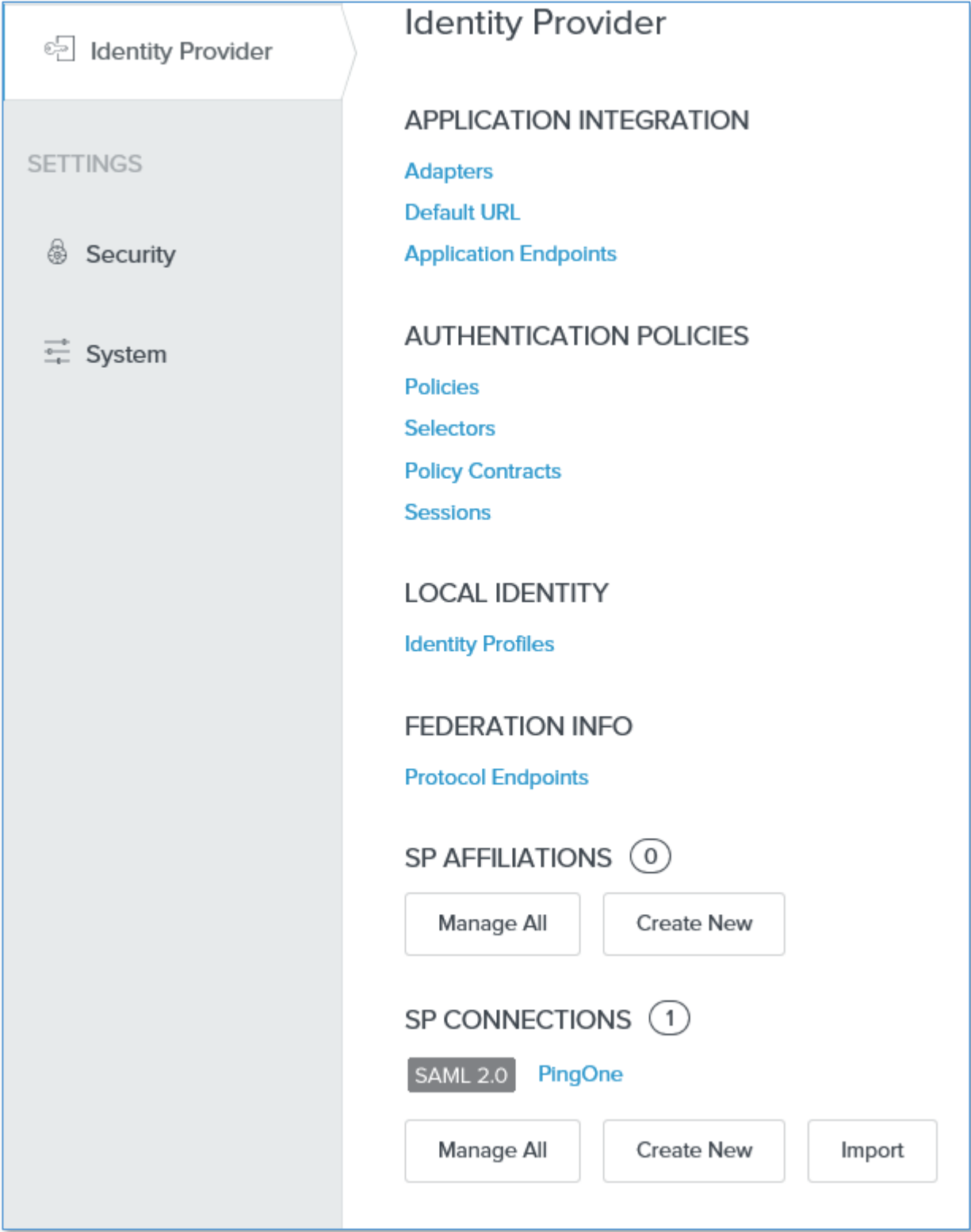


Last Revised: May 2019

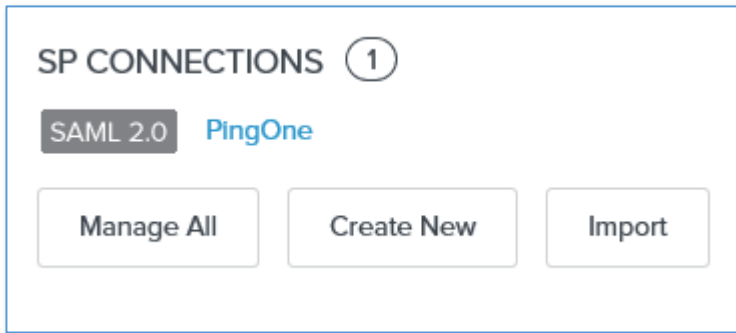
## LEGAL NOTICE

This document is furnished "AS IS" without warranty of any kind. This document is not supported under any Citrix standard support program. Citrix Systems, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix Systems, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix Systems, Inc. and its licensors, and are furnished under a license from Citrix Systems, Inc. This document and the software may be used and copied only as agreed upon by the Beta or Technical Preview Agreement.

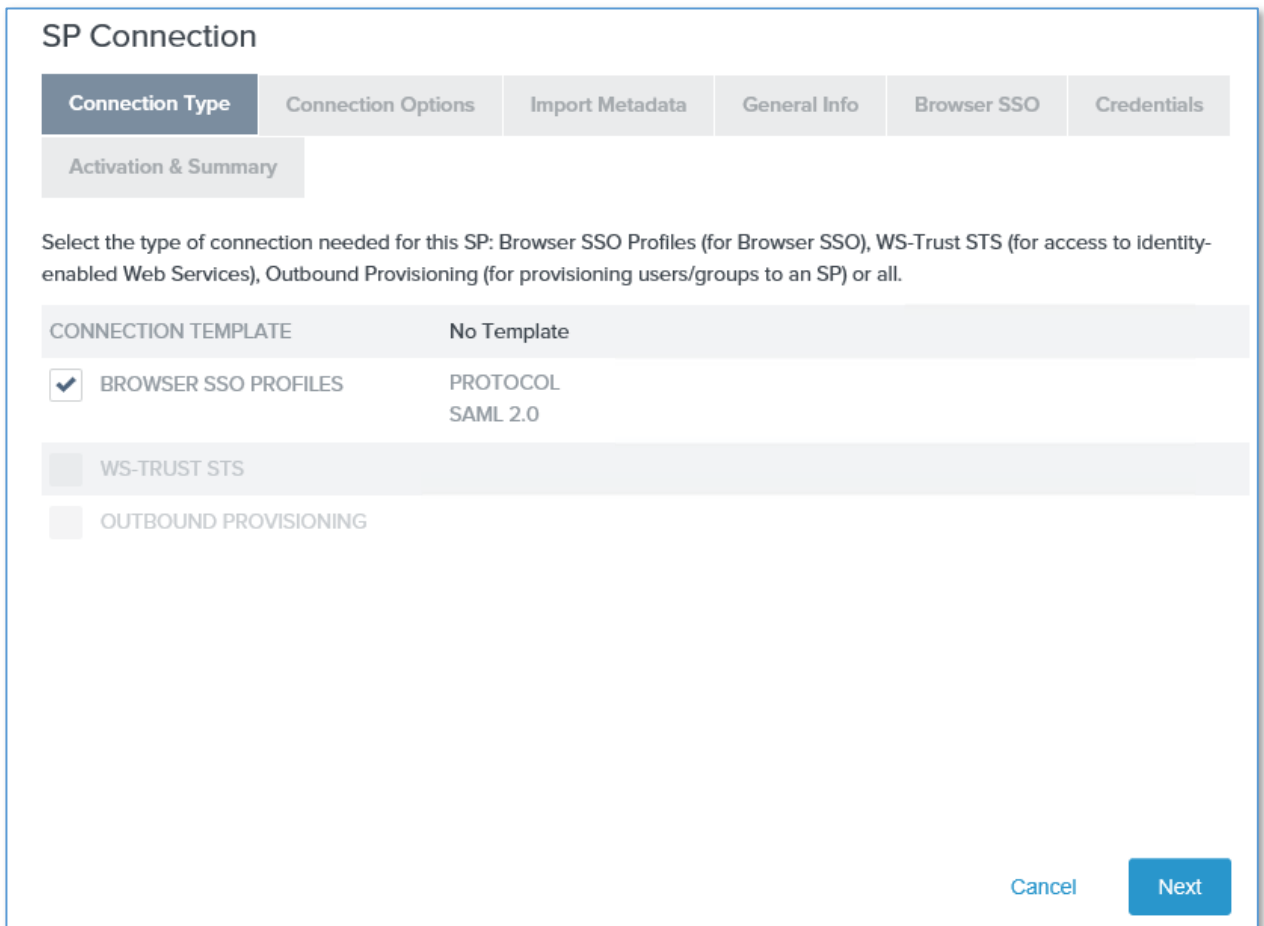
Copyright © 2019 Citrix Systems, Inc. All rights reserved. Citrix, Citrix Content Collaboration, and ShareFile are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.

Steps	Description
1.	<p>Log in to the Ping administrative console.</p> <p>For example, login to <a href="https://pingfed.domain.com:9999/pingfederate/app">https://pingfed.domain.com:9999/pingfederate/app</a></p>
2.	<p>Select <b>Identity Provider</b>.</p>  <p>The screenshot shows the 'Identity Provider' configuration page. On the left, a sidebar is visible with 'Identity Provider' selected. Under 'SETTINGS', 'Security' and 'System' are listed. The main content area is titled 'Identity Provider' and contains several sections:</p> <ul style="list-style-type: none"> <li><b>APPLICATION INTEGRATION</b>: Includes links for Adapters, Default URL, and Application Endpoints.</li> <li><b>AUTHENTICATION POLICIES</b>: Includes links for Policies, Selectors, Policy Contracts, and Sessions.</li> <li><b>LOCAL IDENTITY</b>: Includes a link for Identity Profiles.</li> <li><b>FEDERATION INFO</b>: Includes a link for Protocol Endpoints.</li> <li><b>SP AFFILIATIONS</b>: Shows 0 items, with buttons for 'Manage All' and 'Create New'.</li> <li><b>SP CONNECTIONS</b>: Shows 1 item, 'SAML 2.0 PingOne', with buttons for 'Manage All', 'Create New', and 'Import'.</li> </ul>

3. Under **SP Connections** section and select **Create New**.



4. On the **Connection Type** tab, select **Browser SSO Profiles** and select **SAML 2.0** as the protocol type. Click **Next**.



5. On the **Connection Options** tab, select **Browser SSO**.

## SP Connection

Connection Type	Connection Options	Import Metadata	General Info	Browser SSO	Credentials
Activation & Summary					
Please select options that apply to this connection.					
<input checked="" type="checkbox"/> BROWSER SSO					
<input type="checkbox"/> IDP DISCOVERY					
<input type="checkbox"/> ATTRIBUTE QUERY					
<p style="text-align: right;"><a href="#">Cancel</a> <a href="#">Previous</a> <a href="#">Next</a></p>					

6. On the **Import Metadata** tab, select **None**.

Connection Type	Connection Options	Import Metadata	General Info	Browser SSO	Credentials
Activation & Summary					
To populate many connection settings automatically, you can upload the partner's metadata file, or specify a URL where PingFederate can download it. To periodically reload the connection settings from the URL, select Enable Automatic Reloading.					
METADATA <input checked="" type="radio"/> NONE <input type="radio"/> FILE <input type="radio"/> URL					
<p style="text-align: right;"><a href="#">Cancel</a> <a href="#">Previous</a> <a href="#">Next</a></p>					

7. On the **General Info** tab, enter information in these required fields:

**Partner's Entity ID:** <https://subdomain.sharefile.com/saml/info>

**Connection Name:** https://subdomain.sharefile.com

**Base URL:** <https://subdomain.sharefile.com>

### SP Connection

Connection Type	Connection Options	Import Metadata	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

COMPANY

CONTACT NAME

CONTACT NUMBER

CONTACT EMAIL

APPLICATION NAME

APPLICATION ICON URL

LOGGING MODE

NONE

STANDARD

ENHANCED

FULL

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

## SP Connection

Connection Type

Connection Options

Import Metadata

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

9. In the **SAML Profiles** tab, select these options: **IDP-initiated SSO** and **SP-initiated SSO**.

## 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

IDP-INITIATED SSO

IDP-INITIATED SLO

SP-INITIATED SSO

SP-INITIATED SLO

Cancel

Save Draft

Next

10. In the **Assertion Lifetime** tab, keep the default values.

## SP Connection | Browser SSO

SAML Profiles

Assertion Lifetime

Assertion Creation

Protocol Settings

Summary

When an assertion is issued to the SP, there is a timeframe of validity before and after issuance. Please specify these parameters below.

MINUTES BEFORE

MINUTES AFTER

Cancel

Save Draft

Previous

Next

11. On the **Assertion Creation**, select **Configure Assertion Creation**.

## 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

12. Choose the option **Standard** for **Identity Mapping**.



## SP Connection | Browser SSO | Assertion Creation

Identity Mapping

Attribute Contract

Authentication Source Mapping

Summary

Identity mapping is the process in which users authenticated by the IdP are associated with user accounts local to the SP. Select the type of name identifier that you will send to the SP. Your selection may affect the way that the SP will look up and associate the user to a specific local account.

**STANDARD:** Send the SP a known attribute value as the name identifier. The SP will often use account mapping to identify the user locally.

**PSEUDONYM:** Send the SP a unique, opaque name identifier that preserves user privacy. The identifier cannot be traced back to the user's identity at this IdP and may be used by the SP to make a persistent association between the user and a specific local account. The SP will often use account linking to identify the user locally.

INCLUDE ATTRIBUTES IN ADDITION TO THE PSEUDONYM.

**TRANSIENT:** Send the SP an opaque, temporary value as the name identifier.

INCLUDE ATTRIBUTES IN ADDITION TO THE TRANSIENT IDENTIFIER.

Cancel

Save Draft

Next

13. In the **Attribute Contract** tab, set SAML\_SUBJECT as the **Attribute Contract**.

Set the **Subject Name Format** to **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.

ShareFile as the service provider requires email attribute as outgoing NameID format for SAML 2.0.

License Warning: Approaching expiration date

## 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:1.1:nameid-format:unspecified  
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress  
urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName  
urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName  
urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos  
urn:oasis:names:tc:SAML:2.0:nameid-format:entity

Extend the Contract

urn:oasis:names



Add

Cancel

Save Draft

Previous

Next

14. In the **Authentication Source Mapping** tab, select **Map New Adapter Instance**.

## 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

that extends **email** as **NameID**.

15. In Adapter Instance tab, in Adapter Instance select **PingONE HTML Form Adapter**.

\*\*The format of the adapter can be HTML Forms, Kerberos, or HTTP Basic. For the purpose of this article, HTML Forms is the adapter mapping used for this connection.

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: PingOne HTML Form Adapter

**Adapter Contract**

- givenName
- mail
- memberOf
- objectGUID
- policy.action
- sn
- username
- userPrincipalName

OVERWRITE INSTANCE SETTINGS

Manage Adapter Instances

Cancel Save Draft Next

16. In the **Mapping Method** tab, choose the option **Use Only the Adapter Contract Values in the SAML Assertion**.

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](#)

17. In the **Attribute Contract Fulfillment** tab, choose the option **Adapter** for Source, and choose **mail** as Value.

SP Connections | 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_SUBJECT	Adapter	mail	None available

[Cancel](#) [Save Draft](#) [Previous](#) [Next](#)

18. In the **Issuance Criteria** tab, skip this section without any modifications by clicking **Next**.

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

PingFederate can evaluate various criteria to determine whether users are authorized to access SP resources. Use this optional screen with this conditional authorization.

Source	Attribute Name	Condition	Value	Error R
- SELECT -	- SELECT -	- SELECT -		

Cancel Save Draft Previous Next

19.

Once completed, verify the summary tabs matches the formatting.

SP Connections | 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 PingOne HTML Form Adapter

**Mapping Method**

Adapter HTML Form IdP Adapter

Mapping Method Use only the Adapter Contract values in the mapping

**Attribute Contract Fulfillment**

SAML\_SUBJECT mail (Adapter)

**Issuance Criteria**

Criterion (None)

[Cancel](#)

Save Draft

Previous

Done

SP Connections | SP Connection | Browser SSO | Assertion Creation

Identity Mapping

Attribute Contract

Authentication Source Mapping

Summary

Summary information for your Assertion Creation configuration. Click a heading link to edit a configuration setting.

Assertion Creation

Identity Mapping

Enable Standard Identifier true

Attribute Contract

Attribute SAML\_SUBJECT

Subject Name Format urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

Authentication Source Mapping

Adapter instance name PingOne HTML Form Adapter

Adapter Instance

Selected adapter PingOne HTML Form Adapter

Mapping Method

Adapter HTML Form IdP Adapter

Mapping Method Use only the Adapter Contract values in the mapping

Attribute Contract Fulfillment

SAML\_SUBJECT mail (Adapter)

Issuance Criteria

Criterion (None)

Cancel

Save Draft

Previous

Done

20. In the **Protocol Settings**, select Configure Protocol Settings.

## SP Connections | SP Connection | Browser SSO

SAML Profiles

Assertion Lifetime

Assertion Creation

Protocol Settings

Summary

This task provides the configuration for specific endpoints and security considerations applicable to selected profiles. Click the button below to create or revise this configuration.

### Protocol Settings

#### OUTBOUND SSO BINDINGS

INBOUND BINDINGS POST, Redirect, Artifact, SOAP

SIGNATURE POLICY SAML-standard

ENCRYPTION POLICY No Encryption

Configure Protocol Settings

Cancel

Save Draft

Previous

Next

21. In the **Assertion Consumer Service URL** tab, select Binding: **POST**. In the **Endpoint URL** enter: <https://subdomain.sharefile.com/saml/acs>
- Select **Add**.



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://subdomain.sharefile.com/saml/acs	<a href="#">Edit</a>   <a href="#">Delete</a>

[Cancel](#)

22. In the **Allowable SAML Bindings** tab, select only the **POST** option, de-selecting all other values.

SP Connections | SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL   **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](#)

23. In the **Signature Policy** tab, select **Next** without modifying default values.

The screenshot shows a configuration page for 'Signature Policy'. At the top, there are four tabs: 'Assertion Consumer Service URL', 'Allowable SAML Bindings', 'Signature Policy' (which is selected and highlighted in dark blue), and 'Encryption Policy'. Below the tabs is a 'Summary' section. The main content area contains a paragraph of text: '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.' Below this text are three checkbox options: 'REQUIRE AUTHN REQUESTS TO BE SIGNED WHEN RECEIVED VIA THE POST OR REDIRECT BINDINGS' (unchecked), 'ALWAYS SIGN ASSERTION' (unchecked), and 'SIGN RESPONSE AS REQUIRED' (checked). At the bottom right, there are four buttons: 'Cancel' (text link), 'Save Draft' (dark grey button), 'Previous' (white button), and 'Next' (blue button).

24. In the **Encryption Policy** tab, select **None** as the value.

## SP Connections | SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL

Allowable SAML Bindings

Signature Policy

Encryption Policy

Summary

Encryption may be applied to SAML messages for an added layer of protection in transport. If enabled, SAML Response messages may always be signed, regardless of the signature policy.

NONE

THE ENTIRE ASSERTION

ONE OR MORE ATTRIBUTES

SAML\_SUBJECT

[Cancel](#)

Save Draft

Previous

Next

25. Verify settings in Summary and select **Done**.

SP Connections | SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL

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: https://hietcloud.sharefile.com/saml/acs (POST)

Allowable SAML Bindings

Artifact	false
POST	true
Redirect	false
SOAP	false

Signature Policy

Require digitally signed AuthN requests	false
Always Sign Assertion	false
Sign Response As Required	true

Encryption Policy

Status Inactive

Cancel

Save Draft

Previous

Done

26. Review Protocol Settings. Click **Next**.

## SP Connections | SP Connection | Browser SSO

SAML Profiles

Assertion Lifetime

Assertion Creation

Protocol Settings

Summary

This task provides the configuration for specific endpoints and security considerations applicable to selected profiles. Click the button below to create or revise this configuration.

### Protocol Settings

OUTBOUND SSO BINDINGS POST

INBOUND BINDINGS POST

SIGNATURE POLICY SAML-standard

ENCRYPTION POLICY No Encryption

Configure Protocol Settings

Cancel

Save Draft

Previous

Next

27.

Review Summary for Browser SSO configuration. Click **Done**.

SP Connections | SP Connection | Browser SSO

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

Summary information for your Browser SSO configuration. Click a heading link to edit a configuration setting.

Browser SSO

SAML Profiles

IdP-Initiated SSO	true
IdP-Initiated SLO	false
SP-Initiated SSO	true
SP-Initiated SLO	false

Assertion Lifetime

Valid Minutes Before	5
Valid Minutes After	5

Assertion Creation

Identity Mapping

Enable Standard Identifier	true
----------------------------	------

Attribute Contract

Attribute	SAML_SUBJECT
Subject Name Format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

Authentication Source Mapping

Adapter instance name	PingOne HTML Form Adapter
-----------------------	---------------------------

Adapter Instance

Selected adapter	PingOne HTML Form Adapter
------------------	---------------------------

Mapping Method

Adapter	HTML Form IdP Adapter
Mapping Method	Use only the Adapter Contract values in the mapping

Attribute Contract Fulfillment

SAML_SUBJECT	mail (Adapter)
--------------	----------------

Issuance Criteria

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

Protocol Settings

Assertion Consumer Service URL

Endpoint	URL: https://hietcloud.sharefile.com/saml/acs (POST)
----------	--

Allowable SAML Bindings

Artifact	false
POST	true
Redirect	false
SOAP	false

Signature Policy

Require digitally signed AuthN requests	false
Always Sign Assertion	false
Sign Response As Required	true

Encryption Policy

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

28. Click **Next**.

The screenshot shows the 'SP Connections | SP Connection' page with the 'Browser SSO' tab selected. The navigation tabs are 'Connection Type', 'Connection Options', 'Import Metadata', 'General Info', 'Browser SSO', and 'Credentials'. Below the tabs is the 'Activation & Summary' section. The main content area contains the text: '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.' Below this text is a 'BROWSER SSO CONFIGURATION' section with a 'Configure Browser SSO' button. At the bottom right, there are four buttons: 'Cancel', 'Save Draft', 'Previous', and 'Next'.

29. In **Credentials** tab, click **Configure Credentials**.

The screenshot shows the 'SP Connections | SP Connection' page with the 'Credentials' tab selected. The navigation tabs are 'Connection Type', 'Connection Options', 'Import Metadata', 'General Info', 'Browser SSO', and 'Credentials'. Below the tabs is the 'Activation & Summary' section. The main content area contains the text: 'For each credential shown here, configure the necessary settings.' Below this text is a 'Credential Requirement' section with a table showing 'DIGITAL SIGNATURE' and 'Not Configured'. Below the table is a 'Configure Credentials' button. At the bottom right, there are four buttons: 'Cancel', 'Save Draft', 'Previous', and 'Next'.





31. Select **Manage Certificates**. From **Select Action**, select **Export**.

License Warning: Approaching expiration date

SP Connections | SP Connection | Credentials | Certificate Management

Establish and maintain your server's signing certificates, which may be used to sign assertions, security tokens, requests, and responses. These certificates may also be used for decryption.

SERIAL	SUBJECT DN	EXPIRES	ACTIVE	ACTION
[REDACTED]	[REDACTED]	Mon May 23 11:25:24 PDT 2022 Status: Valid	<input checked="" type="checkbox"/>	Select Action ^

Create New Import

- Activate
- Export**
- Certificate Signing
- Certificate Rotation
- Check Usage

Cancel Save

32. In the **Export Certificate** tab, select **Certificate Only** to export. Click **Export** again to download the .crt file.

SP Connections | SP Connection | Credentials | Certificate Management | Export Certificate

Export Certificate Export & Summary

You have a choice of exporting the certificate and the key or just the certificate.

CERTIFICATE ONLY

CERTIFICATE AND PRIVATE KEY

Cancel Next

33. Open the certificate (.crt) file in Notepad or any text editor.



35.

SP Connections | SP Connection | Credentials

Digital Signature Settings Summary

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

Credentials

Digital Signature Settings

Selected Certificate	[REDACTED]
Include Certificate in KeyInfo	false
Selected Signing Algorithm	RSA SHA256

Cancel Save Draft Previous Done

36.

Review Summary for Credentials. Click **Next**.

SP Connections | SP Connection

Connection Type Connection Options Import Metadata General Info Browser SSO Credentials

Activation & Summary

For each credential shown here, configure the necessary settings.

Credential Requirement

DIGITAL SIGNATURE [REDACTED]

Configure Credentials

Cancel Save Draft Previous Next

37. Review **Activation and Summary**. Copy the **SSO Application Endpoint** URL. This will be used as the **Login URL** in the ShareFile Admin Settings. Click **Save**.

<https://ExternalDNSnameofyourPingFederate.com:9031/idp/startSSO.ping?PartnerSpId=https://subdomain.sharefile.com/saml/info>

### 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.					
SSO Application Endpoint	<a href="https://pingfed.██████████.com:9031/idp/startSSO.ping?PartnerSpId=https%3A%2F%2F██████████.sharefile.com%2Fsaml%2Finfo">https://pingfed.██████████.com:9031/idp/startSSO.ping?PartnerSpId=https%3A%2F%2F██████████.sharefile.com%2Fsaml%2Finfo</a>				<input checked="" type="checkbox"/>
<b>Summary</b>					
SP Connection					
<b>Connection Type</b>					
Connection Role	SP				
Browser SSO Profiles	true				
Protocol	SAML 2.0				
Connection Template	No Template				
WS-Trust STS	false				
Outbound Provisioning	false				
<b>Connection Options</b>					
Browser SSO	true				
IdP Discovery	false				
Attribute Query	false				
<b>General Info</b>					
Partner's Entity ID (Connection ID)	<a href="https://██████████.sharefile.com/saml/info">https://██████████.sharefile.com/saml/info</a>				
Base URL	<a href="https://██████████.sharefile.com">https://██████████.sharefile.com</a>				
Browser SSO					

38. Go to your ShareFile account: <https://subdomain.sharefile.com>

Login with Administrator account > **Settings** > **Admin Settings** > **Security** > **Login & Security Policy** > scroll down on this page to **Single sign on / SAML 2.0 Configuration**.

39. Configure **Single sign on / SAML 2.0 Configuration** with the below:

## **Basic Settings**

- **Enable SAML:** Select **Yes**
- **ShareFile Issuer / Entity ID:** <https://subdomain.sharefile.com/saml/info>
- **Your Issuer / Entity ID:** <https://subdomain.sharefile.com/saml/info>
- **X.509 Certificate:** Click **Change**, then copy and paste the certificate text from the **Certificate** file downloaded in the step above
- **Login URL:** Add login URL as the SSO Application Endpoint URL from PingFederate Server

### **Example Login URL:**

<https://ExternalDNSnameofyourPingFederate.com:9031/idp/startSSO.ping?PartnerSpId=https://subdomain.sharefile.com/saml/info>

- **Logout URL:** Leave blank  
(When users log out of ShareFile, they will be redirected to ShareFile login page <https://subdomain.sharefile.com>.)

## Basic Settings

Enable SAML: ?

Yes  No

ShareFile Issuer / Entity ID: ?

Your IDP Issuer / Entity ID: ?

X.509 Certificate: ?

Saved [Change](#)

Login URL: ?

Logout URL: ?

40.

### Optional Settings

- **Require SSO Login:** *Optional*

After single-sign-on is successfully validated, checking **Yes** for this option will require all non-admin Employees to log in using PingFederate

Admins will have the choice to login using PingFederate (on the left) or their email address as the username and a native ShareFile password (on the right).

- **SSO IP Range:** *Optional*

(Limit requiring non-admin Employees to login from a specific IP range. Employees outside of this specified range will not be required to use OneLogin to login.)

- **SP-initiated SSO Certificate:** Select **HTTP Redirect with no signature**
- **Enable Web Authentication: Yes** (Choose **No** when you do not want to allow single sign on logins via a web browser. This means Windows authentication will need to be available. **No** is not recommended).
- **SP-initiated Auth Context:** Select **User Name and Password**.
- **Active Profile Cookies:** Leave blank
- Click **Save**

Optional Settings

Require SSO Login: (?)

Yes  No

SSO IP Range: (?)

SP-Initiated SSO certificate: (?)

HTTP Redirect with no signature ▾

Enable Web Authentication: (?)

Yes  No

SP-Initiated Auth Context: (?)

User Name and Password ▾ Minimum ▾

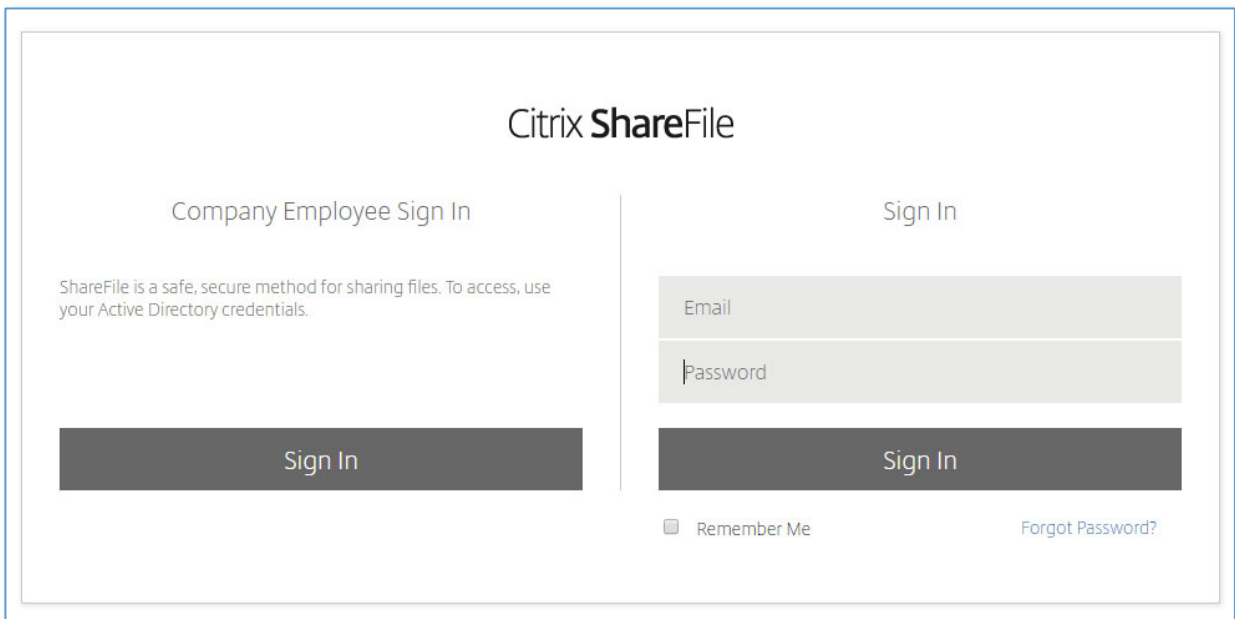
Active Profile Cookies: (?)

**Save** **Cancel**

41. Test successful authentication by going to your ShareFile URL:  
<https://subdomain.sharefile.com>

*\*\*Testing single-sign-on logins in private/incognito browser mode is best.*

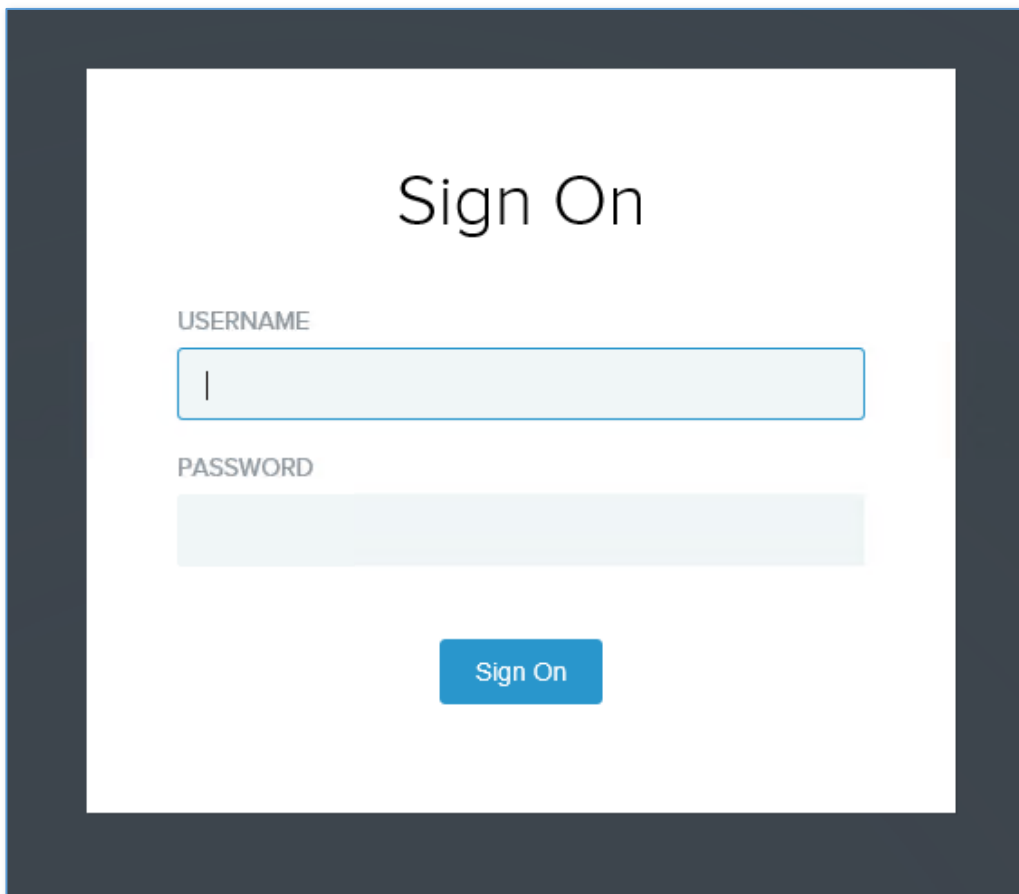
Click **Sign in** under **Company Employee Sign In**



The image shows the Citrix ShareFile login interface. At the top center is the logo "Citrix ShareFile". Below it, there are two main sections. The left section is titled "Company Employee Sign In" and contains the text: "ShareFile is a safe, secure method for sharing files. To access, use your Active Directory credentials." Below this text is a dark grey "Sign In" button. The right section is titled "Sign In" and contains two input fields: "Email" and "Password". Below these fields is a dark grey "Sign In" button. At the bottom of the right section, there is a checkbox labeled "Remember Me" and a link labeled "Forgot Password?".

**\*\*Make sure the user logging in with single sign-on has an Active Directory or Identity Provider email address that matches their email address in their ShareFile account.**

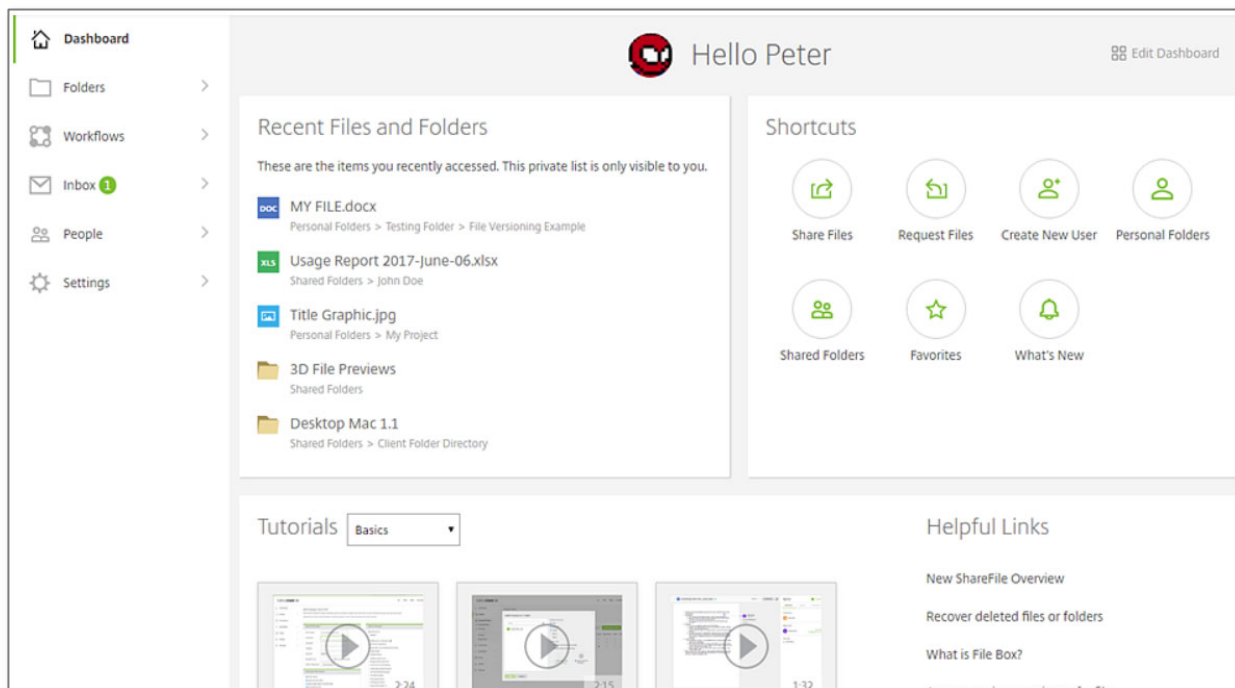
Sign in will redirect you PingFederate SSO Endpoint URL for sign in:



The image shows a "Sign On" form. At the top center is the title "Sign On". Below it, there are two input fields: "USERNAME" and "PASSWORD". The "USERNAME" field has a vertical cursor. Below the "PASSWORD" field is a blue "Sign On" button.



Successful logins will authenticate users into their ShareFile account **Dashboard**.



42. Done!

43. Common Errors:

**User Not Valid For This Provider:** This generally indicates the email attribute sent to ShareFile (SP) does not match the email attribute of the user who logged into Ping Federate (IDP). Ensure the email attribute of the AD account exactly matches the email attribute of the ShareFile employee user account.

**Failures redirect you to the ShareFile Login Page:** This could be any number of symptoms:

- Review the settings from this article
- Confirm the time settings of your server in relation to an NTP server.
- Confirm the certificate you exported from Ping Federate exactly matches the certificate value you saved in ShareFile.
- Ensure you are not encrypting SAML assertions or using unsupported protocols.