Configuration Guides

June 4, 2025

CONFIGURATION GUIDES

Table of Contents

Configuration Guide Overview

Ping Identity supports standards-based identity and access management (IAM) integrations with a wide range of business applications.

These configuration guides cover SAML single sign-on for PingFederate and PingOne. To search and discover more integrations, find downloads, and read documentation, visit the Ping Identity Integration Directory.

Adobe Creative Suite

Configuring SAML SSO with Adobe Creative Cloud and PingFederate

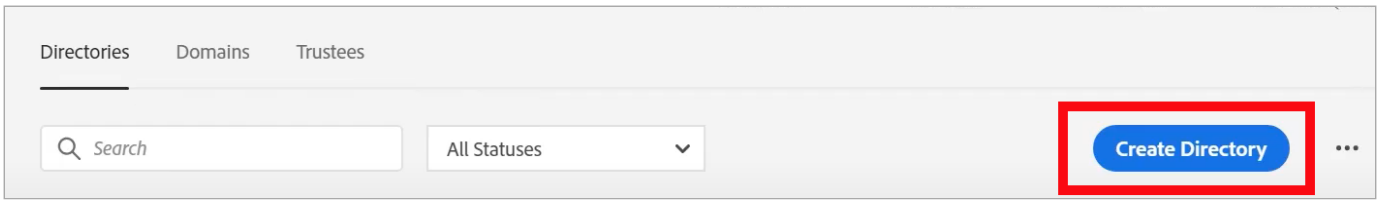
Learn how to enable Adobe Creative Cloud sign-on from the PingFederate console (IdP-initiated sign-on) and direct Adobe Creative Cloud sign-on using PingFederate (SP-initiated sign-on).

Before you begin

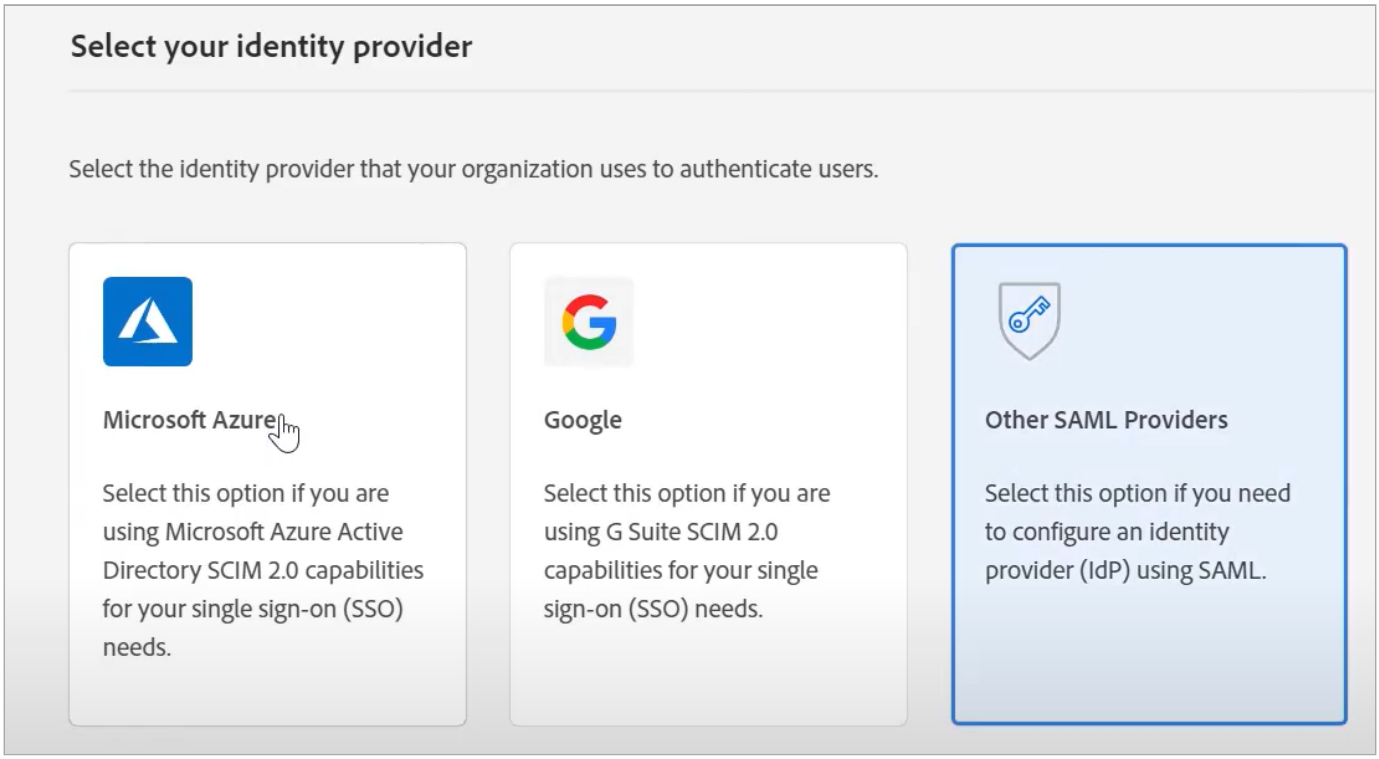
- Configure PingFederate to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- You must have access to the Adobe Creative Cloud Admin Portal. For this, you must have an Enterprise/Business Plan.
- Populate Adobe Creative Cloud with at least one user to test access.
- You must have administrative access in PingFederate.

Create a directory within the Adobe admin portal

1. Sign on to the Adobe admin portal.
2. Click the **Settings** tab.
3. Select **Identity** and click **Create Directory**.



4. Enter a name for the **Directory** and select **Federated ID**.
5. Click **Next**.
6. Select **Other SAML Providers**.



7. Click **Next**.
8. Download the **Copy** and note the **Entity ID** and **ACS URL** values.

Create a PingFederate service provider (SP) connection for Adobe Creative Cloud

1. Sign on to the PingFederate administrative console.
2. Configure using **Browser SSO** profile **SAML 2.0**.
3. Set **Partner's Entity ID** to the entity ID value that you copied previously.
4. Enable the following **SAML Profiles**:
    - **IdP-Initiated SSO**
    - **SP-Initiated SSO**
5. In **Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment**, map the **SAML_SUBJECT** to your email attribute, map the **FirstName** to your first name attribute, and map the **LastName** to your last name attribute.
6. In **Protocol Settings: Assertion Consumer Service URL**, set **Binding** to **POST** and set **Endpoint URL** to the ACS URL value that you copied previously.
7. In **Protocol Settings: Allowable SAML Bindings**, enable **POST.**
8. In **Credentials: Digital Signature Settings**, select the **PingFederate Signing Certificate**.
9. Export the metadata file and certificate from PingFederate to upload to the Adobe Admin Console.

Test the PingFederate IdP-initiated SSO integration

1. Go to the **PingFederate SSO Application Endpoint** for the Adobe Creative Cloud connection.
2. Authenticate with PingFederate.

   You're redirected to your Adobe Creative Cloud.

Test the PingFederate SP-initiated SSO integration

1. Go to your Adobe Creative Cloud.
2. When you're redirected to PingFederate, enter your PingFederate username and password.

   After successful authentication, you're redirected back to Adobe Creative Cloud.

Aha! Ideas

Configuring SAML SSO with Aha! Ideas and PingOne

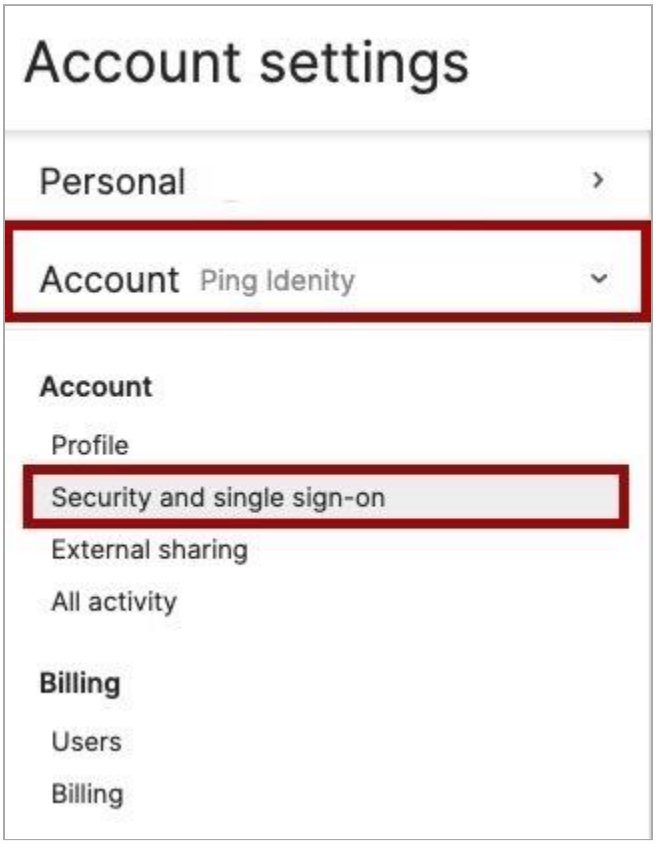
Learn how to configure SAML SSO using Aha! Ideas and PingOne.

About this task

Learn more about Aha! and SAML SSO in Aha! Roadmaps | Account SSO | SAML 2.0 on the Aha! support site.

Obtain your SAML configuration from Aha! Ideas

1. Sign on to your Aha! Ideas admin account.
2. On the **Account settings** page, go to **Account → Security and single sign-on**.



3. In the **Single sign-on** section, in the **Identity provider** list, select **SAML 2.0**.

The **SAML 2.0 Configuration** page opens.

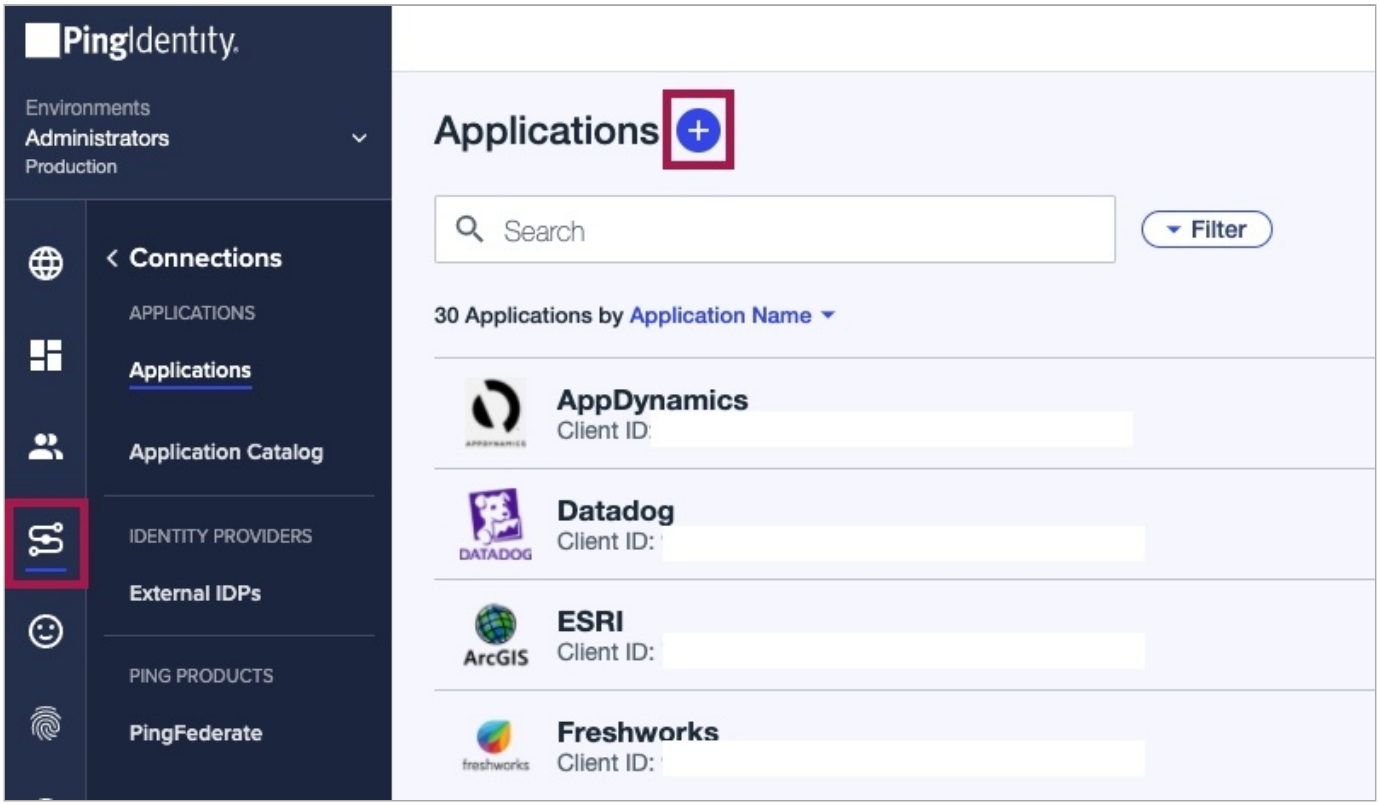
Keep this tab open as you will need these settings in the next procedure.

Configure Aha! Ideas in PingOne

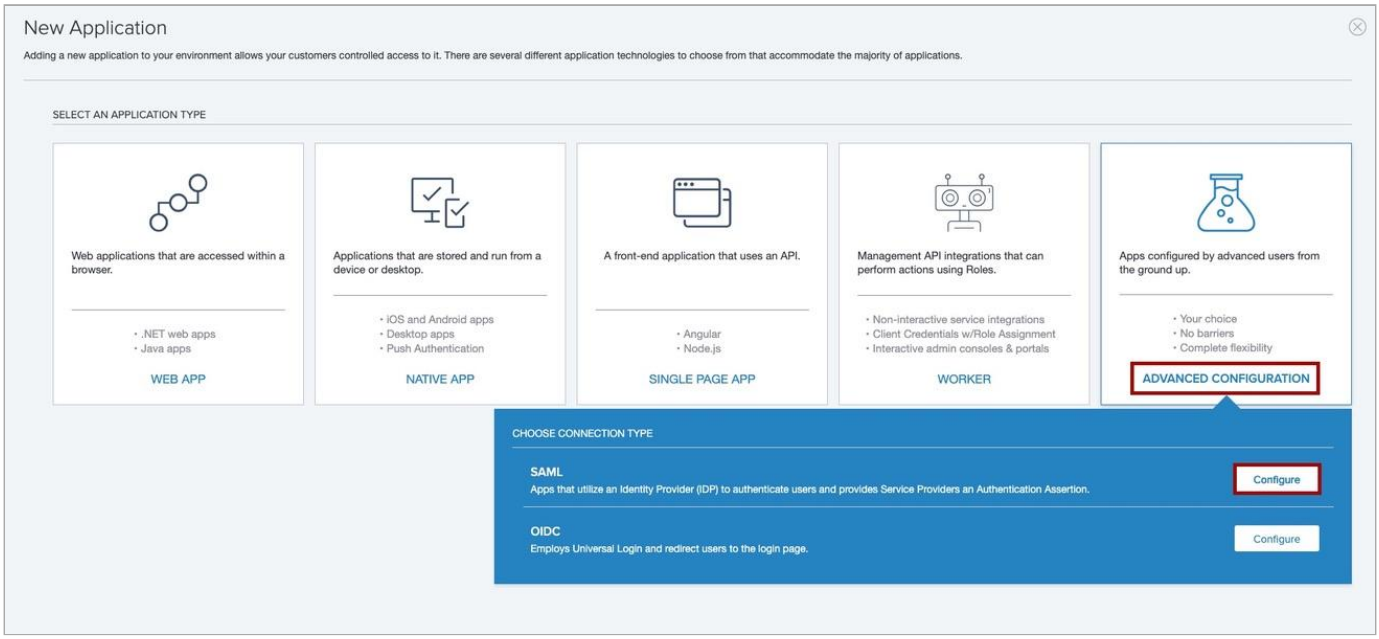
1. In a new tab, sign on to your PingOne SSO admin account.

   You'll use the settings from the previous procedure to configure Aha! Ideas in PingOne.

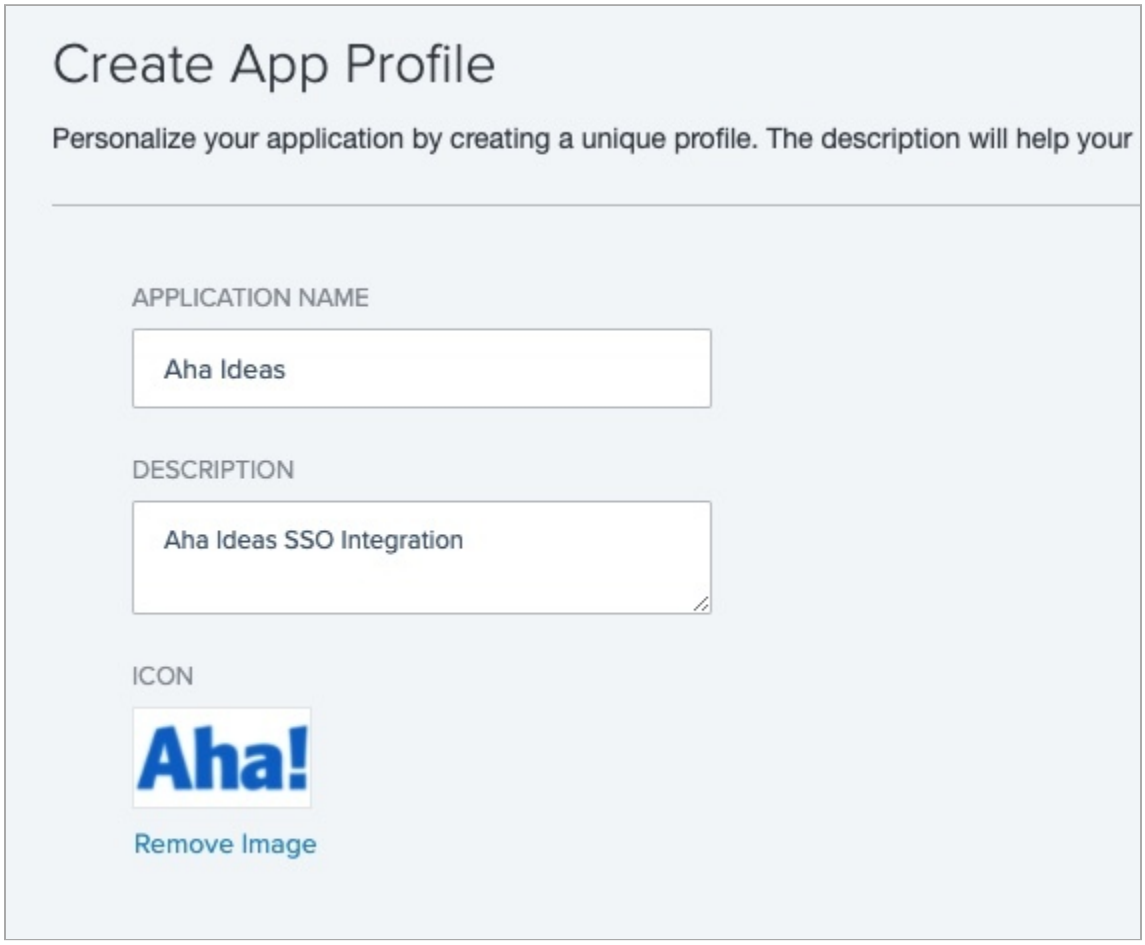
2. Go to **Connections → Applications** and click the + icon.



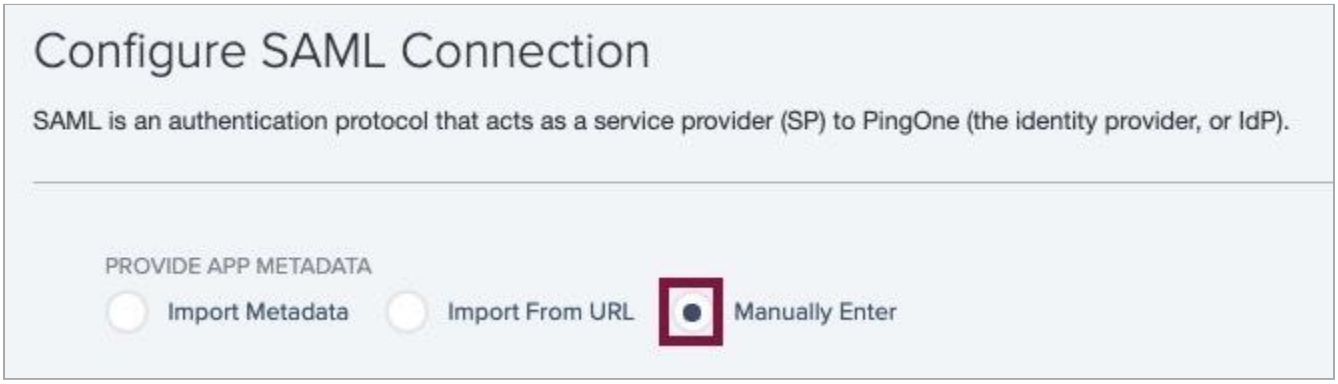
3. On the **New Applications** page, click **Advanced Configuration** and on the **SAML** line, click **Configure**.



4. On the **Create App Profile** page, enter:
    - **Application Name** (Required)
    - **Description** (Optional)
    - **Icon** (Optional)

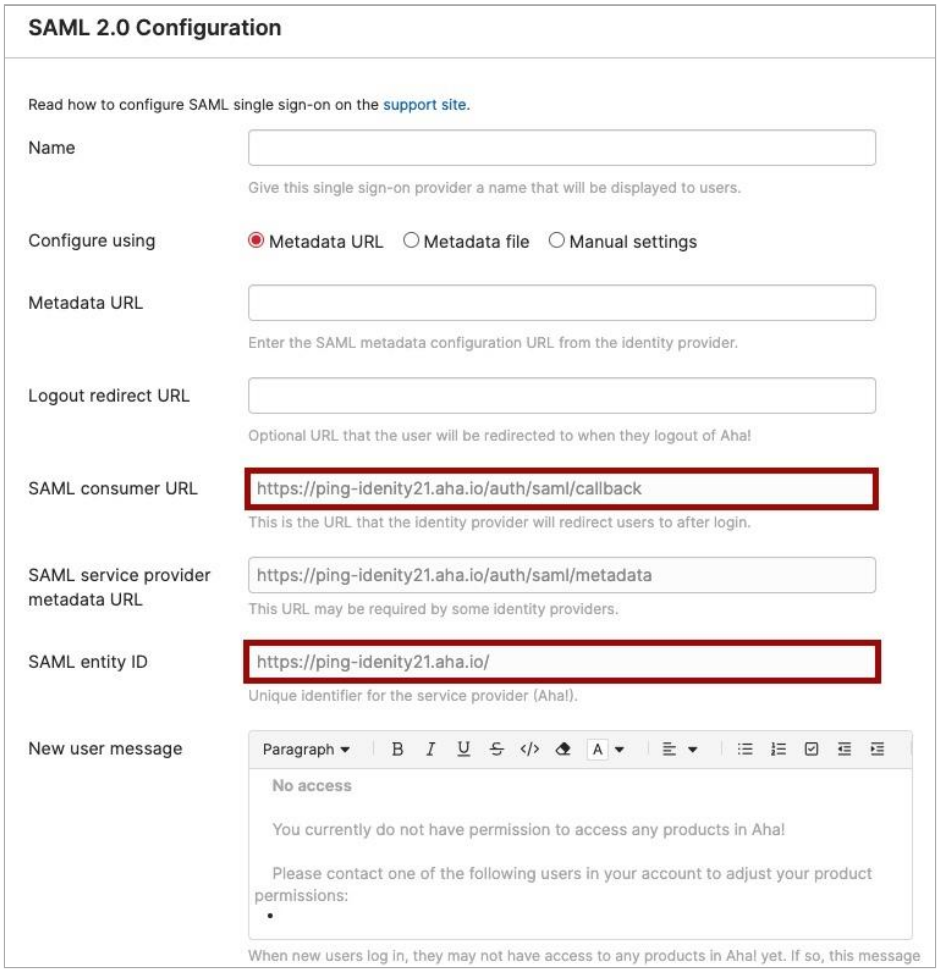


5. On the **Configure SAML Connection** page, in the **Provide App Metadata** section, click **Manually Enter**.

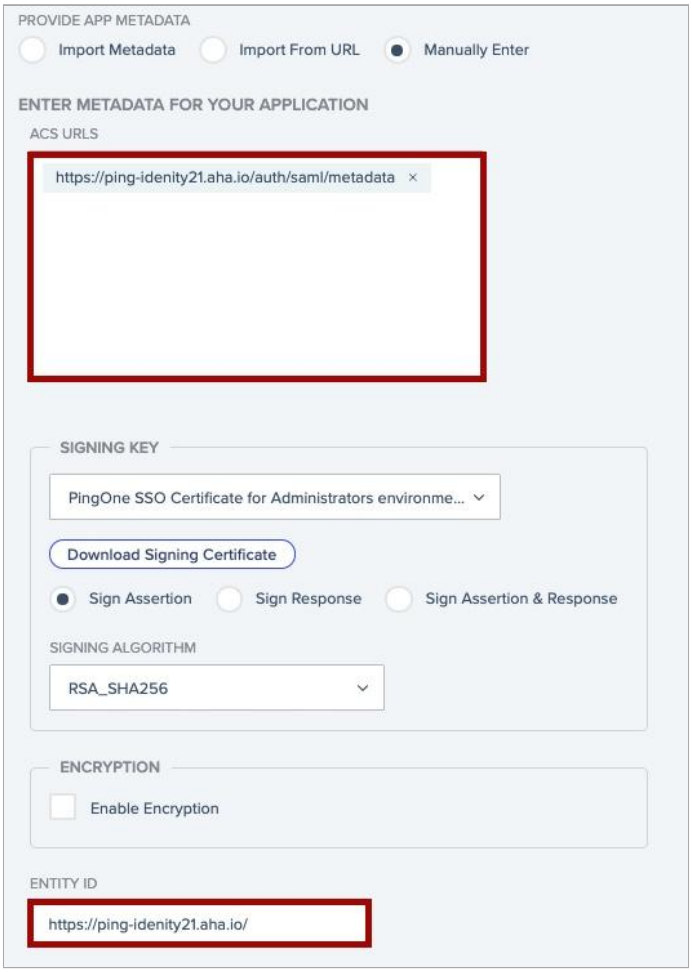


6. On your Aha! Ideas tab, copy the **SAML consumer URL** and **SAML Entity ID** values to a text editor.

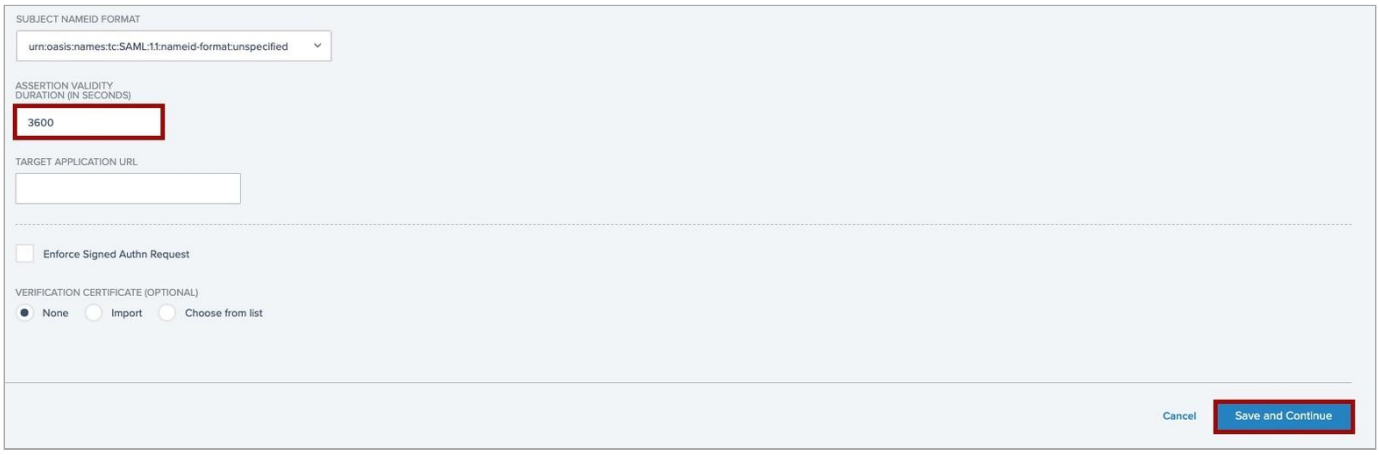
> **Note**
>
> The URLs are hard-coded and grayed-out, but you can still copy them.



7. In your PingOne SSO account, paste the **SAML consumer URL**value into the **ACS URLS** section and the **SAML entity ID** value into the **Entity ID** section.



8. Enter a value in the **Assertion Validity Duration** field, such as 3600, and then click **Save and Continue**.

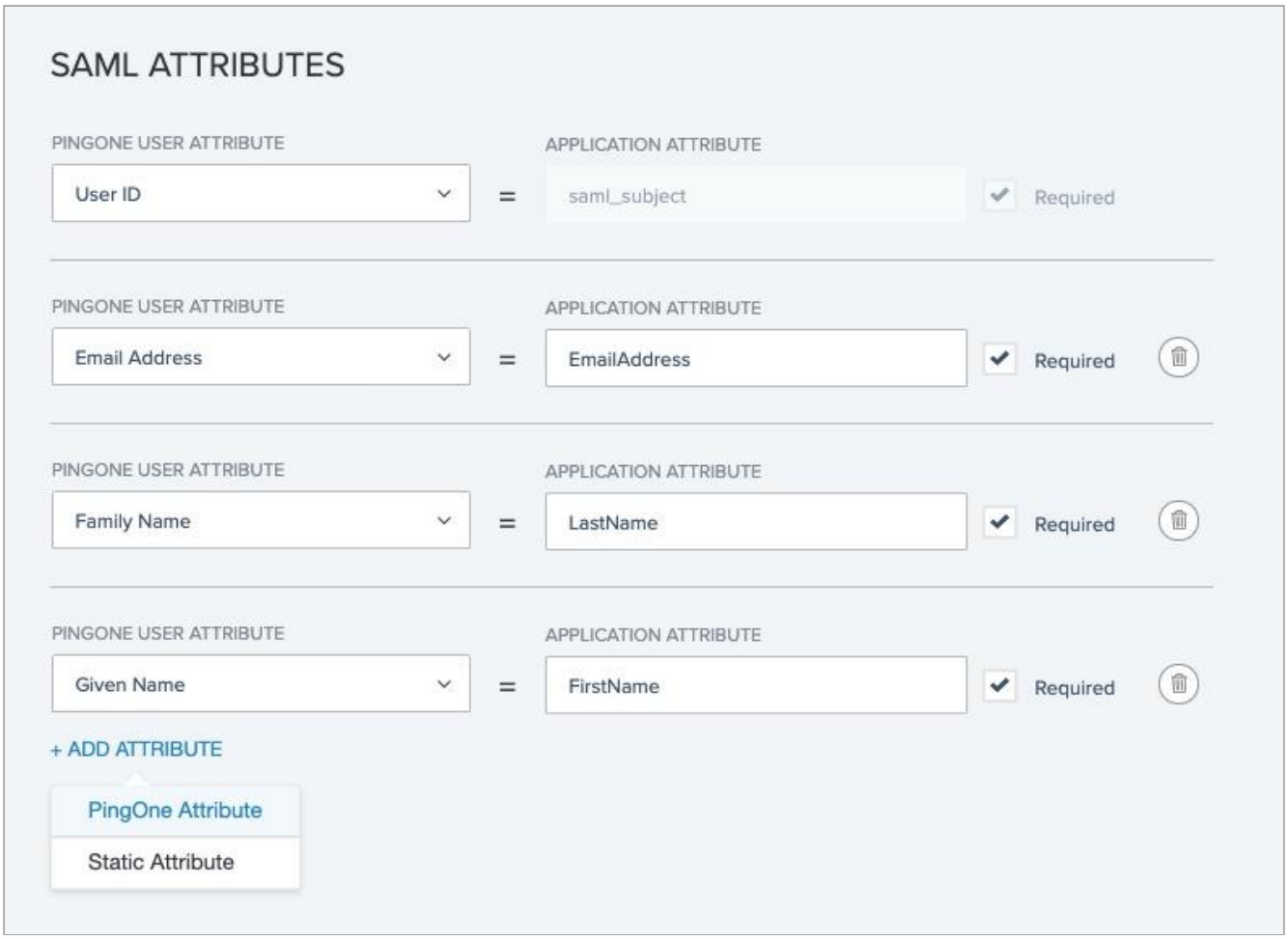


9. On the **Attribute Mapping** page, add the following **PingOne Attributes**:

User Attribute	Application Attribute
Email Address	**EmailAddress**

User Attribute	Application Attribute
Family Name	**LastName**
Given Name	**FirstName**

> **Note**
>
> Leave the default **User ID** attribute.



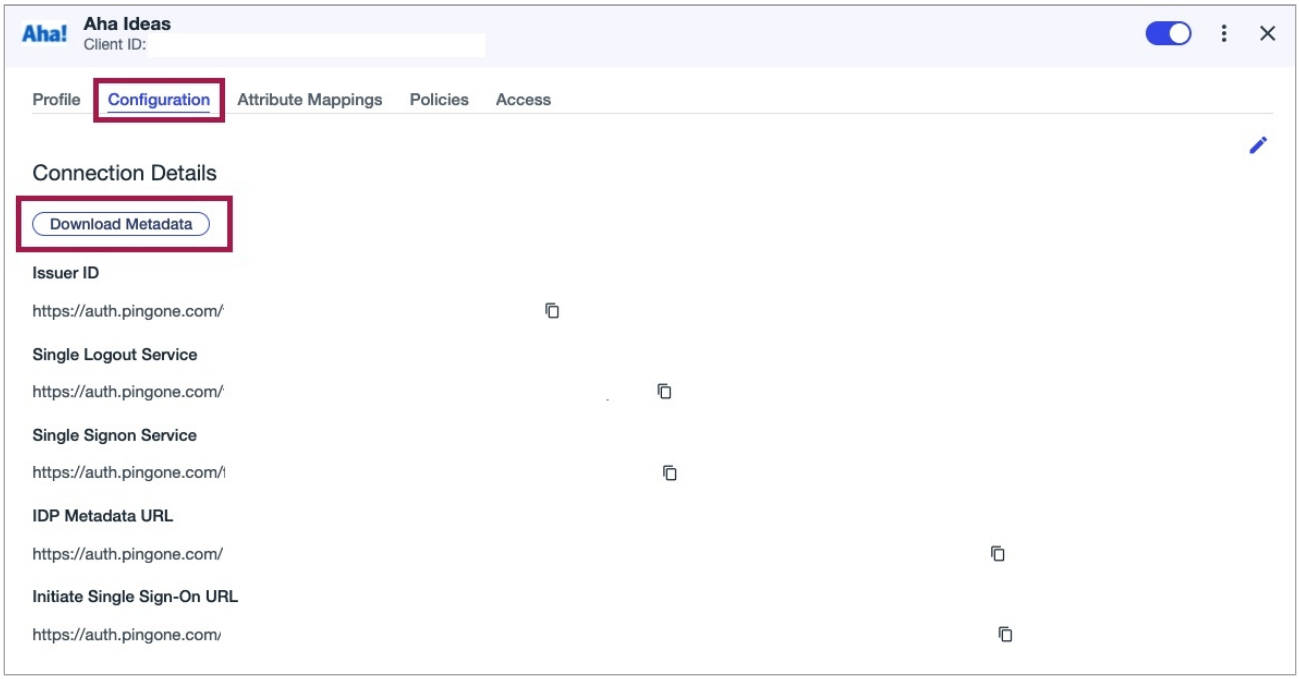
10. Click **Save and Close**.

    The **Applications** page opens.

11. In the **Applications** page:

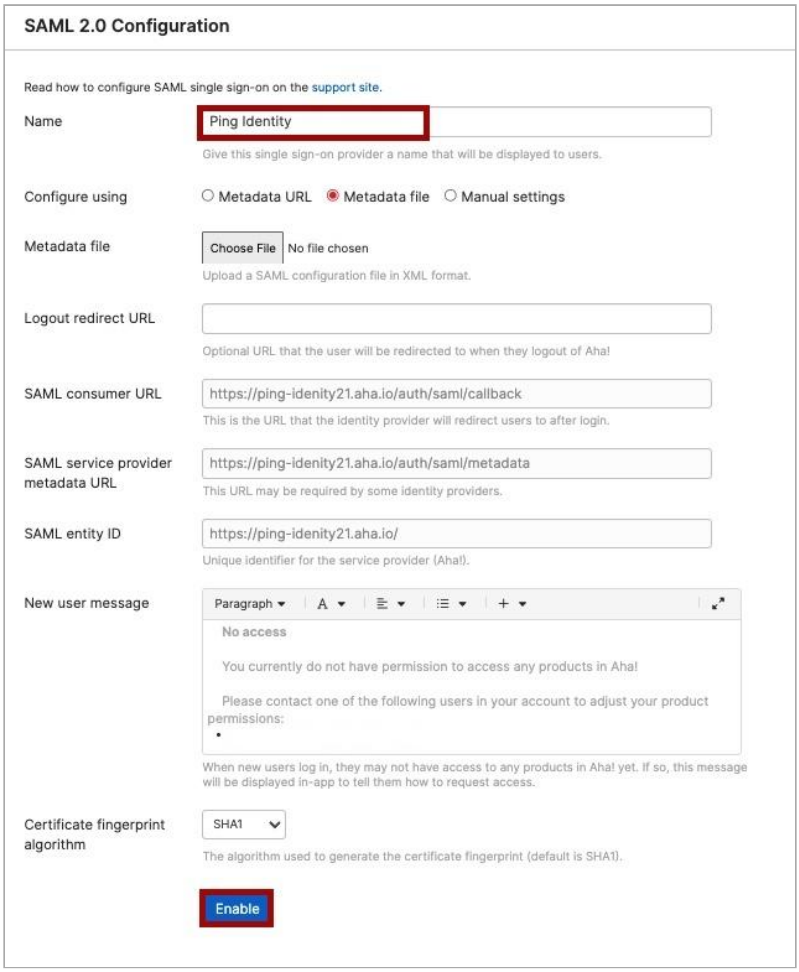
    1. Click the toggle to enable the configuration by selecting the slider.
    2. On the **Configuration** tab, in the **Download Metadata** section, click **Download**.

       You'll upload this in Aha! Ideas in the next step.



12. On your Aha! Ideas tab, in the **Configure using** section, click **Metadata file** and click **Choose File** to upload the file that you downloaded in the previous step.

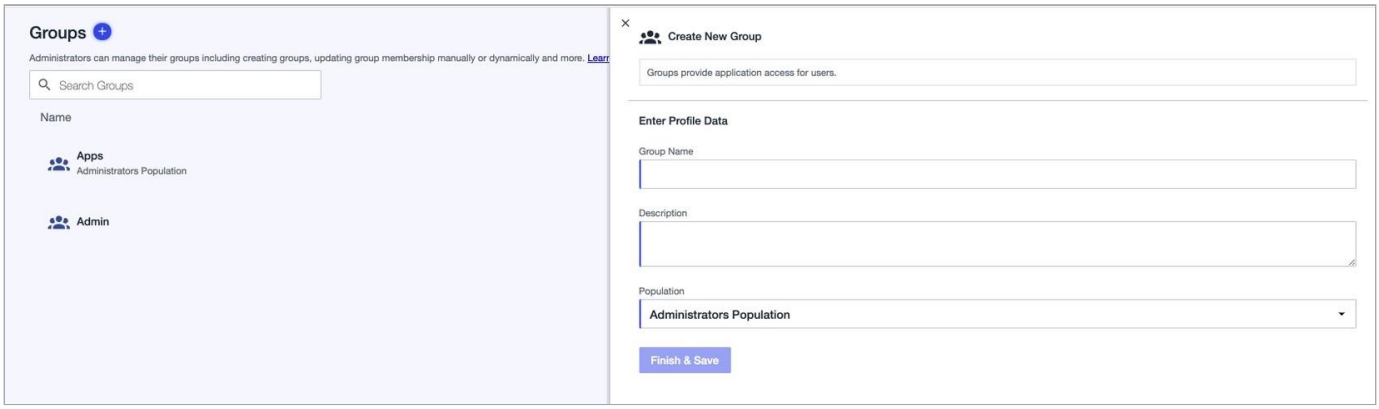
13. Enter a **Name** for the connection, such as Ping Identity, and click **Enable** to turn on the configuration.



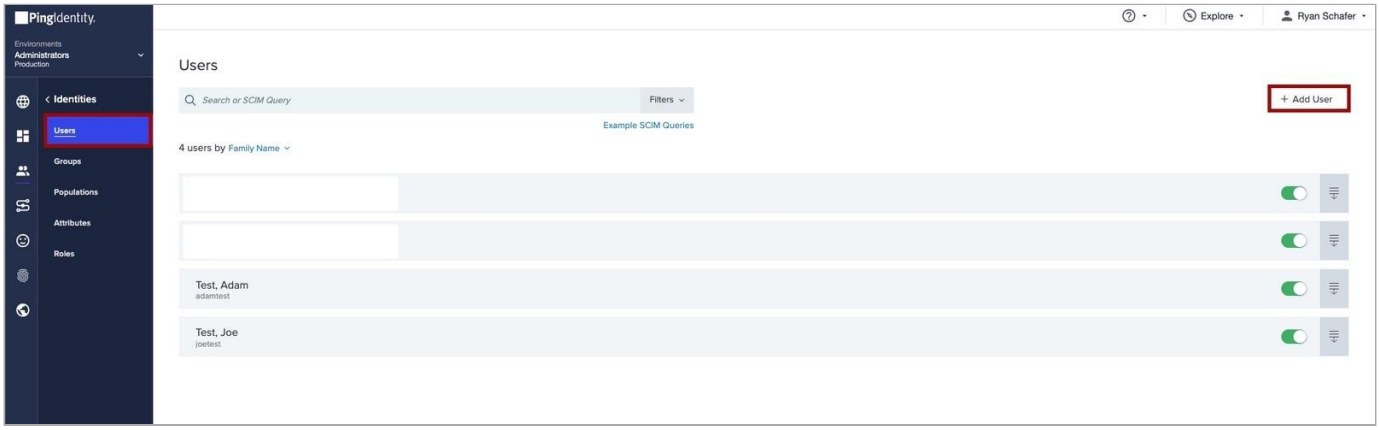
Create and assign identities

If you've already assigned identities and groups in PingOne, move on to Test the integration.

1. In PingOne, go to **Identities → Groups** and click the + icon next to **Groups**.
2. On the **Create New Group** page, enter values for the following:
    - **Group Name** (Required)
    - **Description** (Optional)
    - **Population** (Optional)
3. Click **Finish & Save**.



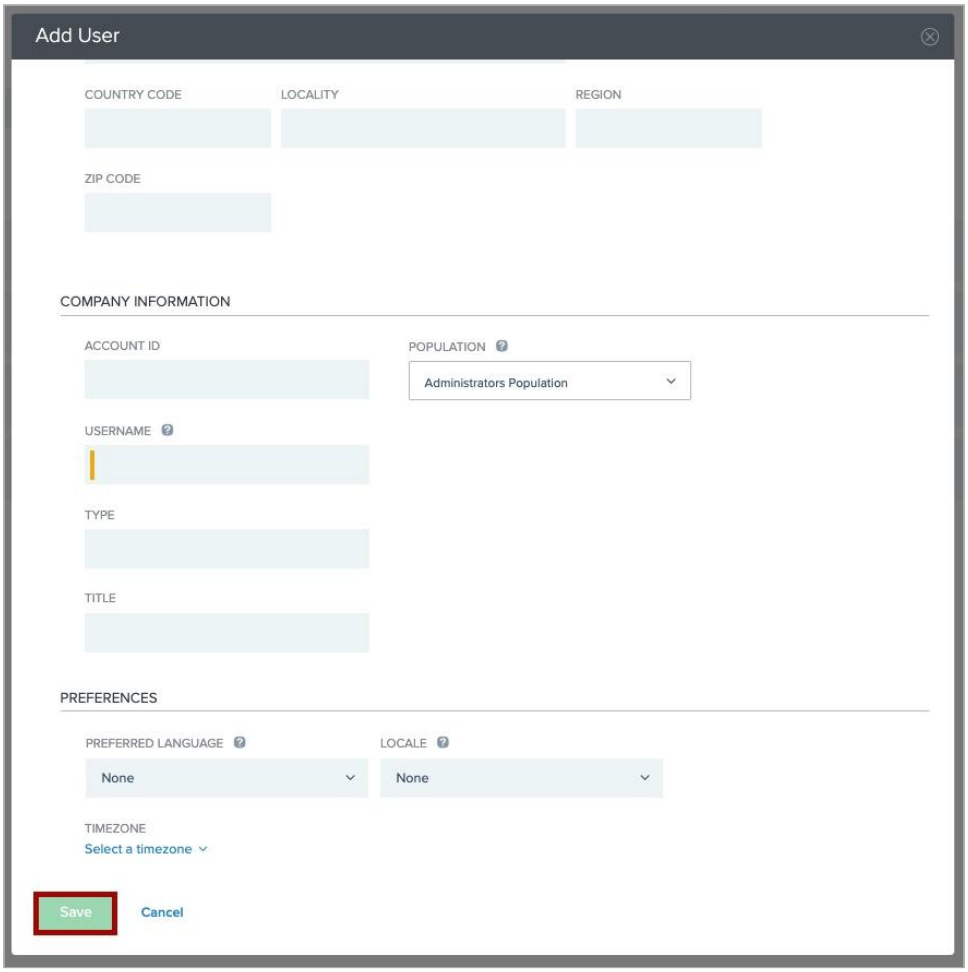
4. To add identities to the group, on the **Identities** tab, go to **Users → + Add User**.



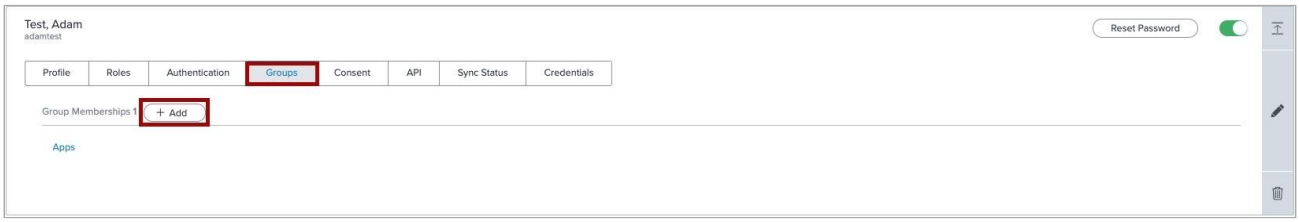
5. On the **Add User** page, enter in all the necessary information for a user.

> **Important**
>
> Verify that the email address is correct, as this is the value passed in the SAML assertion.

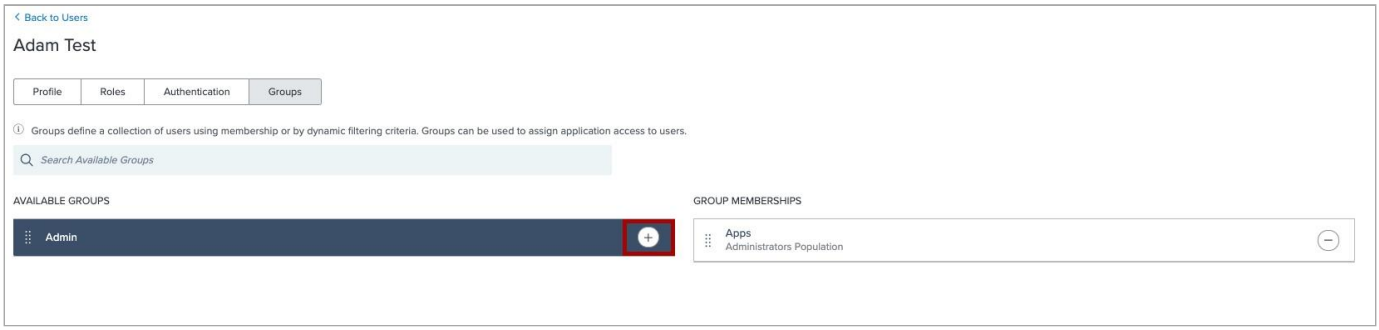
6. Click **Save**.



7. To assign the user that you created to the group that you created previously, locate the user you created and:
    1. Expand their section.
    2. Select the **Groups** tab.
    3. Click **+ Add**.

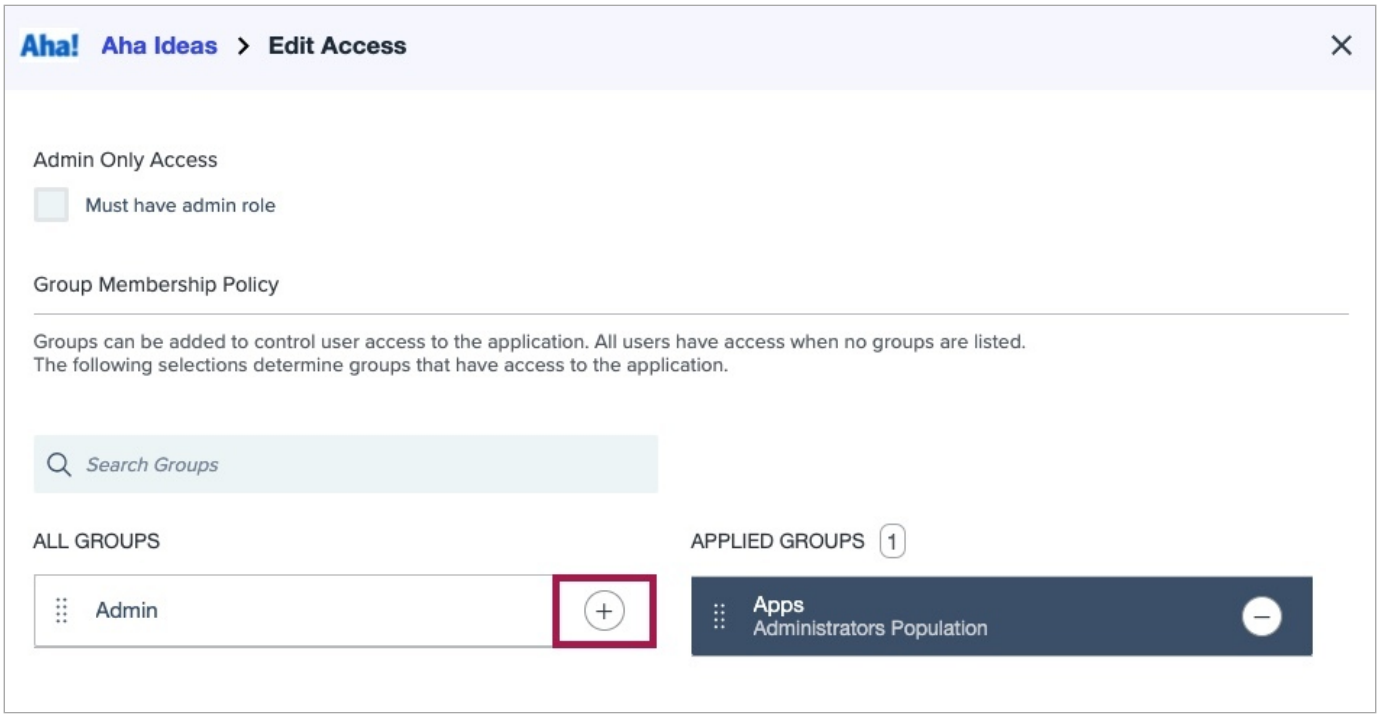


8. In the **Available Groups** section, select the group that you created and click the ⊕ icon to add it to the user's group memberships. Click **Save**.



9. On the **Connections** tab, for the Aha! Ideas application:
    1. Click the **Access** tab.
    2. Click the **Pencil** icon to edit the configuration.

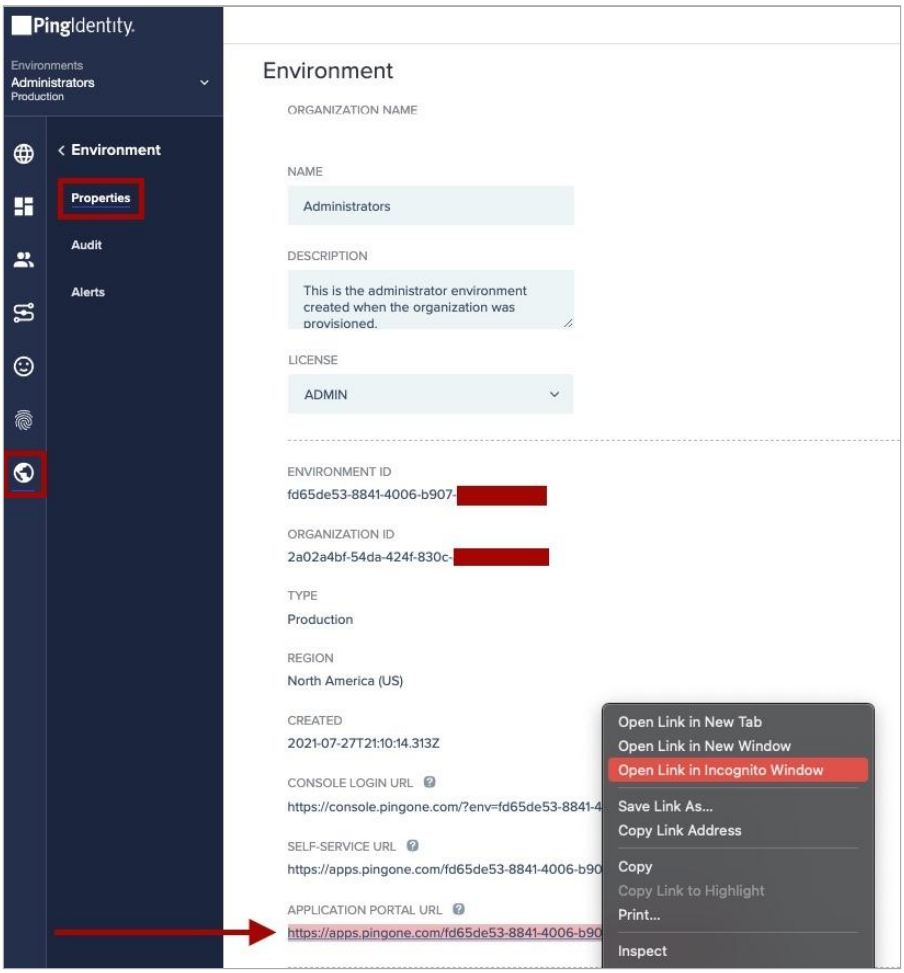
10. Select the group that you created and add it to the **Applied Groups** section. Click **Save**.



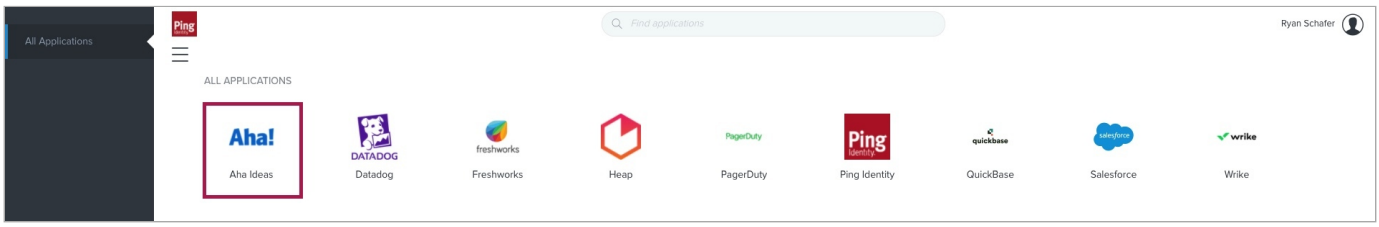
Test the integration

1. In the PingOne admin console, go to **Dashboard → Environment Properties**.

2. Right-click on the **Application Portal URL** and open it in a private browser session.



3. In your private browser window, sign on as the test user that you created and click the Aha! Ideas tile.



You're now signed on to the user's Aha! Ideas account.

Atlassian Cloud

Configuring SAML SSO with Atlassian Cloud and PingFederate

About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
`SAML_SUBJECT`	Email Address	Required
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname`	First Name	Required
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname`	Surname	Required
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name`	ID (not email)	Required

The following table details the references that are used within this guide that are environment specific. Replace these with the suitable value for your environment.

Reference	Description
TenantSSOID	Tenant single sign-on (SSO) ID, retrieved from Atlassian Cloud SAML Single Sign-on configuration as part of EntityID and Assertion Consumer Service (ACS) URL.

Create a PingFederate SP connection for Atlassian Cloud

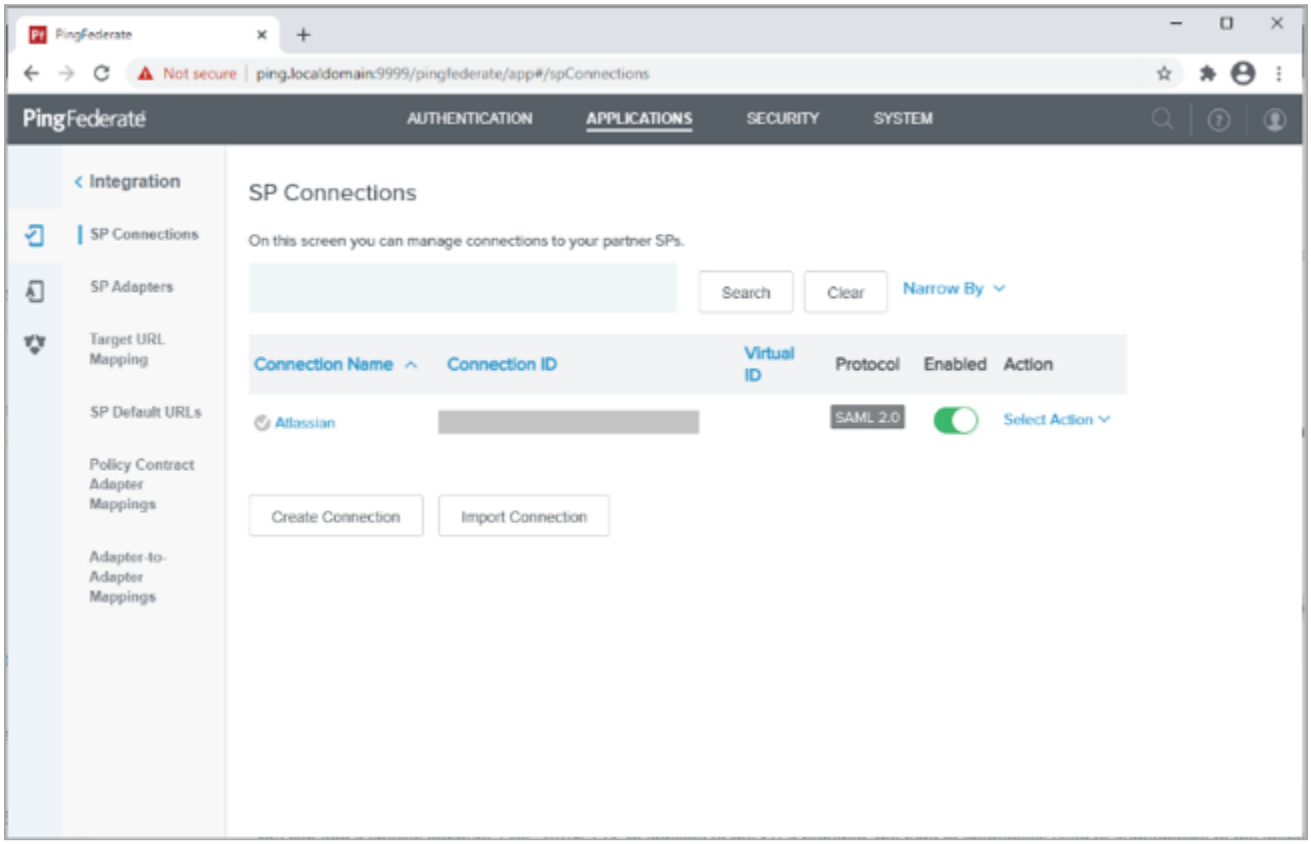
> **Note**
> The following configuration is untested, and is provided as an example. Additional steps might be required.

1. In Atlassian Cloud, go to **Security → SAML Single Sign-on** and sign on to Atlassian Cloud as an administrator.
2. Make a note of the **Entity ID** and **ACS URL** values.

   You will need these later.
3. Sign on to the PingFederate administrative console.
4. Using the details retrieved from the application UI:
   - Configure using **Browser SSO** profile **SAML 2.0**.

- Enable the **IDP-Initiated SSO** SAML profile.
- Enable the **SP Initiated SSO** SAML profile.
- In **Assertion Creation → Attribute Contract**, set the **Subject Name Format** to `urn:oasis:names:tc:SAML:2.0:attrname-format:emailAddress`.
- Add the following attributes as type `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`:
  - `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname`
  - `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname`
  - `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name`
- In **Assertion Creation → Attribute Contract Fulfilment**:
  - Map attribute **SAML_SUBJECT** to the attribute **mail**.
  - Map attribute **givenname** to the attribute **givenName**.
  - Map attribute **surname** to the attribute **sn**.
  - Map attribute **name** to the non-email unique identifier, such as **uid**.
- In **Protocol Settings**:
  - For **Assertion Consumer Service URL**, enter the consumer service URL retrieved from Atlassian and configure as index 0.
  - For **Allowable SAML Bindings**, enable **Redirect** and **POST**.

5. Export the signing certificate public key.



Configure the PingFederate IdP connection for Atlassian Cloud

> **Note**
>
> The following configuration is untested and is provided as an example. Additional steps might be required.

1. Sign in to Atlassian Cloud as an administrator.
2. Go to **Security → SAML Single Sign-on**.
3. Click **Add SAML Configuration**.
4. Enter the following details:
    - In the **Identity Provider Entity ID** field, enter the **Issuer** value for your PingFederate environment configuration.
    - In the **Identity Provider SSO URL** field, enter the SSO URL for your PingFederate environment configuration.
    - In a text editor, open the certificate you downloaded during the PingFederate and paste the contents of the certificate into the **Public x509 Certificate** field.
5. Click **Save Configuration**.

Configuring SAML SSO with Atlassian Cloud and PingOne for Enterprise

About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
`SAML_SUBJECT`	Email Address	Required
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname`	First Name	Required
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname`	Surname	Required
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name`	ID (not email)	Required

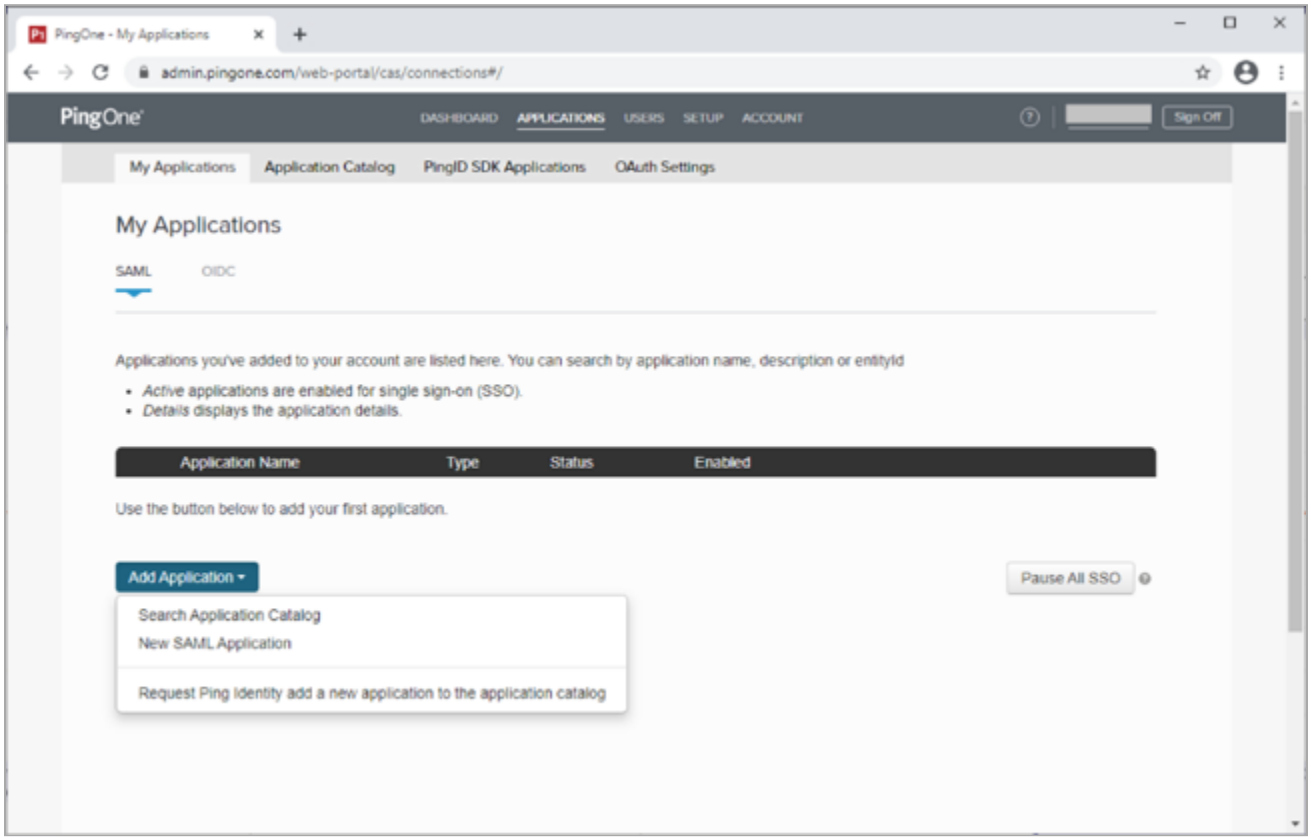
The following table details the references that are used within this guide that are environment specific. Replace these with the suitable value for your environment.

Reference	Description
TenantSSOID	Tenant single sign-on (SSO) ID, retrieved from Atlassian Cloud SAML Single Sign-on configuration as part of EntityID and Assertion Consumer Service (ACS) URL.

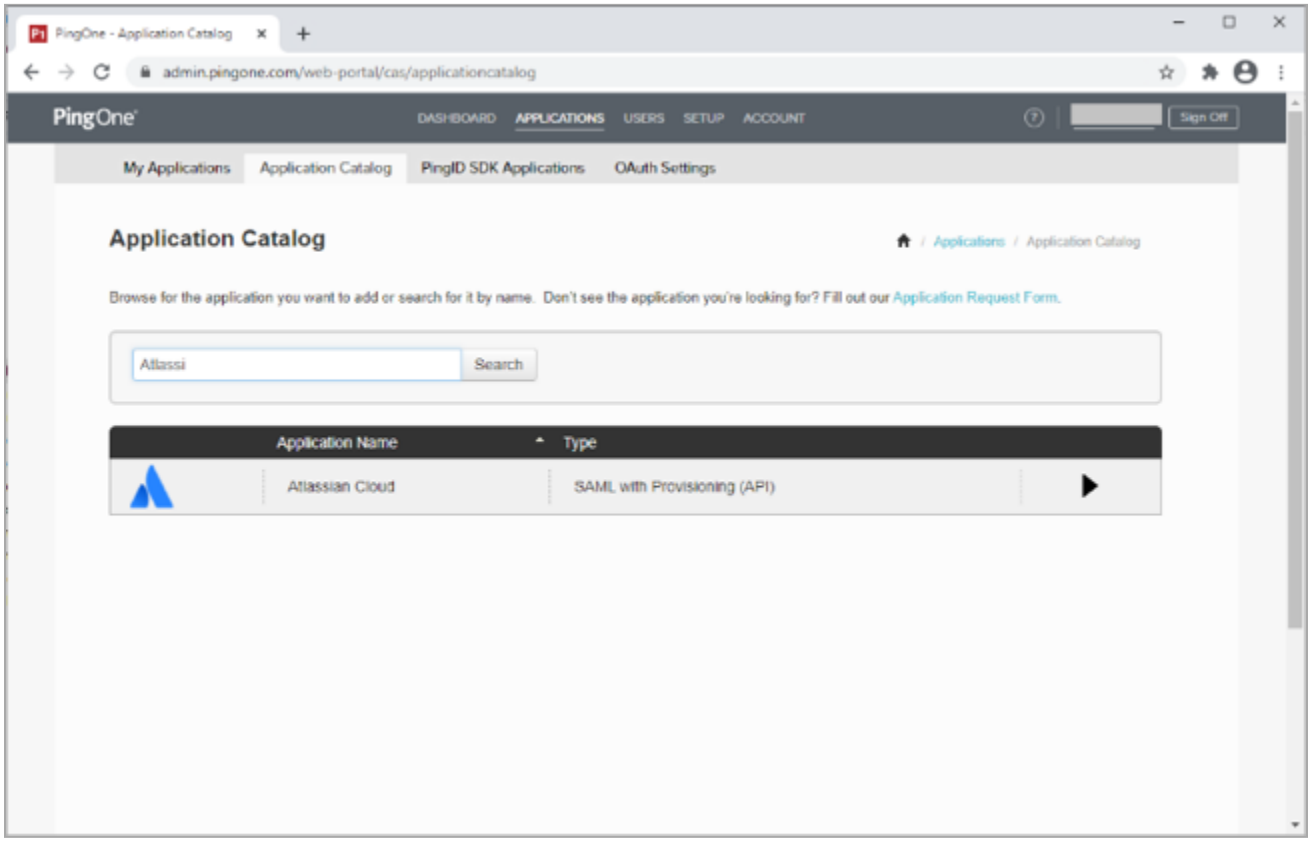
Create a PingOne for Enterprise Application for Atlassian Cloud

> **Note**
>
> The following configuration is untested, and is provided as an example. Additional steps might be required.

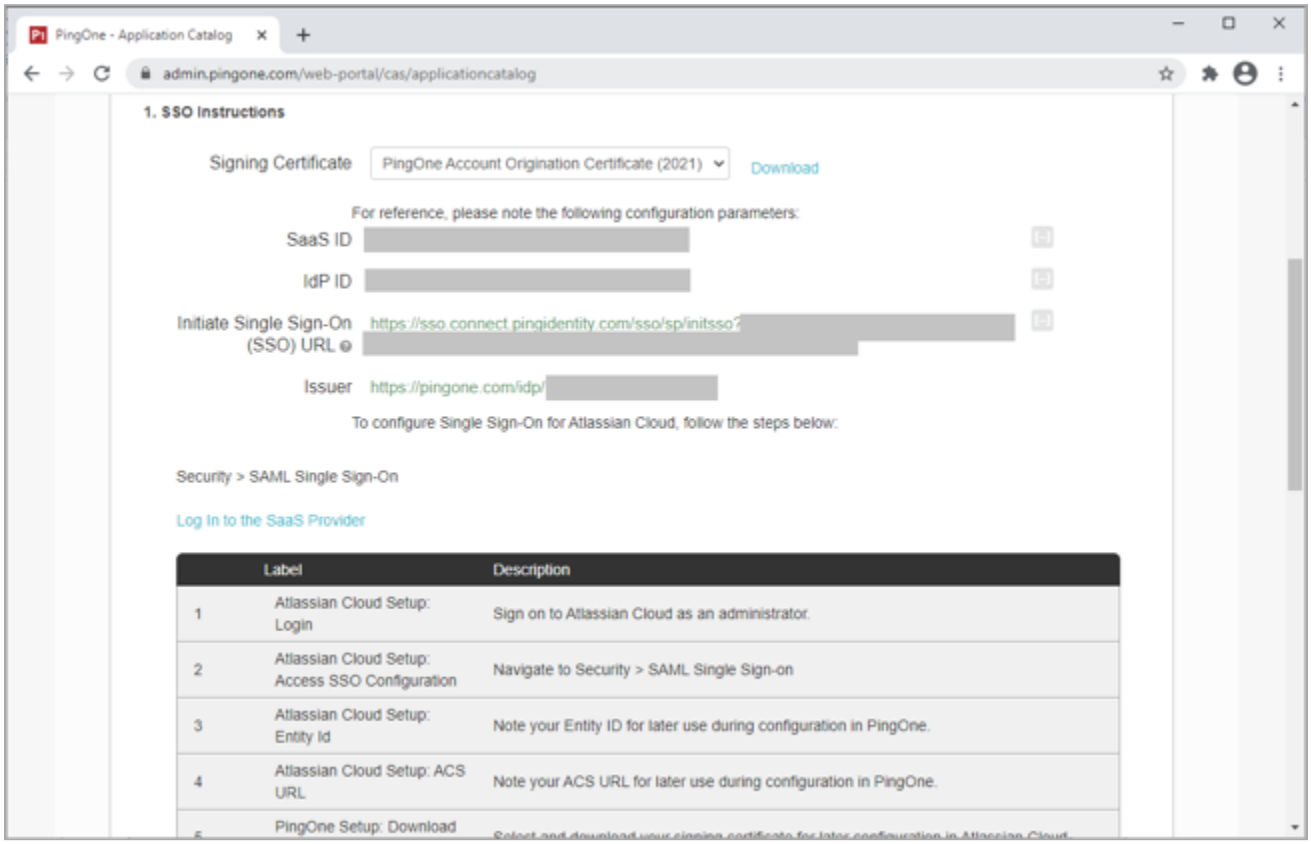
1. In Atlassian Cloud, go to **Security → SAML Single Sign-on** and sign on to Atlassian Cloud as an administrator.
2. Make a note of the **Entity ID** and **ACS URL** values.
3. Sign on to PingOne for Enterprise and go to **Applications → Application Catalog**.
4. On the **SAML** tab, in the **Add Application** list, select **Search Application Catalog**.



5. Search for `Atlassian` and then click the **Atlassian Cloud** row.

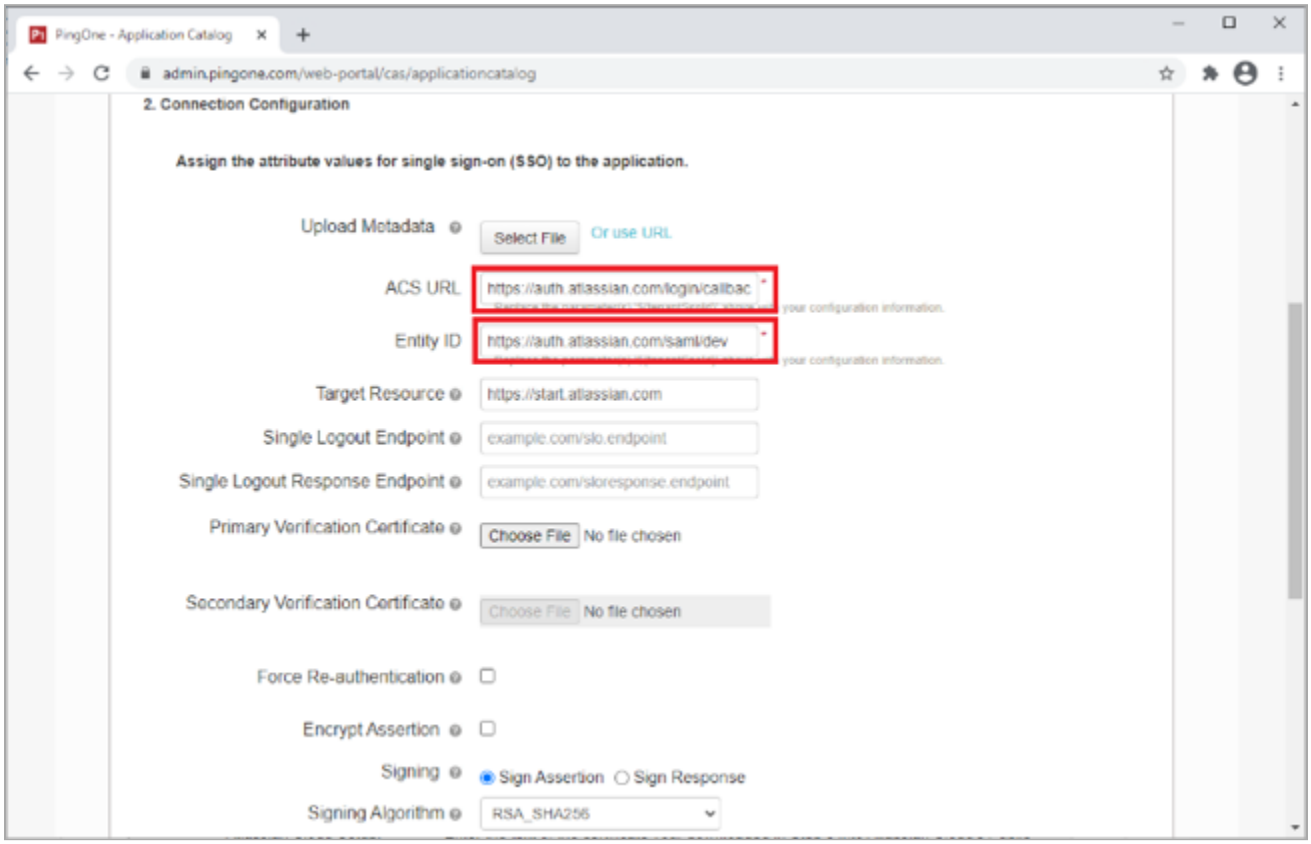


6. Click **Setup**.
7. In the **Signing Certificate** list, select the appropriate signing certificate.
8. Review the steps, and make a note of the **PingOne SaaS ID**, **IdP ID**, **Single Sign-On URL**, and **Issuer** values shown.



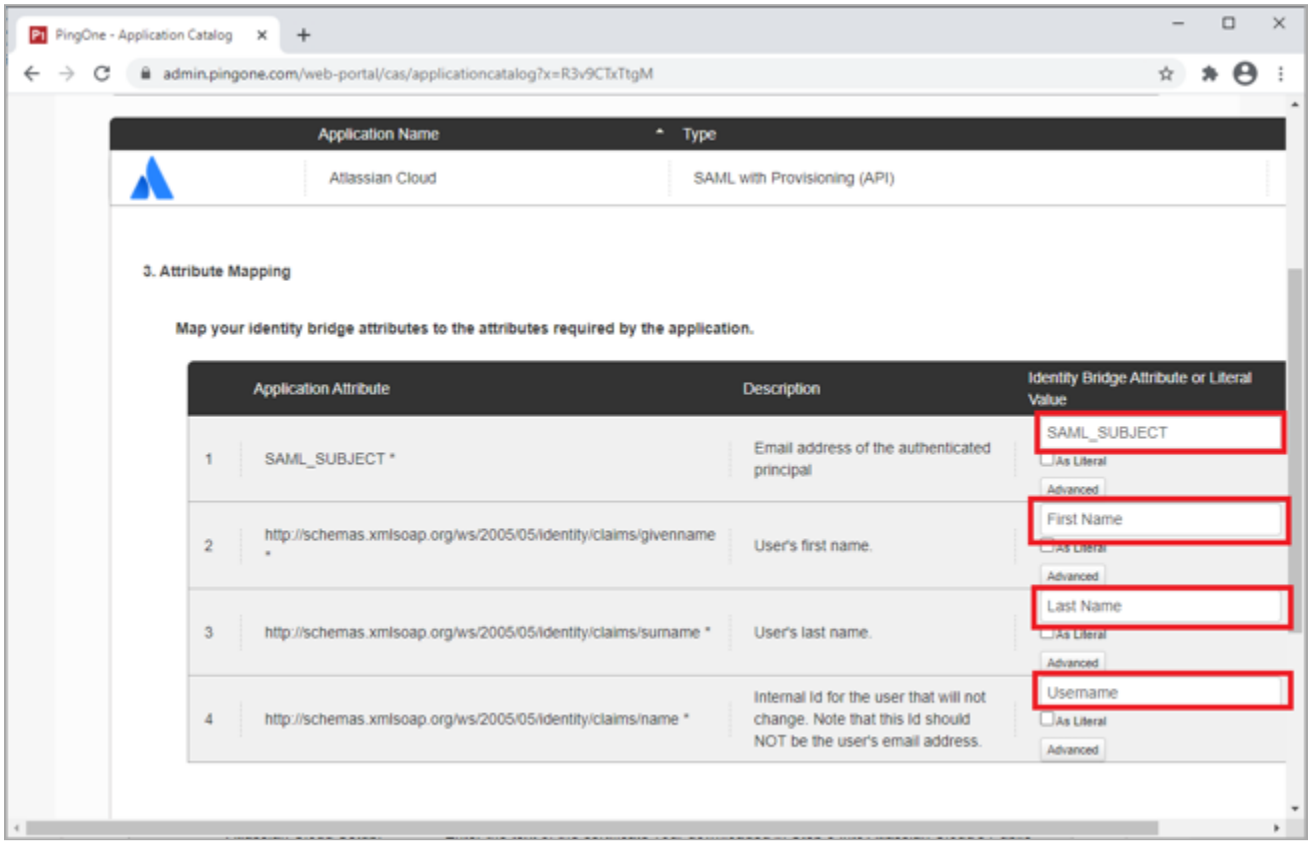
9. Click **Continue to Next Step**.
10. Enter the following.

Attribute	Directions	URL
ACS URL	Enter the ACS URL from step 1b.	https://auth.atlassian.com/login/callback?connection=saml-*tenantSSOID*
Entity ID	Enter the Entity ID from step 1b.	https://auth.atlassian.com/saml/*tenantSSOID*



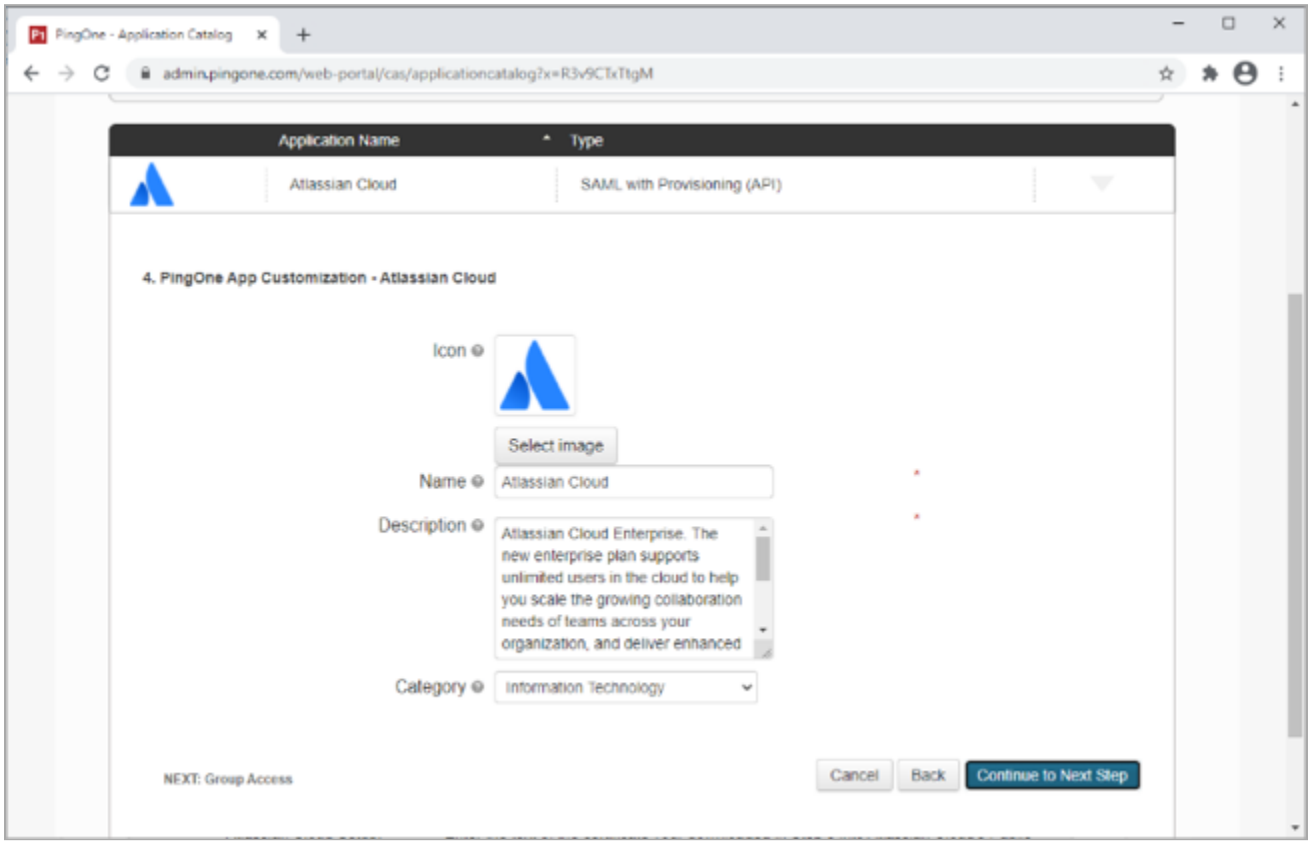
11. Click **Continue to Next Step**.
12. Configure the **Attribute Mapping** section.

Application Attribute	Identity Bridge Attribute or Literal Value
SAML_SUBJECT	Select a suitable attribute containing the email address.
givenname	Select a suitable attribute containing the user's first name.
surname	Select a suitable attribute containing the user's last name.
name	Select a suitable attribute containing the user's unique ID. **Note** This should not be the email address.



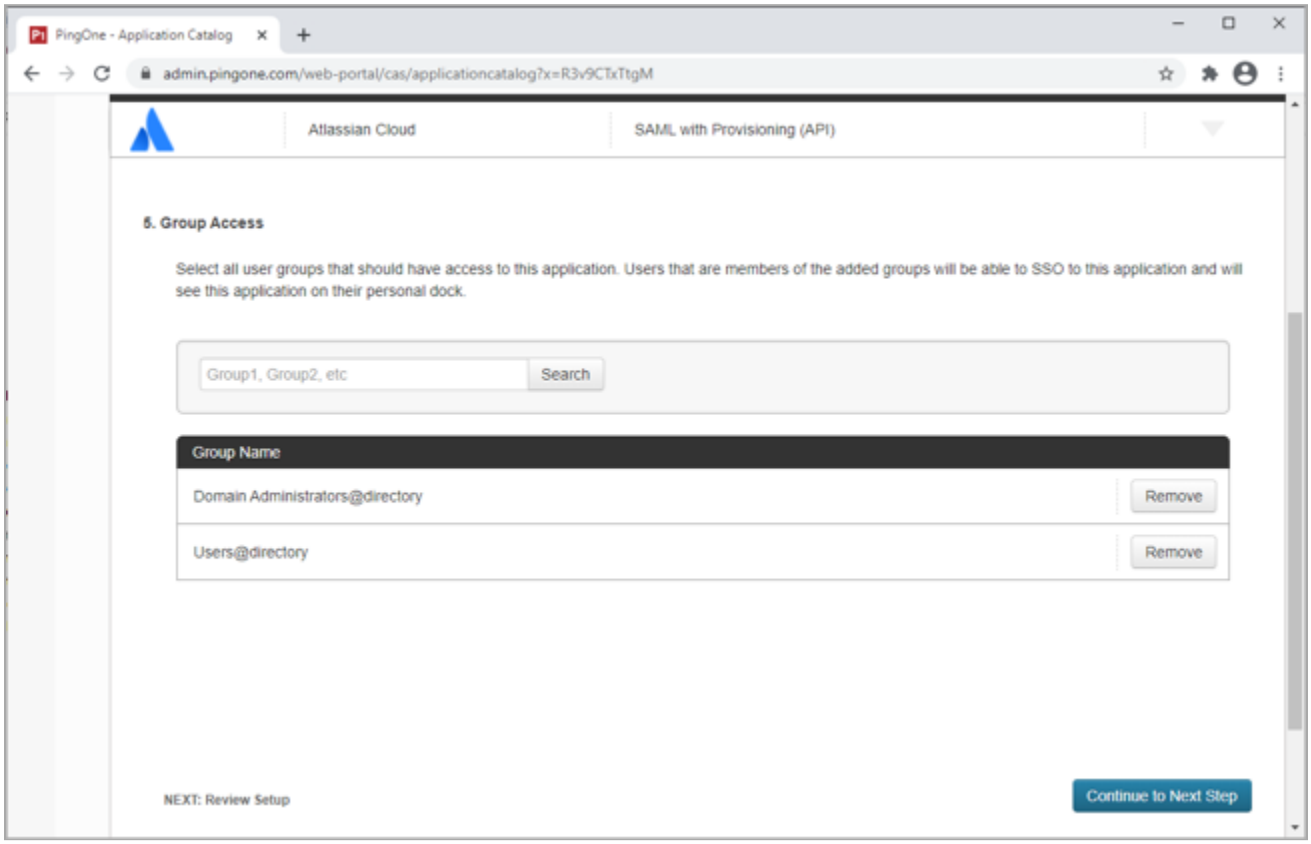
13. Click **Continue to Next Step**.

14. Update the **Name**, **Description**, and **Category** fields as required.



15. Click **Continue to Next Step**.

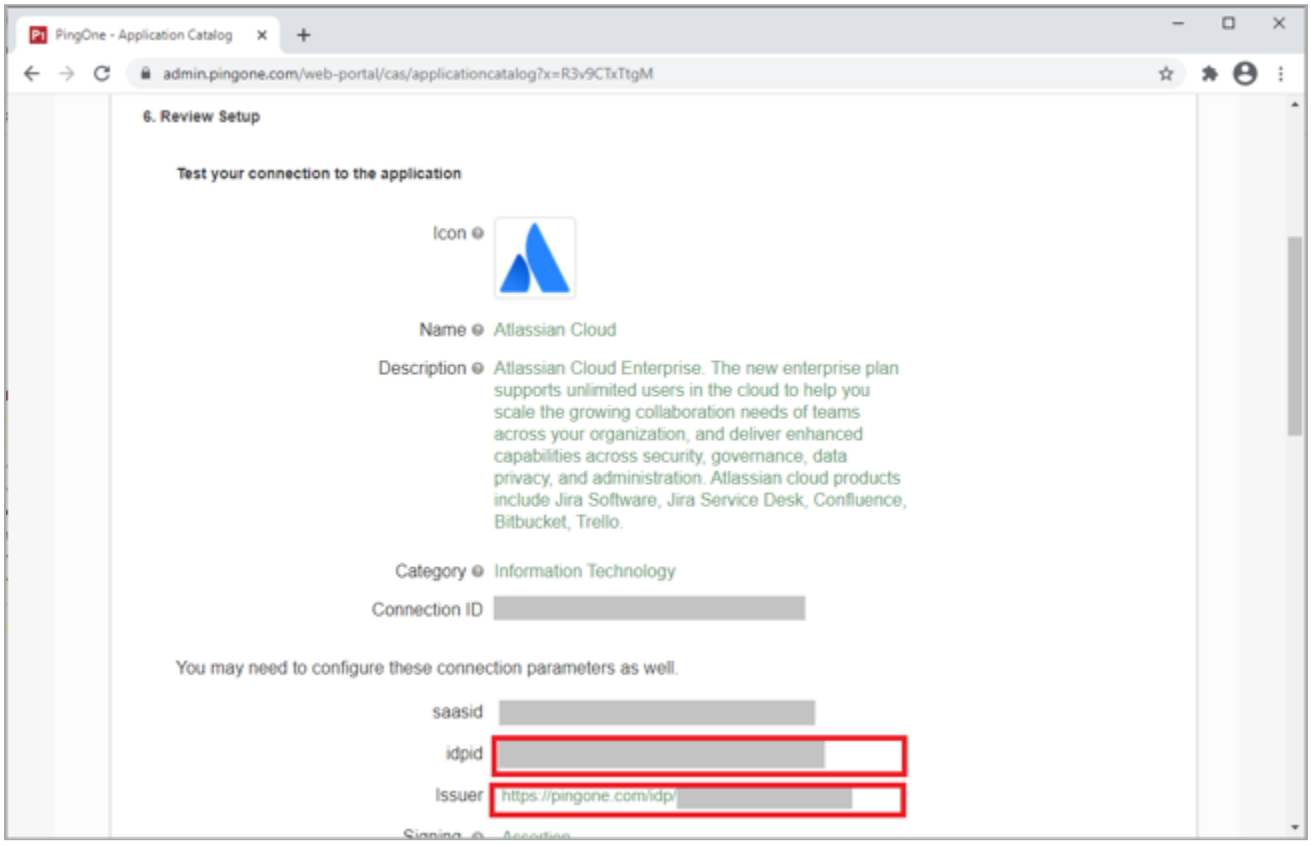
16. Add the user groups for the application.



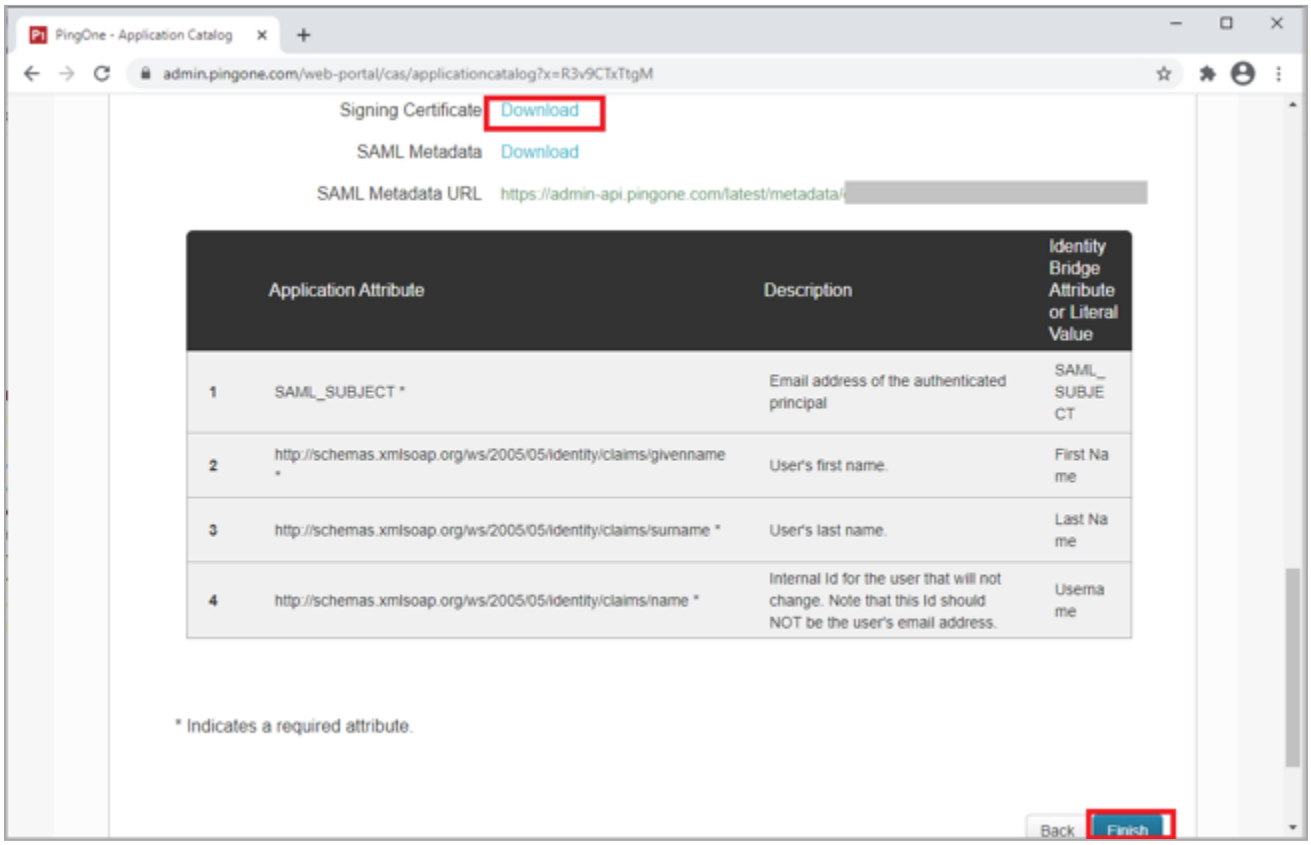
17. Click **Continue to Next Step**.
18. Review the settings.
19. Copy the **Single Sign-On (SSO) URL** value to a temporary location.

    This is the IdP-initiated SSO URL that you can use for testing.
20. Make a note of the **PingOne Issuer** and **PingOne idpid** values.

    You will use these in the Atlassian Cloud configuration.

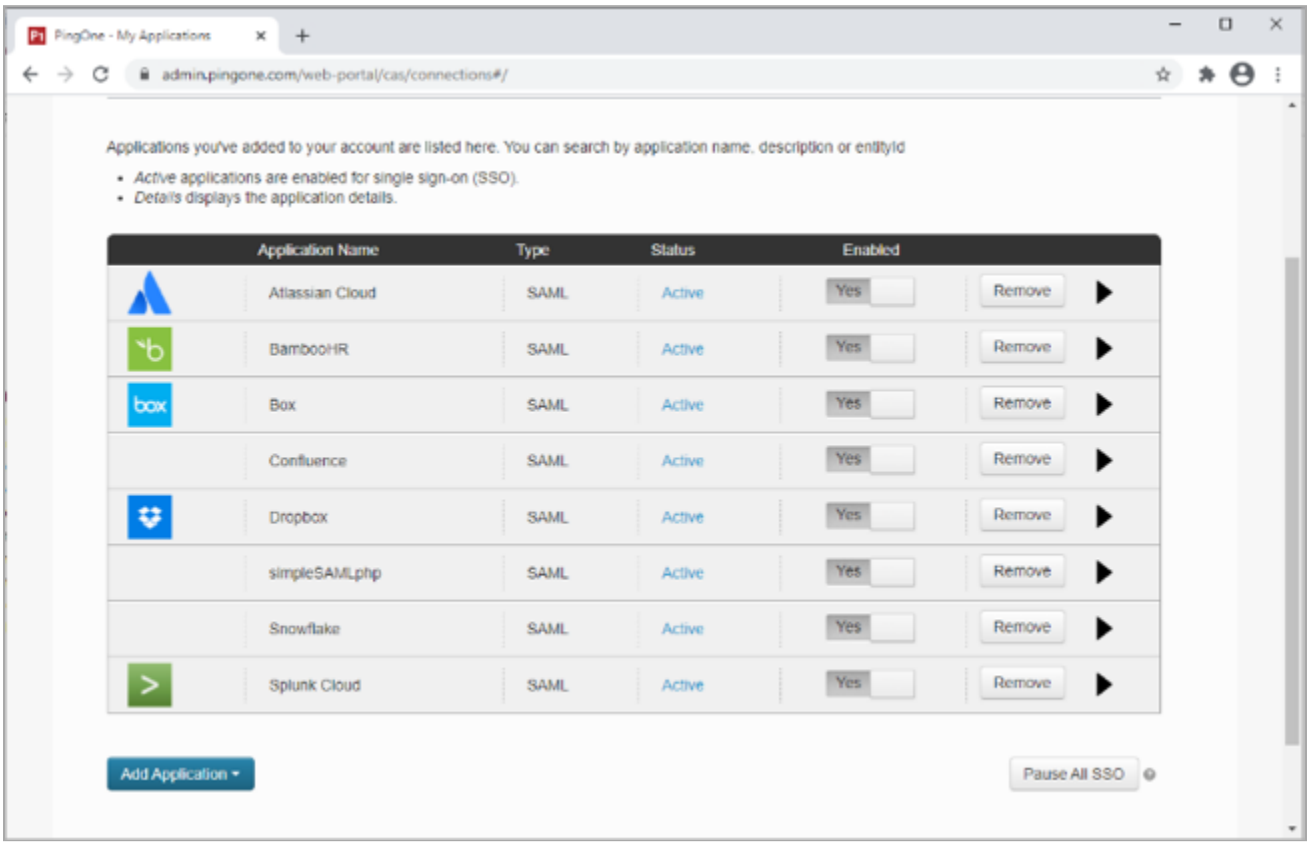


21. On the **Signing Certificate** line, click **Download**. Click **Finish**.



You will use this in the Atlassian Cloud configuration.

Result:



Configure the PingOne for Enterprise IdP connection for Atlassian Cloud

> **Note**
>
> The following configuration is untested and is provided as an example. Additional steps might be required.

1. In Atlassian Cloud, go to **Security → SAML Single Sign-on** and sign on to Atlassian Cloud as an administrator.
2. Click **Add SAML Configuration**.
3. Enter the following:
    - In the **Identity Provider Entity ID** field, enter the **Issuer** value from the PingOne for Enterprise configuration.
    - In the **Identity Provider SSO URL** field, enter `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=idpid`, replacing *idpid* with the one from the PingOne for Enterprise configuration.
    - In a text editor, open the certificate you downloaded during the PingOne for Enterprise configuration, and paste the contents of the certificate into the **Public x509 Certificate** field.
4. Click **Save Configuration**.

Amazon

Configuring SAML SSO with AWS IAM and PingFederate

Enable Amazon Web Services (AWS) sign-on from a PingFederate URL (IdP-initiated sign-on).

Before you begin

- Configure PingFederate to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- Populate AWS with at least one user to test access.
- You must have administrative access to PingFederate and AWS.

Create the PingFederate SP Connection for AWS

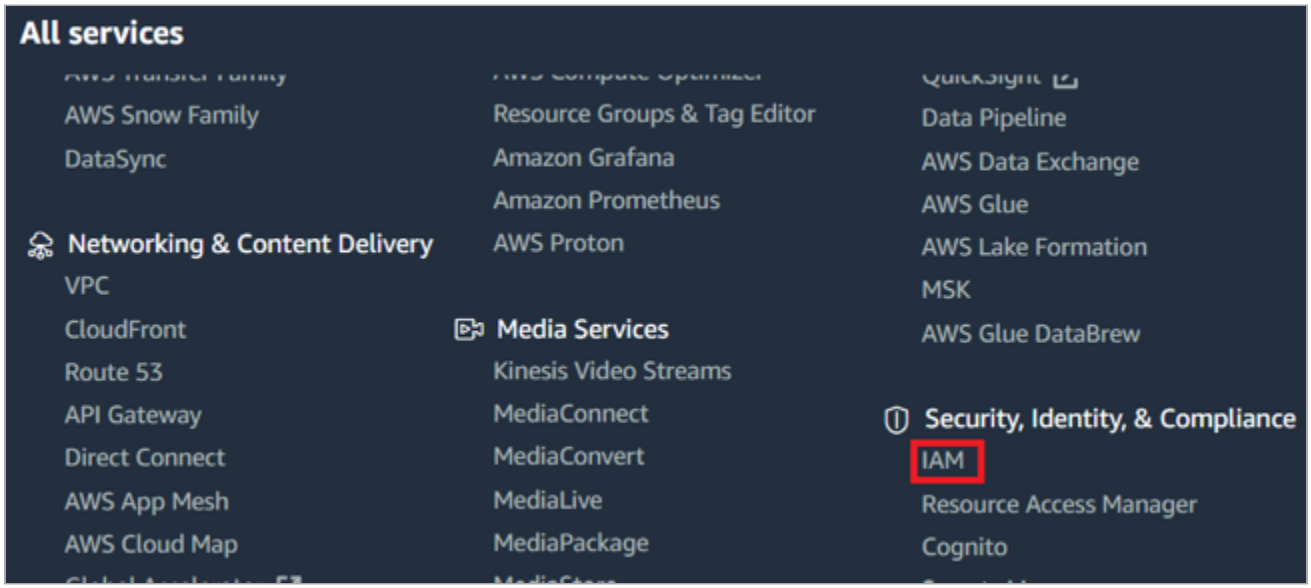
1. Sign on to the PingFederate administrative console.
2. Configure using **Browser SSO** profile **SAML 2.0**.
3. Set **Partner's Entity ID** to `urn:amazon:webservices`.
4. Enable the **IdP-Initiated SSO** SAML profile.
5. Enable the **SP Initiated SSO** SAML profile.
6. In **Assertion Creation → Attribute Contract**:
    - Extend the contract to add the attributes `SAML_NAME_FORMAT` and `https://aws.amazon.com/SAML/Attributes/Role`.
    - Set **https://aws.amazon.com/SAML/Attributes/Role** to have an **Attribute Name Format** of `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.
7. In **Assertion Creation → Authentication Source Mapping → Attribute Contract Fulfillment**:
    - Map **SAML_SUBJECT** to an attribute containing the `username` value.
    - Map **SAML_NAME_FORMAT** to a text value of `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`.
    - Map **https://aws.amazon.com/SAML/Attributes/Role** to a fixed value or your attribute holding the user's AWS role name.
    - In **Protocol Settings → Assertion Consumer Service URL**, set **Binding** to **Post** and set **Endpoint URL** to `https://signin.aws.amazon.com/saml`.
        - In **Protocol Settings → Allowable SAML Bindings**, enable **POST**.

- In **Credentials → Digital Signature Settings**, select the **PingFederate Signing Certificate**.

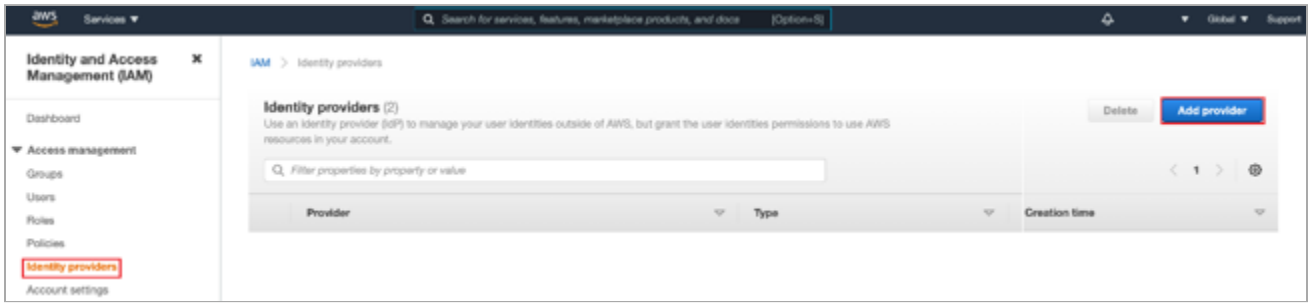
8. Save the configuration.
9. Export the signing certificate.
10. Export the metadata file, open it in a text editor, and copy the value of the **entityID** and the **Location** entry (https://*your value*/idp/SSO.saml2).

Add the PingFederate IdP connection to AWS

1. Sign on to your AWS console as an administrator.
2. In the **Security, Identity, & Compliance** section, select the **IAM** service.



3. Go to **Access Management → Identity Providers**.
4. Click **Add Provider**.

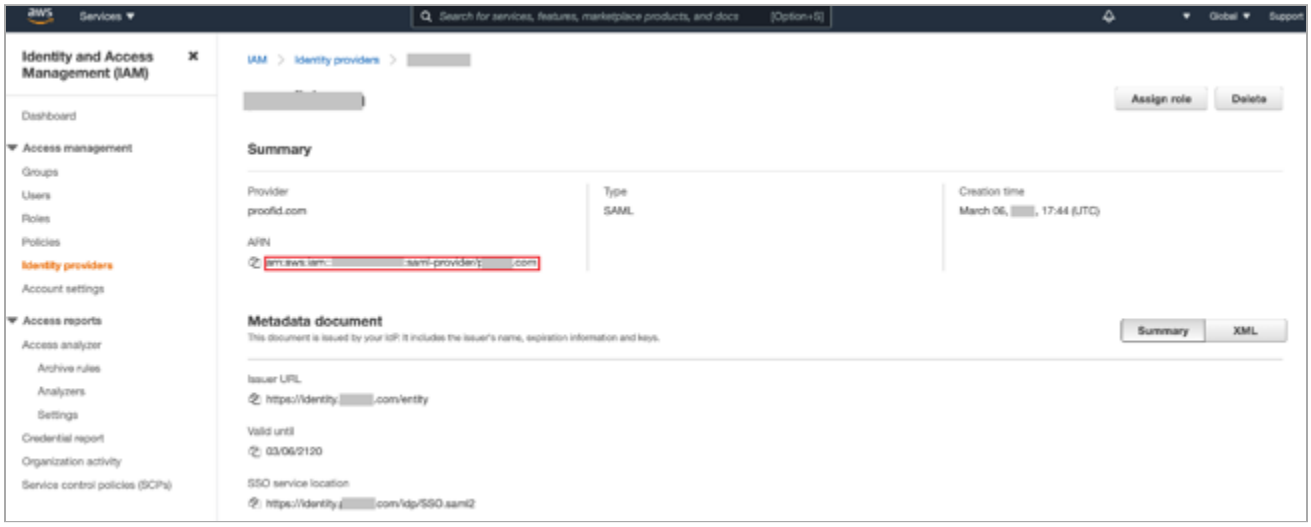


5. Set the following:

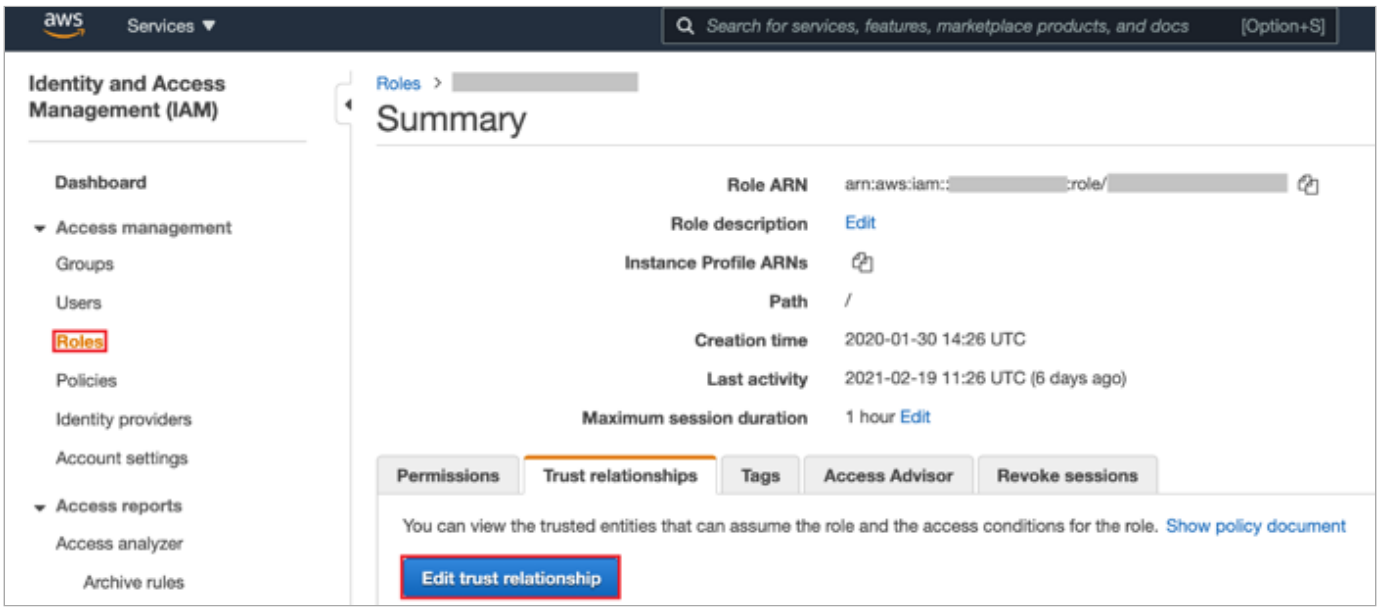
Provider Type	SAML
Provider Name	PingFederate

Metadata Document	Select the PingFederate metadata download file you downloaded previously.

6. Continue through to the final page and click **Create**.
7. Copy the **ARN** value of the provider.



8. In the side menu, select **Roles**.
9. Select the role that PingFederate SSO should have access to and then click the **Trust relationships** tab.
10. Click **Edit Trust Relationship**.

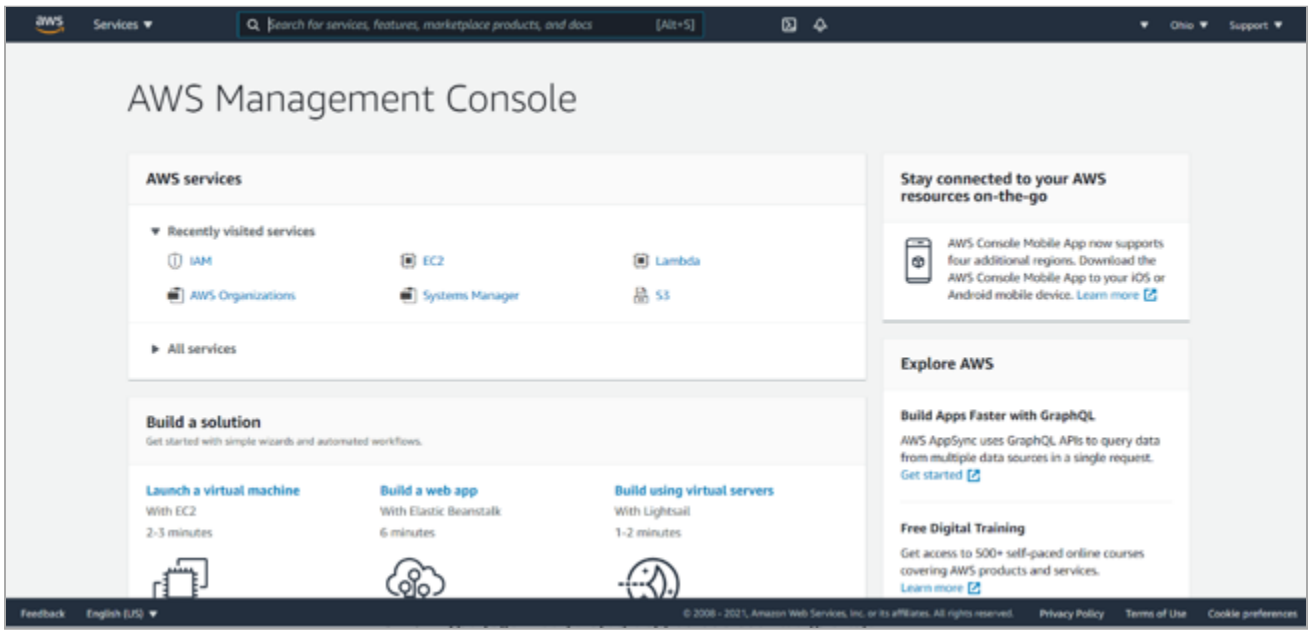


11. Add the provider ARN value you copied previously to the policy for this role.

Test the PingFederate IdP-initiated SSO integration:

1. Go to the PingFederate SSO Application Endpoint for the AWS SP connection.
2. Complete the PingFederate authentication.

   You are redirected to your AWS domain.



Configuring SAML SSO with AWS IAM and PingOne for Enterprise

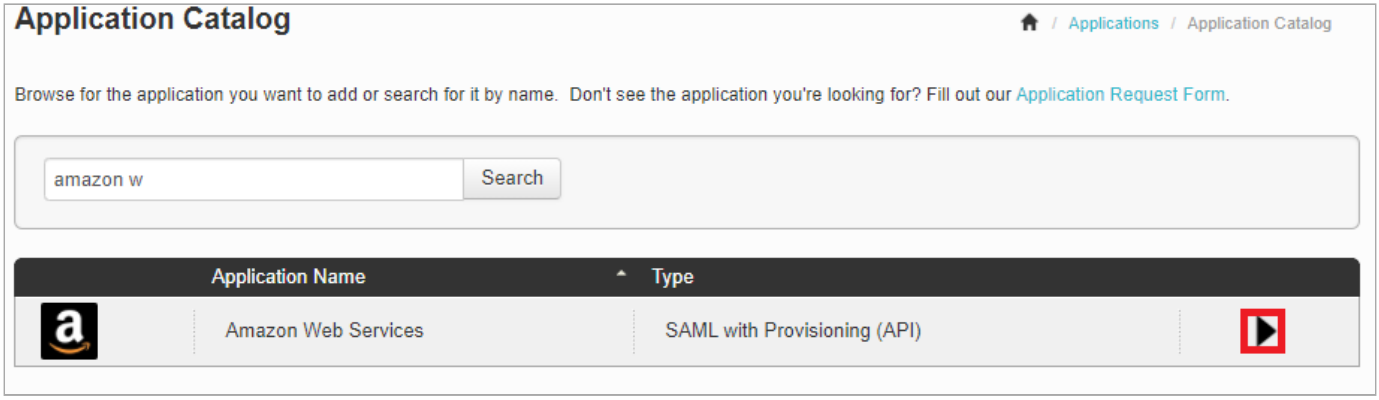
Enable AWS sign-on from the PingOne for Enterprise console (IdP-initiated sign-on).

Before you begin

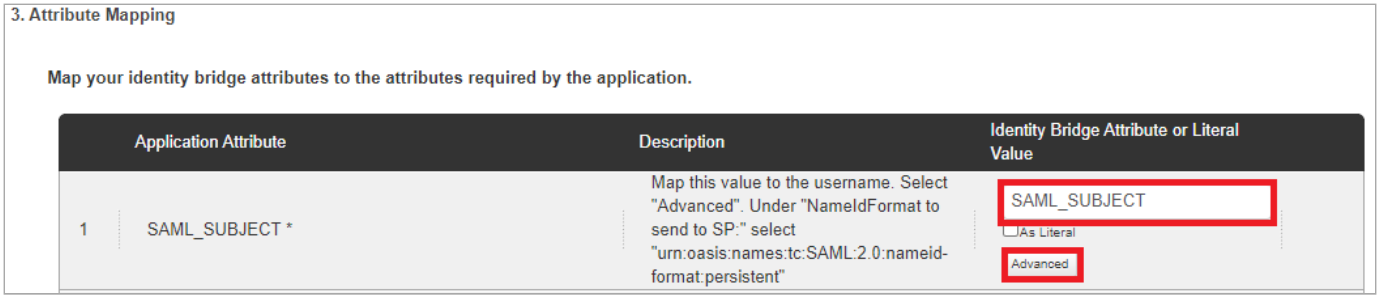
- Link PingOne for Enterprise to an identity repository containing the users that require application access.
- Populate AWS with at least one user to test application access.
- You must have administrative access to PingOne for Enterprise and AWS.

Set up the AWS Application in PingOne for Enterprise and extract the metadata

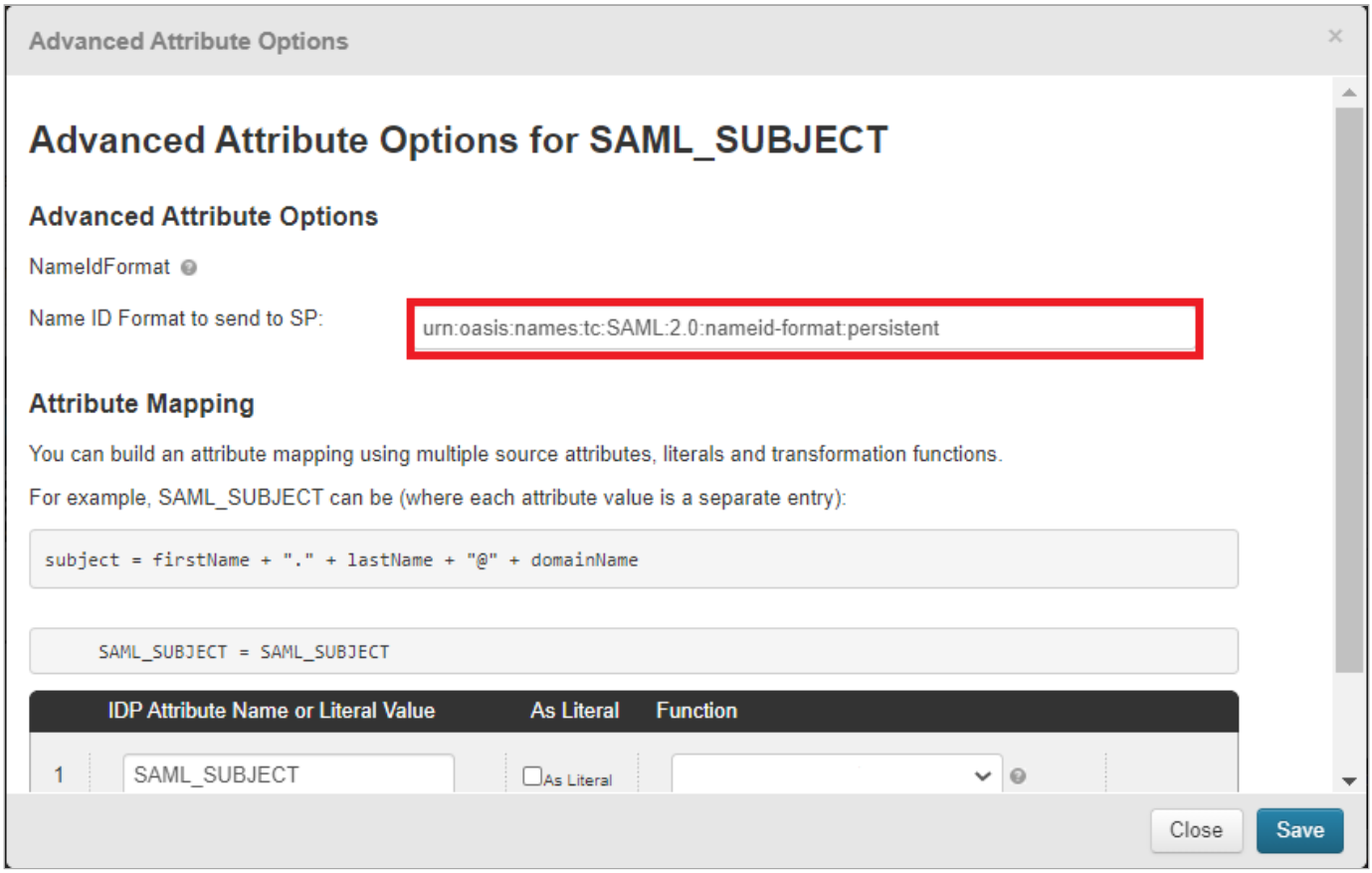
1. Sign on to PingOne for Enterprise and go to **Applications → Application Catalog**.
2. In the **Application Catalog**, search for `Amazon Web Services`.
3. Click the right arrow to expand the **Amazon Web Services** entry and then click **Setup**.



4. Click **Continue to Next Step** twice.
5. Map **SAML_SUBJECT** to the attribute containing the username value.

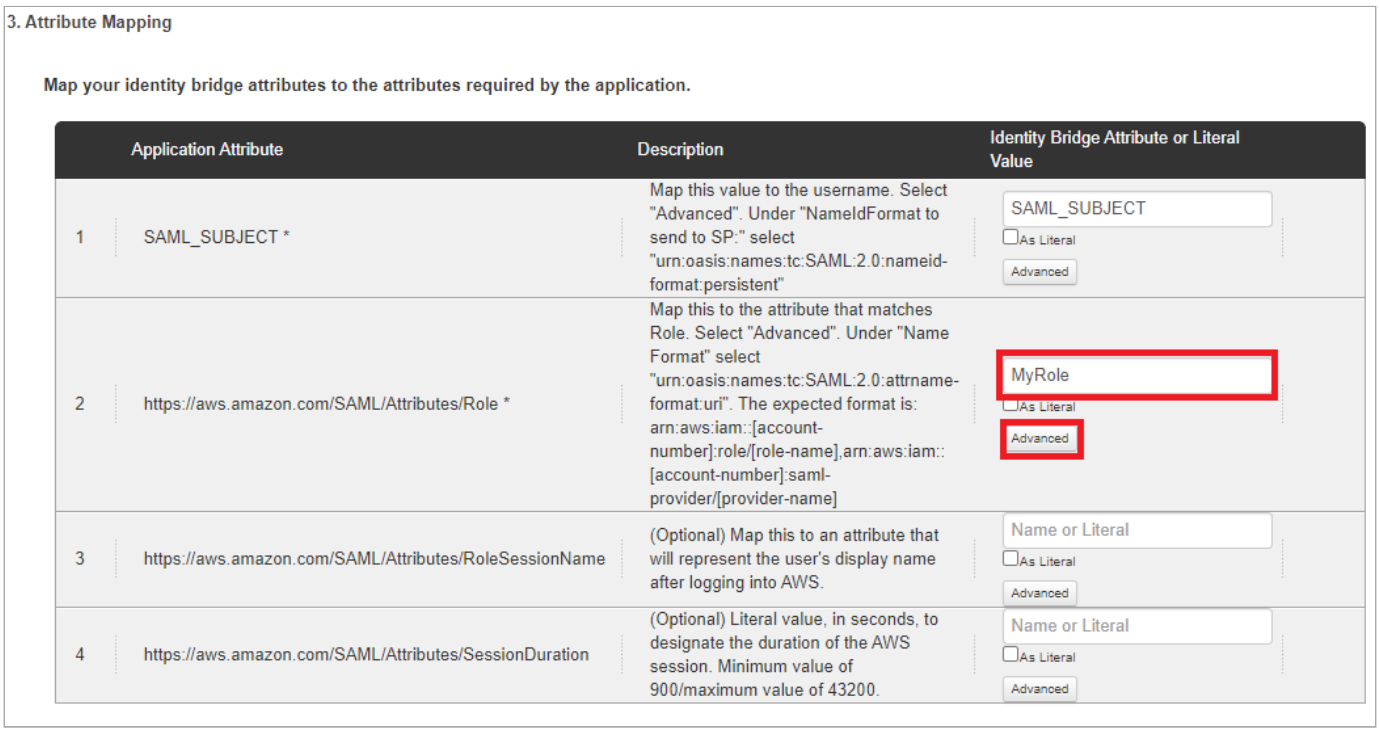


6. Click **Advanced**.
7. Set **Name ID Format to sent to SP** to `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`.

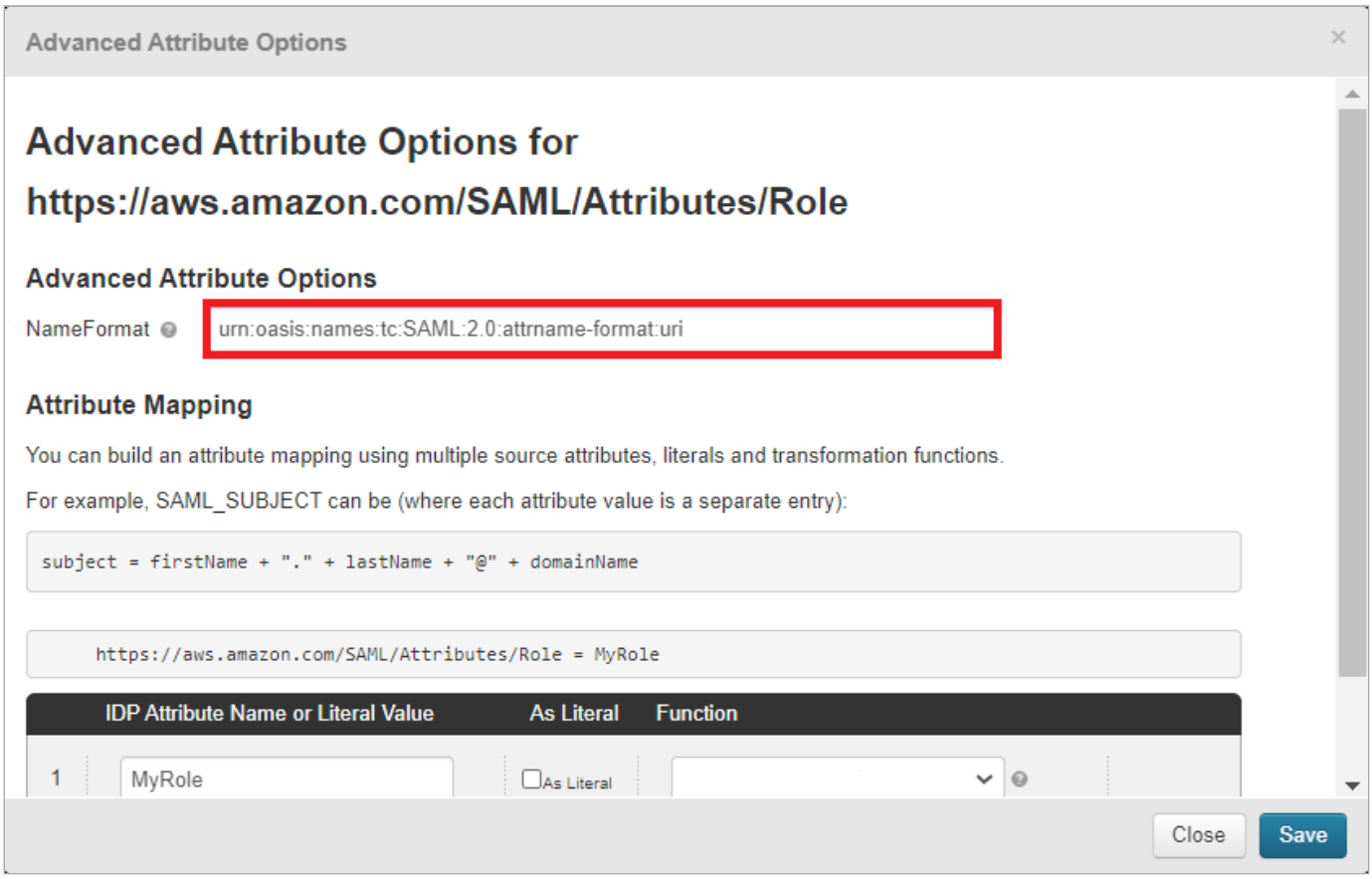


8. Click **Save**.

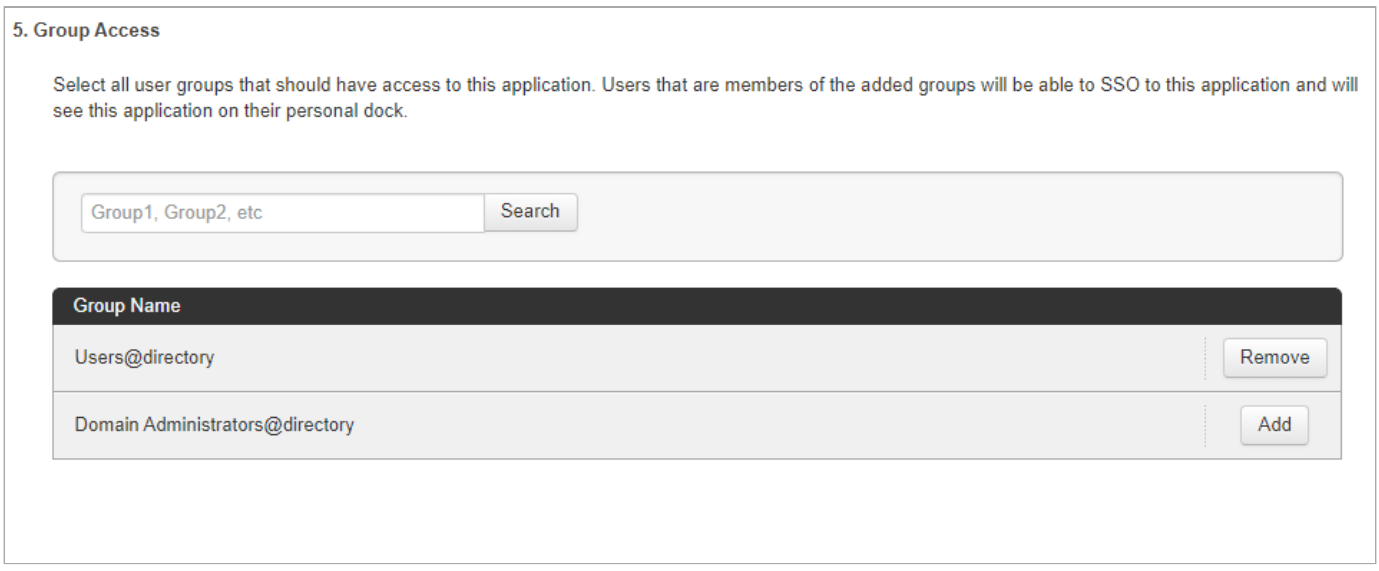
9. Map the **AWS Role** attribute to a fixed value or your attribute holding the user's AWS role name.



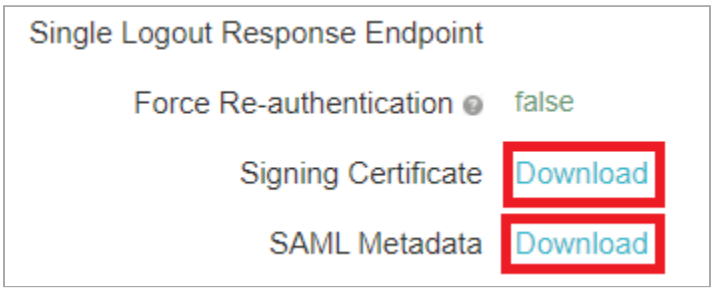
10. Click **Advanced**.
11. Set **NameFormat** to `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.



12. Click **Save**.
13. Click **Continue to Next Step** twice.
14. Click **Add** for each user group that you want to have access to AWS.



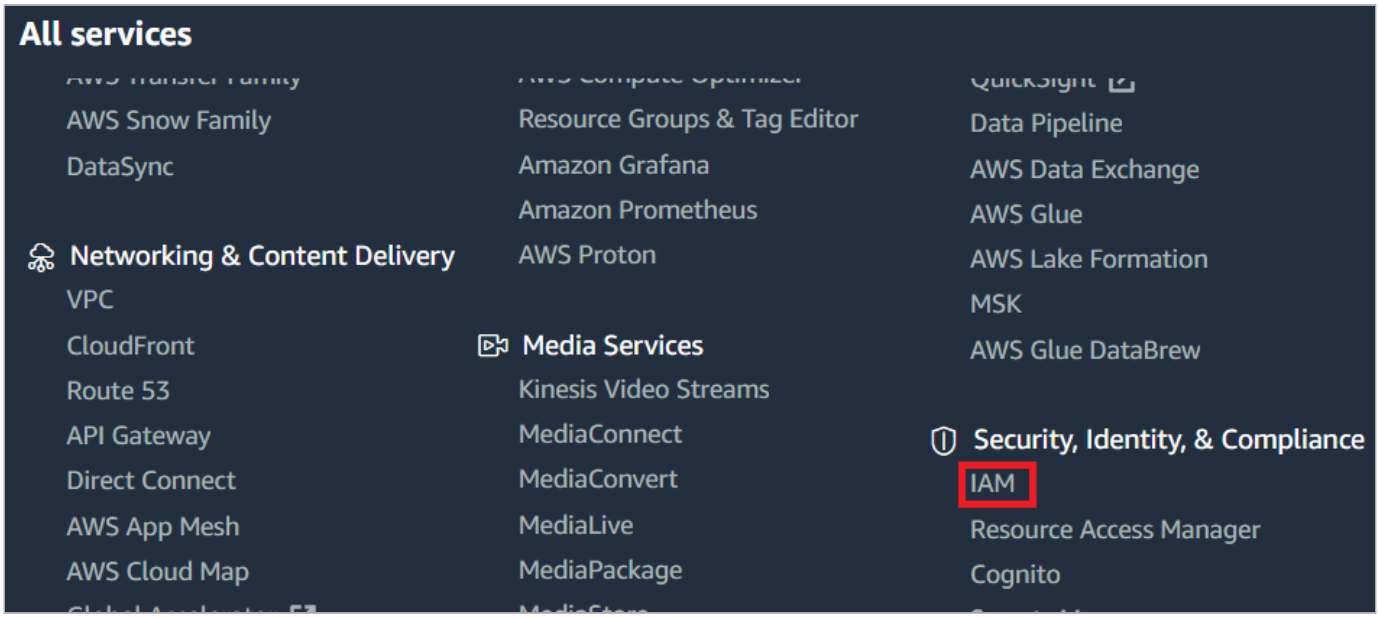
15. Download the metadata.



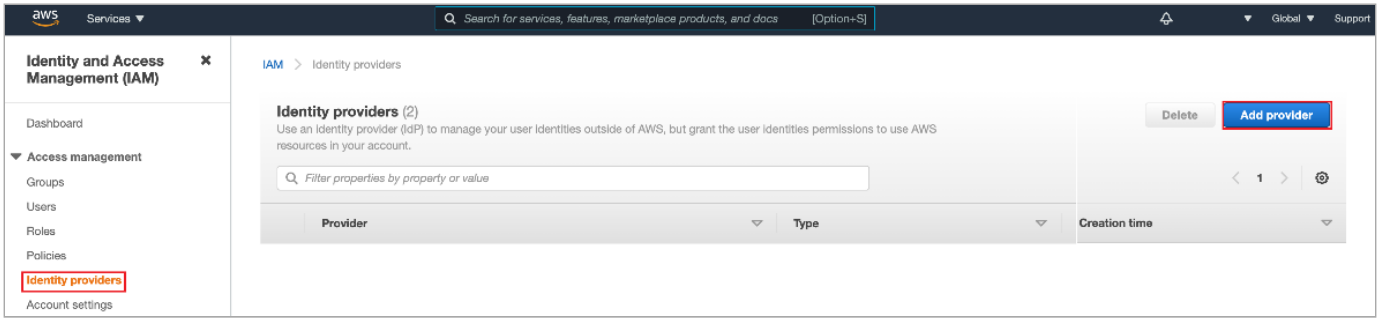
16. Click **Finish**.

Add the PingOne for Enterprise IdP connection to AWS

1. Sign on to your AWS console as an administrator.
2. Select the IAM service.



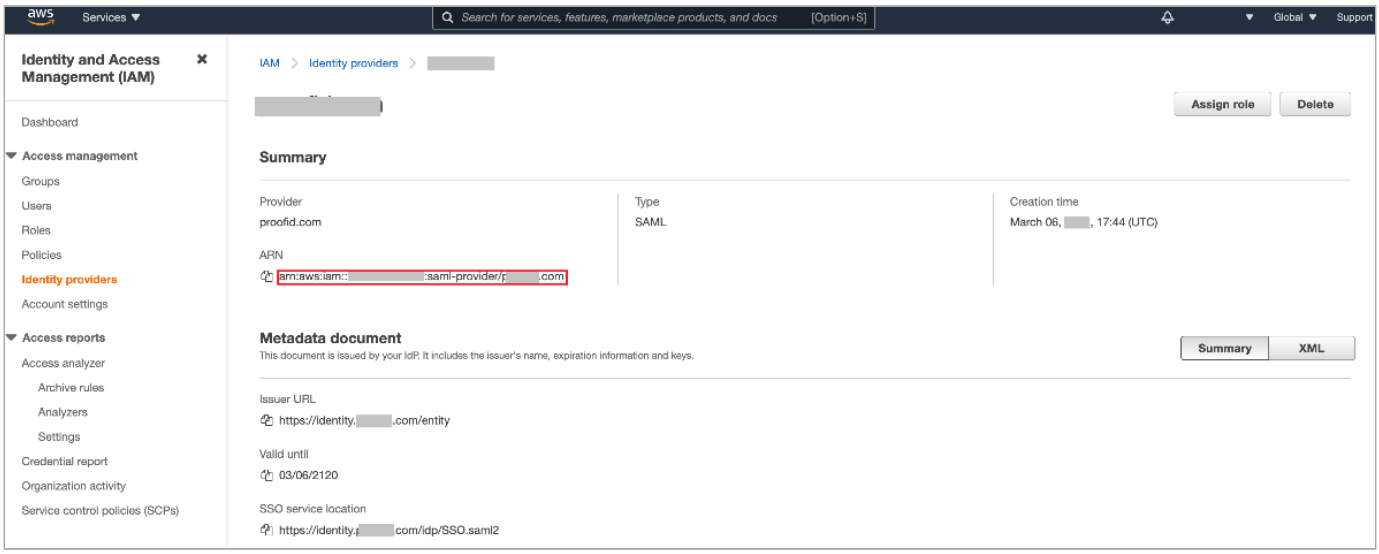
3. Go to **Access Management → Identity Providers** and click **Add Provider**.



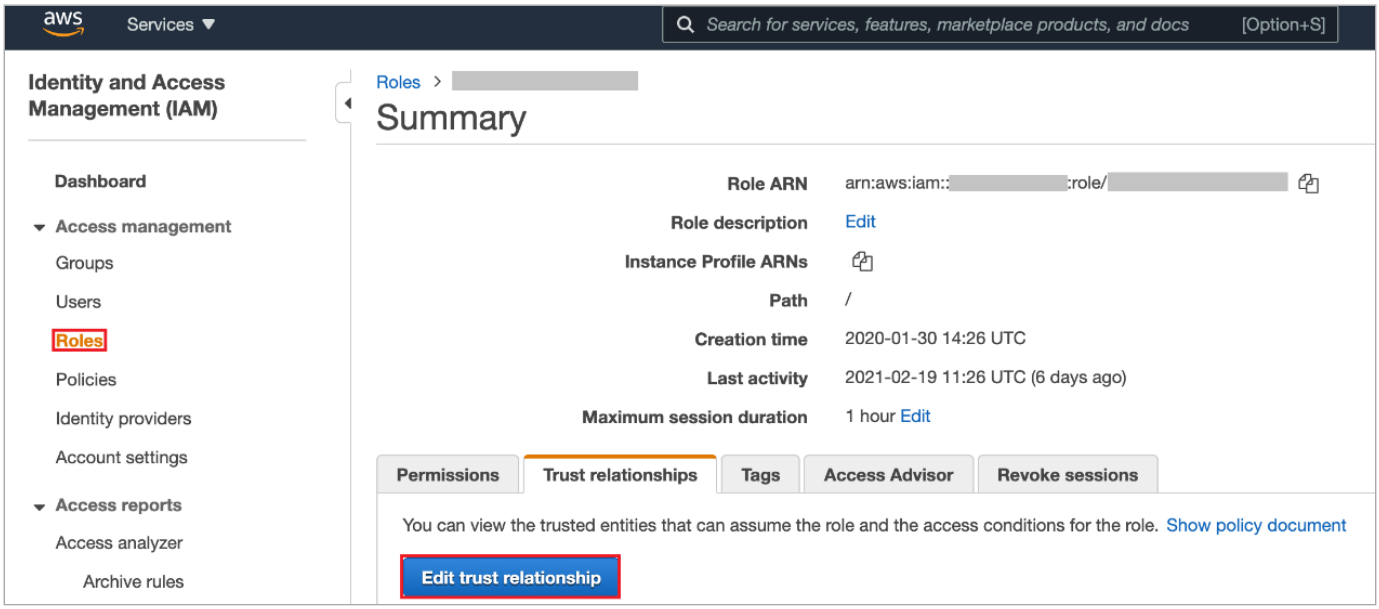
4. Set the following:
    - **Provider Type**: SAML

- **Provider Name**: PingOne for Enterprise
- **Metadata Document**: Select the PingOne for Enterprise metadata download file

5. Continue through to the final screen and click **Create**.
6. Copy the **ARN** value of the provider.



7. Select **Roles** from the side menu, and then select the role that you want PingOne for Enterprise SSO to have access to.
8. Click the **Trust Relationship** tab.
9. Click **Edit Trust Relationship**.



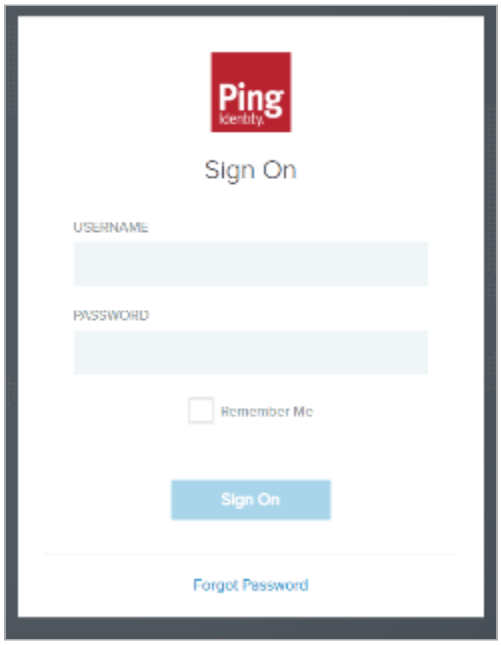
10. Add the provider ARN value that you copied previously to the policy for the role.

Test PingOne for Enterprise IdP-initiated SSO

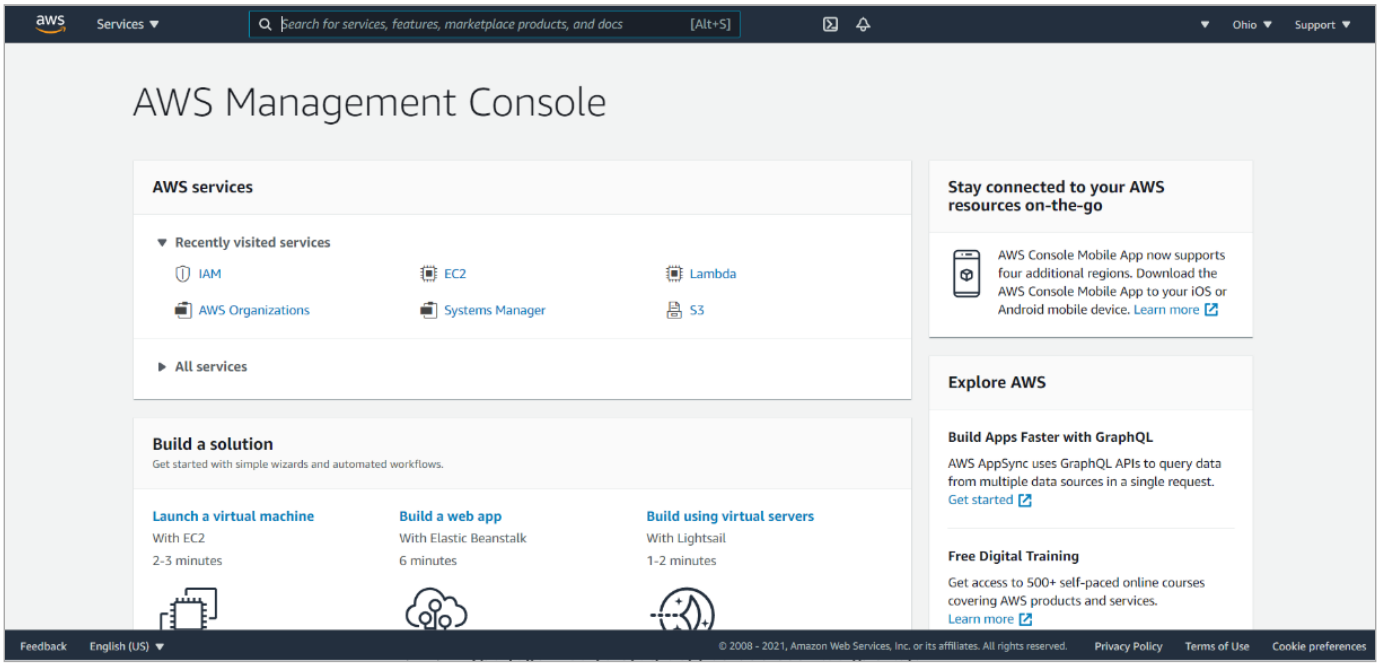
1. Go to your Ping desktop as a user with AWS access.

> **Note**
>
> You can find the Ping desktop URL in the Admin console at **Setup → Dock → PingOne Dock URL**

2. Authenticate with PingOne for Enterprise.



You're redirected to your AWS domain.



Configuring SAML SSO with Amazon Managed Grafana and PingOne

Learn how to configure SAML SSO for Amazon Managed Grafana and PingOne.

About this task

> **Note**
>
> Amazon Managed Grafana only supports SP-initiated SSO that is initiated from the Grafana Workspace URL.

Configuring an Amazon Managed Grafana connection

Steps

1. Set up the Amazon Managed Grafana application in PingOne:
    1. Go to **Applications → Application Catalog**.
    2. In the **Application Catalog**, search for `Grafana`.
    3. Expand the **Amazon Managed Grafana** entry and click **Setup**.
    4. Review the instructions to configure SAML with the Amazon Managed Grafana console.
    5. Click **Continue to Next Step**.
2. In the **ACS URL**field, replace the `${namespace}` and `${region}` variables with your Grafana namespace and your AWS region.
3. In the **Entity ID** field, replace the `${namespace}` and `${region}` variables with your Grafana namespace and your AWS region.

4. Click **Continue to Next Step**.

Mapping Amazon Managed Grafana attributes

About this task

PingOne will automatically populate required SAML attributes.

For Amazon Managed Grafana, the required attributes are:

- `SAML_SUBJECT`
- `mail`
- `givenName`

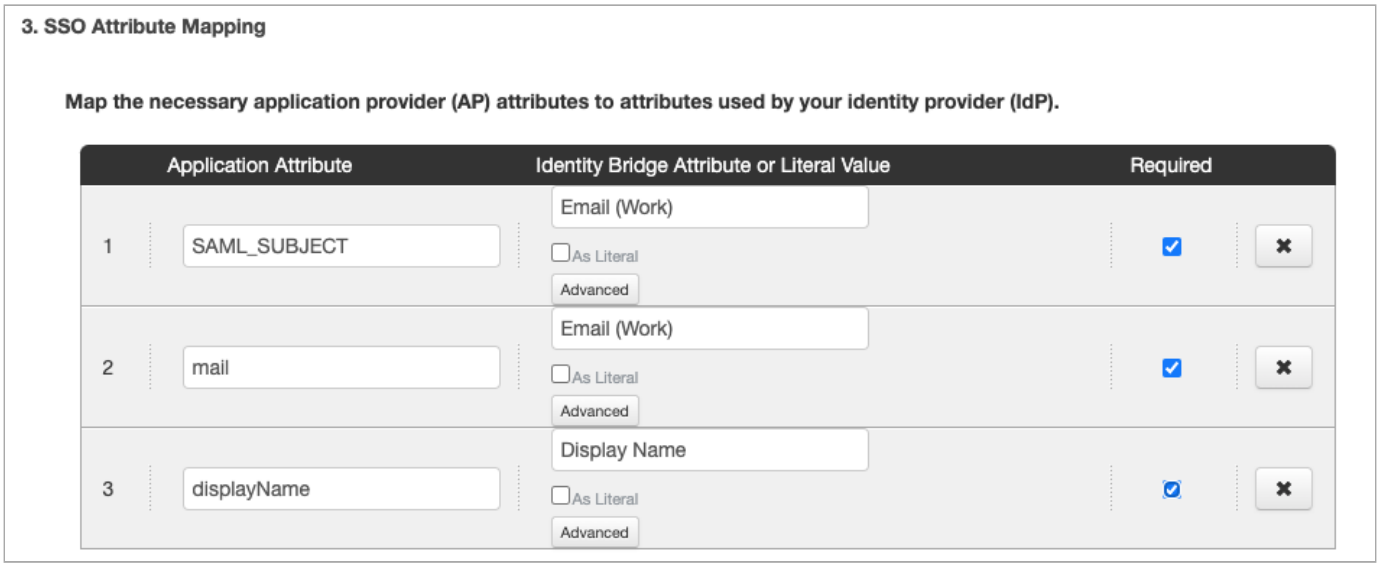
> **Note**
>
> You must set `SAML_SUBJECT` to Name ID format: `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`

Steps

1. In the **Application Attribute** field, enter the attribute name as it appears in the application.
2. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following.

   Choose from:

   - Enter or select a directory attribute to map to the application attribute.
   - Select **As Literal**, then enter a literal value to assign to the application attribute.
3. **Optional:** To create advanced attribute mappings, click **Advanced**.



4. Click **Continue to Next Step**.

Customizing Amazon Managed Grafana boxes

Steps

1. To change the application icon, click **Select Image** and upload a local image file.

   The image file must be:

   - PNG, GIF, or JPG format
   - 312 x 52 pixels maximum
   - 2 MB maximum file size

   > **Note**
   >
   > Images are scaled to 64 X 64 pixels for display.

2. To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
3. To change the description of the application, in the **Description** field, enter the new description.
4. To change the category the application is assigned on the dock, in the **Category** list, select a category.
5. Click **Continue to Next Step**.

Assigning Amazon Managed Grafana group access

About this task

The **Group Access** tab shows every user group that you've created.

Steps

1. To add a group's access to Amazon Managed Grafana, on the row for that group, click **Add**.
2. To remove a group's access, on the row for that group, click **Remove**.
3. After you finish assigning groups, click **Continue to Next Step**.

Configuring Amazon Managed Grafana SAML

Steps

1. In PingOne, on the **Review Setup** tab, either:

   Choose from:

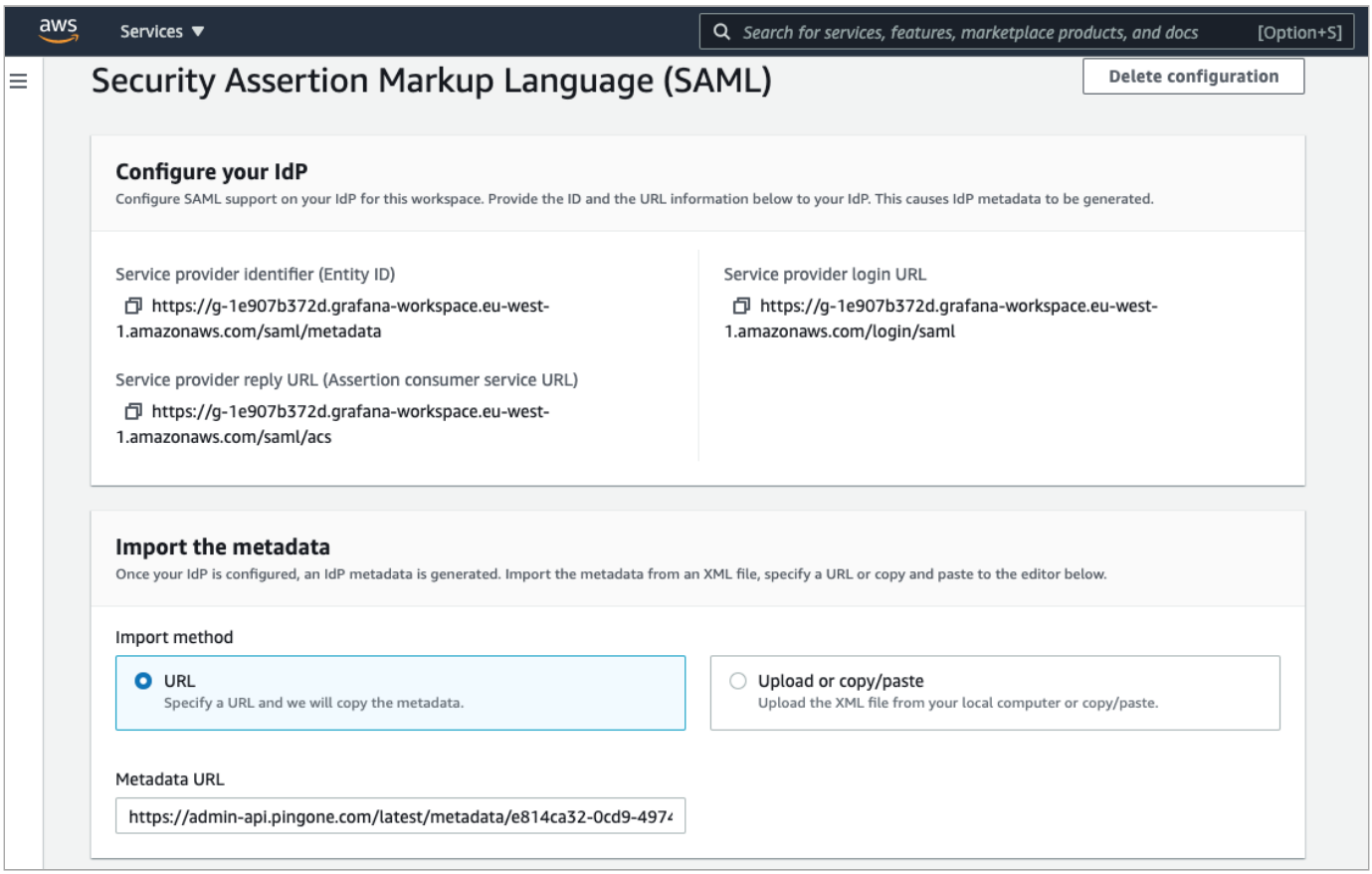
   - Click **Download** to download the SAML metadata file
   - Copy the PingOne SAML Metadata URL.

2. Click **Finish** to add Amazon Managed Grafana to your PingOne dock.
3. In the AWS Console, go to the Amazon Managed Grafana console.

4. To import the SAML metadata into Amazon Managed Grafana, either:

   Choose from:

   - Use the PingOne **SAML Metadata URL** on the Amazon Managed Grafana connection summary page in PingOne.
   - Upload the SAML metadata file.

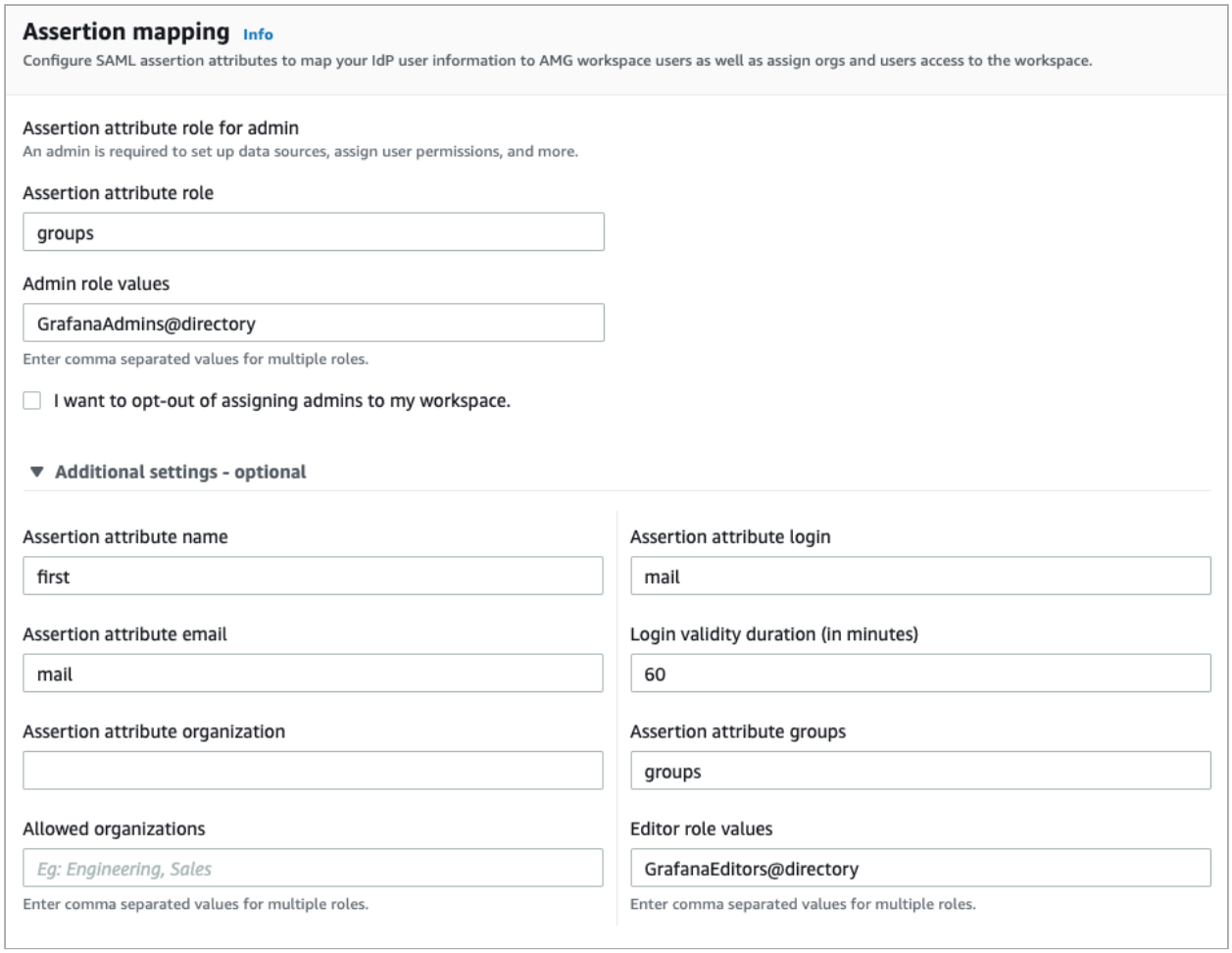


Assigning Amazon Managed Grafana administrators

About this task

During authentication to Amazon Managed Grafana, you can optionally assign the Grafana Admin role to users by defining an admin role attribute and populating a PingOne SAML assertion attribute with the expected agreed-upon value.

For the example configuration, in PingOne, the **memberOf** attribute is mapped to the SAML assertion **groups** attribute. In Amazon Managed Grafana, the SAML assertion **groups** attribute is mapped to the Grafana admin role value, as shown in the following image.

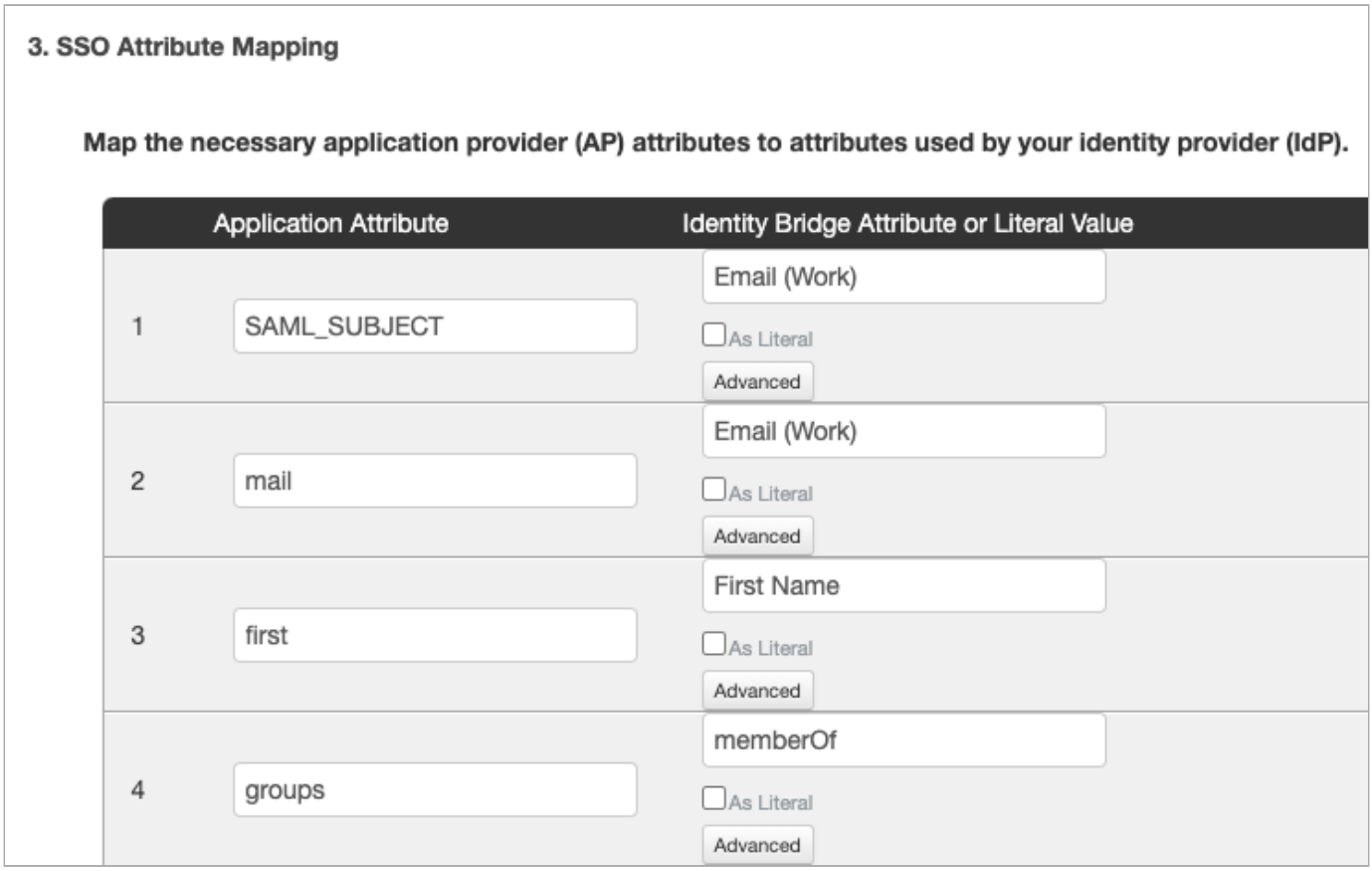


Steps

1. In your Amazon Managed Grafana workspace, go to **SAML Configuration**.
2. In the **Assertion mapping** section, in the **Assertion attribute role** field, enter `groups`.
3. Set the **Admin role values**to the PingOne group for Grafana admins.

> **Note**
>
> The example in step 7 uses GrafanaAdmins@directory. The @directory is appended to any PingOne group name.

4. **Optional:** Set the **Assertion attribute groups**to the **groups** and **Editor role values**to the PingOne group for Grafana editors.
5. Click **Save SAML configuration**.
6. In PingOne, go to **Amazon Managed Grafana application Attribute Mapping**.
7. Map PingOne's **memberOf** attribute to the SAML assertion **groups** attribute.



Result:

Users in the PingOne **GrafanaAdmins** group are Just-In-Time provisioned during authentication as Grafana admins, and users in the PingOne **GrafanaEditors**group are Just-In-Time provisioned during authentication as Grafana editors.

Configuring SAML SSO with AWS Client VPN and PingOne

Learn to configure SAML single sign-on (SSO) using AWS Client VPN and PingOne.

Before you begin

Make sure you have:

- An Amazon Web Services (AWS) account
- An Amazon VPC with an EC2 instance

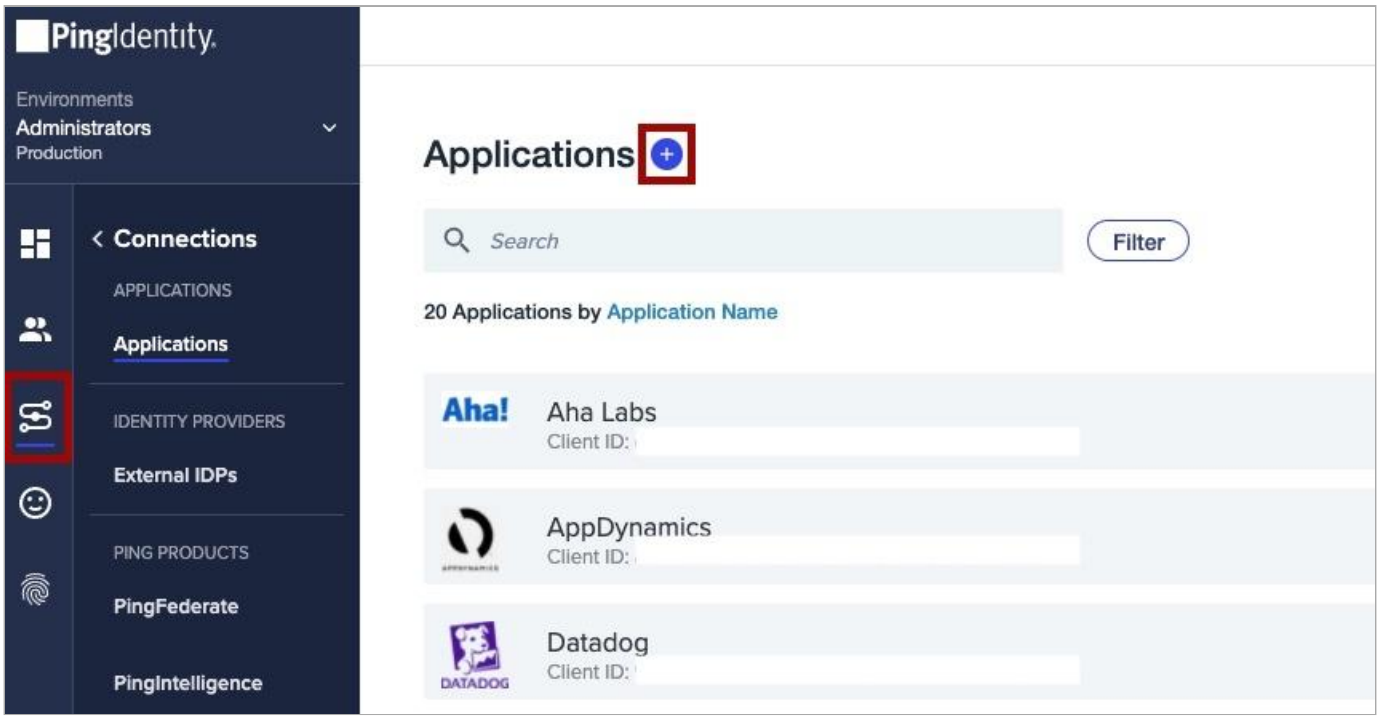
> **Important**
>
> In the instance **Security Group**, allow ICMP traffic from the VPC CIDR range. You need this for testing.

- A private certificate imported into AWS Certificate Manager (ACM)
- PingOne user and group information
- A desktop (Windows or macOS) running the latest AWS Client VPN software

> **Note**
>
> You can download the software here.

Create the AWS Client VPN application in PingOne

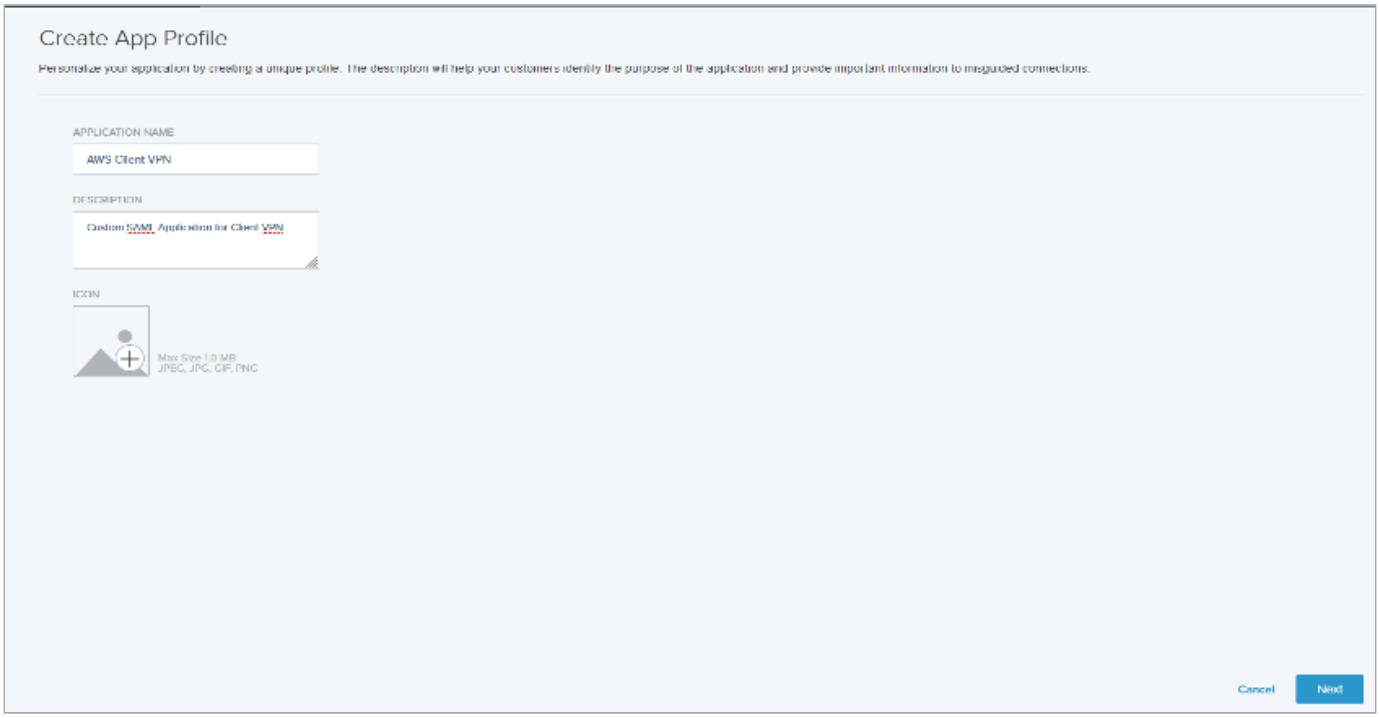
1. In the PingOne admin portal, go to **Connections → Add Application**.



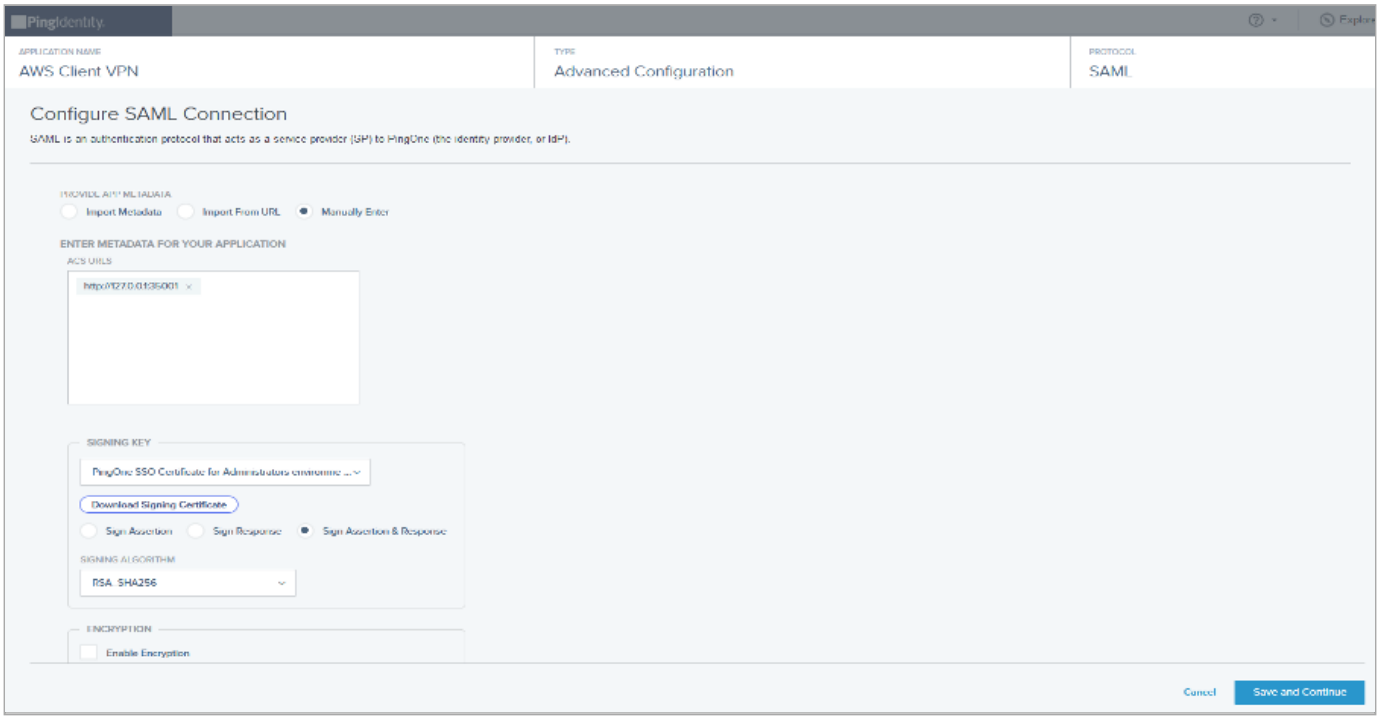
2. Click **Advanced Configuration**.

3. In the **Choose Connection Type** menu, next to **SAML**, click **Configure**.

4. On the **Create App Profile** page, enter an **Application Name**, **Description**, and **Icon** for your application. Click **Next**.



5. For **Configure SAML Connection**, select **Manually Enter** and configure the following:
    - For **ACS URLs**, enter `http://127.0.0.1:35001`.
    - Select **Sign Assertion & Response**.
    - Select **RSA_SHA256** as the algorithm for **Signing the response**.
    - For **Entity ID**, enter `urn:amazon:webservices:clientvpn`.
    - For **Subject nameID format**, enter `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`.
    - For **Assertion Validity Duraction (in seconds)**, enter `300`.
    - For **SLO** options, leave the default settings.
6. After configuring the above values, leave the default settings and click **Save and Continue**.



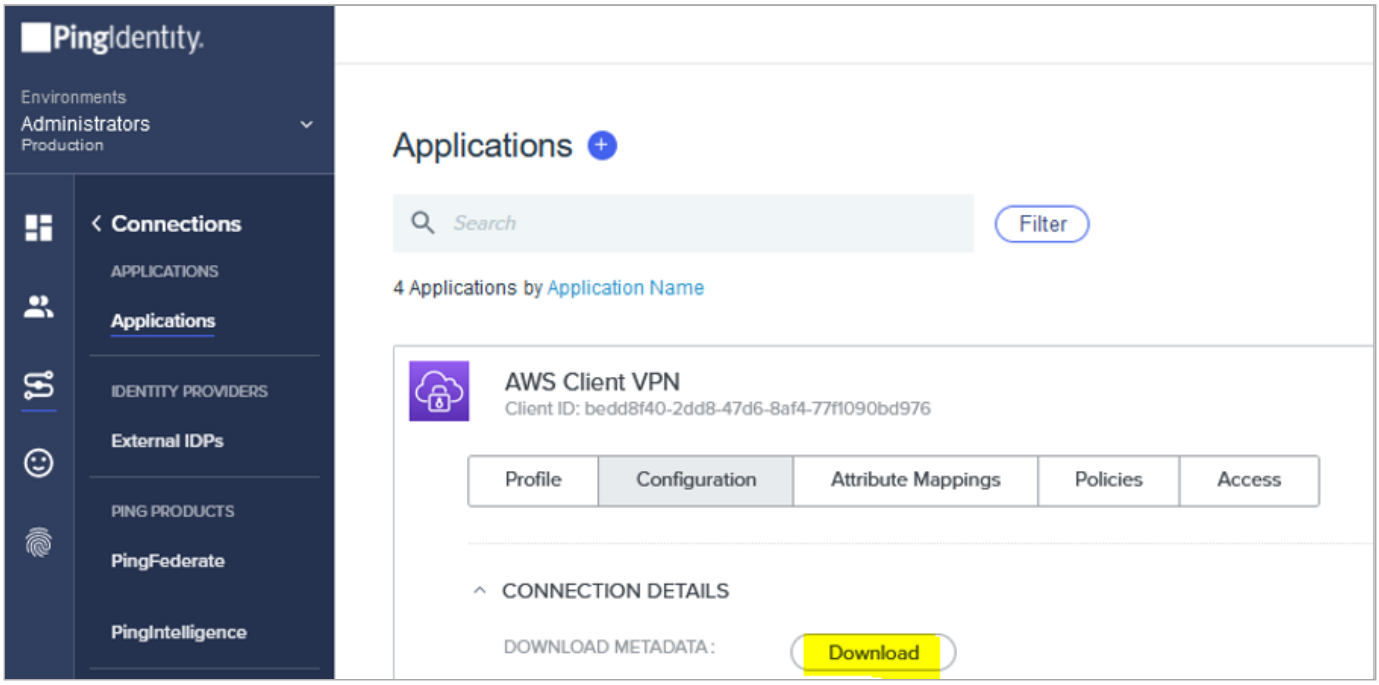
7. Configure **Attribute Mapping** by adding the following **PingOne Attributes**:

PingOne User Attribute	Application Attribute
Username	`saml_subject`
Given Name	`FirstName`
Family Name	`LastName`
Group Names	`memberOf`

Result:

The new application is shown in the **Applications** list.

8. Expand the application details and on the **Policies** tab, click the **Pencil** icon to edit the **Authentication Policy**.
9. Expand the application details and on the **Configuration** tab, download the metadata file.

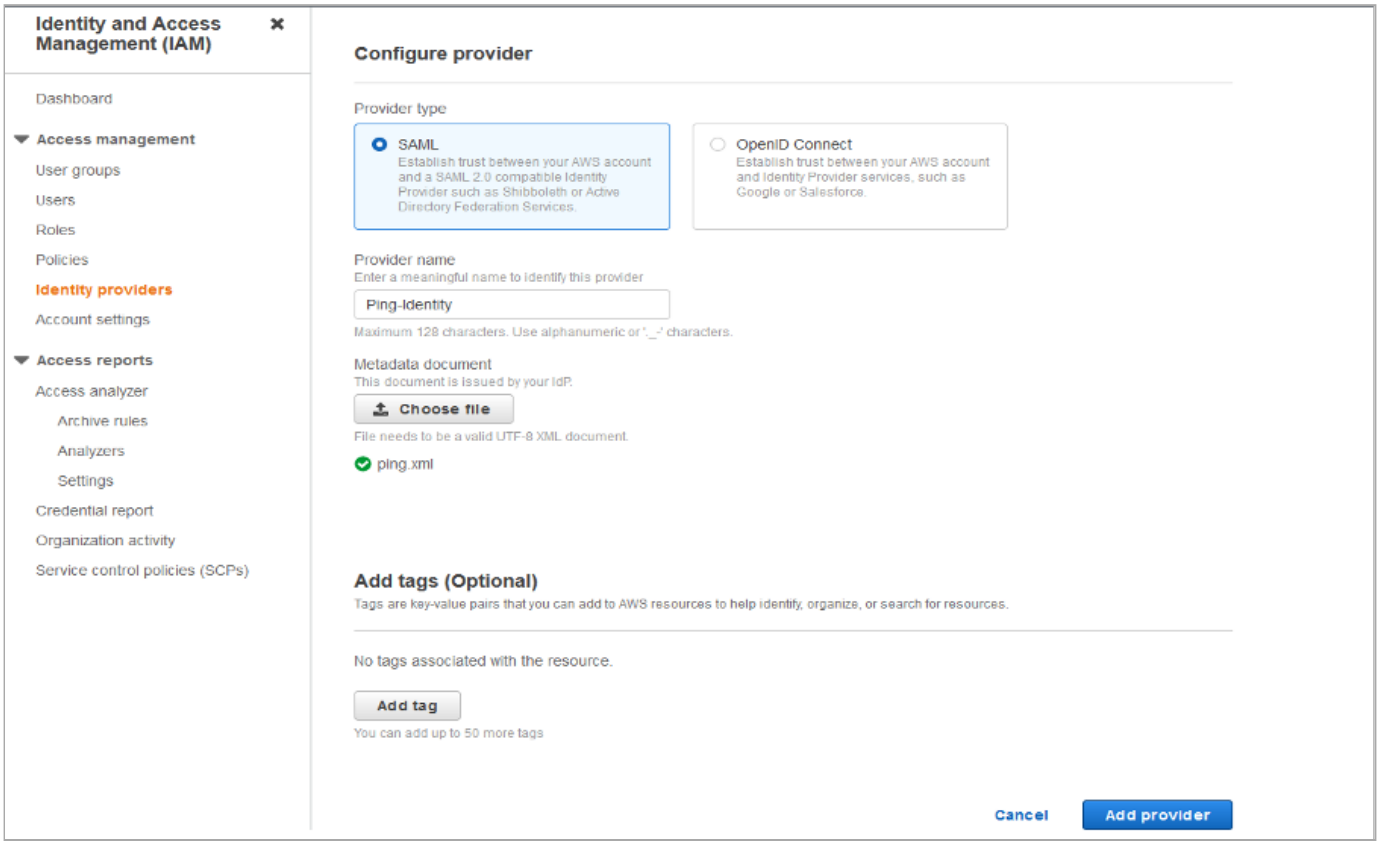


> **Note**
>
> You'll upload this metadata file in the next step.

Add PingOne as your IdP in the AWS Management Console

> **Important**
>
> AWS Client VPN is a separate app and requires a unique IdP definition in AWS. You cannot reuse an IdP already defined for another app, even if it's from the same vendor.

1. In the AWS Management Console, open the **IAM** console and in the **Access management** section, click **Identity providers**.
2. Click **Add Provider**.
3. For **Provider type**, select **SAML**.
4. For **Provider name**, enter a unique name.
5. For **Metadata document**, click **Choose file** and upload the metadata file that you downloaded from PingOne.

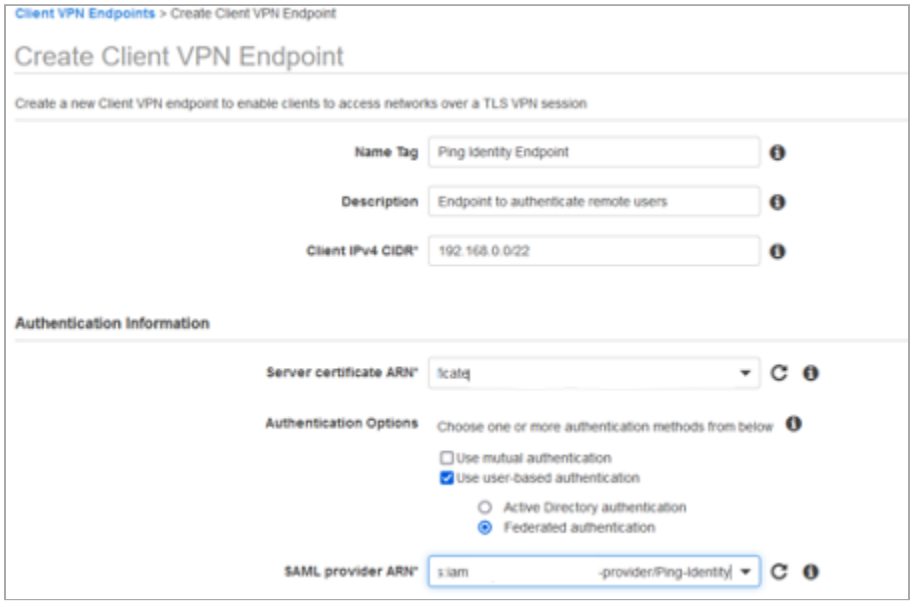


Create an AWS Client VPN endpoint

1. In the **Amazon VPC** console, in the **Virtual Private Network (VPN)** section, click **Client VPN Endpoints**.
2. Click **Create Client VPN Endpoint**.
3. Enter your desired **Name Tag** and **Description**.
4. For **Client IPv4 CIDR**, enter `your-IP-range/22`.

> **Note**
>
> This is the IP range that will be allocated to your remote users.

5. For **Server certificate ARN**, select the certificate you created as a prerequisite.
6. For **Authentication Options**, select **Use user-based authentication** and **Federated authentication**.
7. In the **SAML provider ARN** list, select the PingOne IdP you configured earlier.



8. In the **Other optional parameters** section, select **Enable split-tunnel** and leave the rest of the default values.

> **Note**
>
> Enabling split-tunnel makes sure that only traffic to the VPC IP range is forwarded via the VPN.

9. Configure the other options according to your environment requirements.
10. Click **Create Client VPN Endpoint** to complete the setup.

Configure the AWS Client VPN Endpoint association

1. In the **Amazon VPC** console, in the **Virtual Private Network (VPN)** section, click **Client VPN Endpoints**.
2. Select the VPN you created in the last step.

   It should be in the **Pending** state.
3. Go to **Options → Associations** and click **Associate**.
4. In the **Associations** list, select the target VPC and subnet with which you want to associate your endpoint.
5. **Optional:** Repeat the previous steps to associate your Client VPN endpoint to another subnet for high availability.

Set up SAML group-specific authorization

1. In the **Amazon VPC** console, in the **Virtual Private Network (VPN)** section, click **Authorization**.
2. Click **Authorize Ingress**.
3. For **Destination network to enable**, specify the IP address of your EC2 instance that you created as a prerequisite.
4. In the **Grant access to** section, select **Allow access to users in a specific access group**.
5. In the **Access group ID** field, enter the name of the group that you want to allow access to the EC2 instance.

6. Provide an optional description and click **Add authorization rule**.

Connect to the Client VPN

1. In the **Amazon VPC** console, in the **Virtual Private Network (VPN)** section, click **Client VPN Endpoints**.
2. Select the VPN that you created.

   It should be in the **Available** state.
3. To download the configuration profile to your desktop, click **Download Client Configuration**.
4. Open the **AWS Client VPN** desktop application.
5. Go to **File → Manage Profiles**.
6. Click **Add Profile**, choose the configuration profile that you downloaded, and give it a **Display Name** of your choice.

   Your profile appears in the AWS Client VPN profile list.
7. Select your profile and click **Connect**.

   You're redirected to PingOne for authentication.
8. Sign on to PingOne as a user with access to your EC2 instance.

   After successful authentication, you should be able to reach the EC2 instance in the target VPC.

Test your connection

1. To test your connection, send an ICMP ping to the IP of the instance from your command line terminal.
2. In your browser, use a plugin, such as SAML-tracer, to confirm that the IdP is sending the correct details in the SAML assertion.

Asana

Configuring SAML SSO with Asana and PingOne

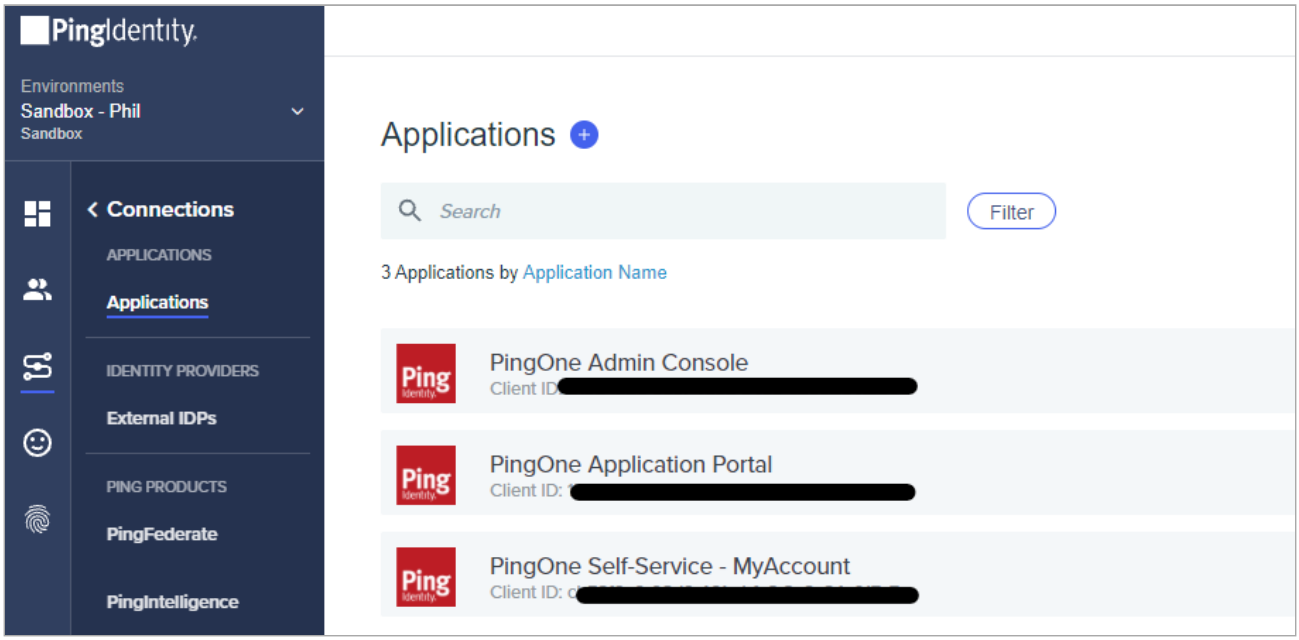
Learn how to enable Asana sign-on from the PingOne console (IdP-initiated sign-on) and direct Asana sign-on using PingOne (SP-initiated sign-on).

Before you begin

- Link PingOne to an identity repository containing the users requiring application access.
- Populate Asana with at least one user to test access.
- You must have administrative access to PingOne and a Super Admin account for an Enterprise Organization on Asana.

Steps

1. Add the Asana application to PingOne:
    1. Sign on to PingOne and go to **Connections → Applications**.
    2. To add a new application, click the + icon next to the **Applications** heading.



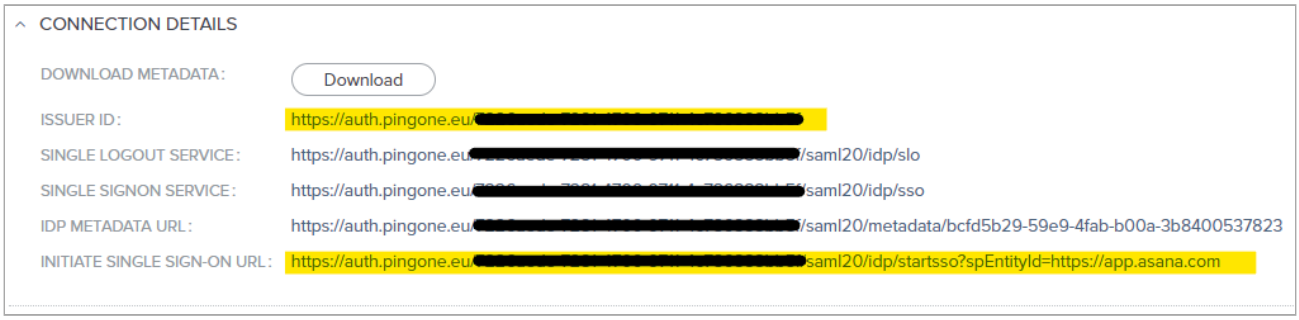
    3. When prompted to select an application type, select **WEB APP**, then click **Configure** next to **SAML** for the chosen connection type.
    4. Enter `Asana` as the application name.
    5. Enter a suitable description.

6. Upload an icon if desired.
7. Click **Next**.
8. For **Provide App Metadata**, select **Manually Enter**.
9. In the **ACS URLS** field, enter `https://app/asana.com/-/saml/consume`.
10. Select the **Signing Key** to use and then click **Download Signing Certificate** to download the certificate as X509 PEM (`.crt`).
11. In the **Entity ID** field, enter `https://app.asana.com`.
12. Leave **SLO Endpoint** and **SLO Response Endpoint** blank. Asana does not support single logout (SLO).
13. Enter a suitable value for **Assertion Validity Duration (in seconds)**. A value of 300 seconds is typical.
14. Click **Save and Continue**.
15. Because Asana expects an email address to identify a user in the SSO security assertion:

    Choose from:

    - If you use email address to sign on through PingOne, click **Save and Close**.
    - If you sign on with a username, select **Email Address** in the **PingOne User Attribute** list to map that to the **SAML_SUBJECT**, then click **Save and Close**.
16. Enable user access to this new application by moving the toggle to the right.
17. On the **Configuration** tab of the newly-created Asana application, copy and save the **Issuer ID** and **Initiate Single Sign-On URL**.

    You will need these when configuring SAML on Asana.



2. Add PingOne as an identity provider (IdP) to Asana:
    1. Sign on to Asana with a Super Admin account for your Enterprise Organization.
    2. Click your profile photo and select **Admin Console** in the menu.
    3. Go to the **Security** tab.
    4. Go to the **SAML authentication** tab.
    5. In **SAML options**, click **Optional**.

> **Note**
>
> This is the recommended value when testing. You can change it later to **Required for all members, except guest accounts**.

6. Paste the **Initiate Single Sign-On URL** value that you saved earlier into the **Sign-in page URL** field.
7. Open the `.crt` file that you downloaded in a text editor and copy and paste the entire contents into the **X.509 certificate** field.
8. Click **Save configuration**.

3. Test the PingOne IdP integration:
    1. Go to your PingOne Application Portal and sign on with a user account.

    > **Note**
    >
    > You can find the PingOne Application Portal URL in the admin console at **Dashboard → Environment Properties**.

    2. Click the **Asana** icon.

    Result:

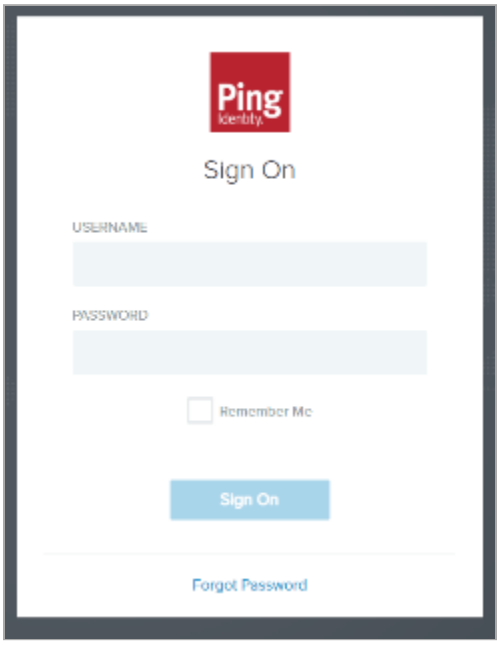
    You're redirected to the Asana website and signed on with SSO.

4. Test the PingOne service provider (SP) integration:
    1. Go to https://app.asana.com/, choose the option to sign on with SSO, and enter your email address only.

    Result:

    You're redirected and presented with a PingOne sign on prompt.

    2. Enter your PingOne username and password.



Result:

After successful authentication, you're redirected back to Asana and signed on.

BambooHR

Configuring SAML SSO with BambooHR and PingFederate

About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

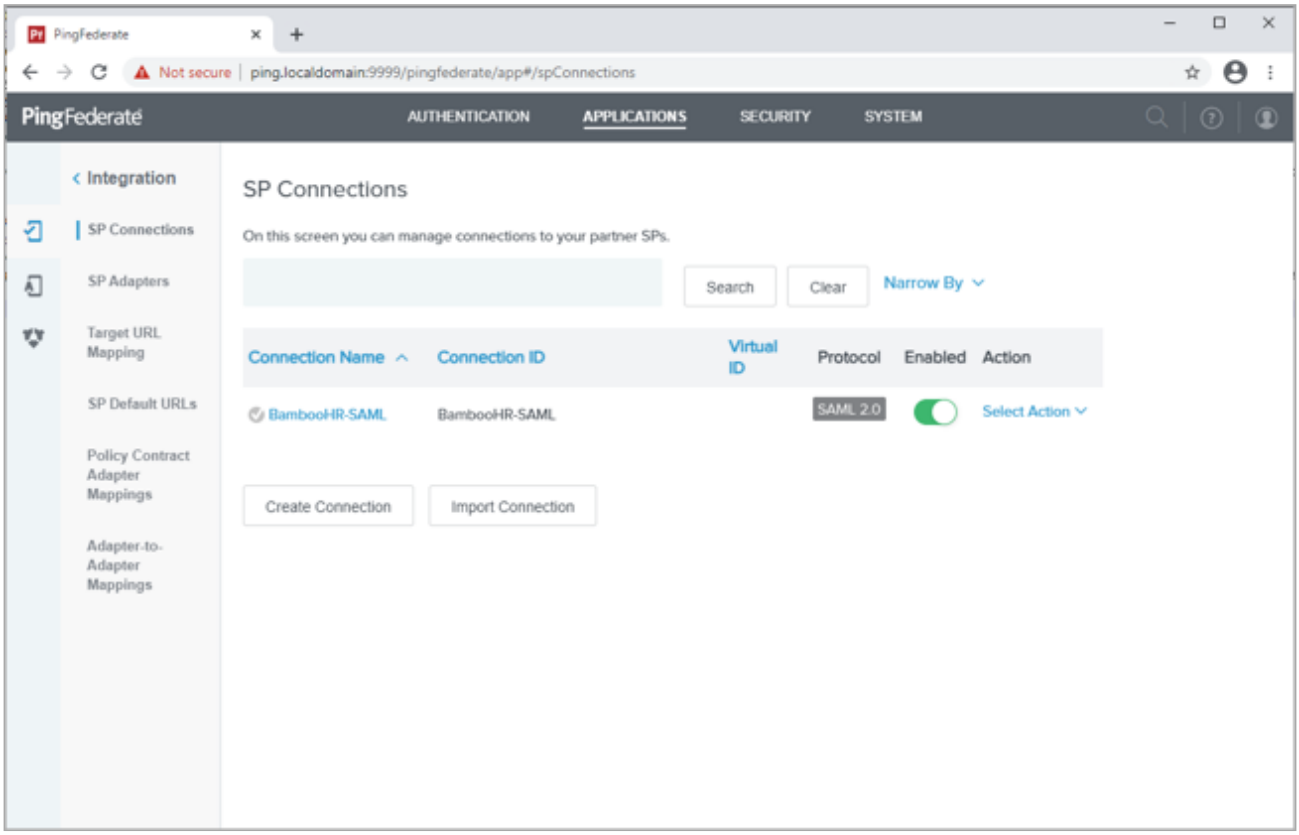
Attribute Name	Description	Required / Optional
`urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`	Email address for user	Required

The following table details the references that are used within this guide which are environment specific. Replace these with the suitable value for your environment.

Reference	Description
tenant	BambooHR Tenant name

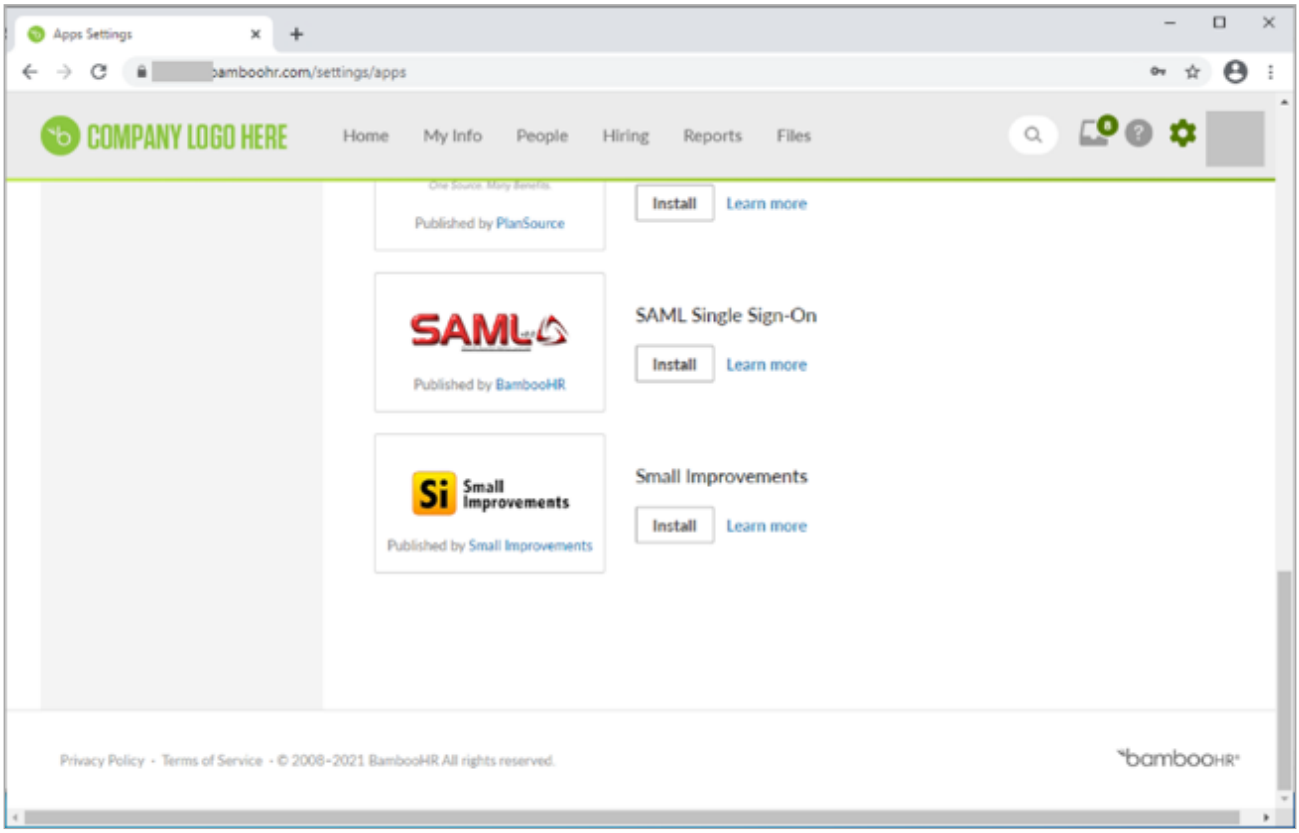
Steps

1. Create the PingFederate service provider (SP) connection for BambooHR.
    1. Sign on to the PingFederate administrative console.
    2. Using the metadata from `https://tenant.bamboohr.com/saml/sp_metadata.php`, create an SP connection in PingFederate:
        - Configure using **Browser SSO** profile **SAML 2.0**
        - Enable the **IdP-Initiated SSO** SAML profile.
        - Enable the **SP initiated SSO** SAML profile.
        - In **Assertion Creation → Attribute Contract**, set the **Subject Name Format** to **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.
        - In **Assertion Creation → Attribute Contract Fulfillment**, map the attribute **SAML_SUBJECT** to the attribute **mail**.
        - In **Protocol Settings → Allowable SAML Bindings**, enable **Redirect**.
    3. Export the metadata for the newly-created SP connection.
    4. Export the signing certificate public key.



2. Configure the PingFederate identity provider (IdP) connection for BambooHR.

    1. Sign on to BambooHR as a Full Admin administrator user.
    2. On the **Settings** page, click **Apps**.
    3. On the **SAML Single Sign-On** application published by BambooHR line, click **Install**.

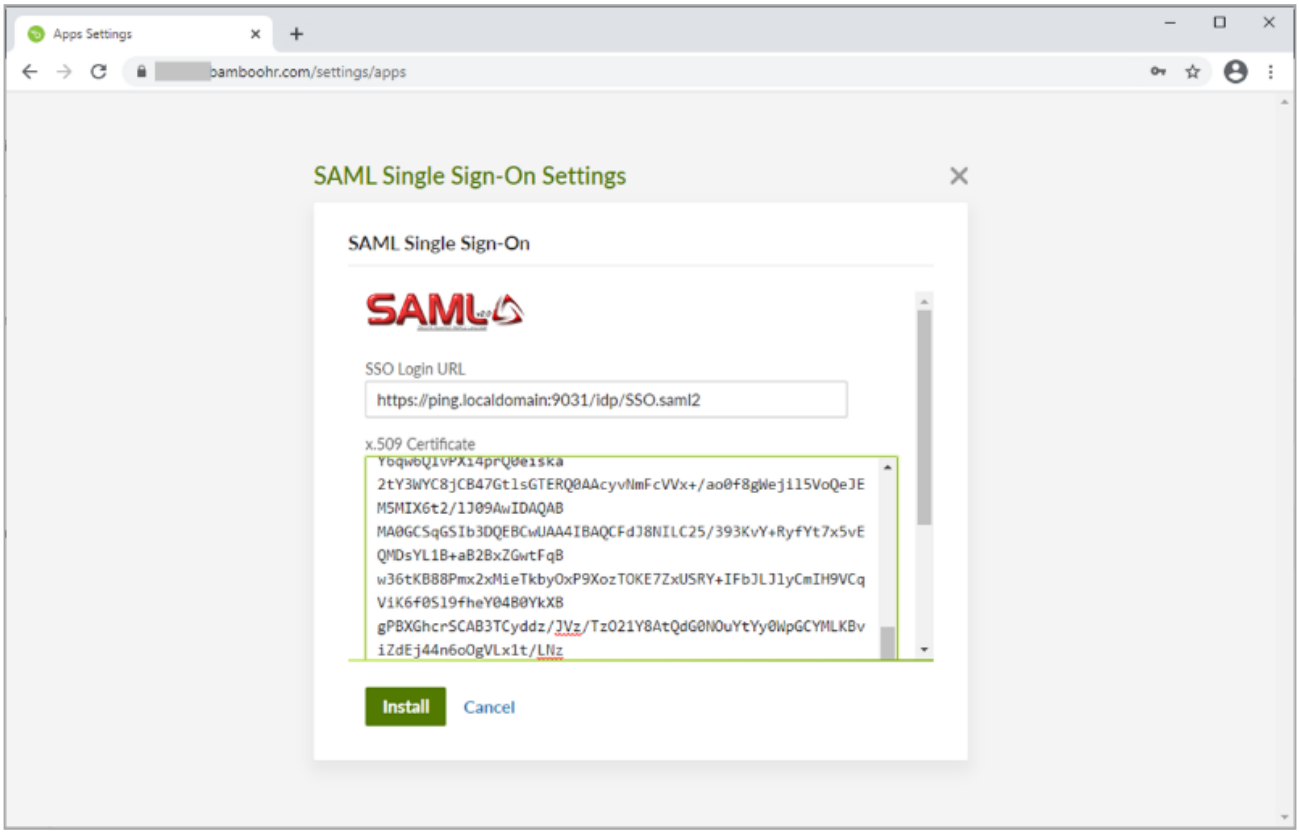


4. In the **SSO Login URL** field, enter the URL Location for **SingleSignOnService Location** retrieved from the PingFederate SP metadata that you downloaded from the BambooHR configuration.

   Example:

   ```
   https://PingFederateHostname:PingFederatePort/idp/SSO.saml2
   ```

5. In a text editor, open the signing certificate that you downloaded in from PingFederate and paste the contents into the **x.509 Certificate** field.

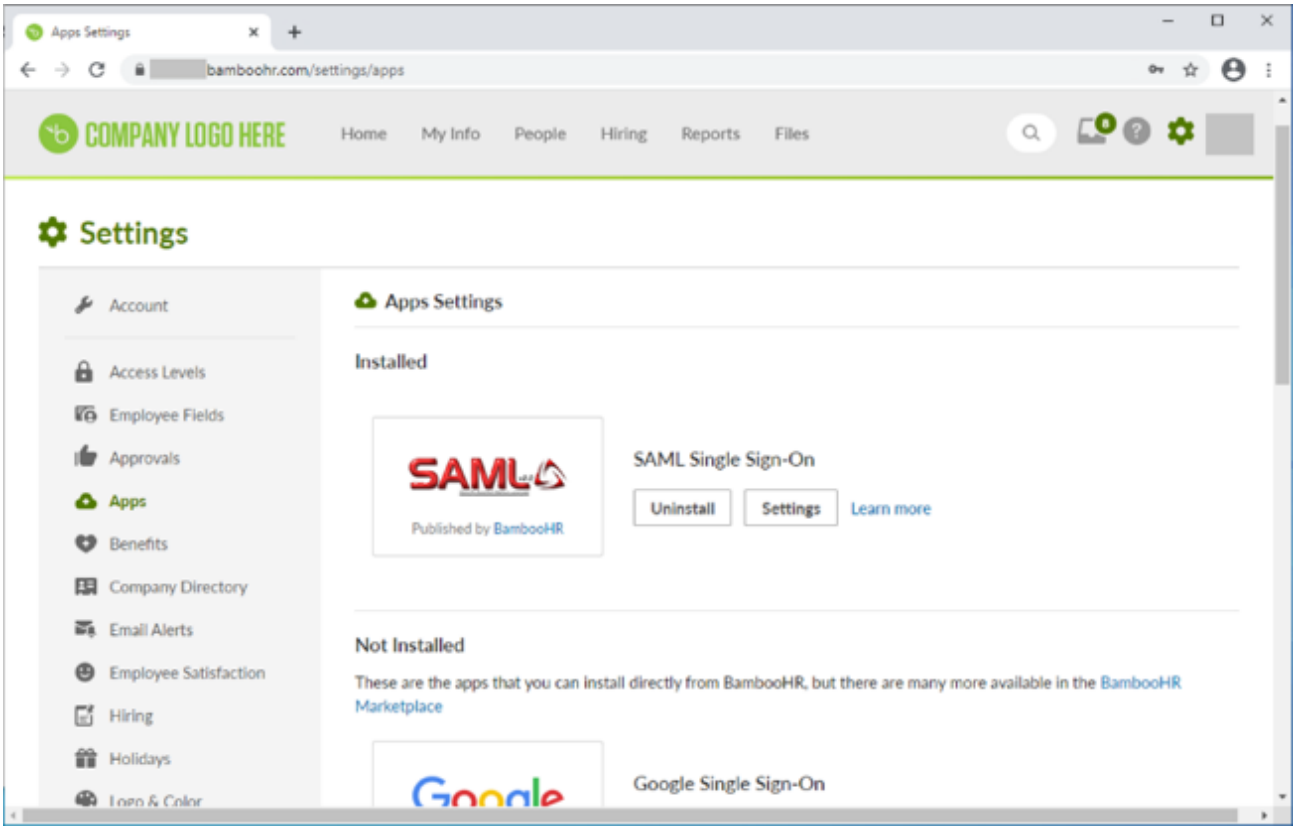


6. Click **Install**.

   Result:

   Your configuration is complete.

   From this point BambooHR will redirect to the configured IdP for authentication for all new sessions. You should complete testing in a private or incognito browser session while keeping the original admin session active. This allows you to change settings or remove the configuration if the integration testing fails.

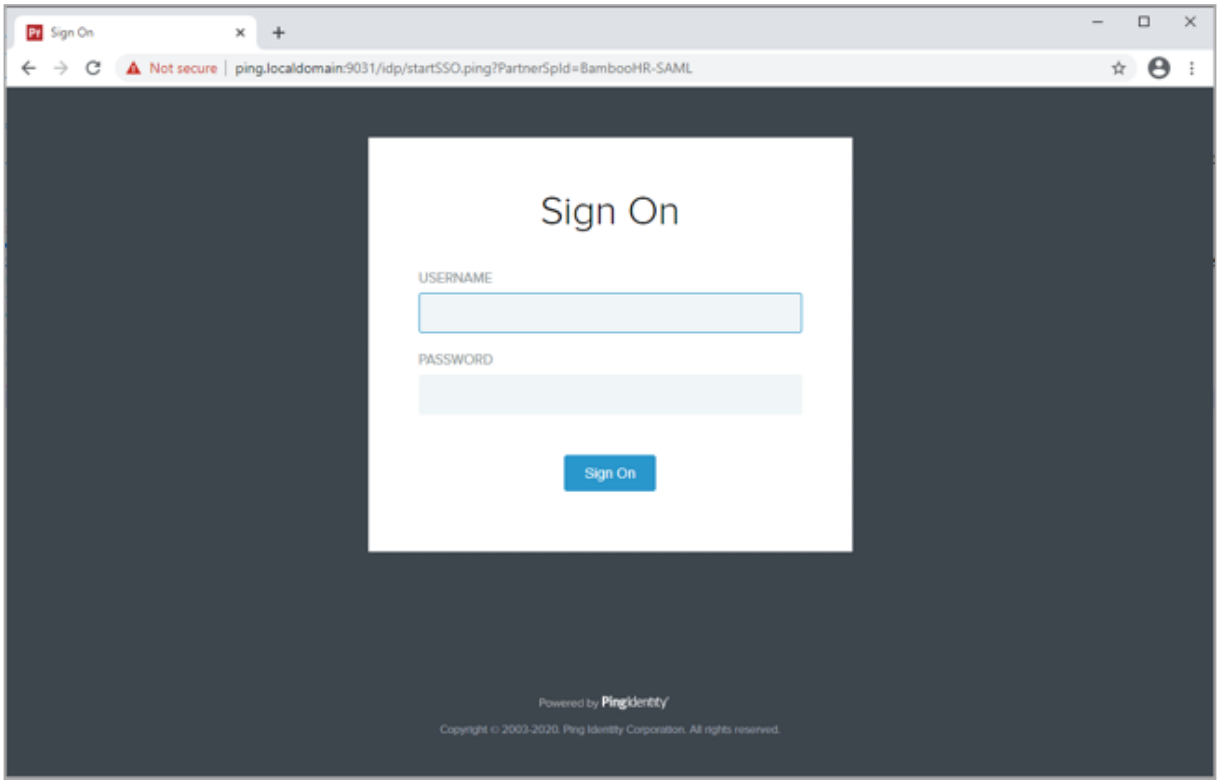


3. Test the integration.

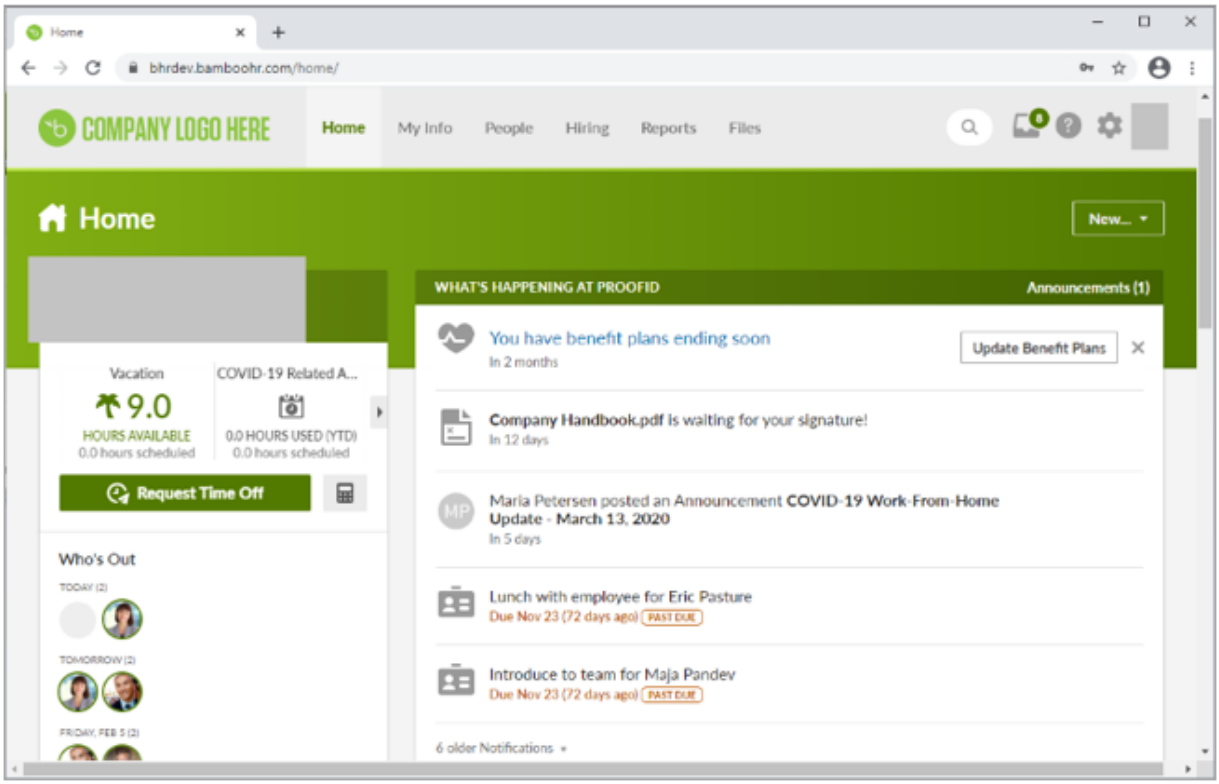
Choose from:

PingFederate IdP-initiated SSO

1. Go to the **SSO Application** in the PingFederate Application configuration to perform IdP-initiated SSO, such as https://*PingFederateHostname*:*PingFederatePort*/idp/startSSO.ping?PartnerSpId=BambooHR-SAML.

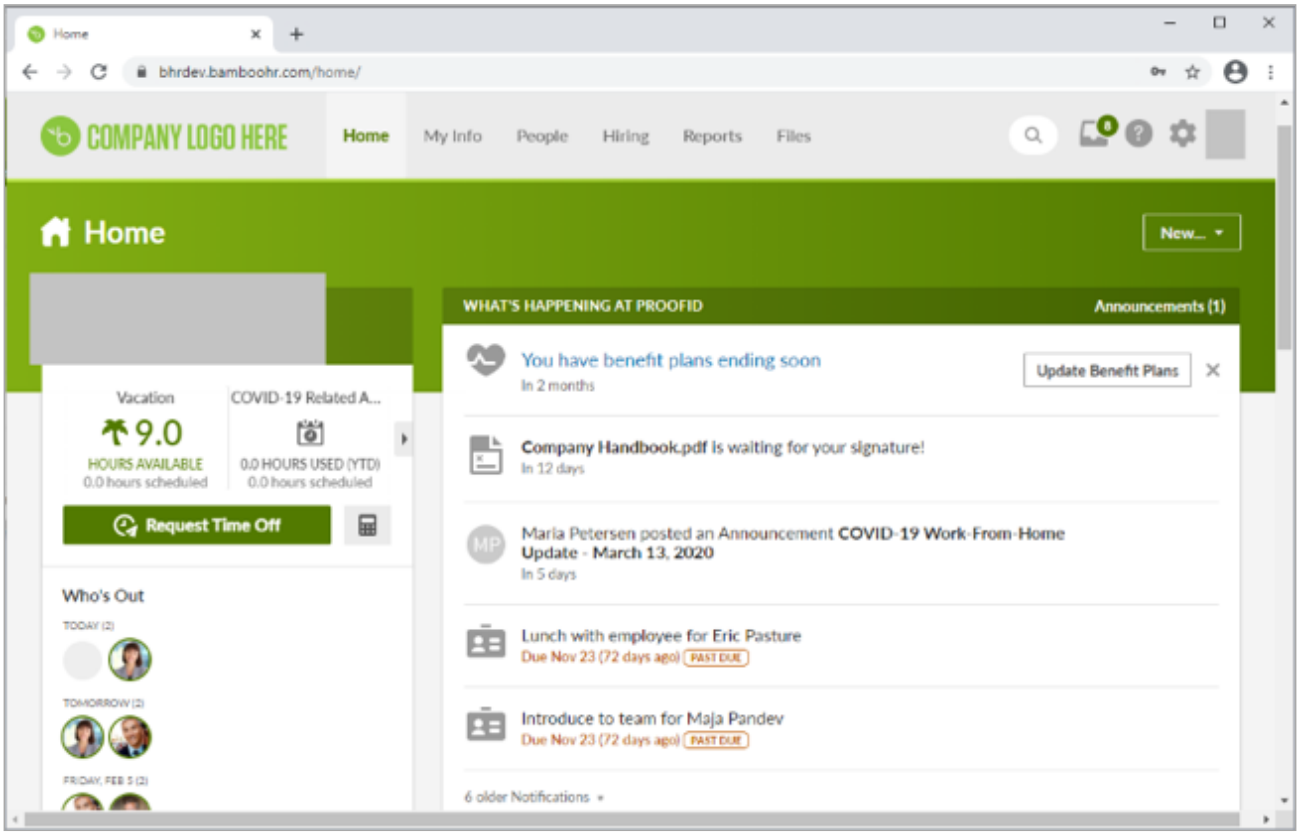


2. Go to the SSO Application Endpoint in the BambooHR configuration



PingFederate SP-initiated SSO

Go to the URL for your BambooHR tenant: https://*tenant*.bamboohr.com



Configuring SAML SSO with BambooHR and PingOne for Enterprise

About this task

The following table details the required and optional attributes to configure in the assertion attribute contract.

Attribute Name	Description	Required / Optional
`urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`	Email address for user	Required

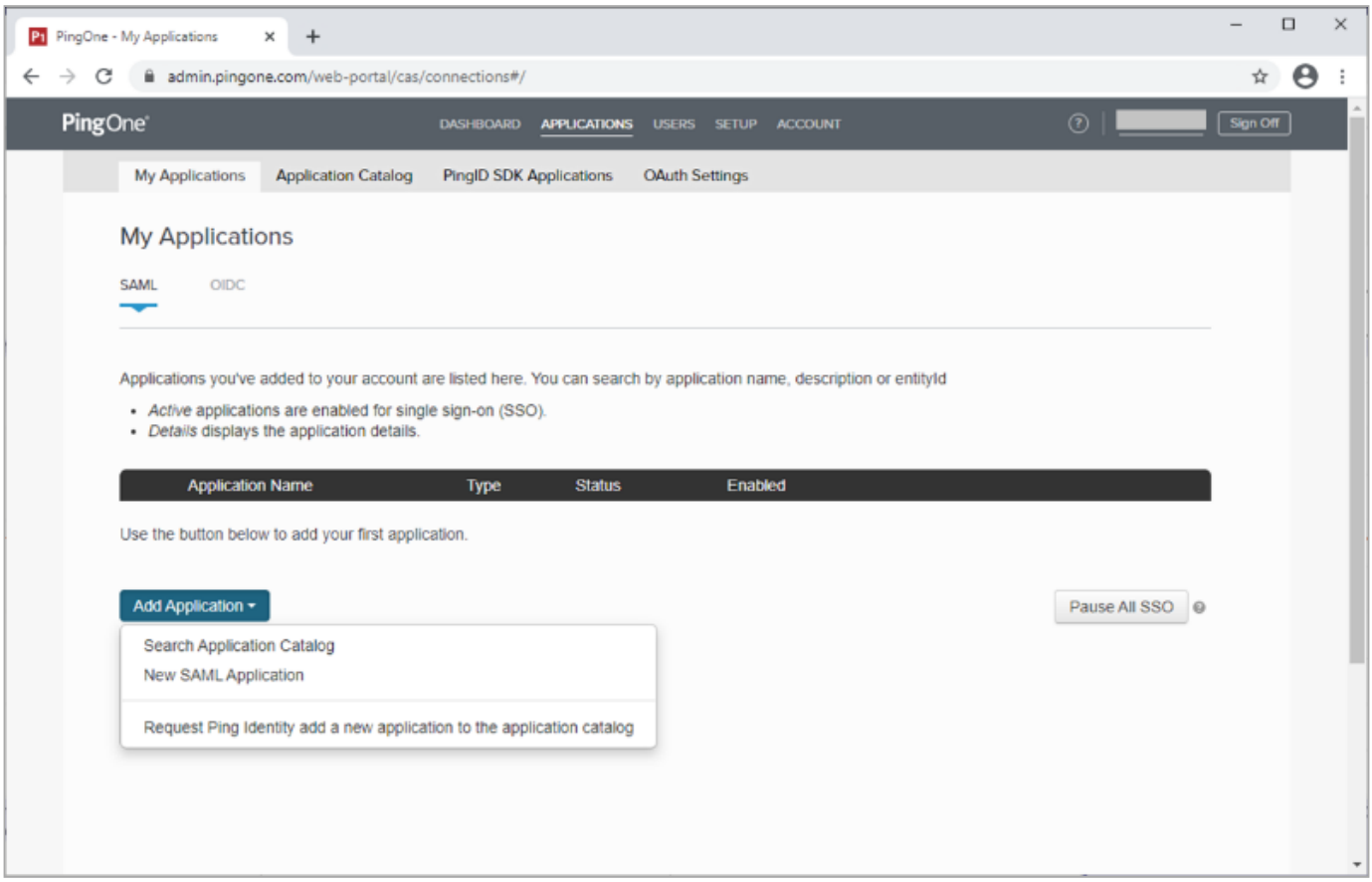
The following table details the environment-specific references used in this guide. Replace these references with the suitable value for your environment.

Reference	Description
tenant	BambooHR Tenant name

Create a PingOne for Enterprise application for BambooHR.

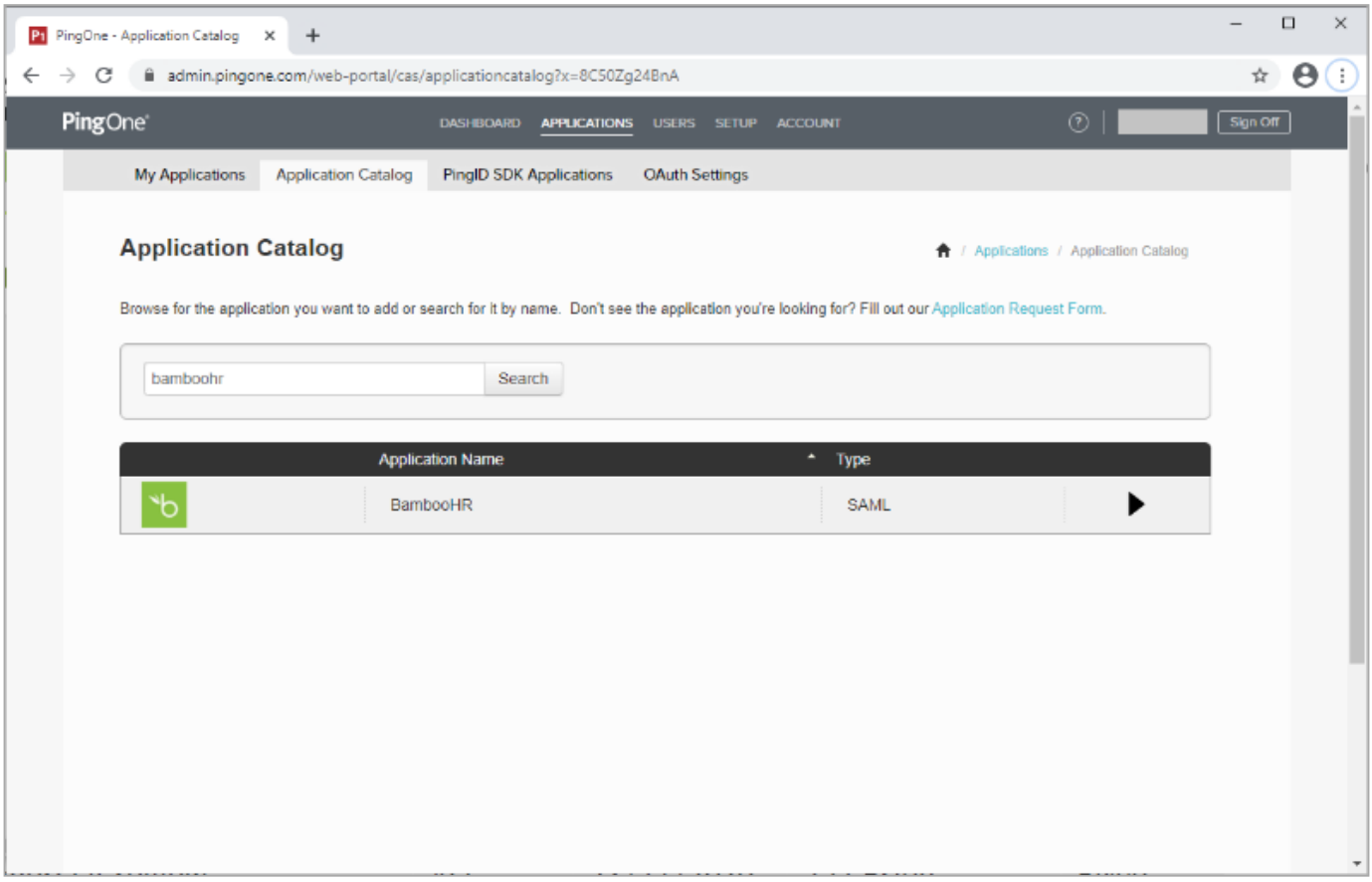
1. Download the BambooHR metadata from `https://tenant.bamboohr.com/saml/sp_metadata.php`.
2. Sign on to PingOne for Enterprise and go to **Applications → Application Catalog**.

3. On the **SAML** tab, in the **Add Application** list, select **Search Application Catalog**.



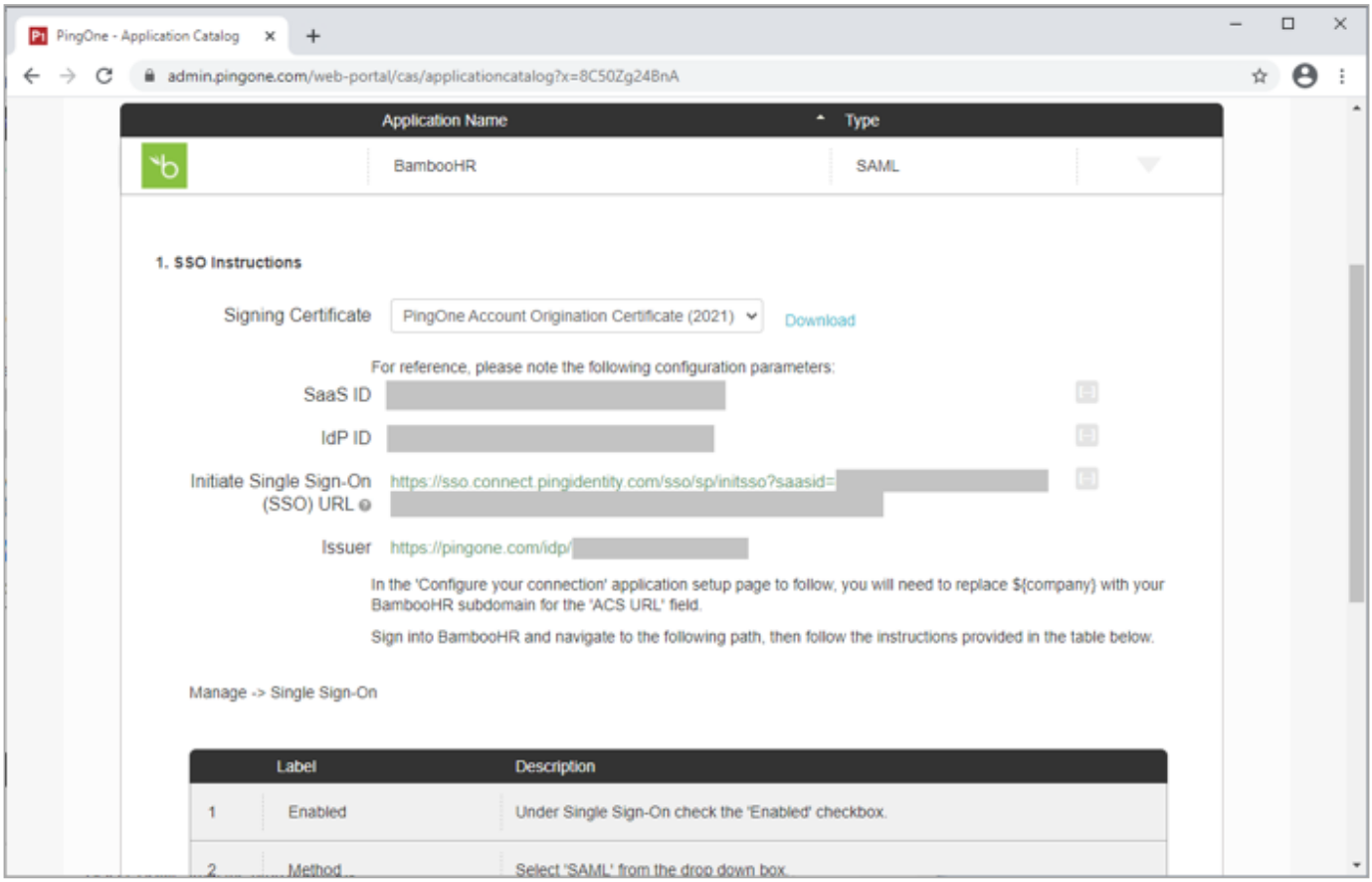
4. Search for `BambooHR`.

5. Click the **BambooHR** row.



6. Click **Setup**.

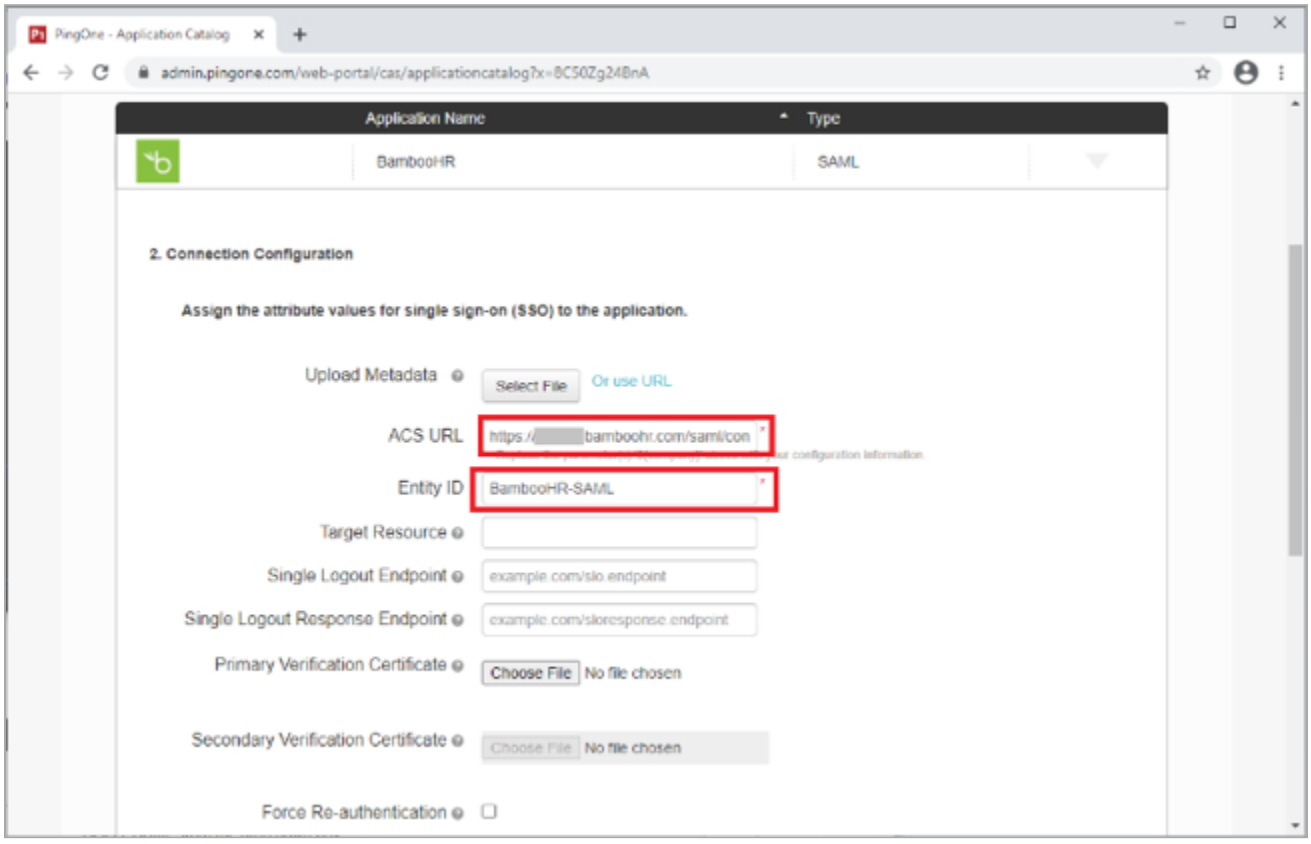
7. In the **Signing Certificate** list, select the appropriate signing certificate.



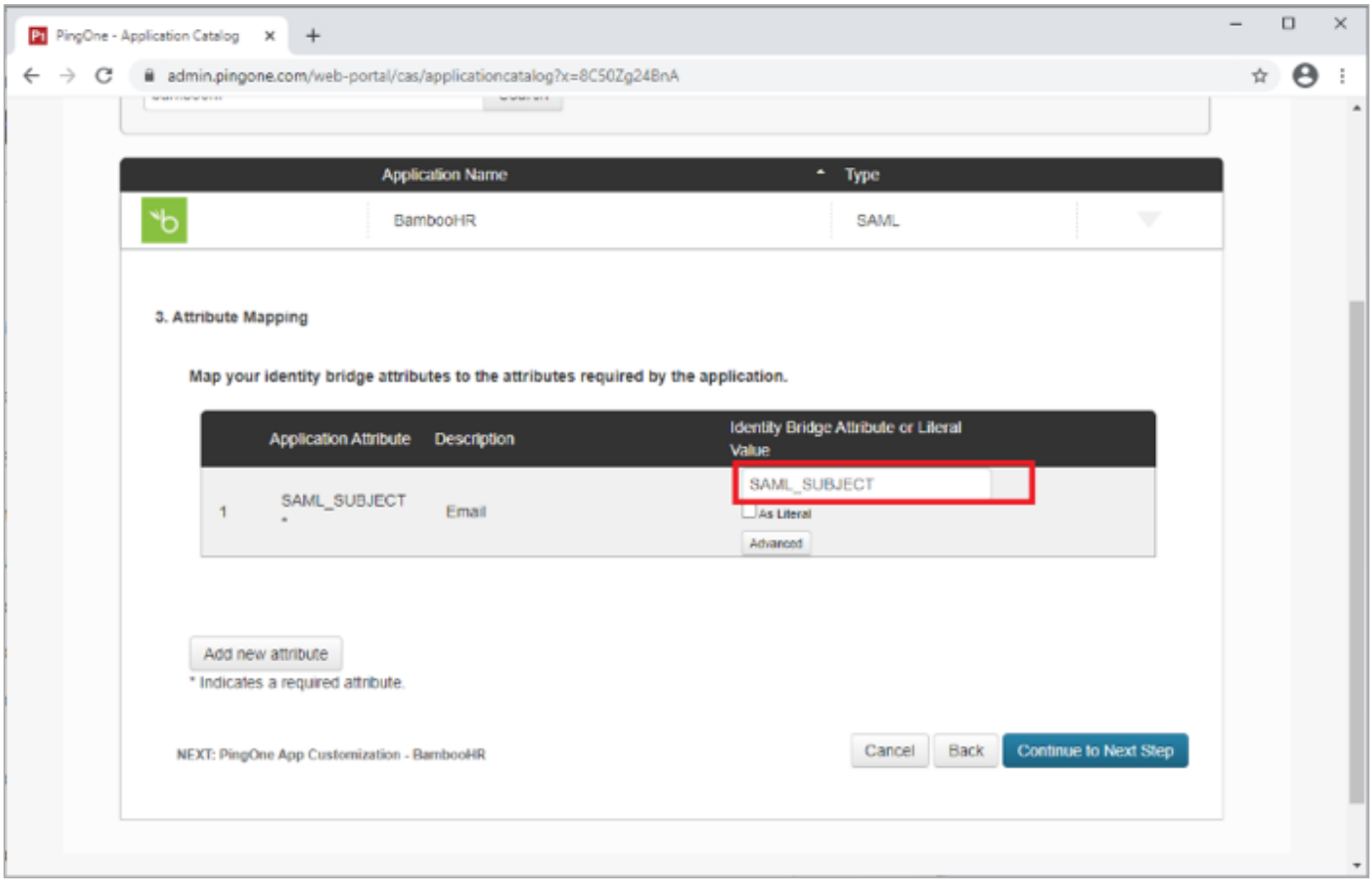
8. Review the steps, and make a note of the PingOne for Enterprise **SaaS ID**, **IdP ID**, **Single Sign-On URL**, and **Issuer** values.
9. Click **Continue to Next Step**.
10. Click **Select File** and upload the BambooHR metadata you downloaded.

> **Note**
>
> If the upload fails, continue with the next steps and explicitly set the parameters based on the attributes in the metadata.

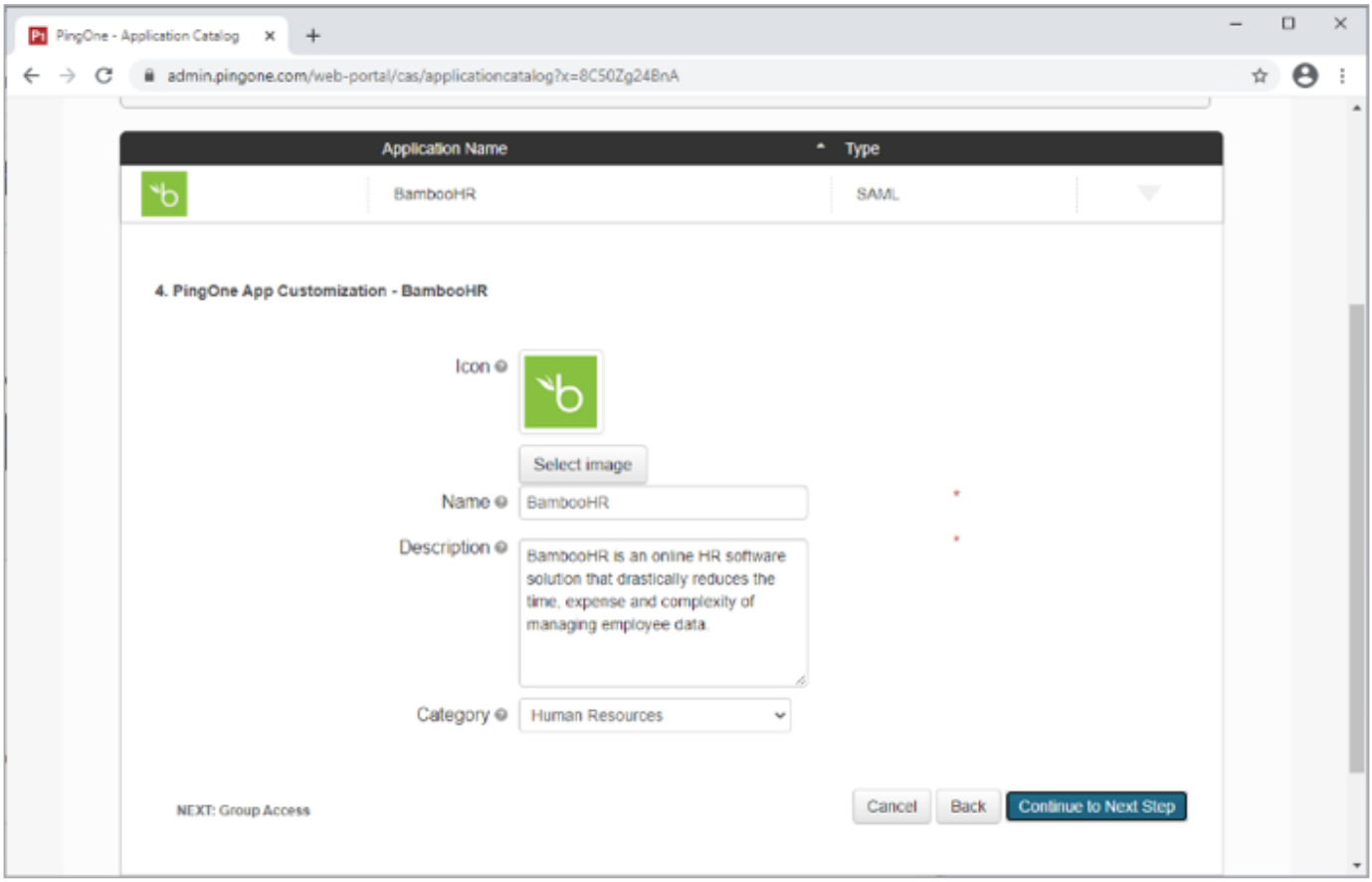
11. Set the **ACS URL** to `https://tenant.bamboohr.com/saml/consume.php`.
12. Set the **Entity ID** to **BambooHR-SAML**.



13. Click **Continue to Next Step**.
14. In the **Attribute Mapping** section, in the **Identity Bridge Attribute or Literal Value** column of the **SAML_SUBJECT** row, select the attribute **SAML_SUBJECT**.

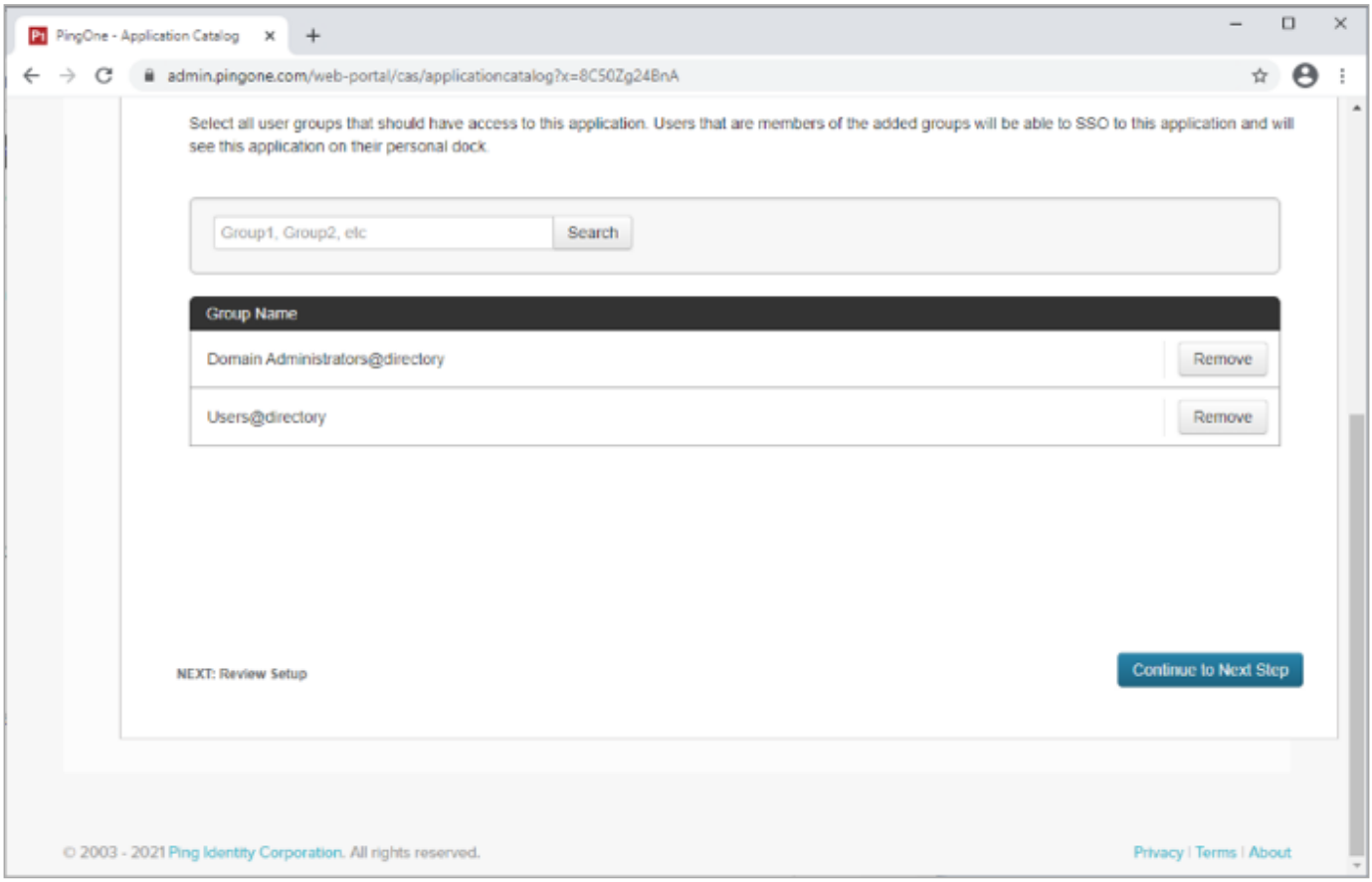


15. Click **Continue to Next Step**.
16. Update the **Name**, **Description**, and **Category** fields as needed.



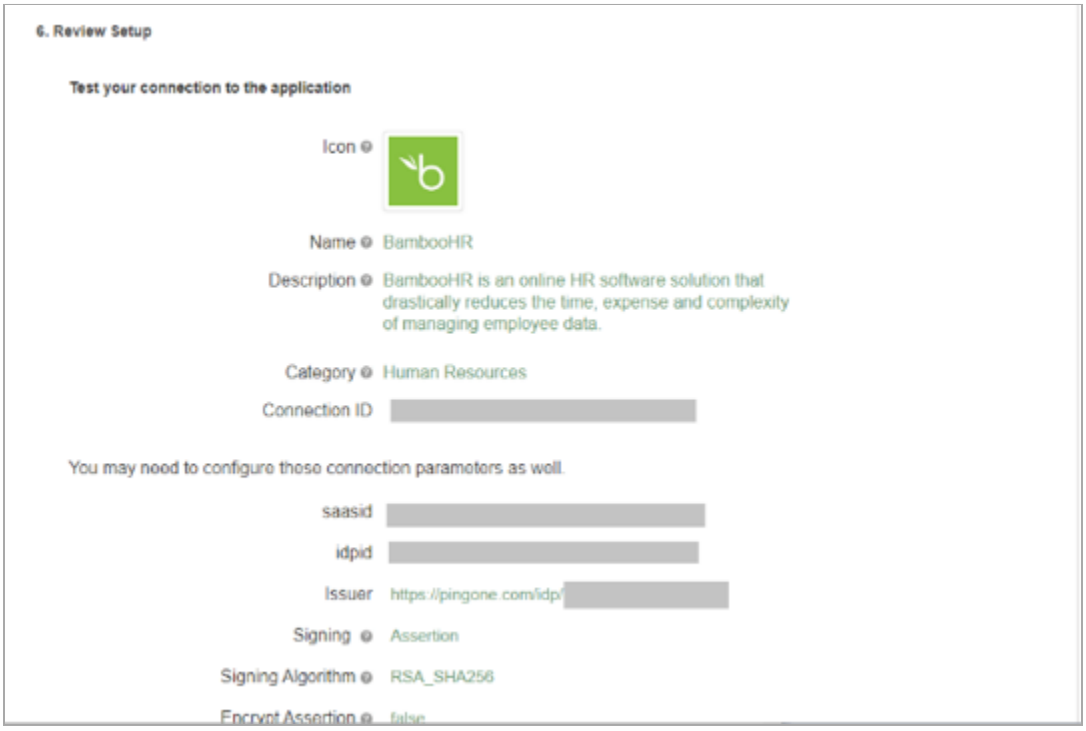
17. Click **Continue to Next Step**.

18. Add the user groups for the application.

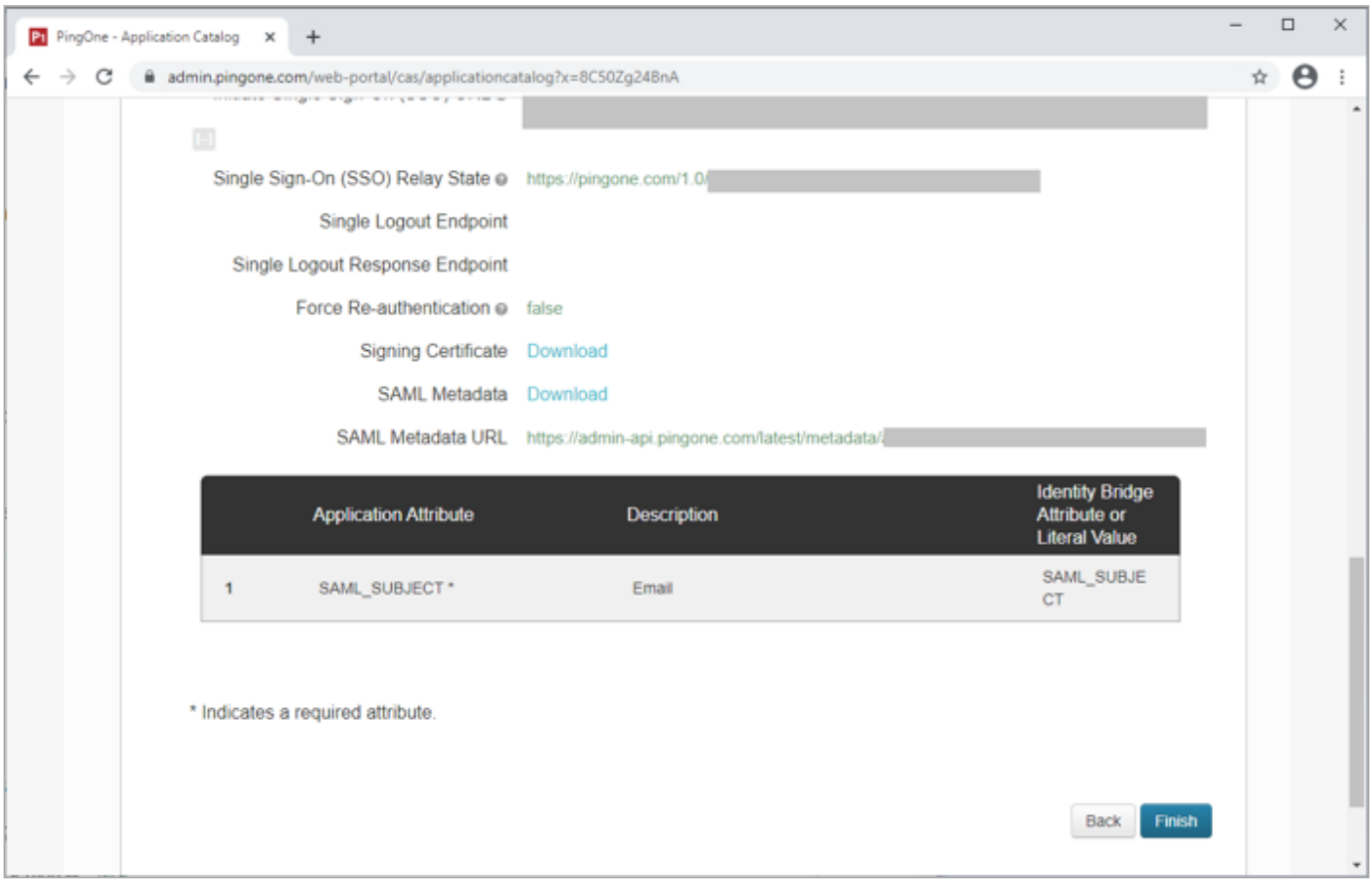


19. Click **Continue to Next Step**.

20. Review your settings.



21. Copy the **Single Sign-On (SSO) URL** value to a temporary location.



This is the IdP-initiated SSO URL that you can use for testing.

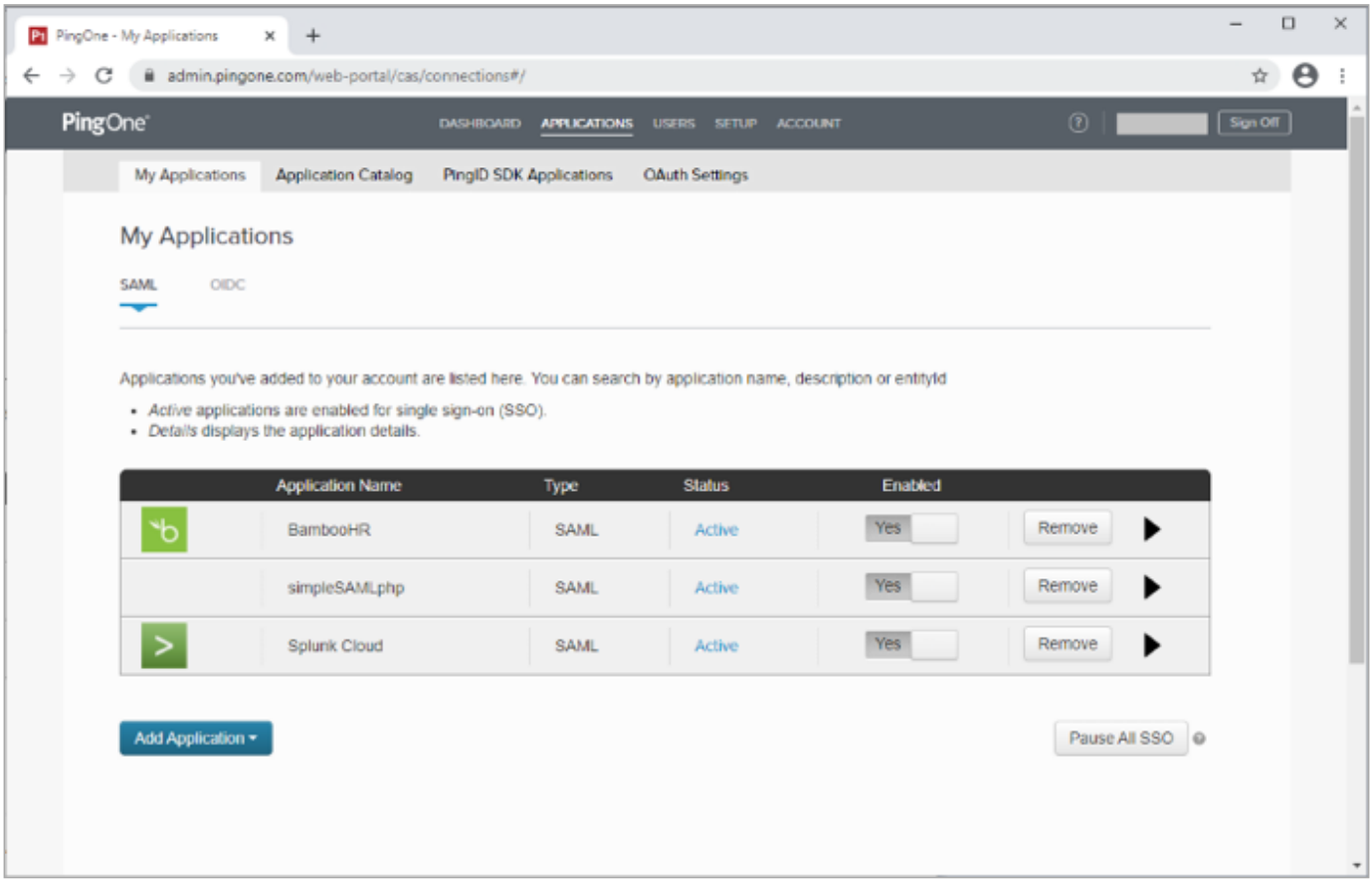
22. On the **Signing Certificate** line, click **Download**.

    You use this in the BambooHR Cloud configuration.

23. On the **SAML Metadata** line, click **Download**.

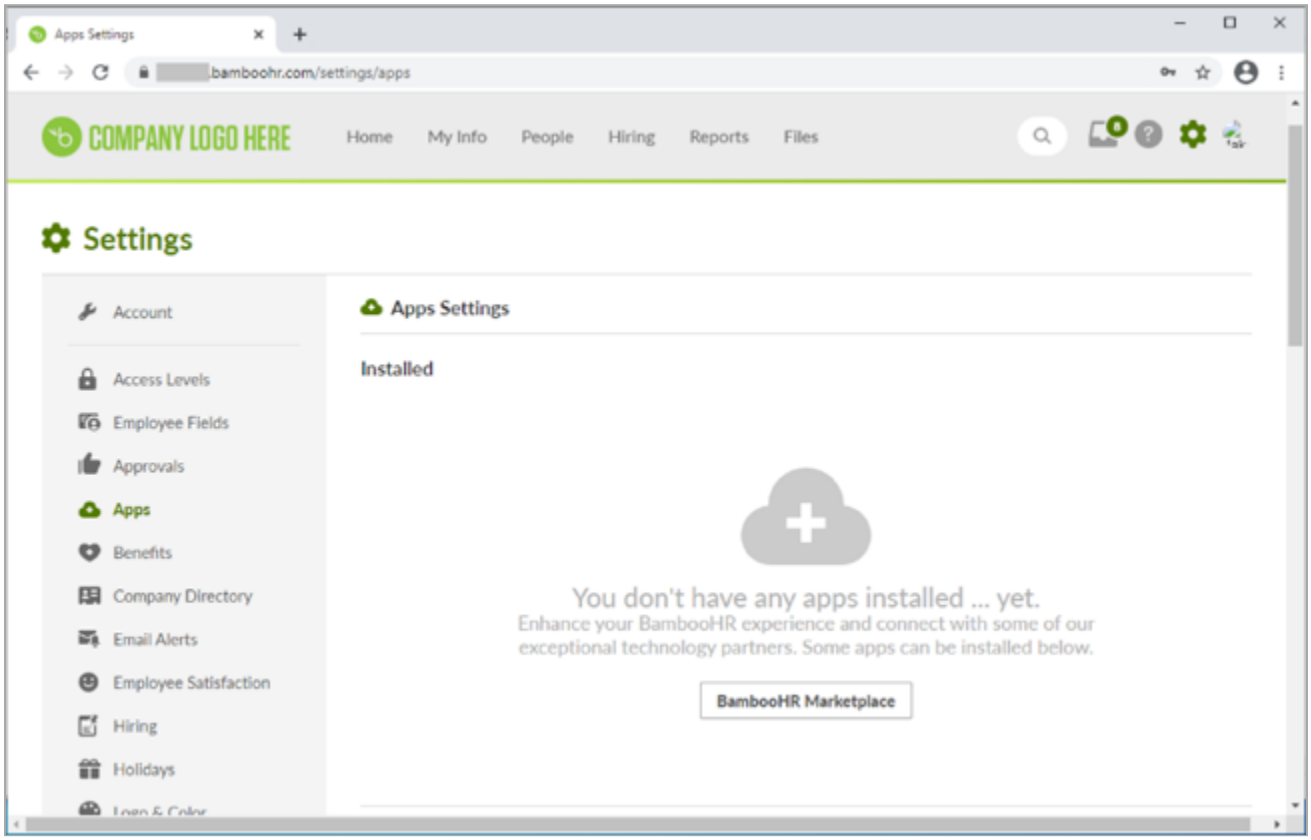
    You use this in the BambooHR Cloud configuration.

24. Click **Finish**.

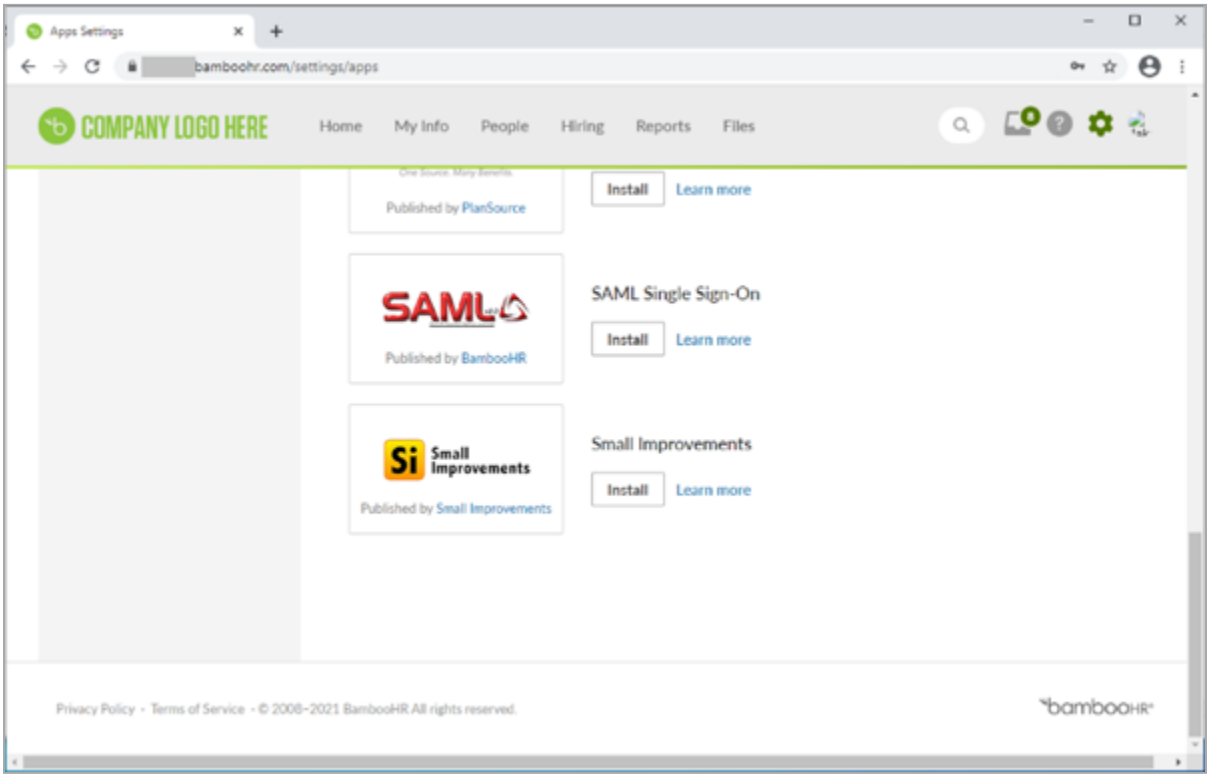


Configure the PingOne for Enterprise IdP connection for BambooHR

1. Sign on to BambooHR as a Full Admin administrator user.
2. On the **Settings** page, click **Apps**.



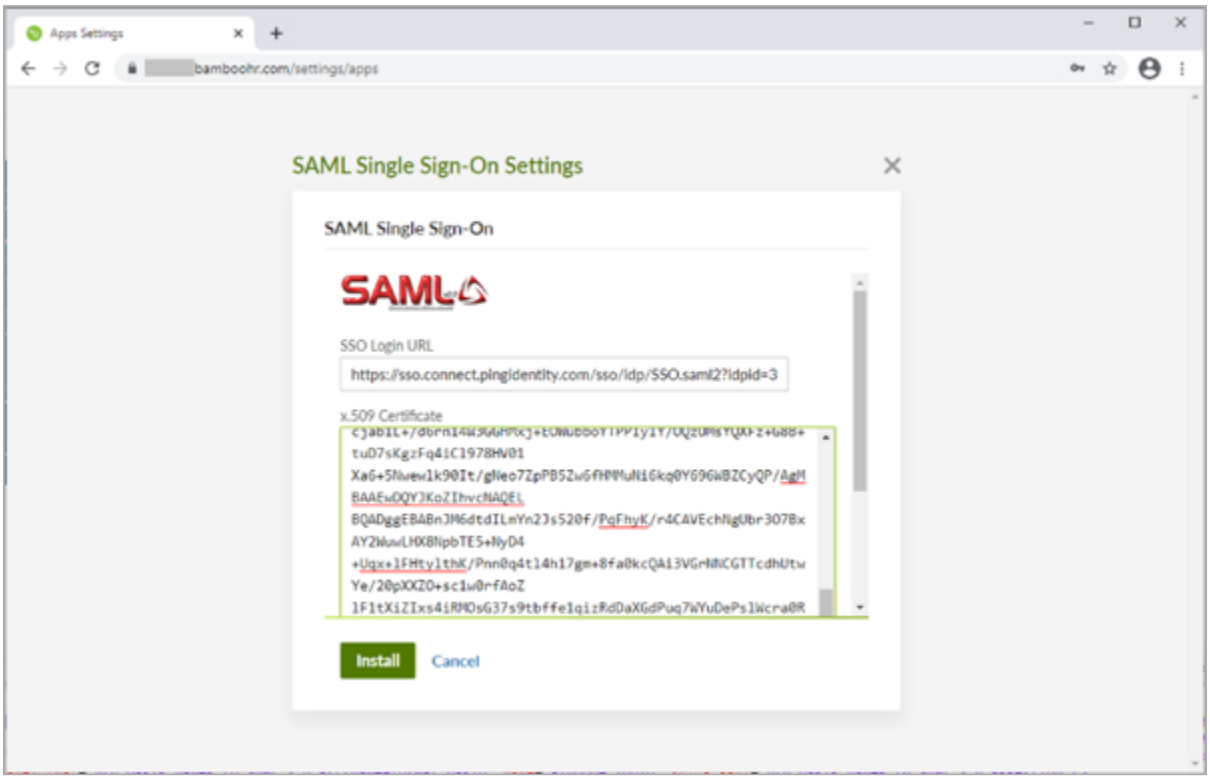
3. On the **SAML Single Sign-On** application published by BambooHR line, click **Install**.



4. In the **SSO Login URL** field, enter the URL Location for **SingleSignOnService Location** retrieved from the PingOne SP metadata that you downloaded from the BambooHR configuration.

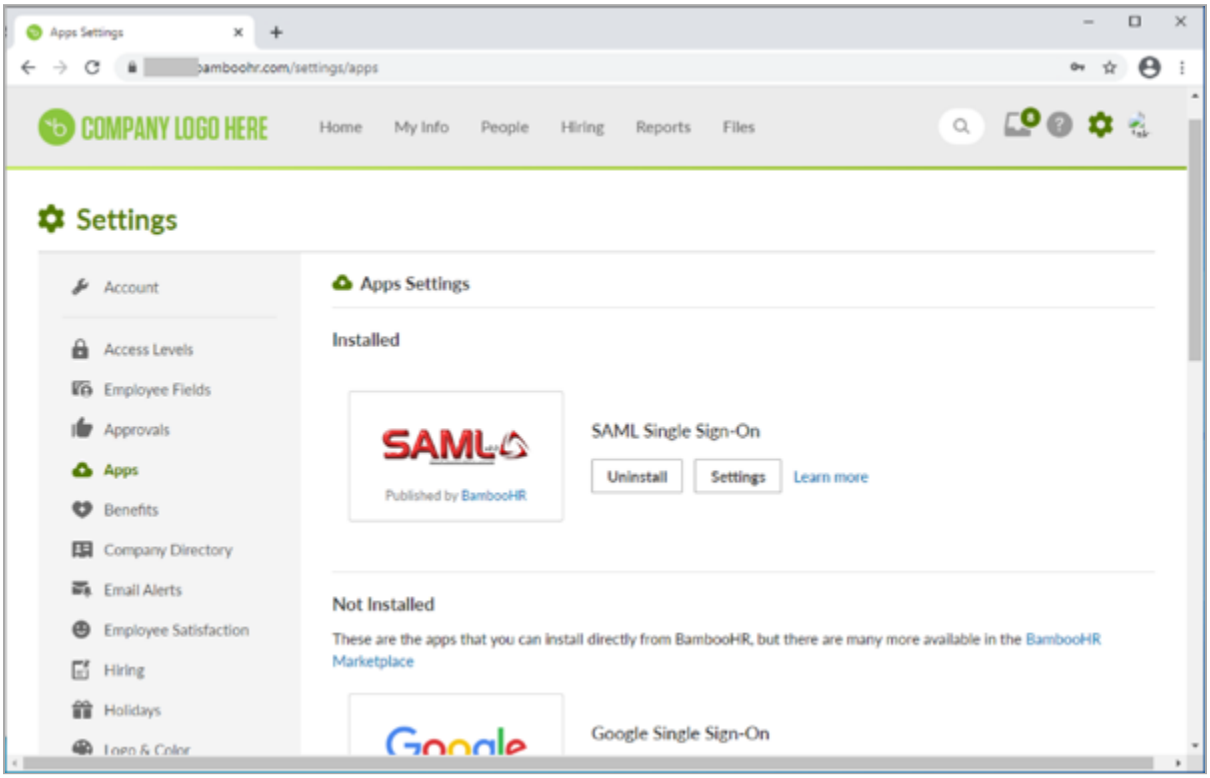
Example:

`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=idpid`



5. In a text editor, open the signing certificate that you downloaded in the PingOne for Enterprise SP configuration and paste the contents into the **x.509 Certificate** field.

6. Click **Install**.



Result:

Your configuration is complete.

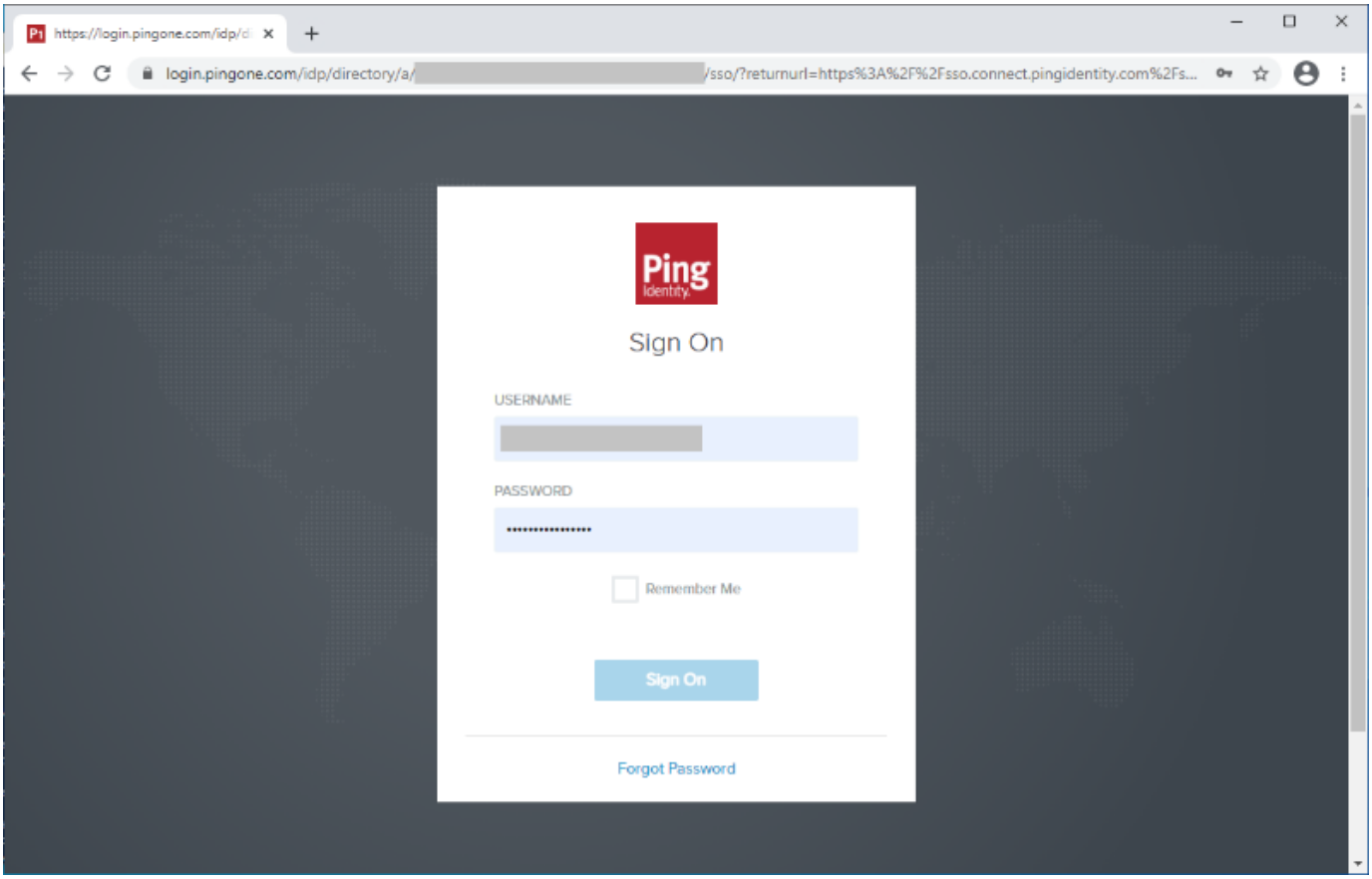
> **Note**
>
> From this point BambooHR will redirect to the configured IdP for authentication for all new sessions. You should complete testing in a private or incognito browser session while keeping the original admin session active. This allows you to change settings or remove the configuration if the integration testing fails.

Test the integration

Choose from:

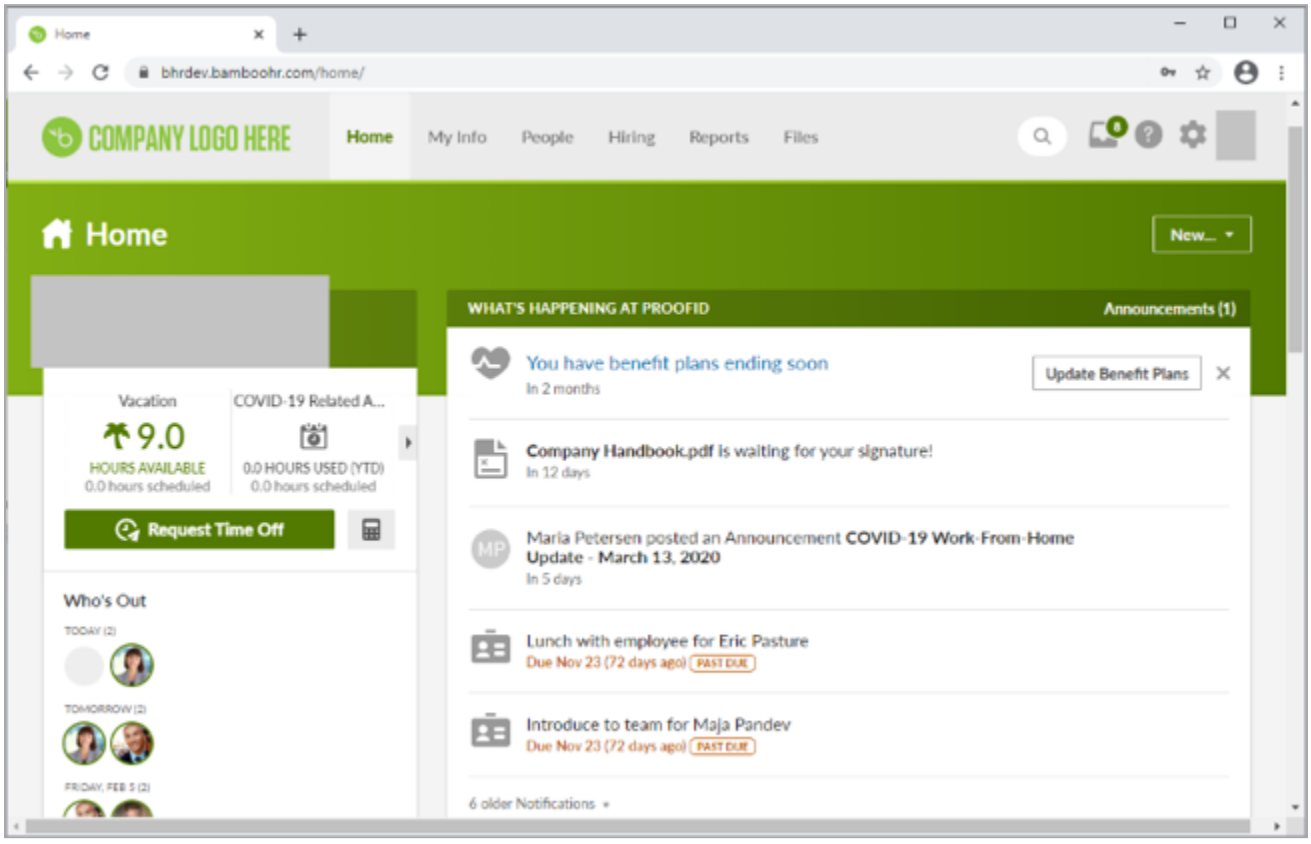
PingOne for Enterprise IdP Initiated SSO

Go to the **Single Sign-On (SSO) URL** in the PingOne Application configuration to perform IdP initiated SSO (`https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=saasid&idpid=idpid`).



PingOne SP Initiated SSO

Go to the URL for your BambooHR tenant, https://*tenant*.bamboohr.com



Box

Configuring SAML SSO with Box and PingFederate

Learn how to configure SAML SSO with Box and PingFederate.

About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

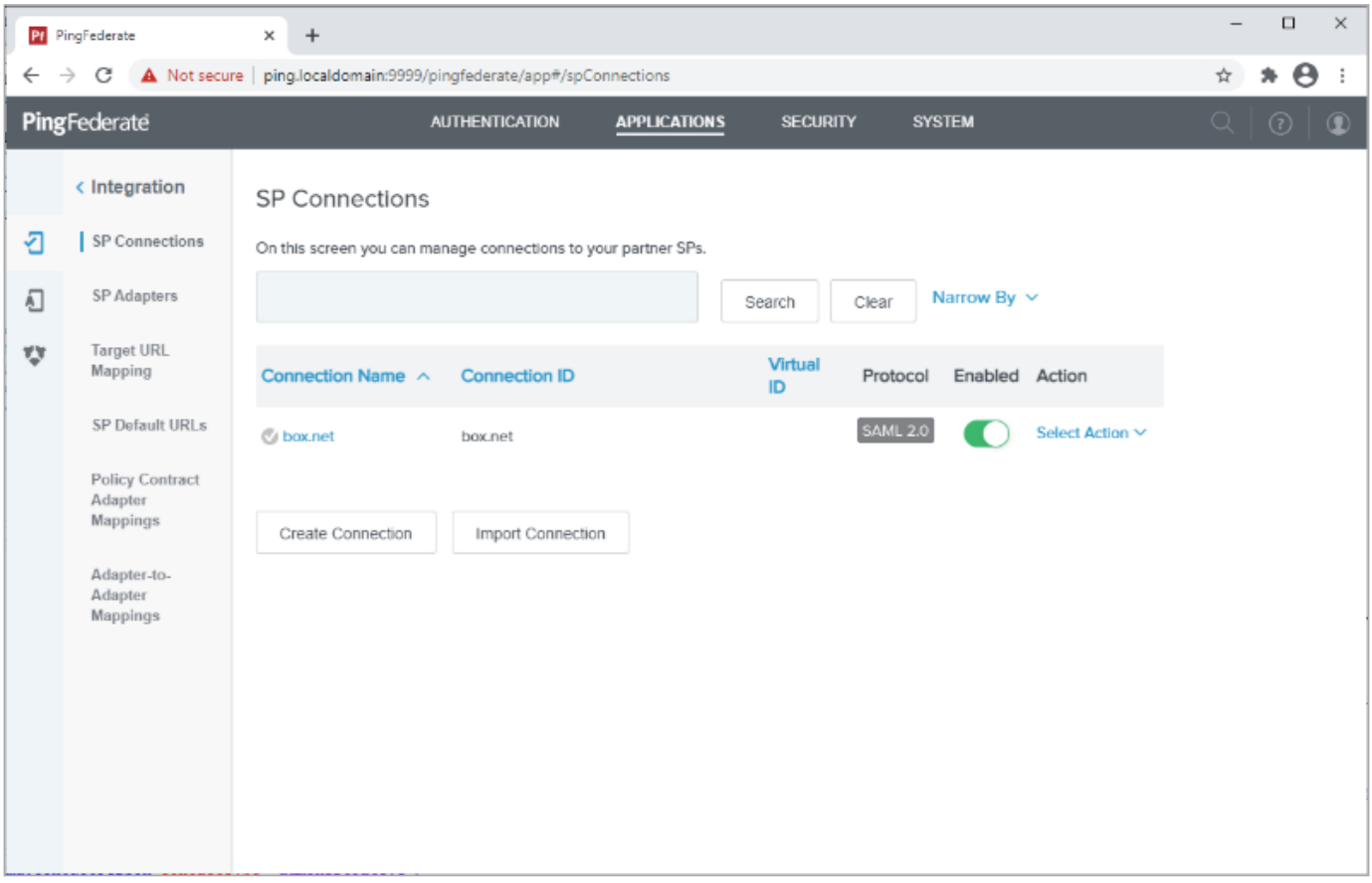
Attribute Name	Description	Required / Optional
`SAML_SUBJECT`	Email	Required
`givenName`	First Name	Optional
`sn`	Last Name	Optional
`memberOf`	Groups	Optional

> **Note**
> The following configuration is untested and is provided as an example. Additional steps might be required.

Create a PingFederate SP connection for Box

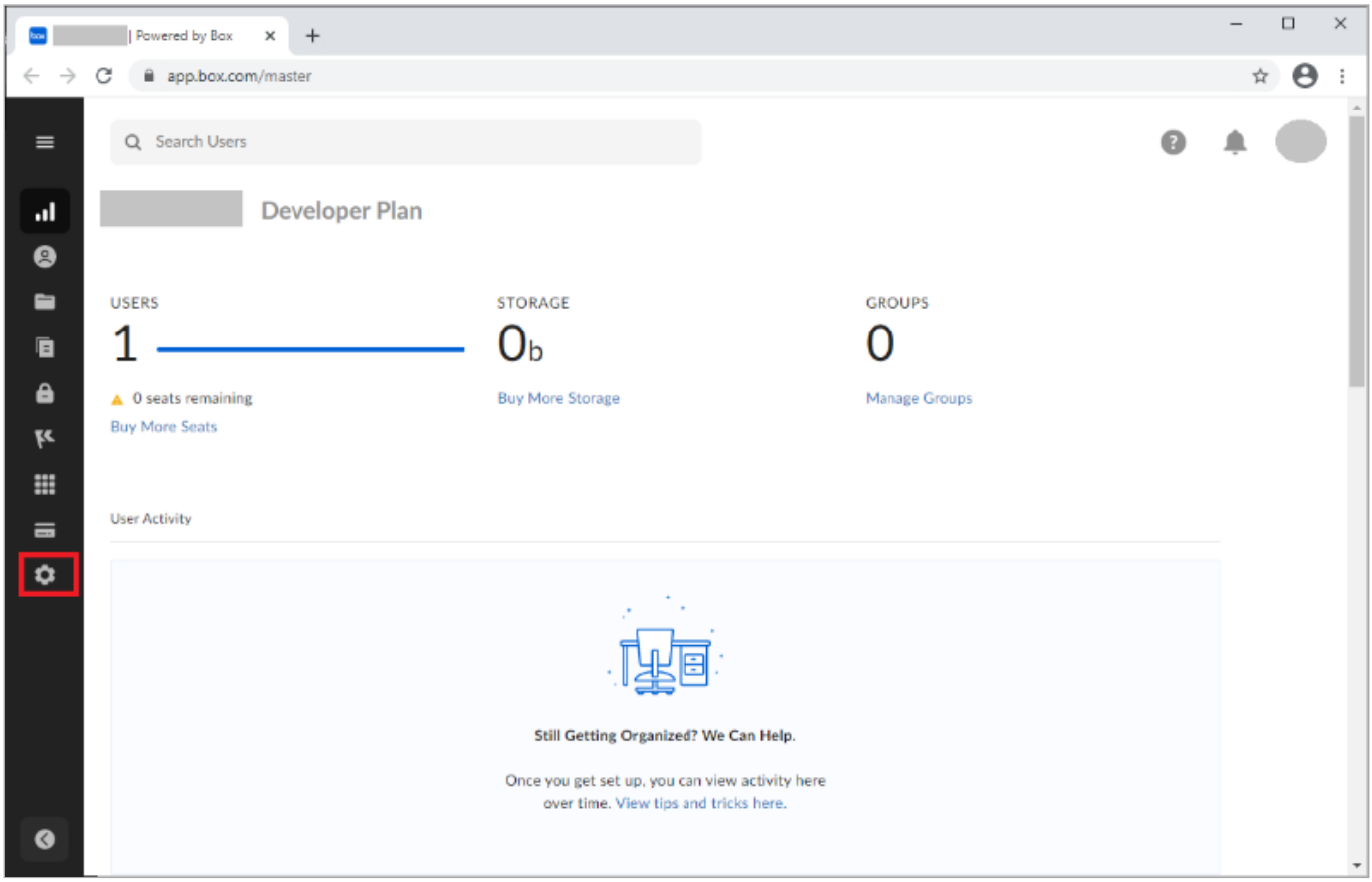
1. Download the Box metadata from https://cloud.app.box.com/s/9y0zm1sqgvkxe8ha2qa3dfhwoivpoyy4.
2. Sign on to the PingFederate administrative console.
3. Using the metadata that you downloaded, create an SP connection in PingFederate:
    1. Configure using **Browser SSO profile SAML 2.0**.
    2. Enable the following **SAML Profiles**:
        - **IdP-Initiated SO**
        - **SP-Initiated SSO**
        - **IdP-Initiated SLO**
        - **SP-Initiated SLO**
    3. In **Assertion Creation: Attribute Contract**, set the **Subject Name Format** to **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.

4. Extend the contract with the following attributes:
    - **givenName**
    - **memberOf**
    - **Sn**
5. In the **Assertion Creation: Attribute Contract Fulfillment** section:
    - Map the attribute **SAML_SUBJECT** to the attribute **mail**.
    - Map the optional attribute **givenName** to the attribute for the user's first name.
    - Map the optional attribute **memberOf** to the attribute for the user's Box roles.
    - Map the optional attribute **Sn** to the attribute for the user's surname or family name.
6. In **Protocol Settings**:
    - In **Assertion Consumer Service URL**, delete **Artifact** and **PAOS Bindings**.
    - In **SLO Service URLs**, delete **Artifact** and **SOAP** bindings.
    - In **Allowable SAML Bindings**, enable **Redirect** and **POST**.
4. Export the metadata for the newly-created SP connection.
5. Export the signing certificate public key.

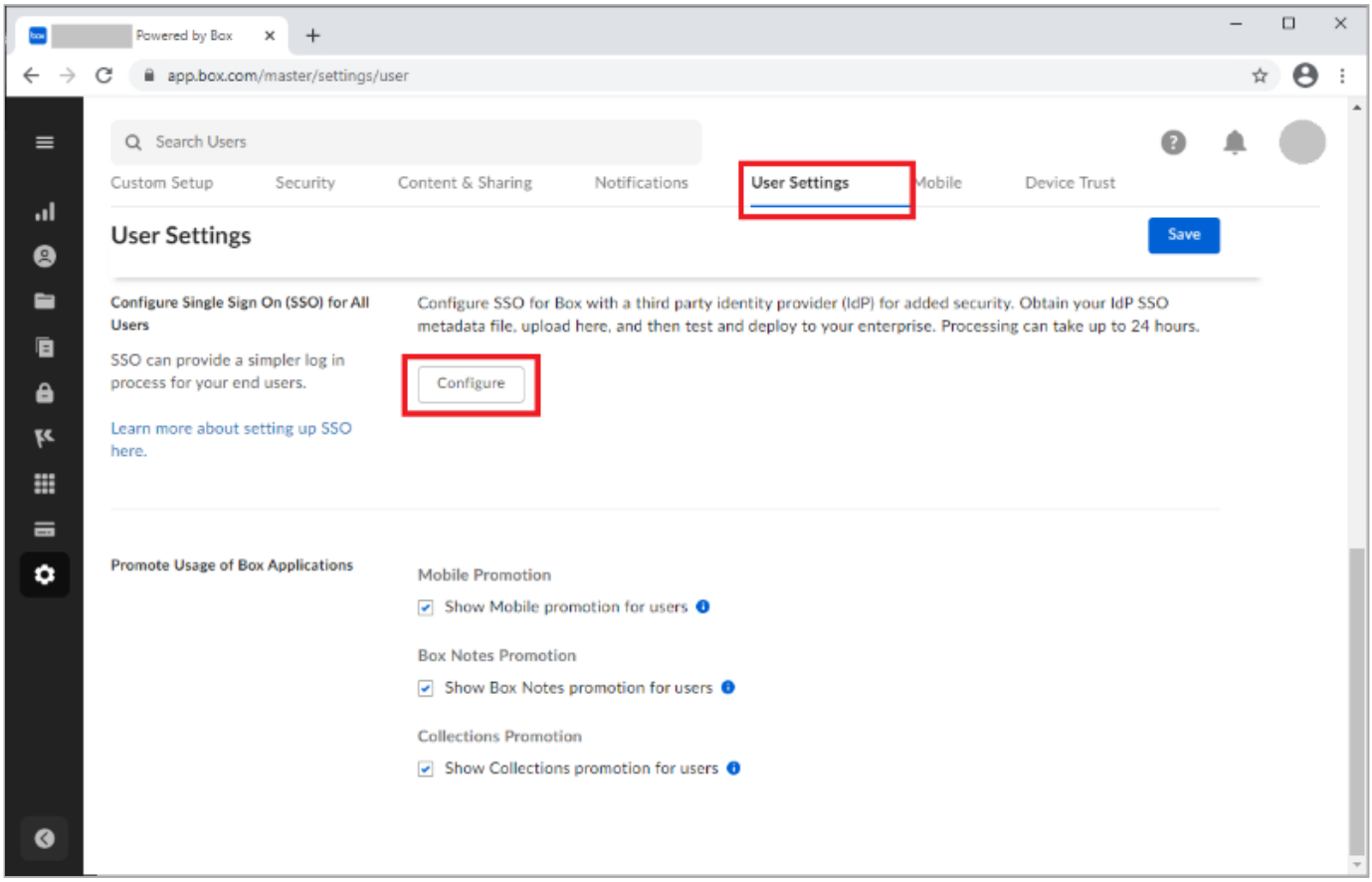


Configure the PingFederate IdP connection for Box

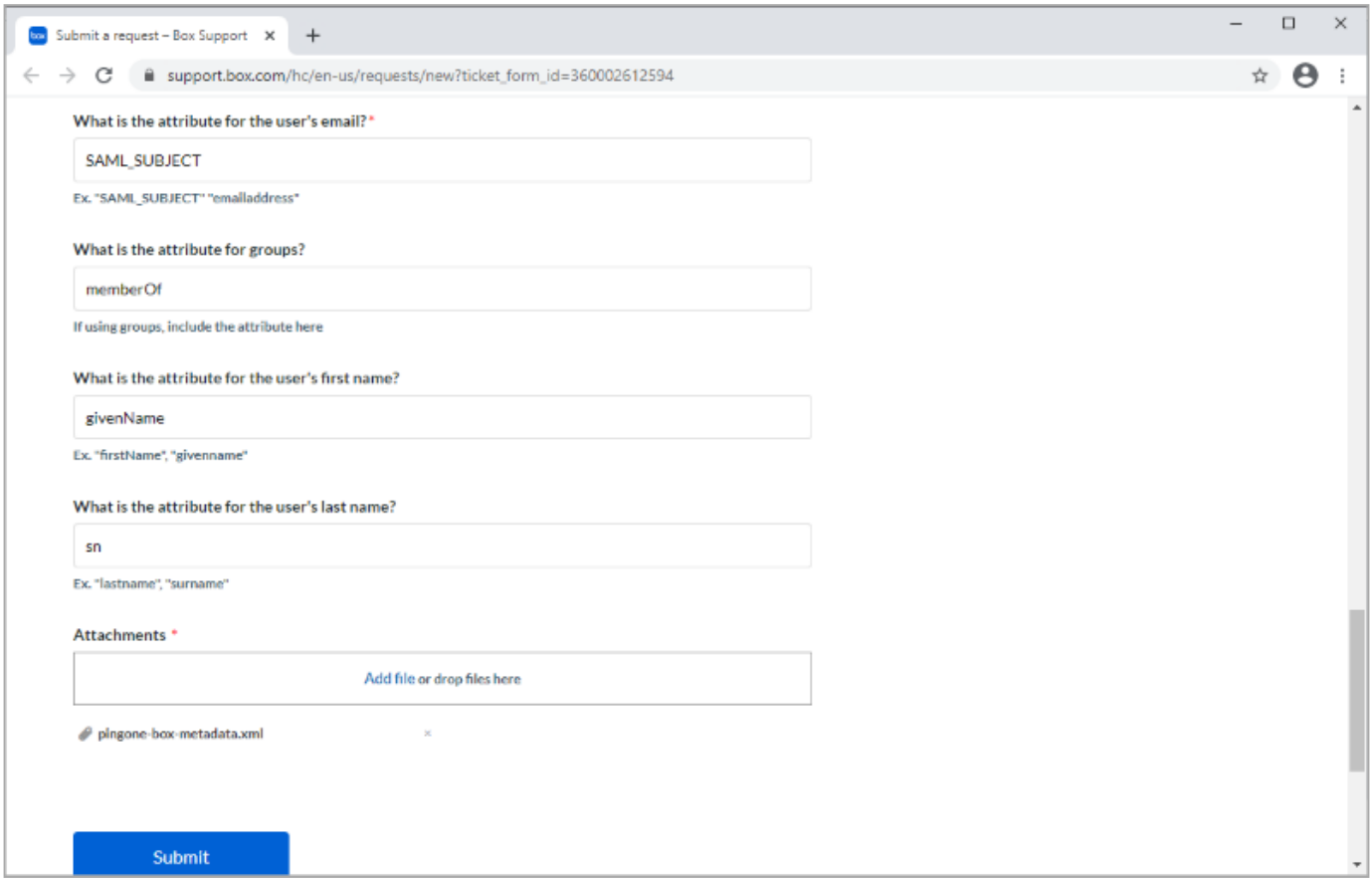
1. Sign on to the Box Admin Console as an administrator.



2. Click **Enterprise Settings**.
3. Click the **User Settings** tab.
4. In the **Configure Single Sign On (SSO) for All Users** section, click **Configure**.



5. Click **'I don't see my provider, or don't have a metadata file.'**
6. Complete the **Box SSO Setup Support Form**:
    1. Review the request form and the **For faster service please read** section.
    2. Complete the required fields:
        - For **Who is your Identity Provider?**, select **Other with Metadata**.
        - For **What is the attribute for the user's email?**, select **SAML_SUBJECT**.
        - For **What is the attribute for groups?**, select **memberOf**.
        - For **What is the attribute for the user's first name?**, select **givenName**.
        - For **What is the attribute for the user's last name?**, select **Sn**.
        - Attach the metadata that you downloaded from the PingFederate configuration.
7. Click **Submit**.



8. After the Box support team completes the configuration, follow any provided instructions and test the integration.

Configuring SAML SSO with Box and PingOne for Enterprise

Learn how to configure SAML SSO with Box and PingOne for Enterprise.

About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

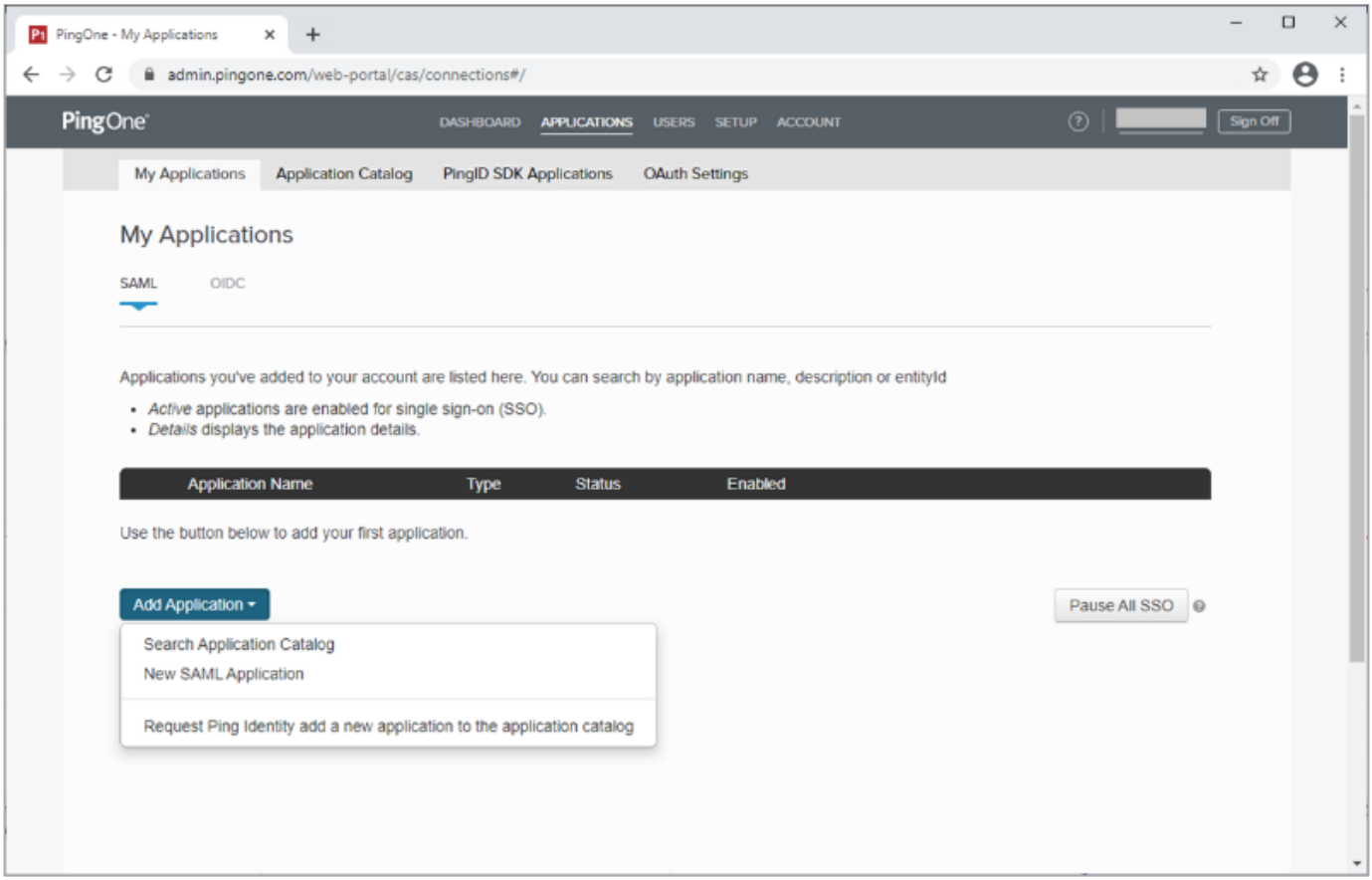
Attribute Name	Description	Required / Optional
`SAML_SUBJECT`	Email	Required
`givenName`	First Name	Optional
`sn`	Last Name	Optional
`memberOf`	Groups	Optional

Note

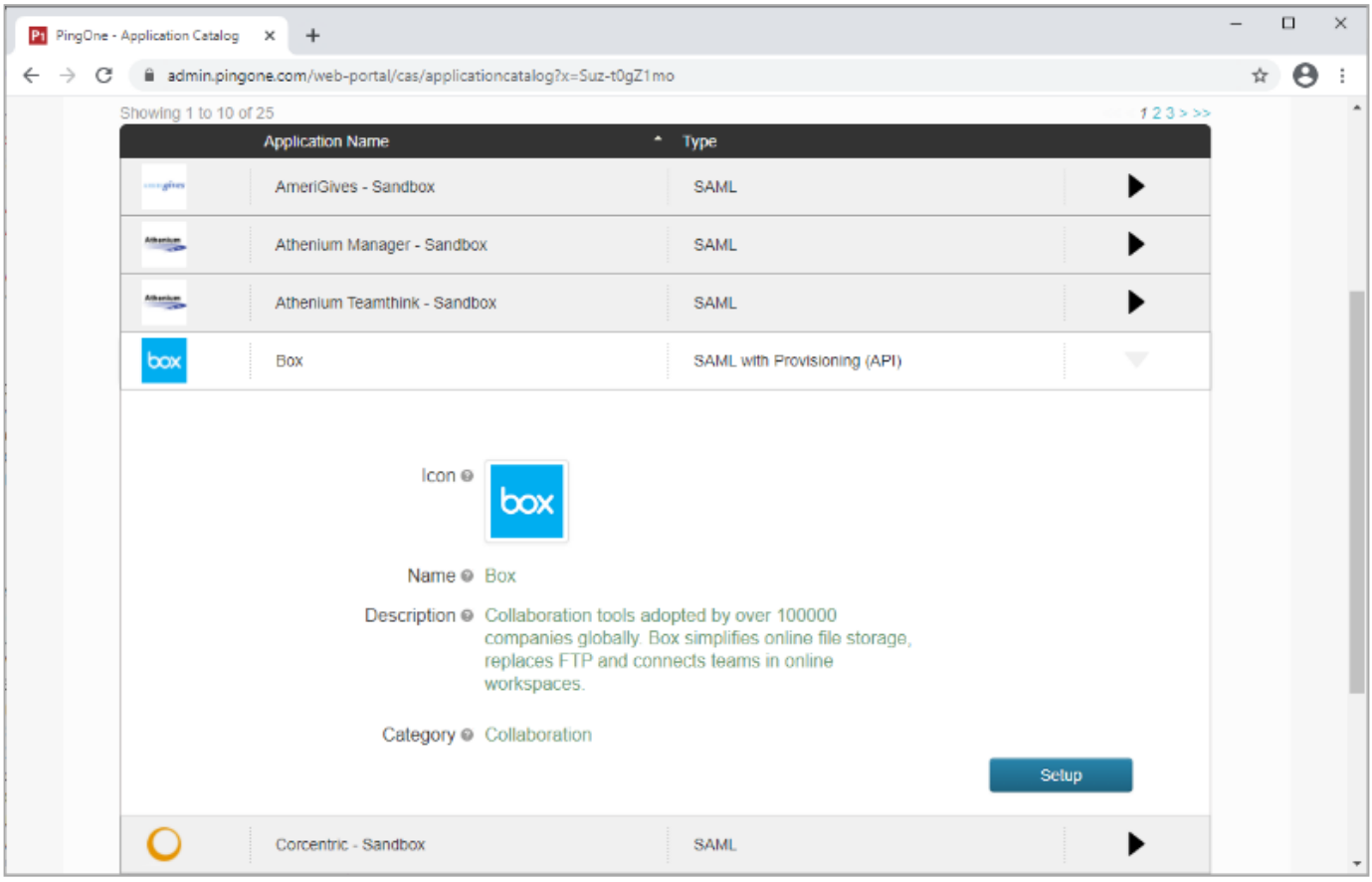
The following configuration is untested and is provided as an example. Additional steps might be required.

Create a PingOne for Enterprise application for Box

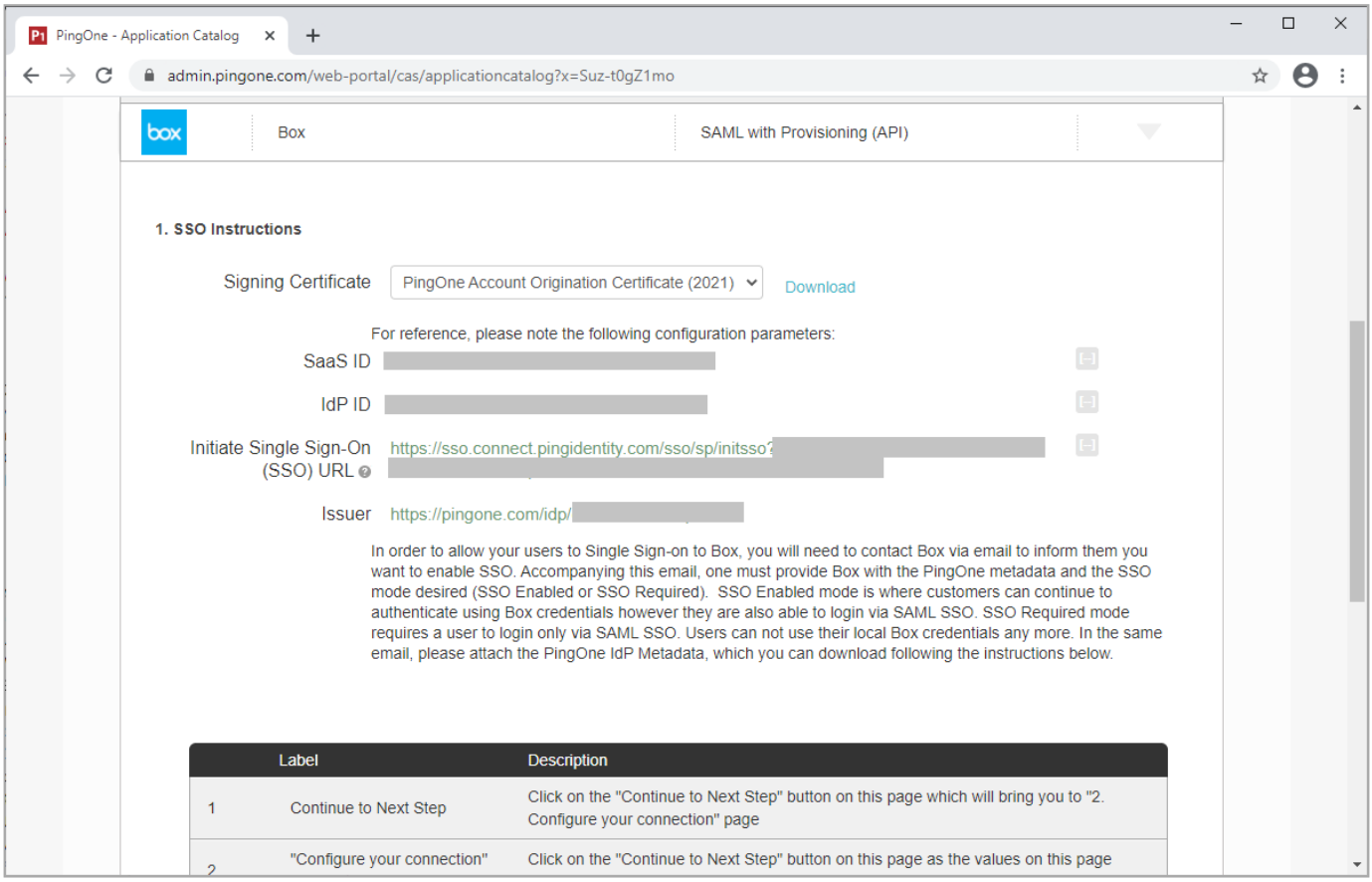
1. Download the Box metadata from https://cloud.app.box.com/s/9y0zm1sqgvkxe8ha2qa3dfhwoivpoyy4.
2. Sign on to PingOne for Enterprise and click **Applications**.
3. On the **SAML** tab, click **Add Application**.



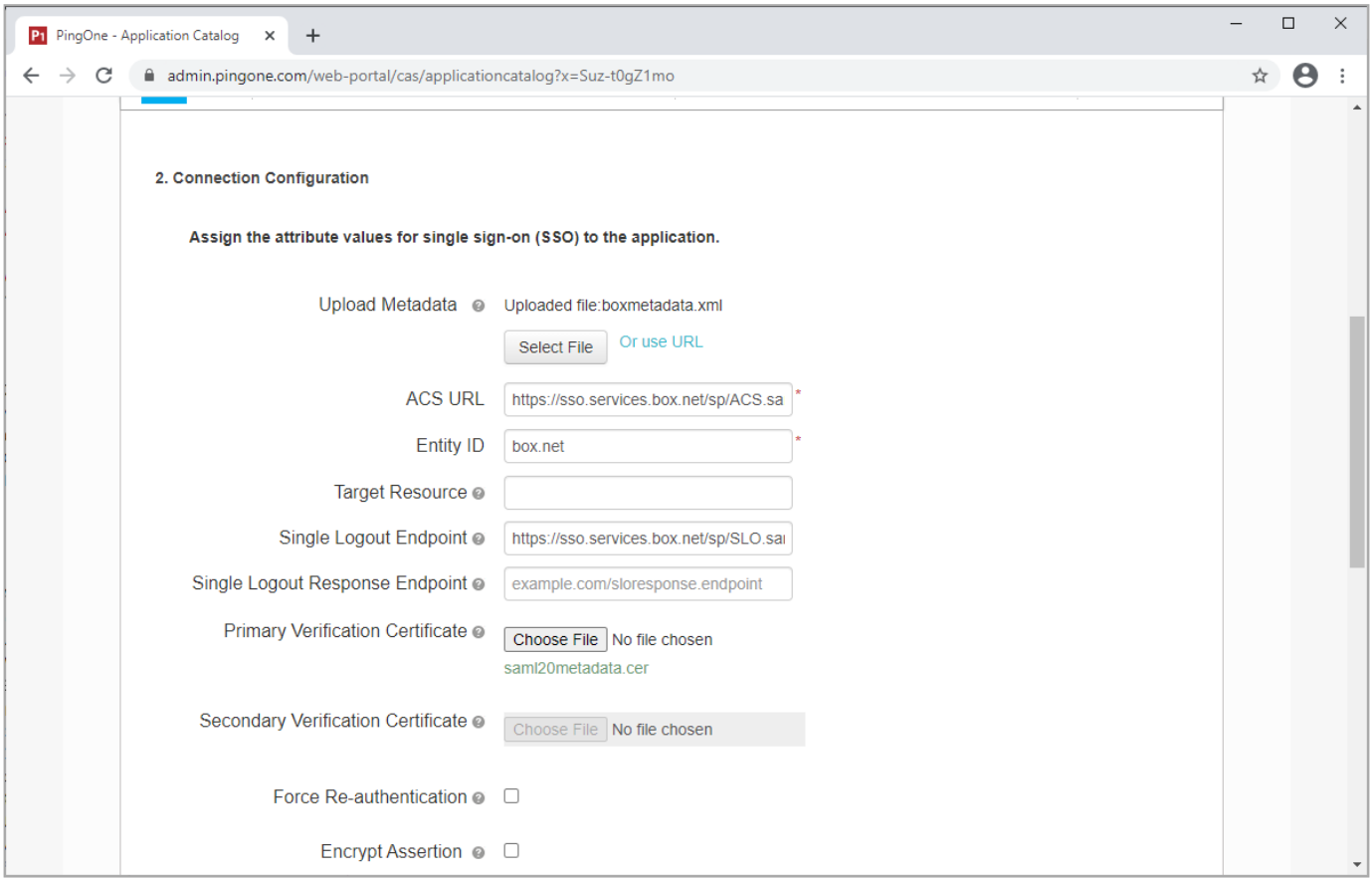
4. Click **Search Application Catalog** and search for `Box`.
5. Click the **Box** row.



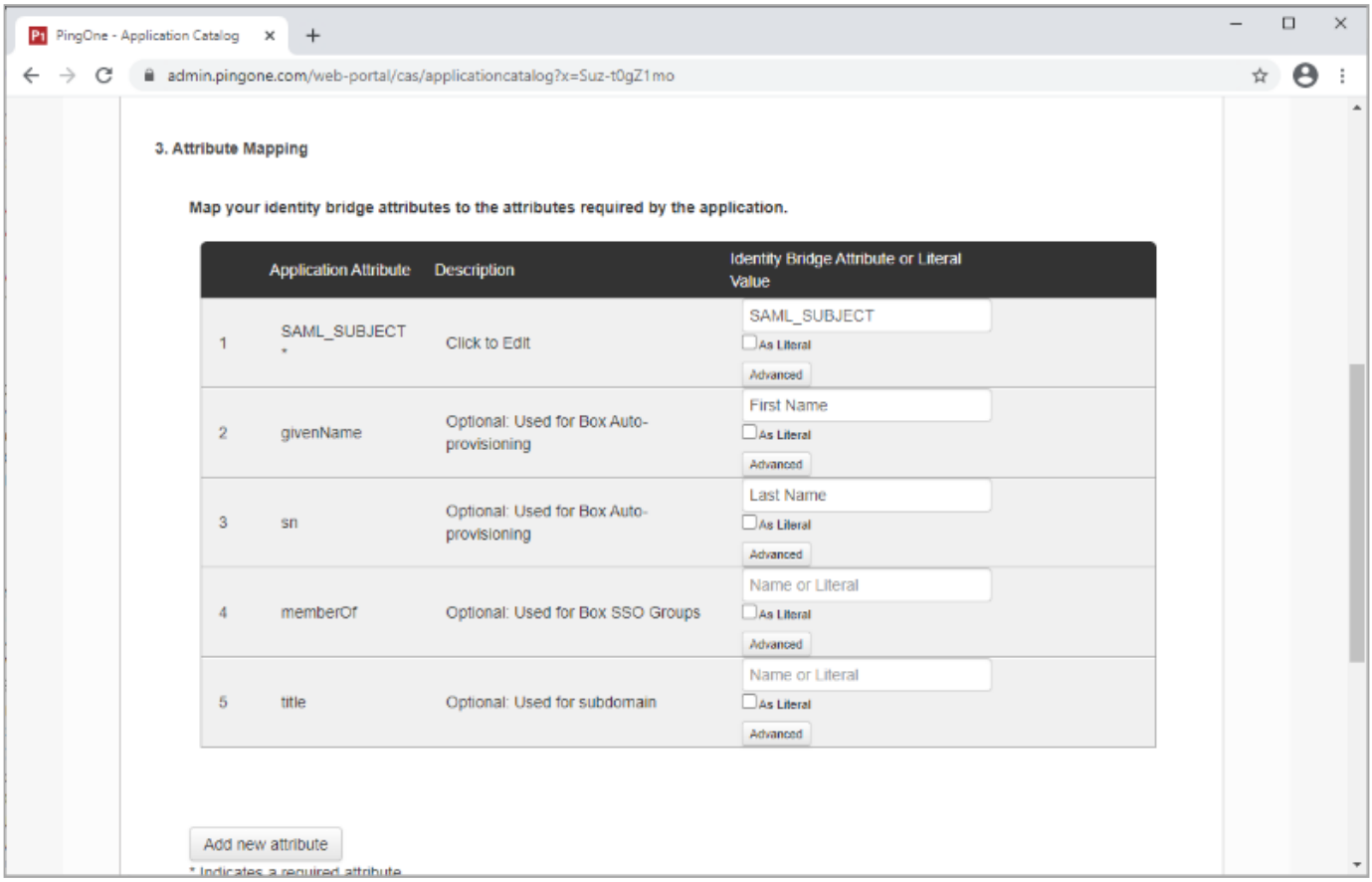
6. Click **Setup**.
7. Select the appropriate signing certificate.
8. Review the steps, and note the **PingOne for Enterprise SaaS ID**, **IdP ID**, **Initiate Single Sign-on (SSO) URL**, and **Issuer** values.



1. Click **Continue to Next Step**.
2. In the **Upload Metadata** section, click **Select File**, and upload the Box metadata file that you downloaded.
3. Ensure that **ACS URL** is set to `https://sso.services.box.net/sp/ACS.saml2` and **Entity ID** is set to `box.net`.

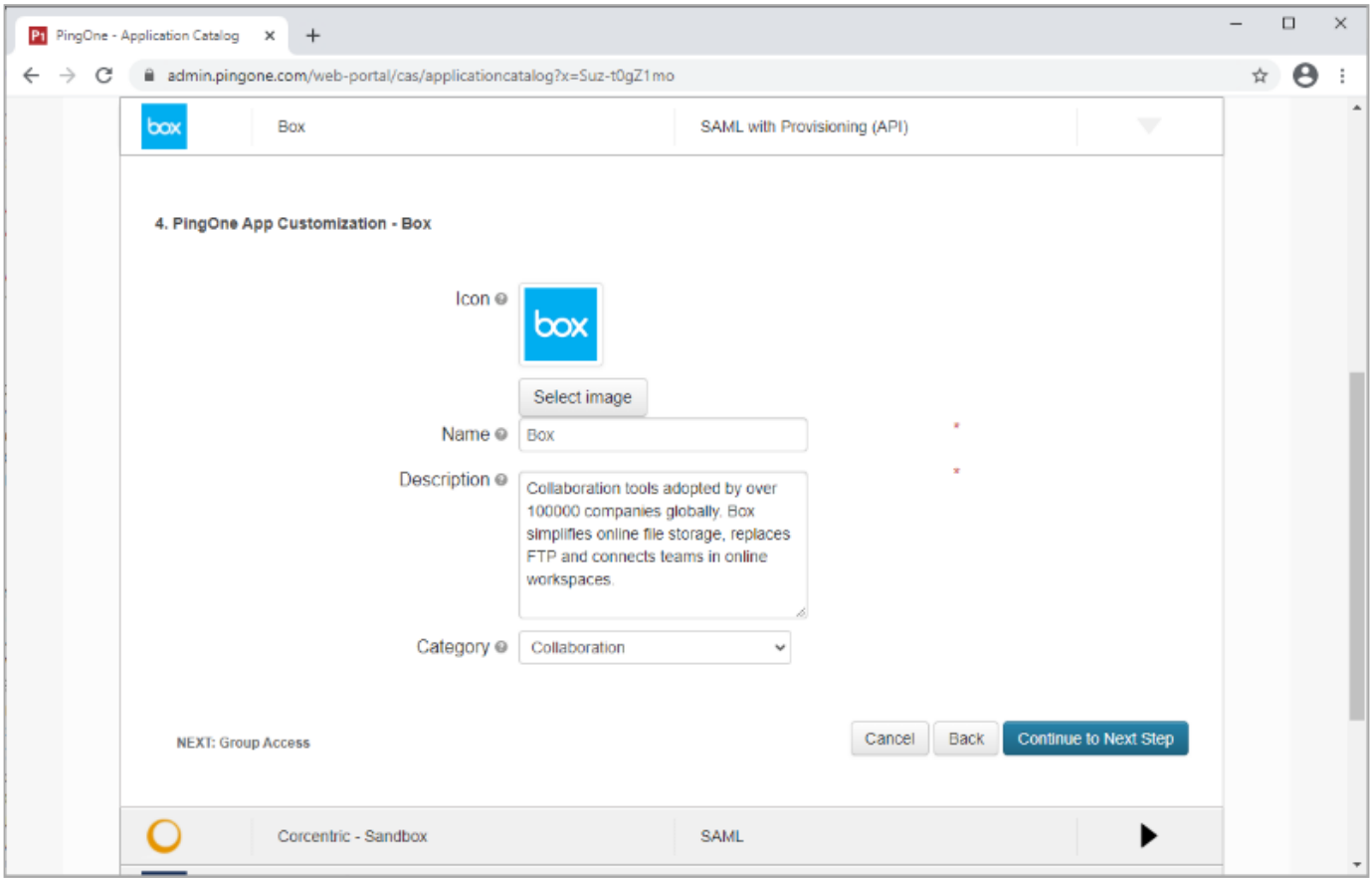


9. Click **Continue to Next Step**.
10. In the Attribute Mapping section, in the **Identity Bridge Attribute or Literal Value**column of the **SAML_SUBJECT**row, select the attribute **SAML_SUBJECT**.
11. Complete the remaining attribute mappings for **givenName**, **sn**, **memberOf**, and **title**.



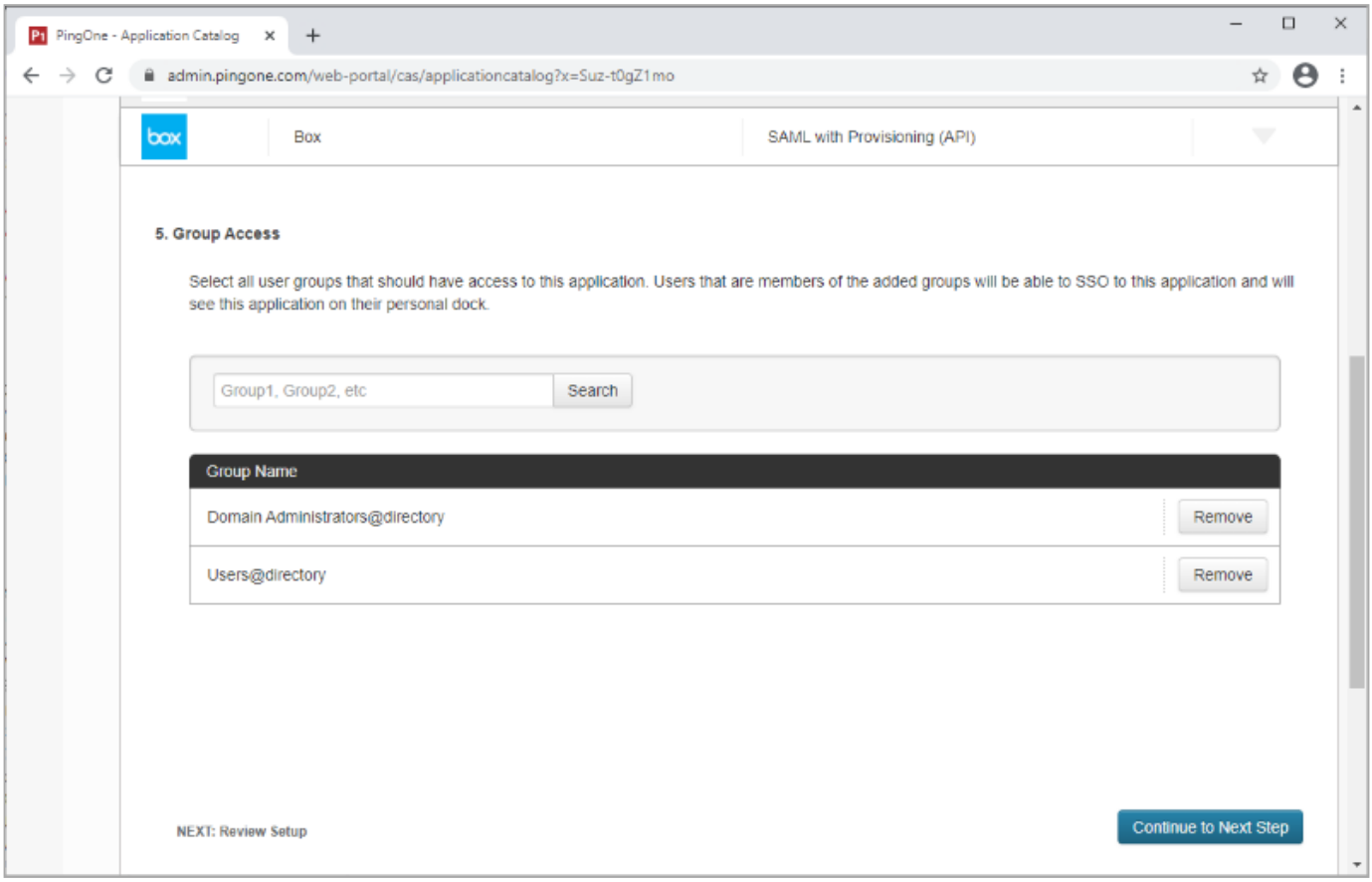
12. Click **Continue to Next Step**.

13. Update the **Name**, **Description**, and **Category** fields as required.



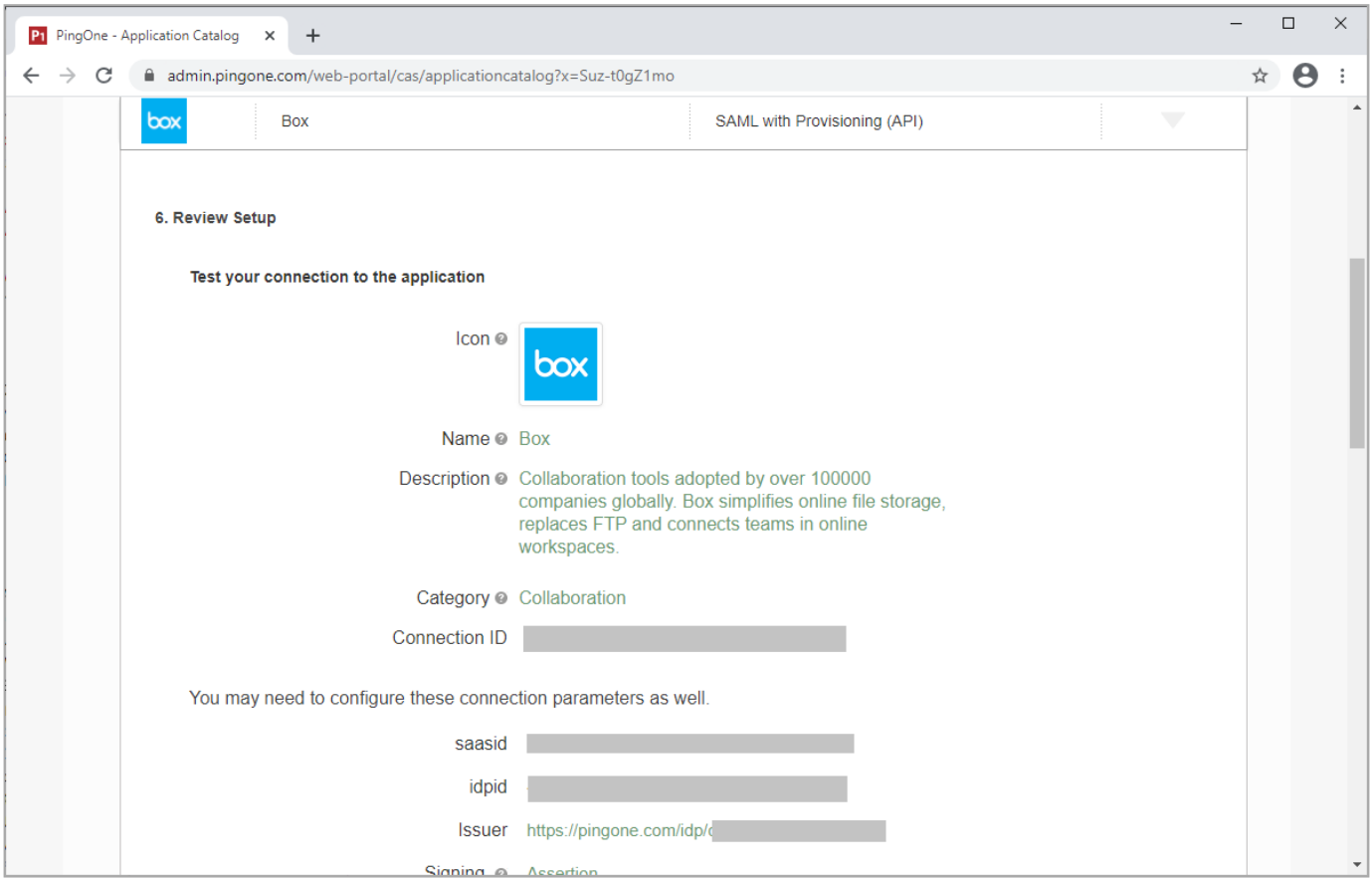
14. Click **Continue to Next Step**.

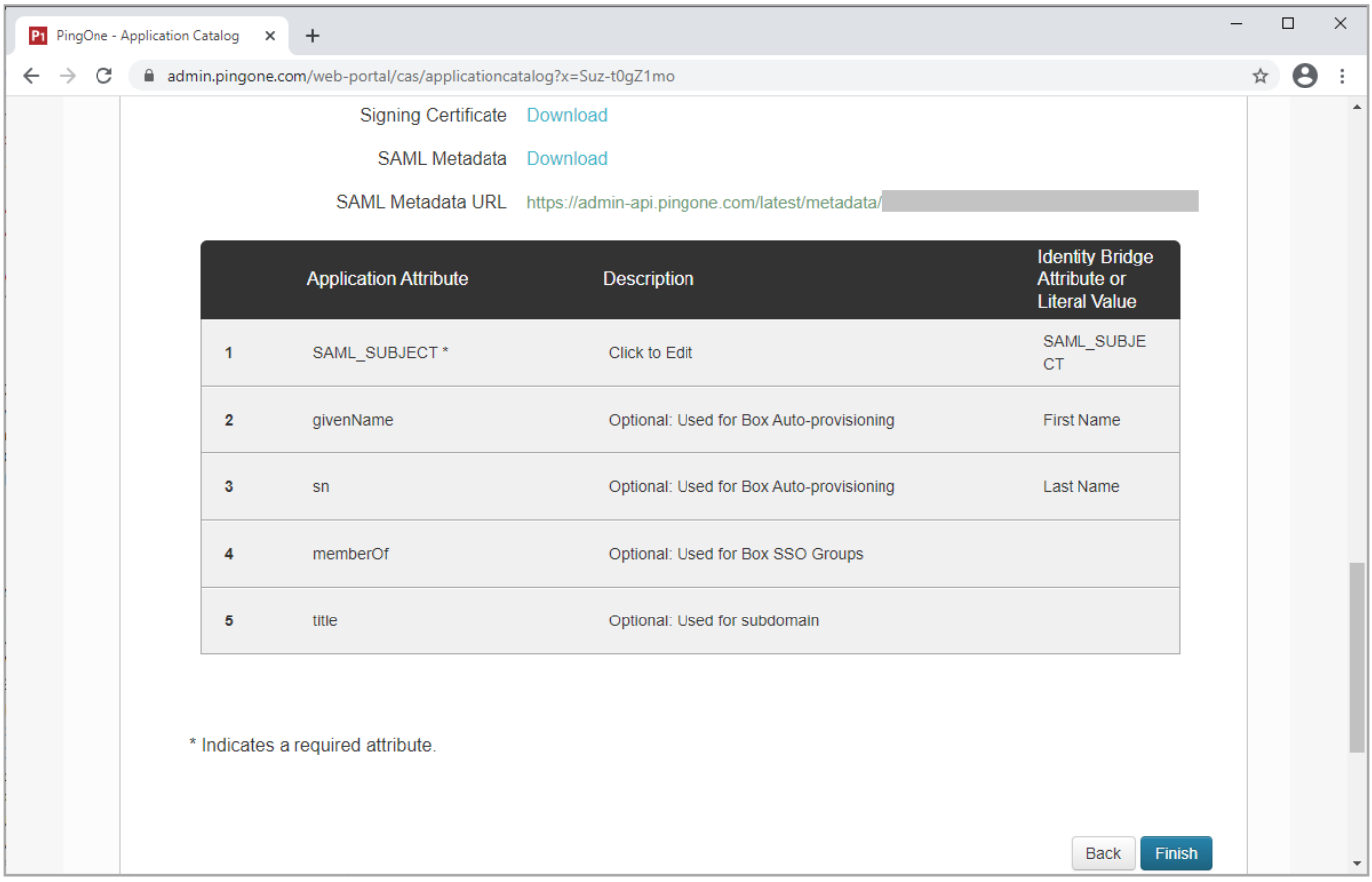
15. Add suitable user groups for the application.



16. Click **Continue to Next Step**.

17. Review the settings.





18. Copy the **Single Sign-On (SSO) URL** value to a temporary location.

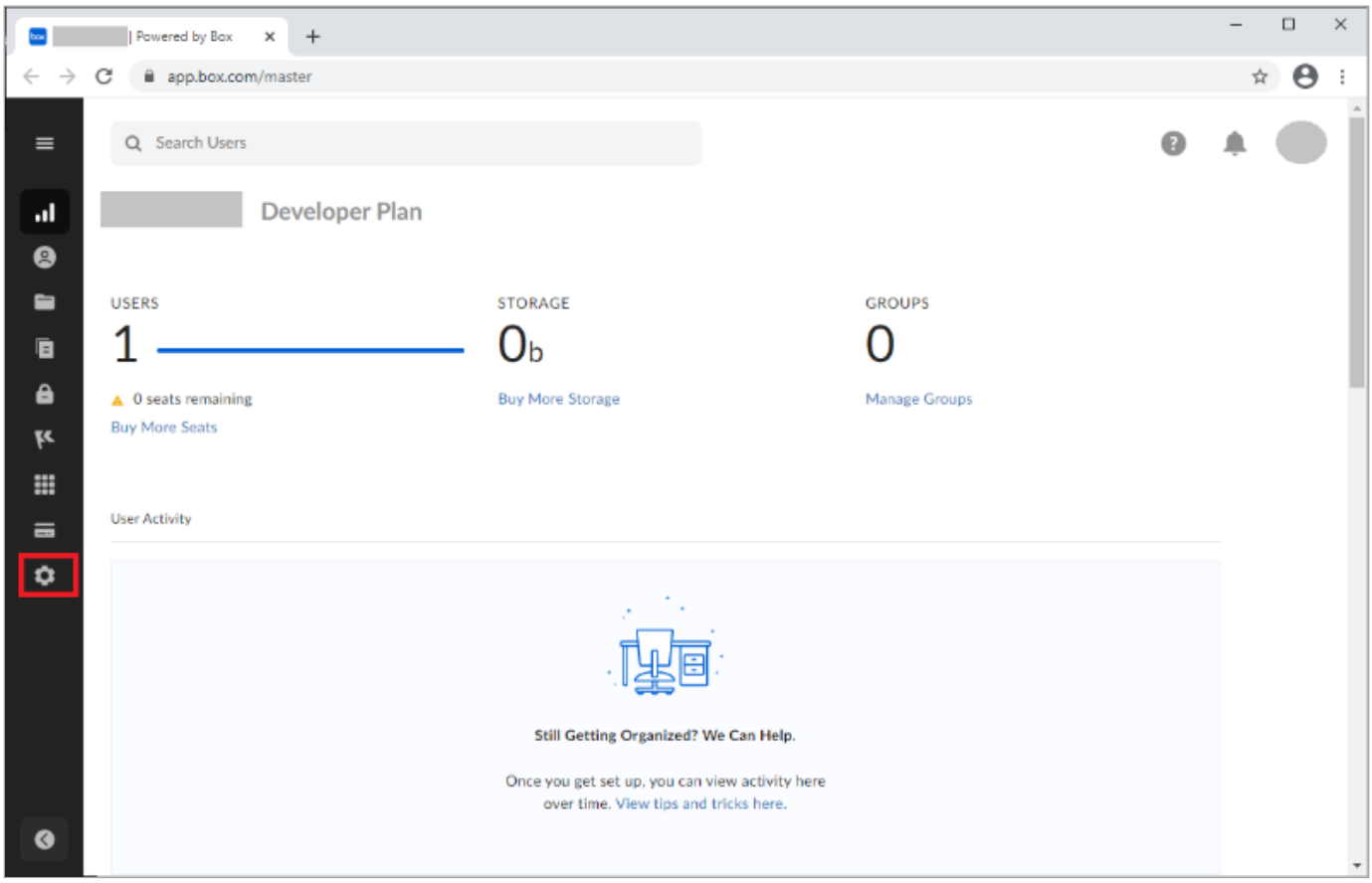
    This is the IdP-initiated SSO URL that you can use for testing.

19. On the **SAML Metadata** row, click **Download**. You will use this for the Box configuration.

20. Click **Finish**.

Configure the PingOne for Enterprise IdP connection for Box

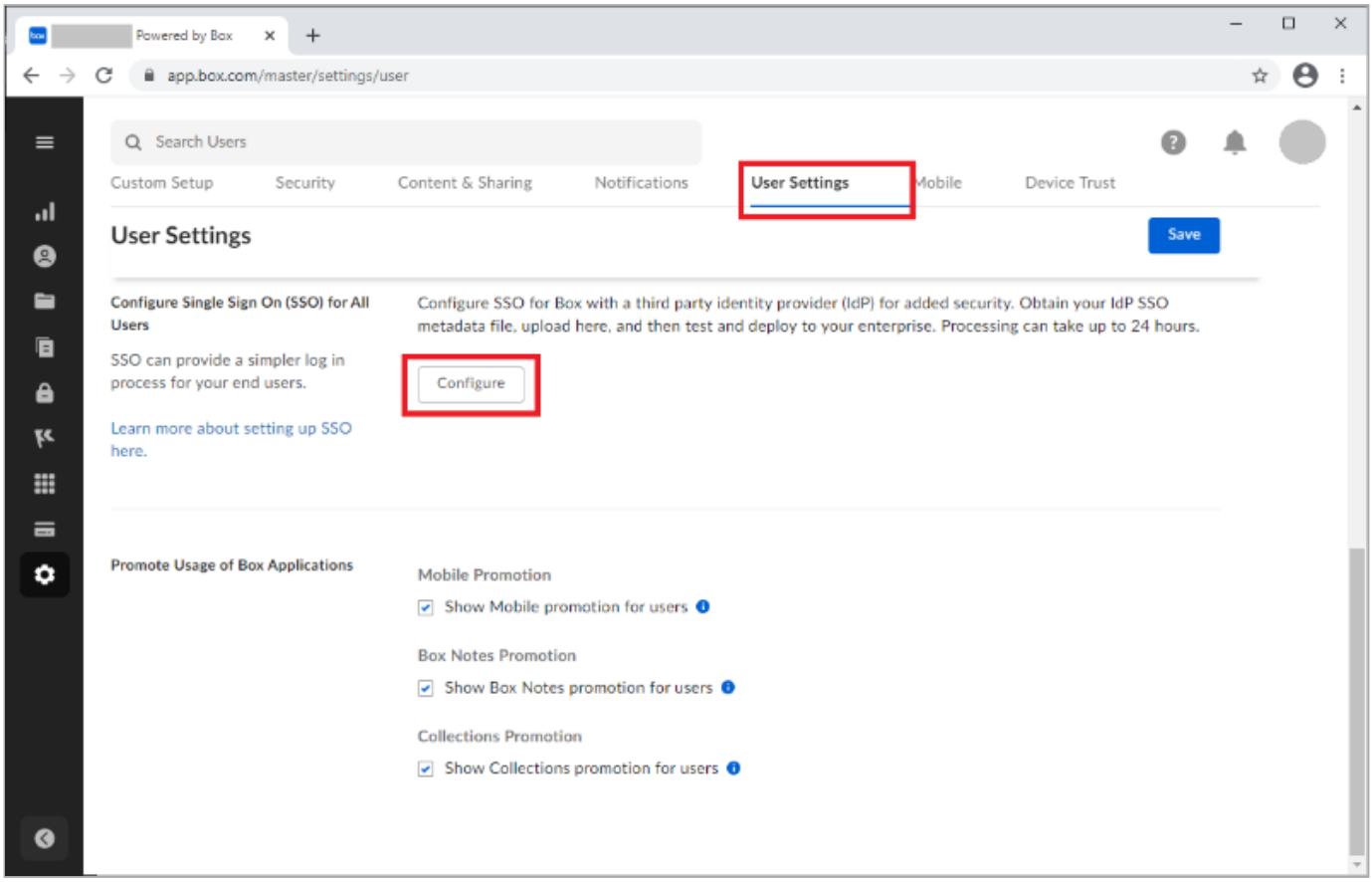
1. Sign on to the Box Admin Console as an administrator.



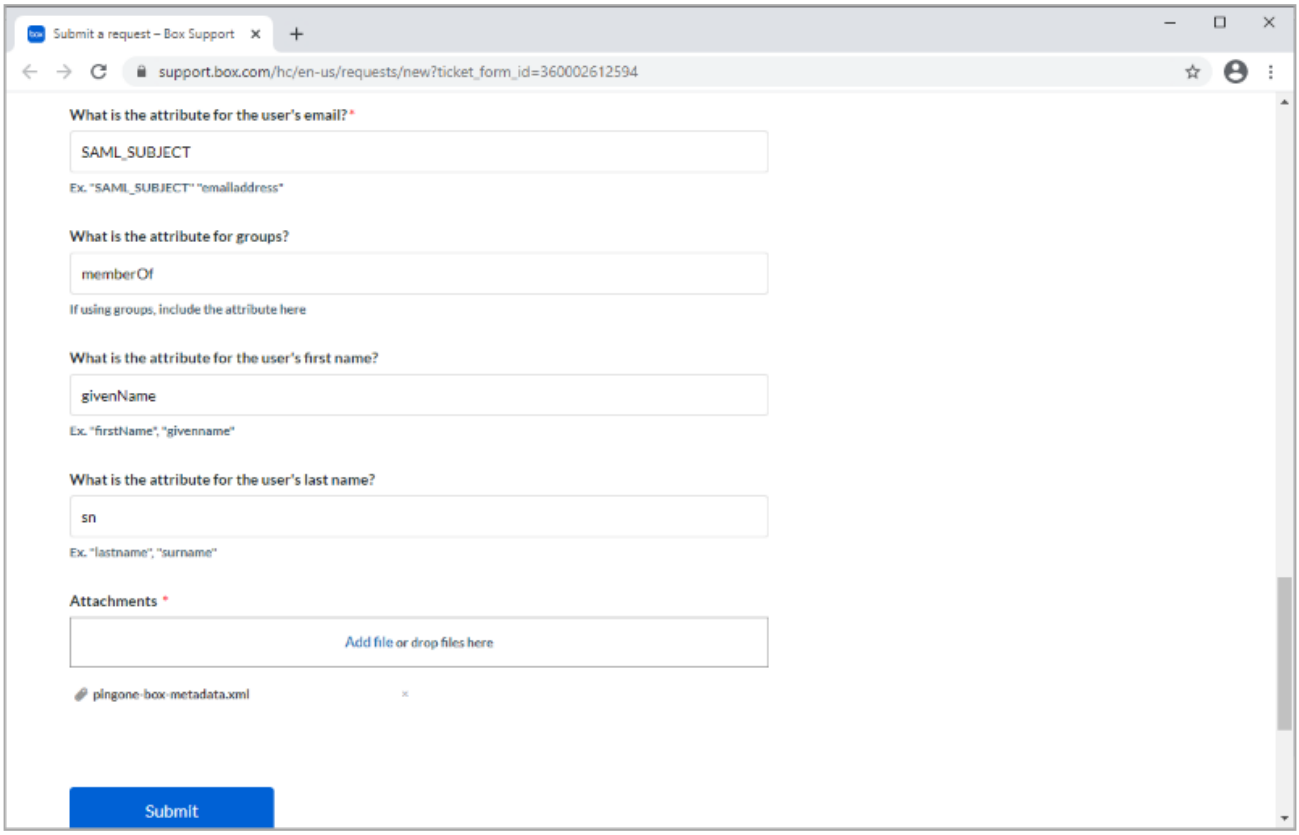
2. Click **Enterprise Settings**.

3. Click the **User Settings** tab.

4. In the **Configure Single sign-on (SSO) for All Users** section, click **Configure**.



5. Click **I don't see my provider, or don't have a metadata file.**
6. Complete the **Box SSO Setup Support Form**:
    - Review the request form and the **For faster service please read** section.
    - Complete all the required fields.
        - For **Who is your Identity Provider**, select **Other with Metadata**.
        - For **What is the attribute for the user's email?**, select **SAML_SUBJECT**.
        - For **What is the attribute for groups?**, select **memberOf**.
        - For **What is the attribute for the user's first name?**, select **givenName**.
        - For **What is the attribute for the user's last name?**, select **Sn**.
        - Attach the metadata that you downloaded from the PingOne for Enterprise configuration.
    - Click **Submit**.



7. After the Box support team completes the configuration, follow any provided instructions and test the integration.

Cloudflare

Configuring SAML SSO with Cloudflare and PingFederate

Learn how to direct Cloudflare sign on using PingFederate (SP-initiated sign-on).

Before you begin

- Configure PingFederate to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- PingFederate's X.509 certificate should be exchanged to verify the signature in SAML assertions.
- An **Email Attribute** is required in the assertion, either the **SAML Subject** or another SAML attribute per the SAML configuration. The value of the **Email Attribute** must be a valid email address. It is used to uniquely identify the user in the organization.
- Populate Cloudflare with at least one user to test access.

Create a PingFederate service provider (SP) connection for Cloudflare:

1. Sign on to the PingFederate administrative console.
2. Create an SP connection for Cloudflare in PingFederate:
    1. Configure using **Browser SSO** profile **SAML 2.0**.
    2. Set **Partner's Entity ID** to `https://team name.cloudflareaccess.com/cdn-cgi/access/callback`.
    3. Enable the **IDP-Initiated SSO** and **SP-Initiated SSO** SAML profiles.
    4. In **Assertion Creation: Attribute Contract**, select **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress** for **SAML_SUBJECT**.
    5. In **Assertion Creation: Authentication Source Mapping: Authentication Source Mapping**, map a new **Adapter Instance** to **HTML Form**.
    6. In **Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment**, map **SAML_SUBJECT**.
    7. In **Protocol Settings: Assertion Consumer Service URL**, set **Binding** to **POST** and set **Endpoint URL** to `/cdn-cgi/access/callback`.

        > **Note**
        > This value is received and updated from Cloudflare.

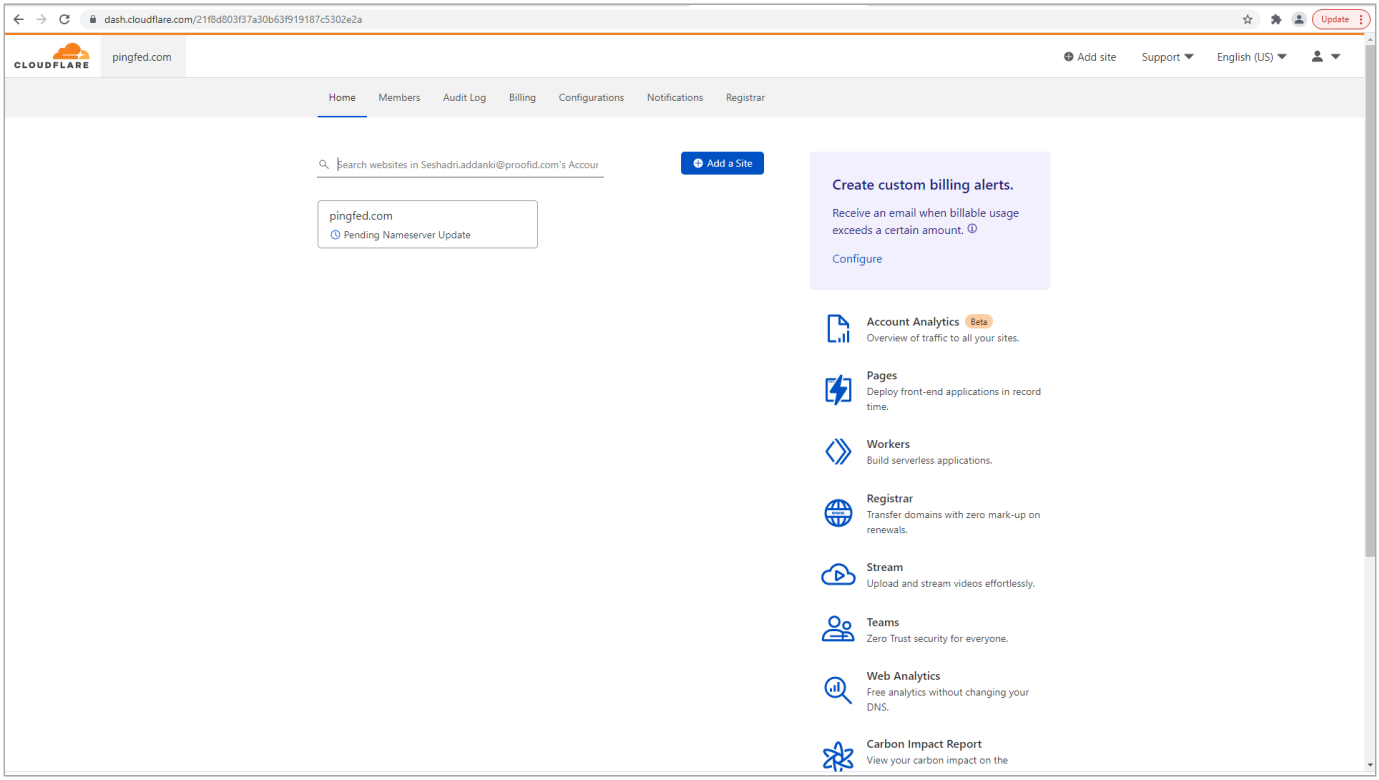
    8. In **Protocol Settings: Allowable SAML Bindings**, enable **POST**.

9. In **Signature Policy**, disable **Always Sign Assertion** and leave **Sign Response As Required** enabled.
10. In **Credentials: Digital Signature Settings**, select the **PingFederate Signing Certificate**, the **Include the Certificate in the Signature *KEY INFO* Element**, and the **Include the Raw Key in the Signature *KEY INFO* Element** check boxes.

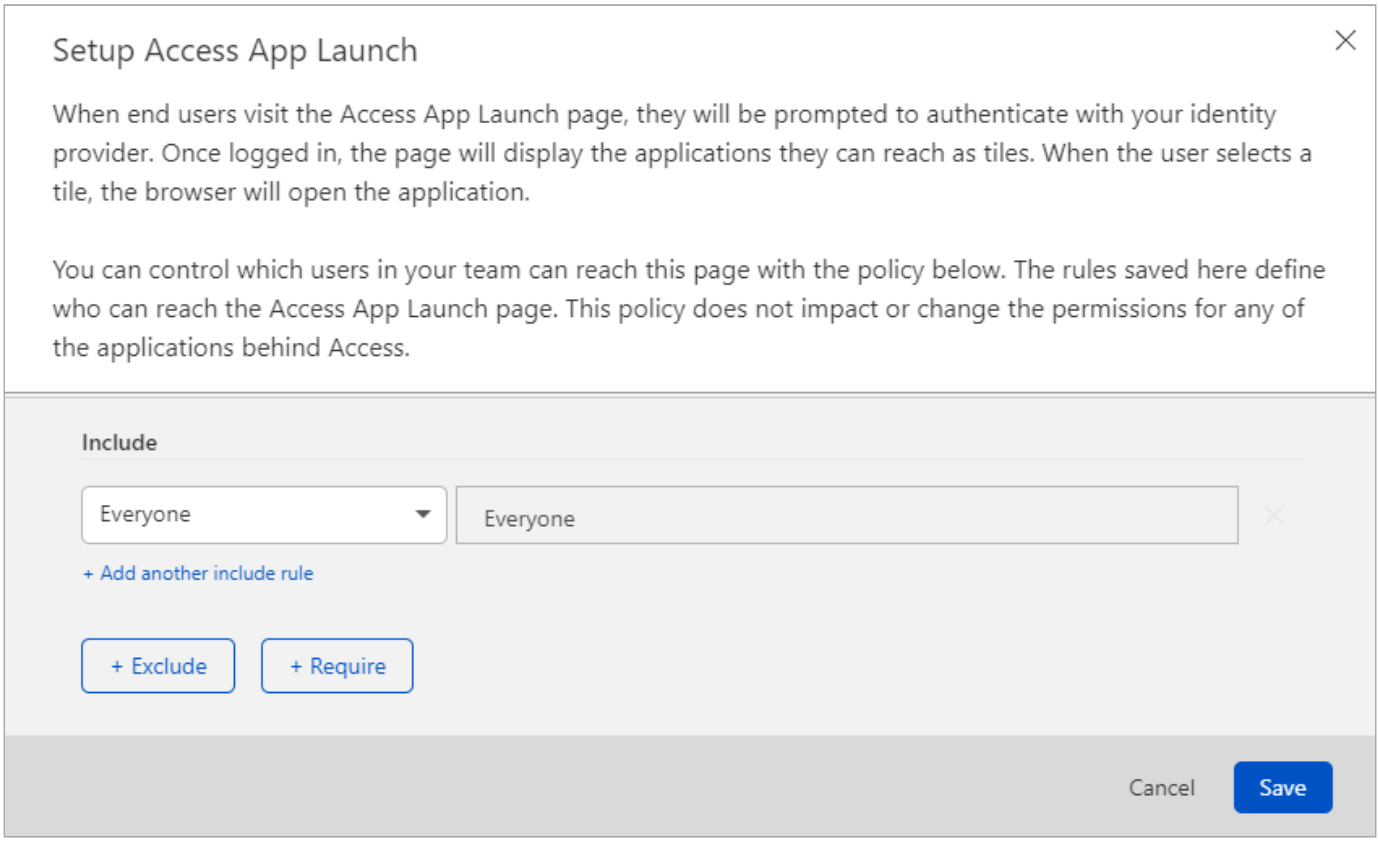
3. Save the configuration.
4. Export the signing certificate.
5. Export and then open the metadata file, and copy the value of:
   - The **entityID**
   - The **Location** entry (`https://your value/idp/SSO.saml2`)

Add the PingFederate IdP connection to Cloudflare

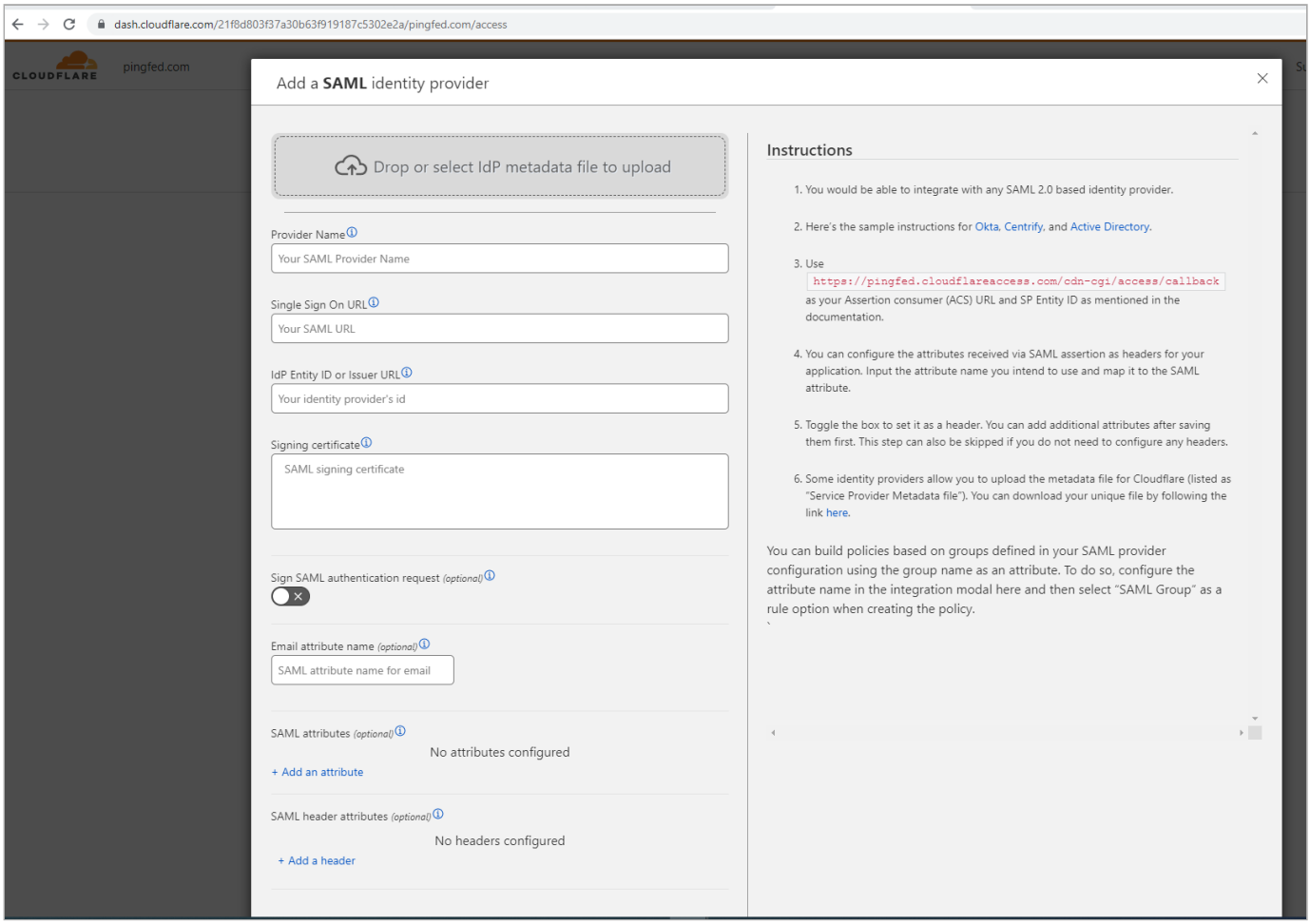
1. Sign on to the Cloudflare application and click **pingfed.com** at the top of the page.



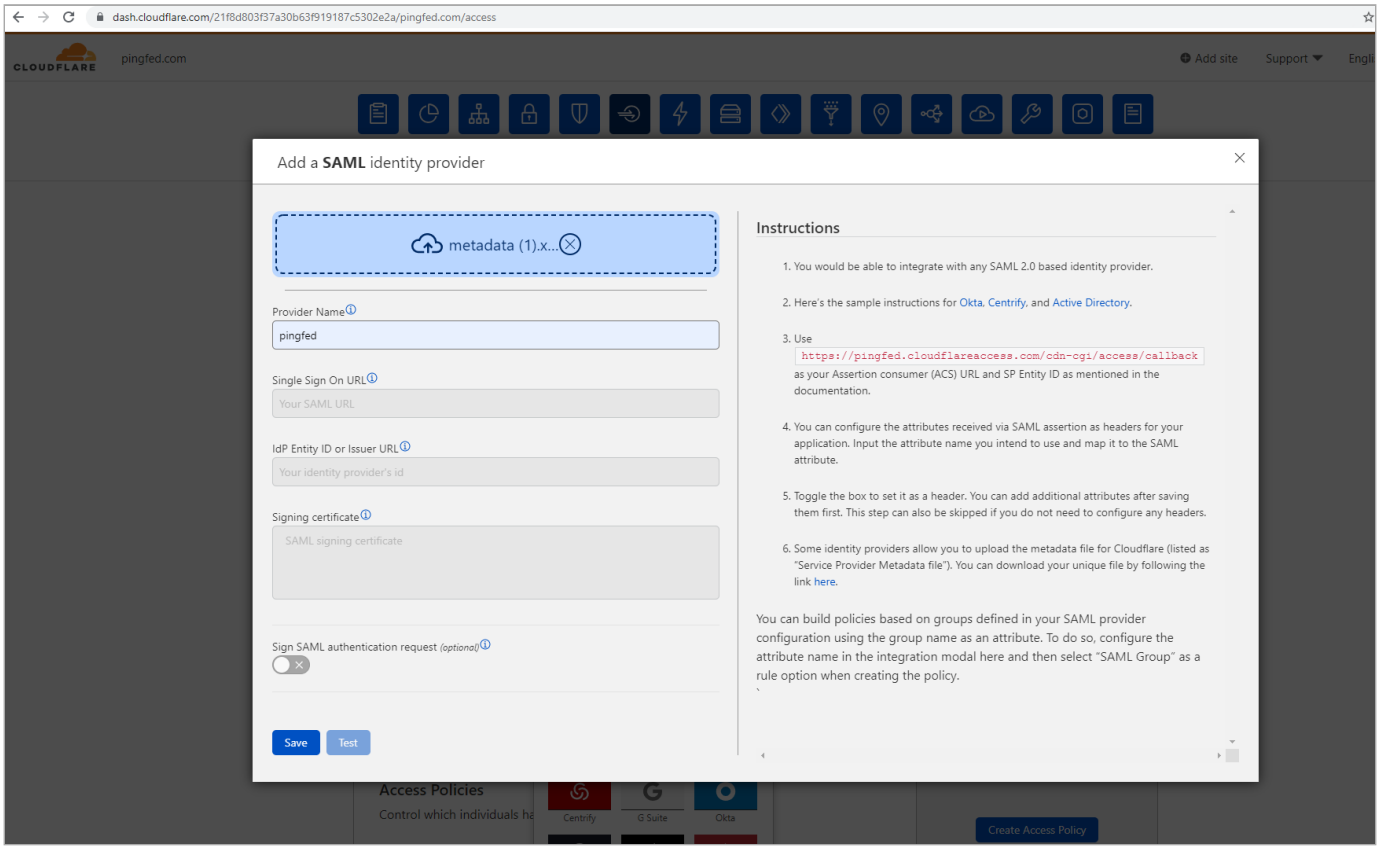
2. Go to **Access → Access App Launch → Setup Access App Launch**.



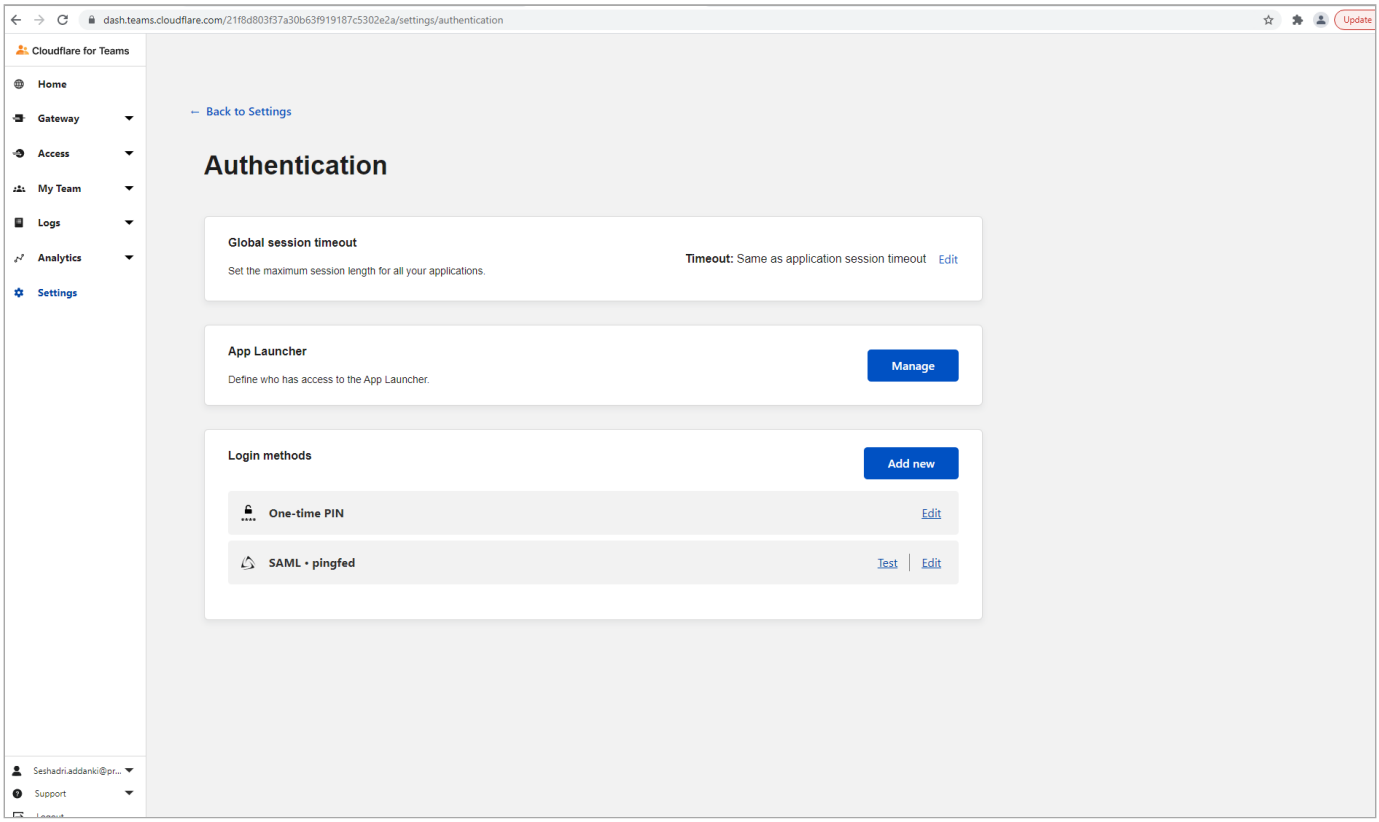
3. Click **Save**.
4. Go to **Access → Login Methods → Add → SAML**.



5. Click **Drop or select IdP metadata file to upload** to upload the IdP metadata file and enter the **Provider Name** value.

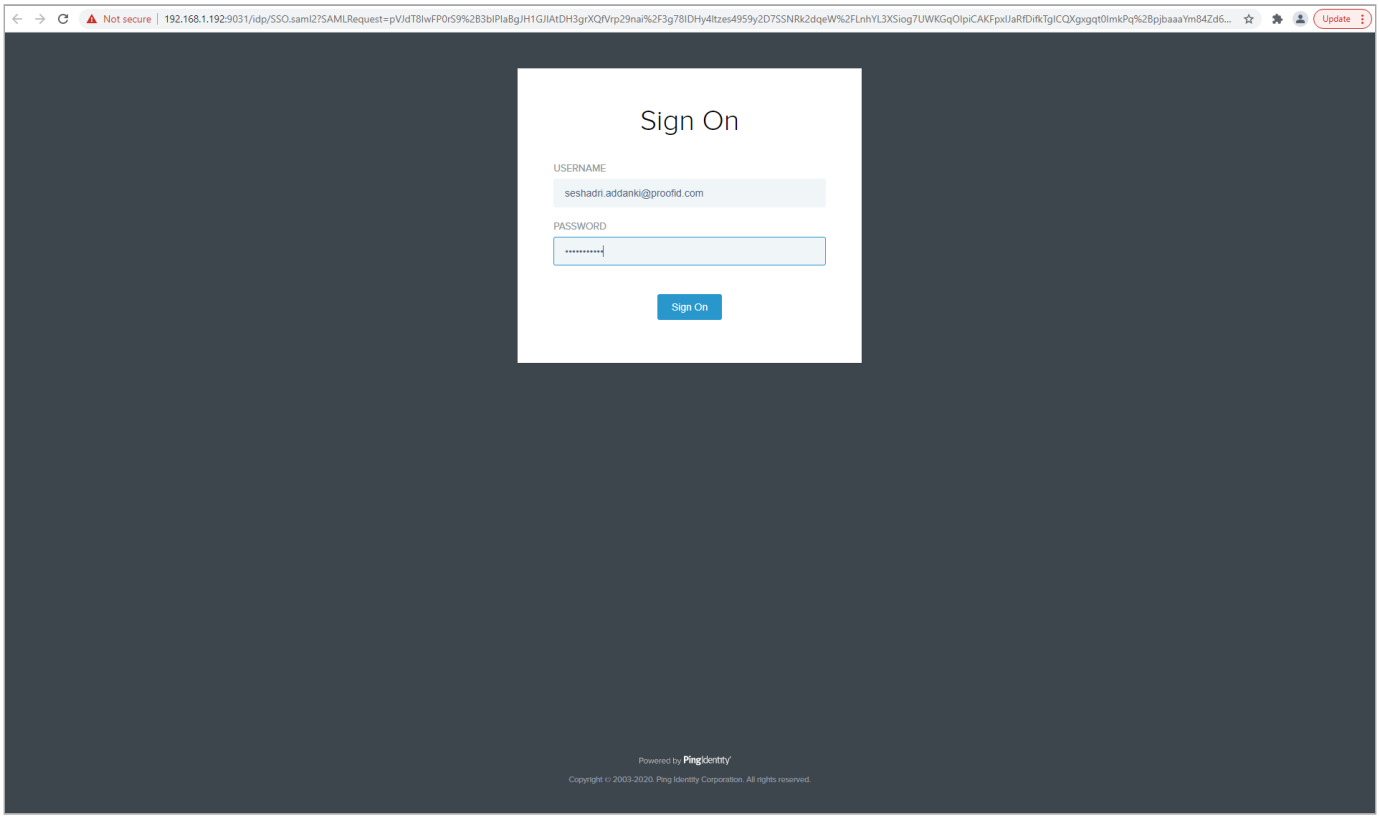


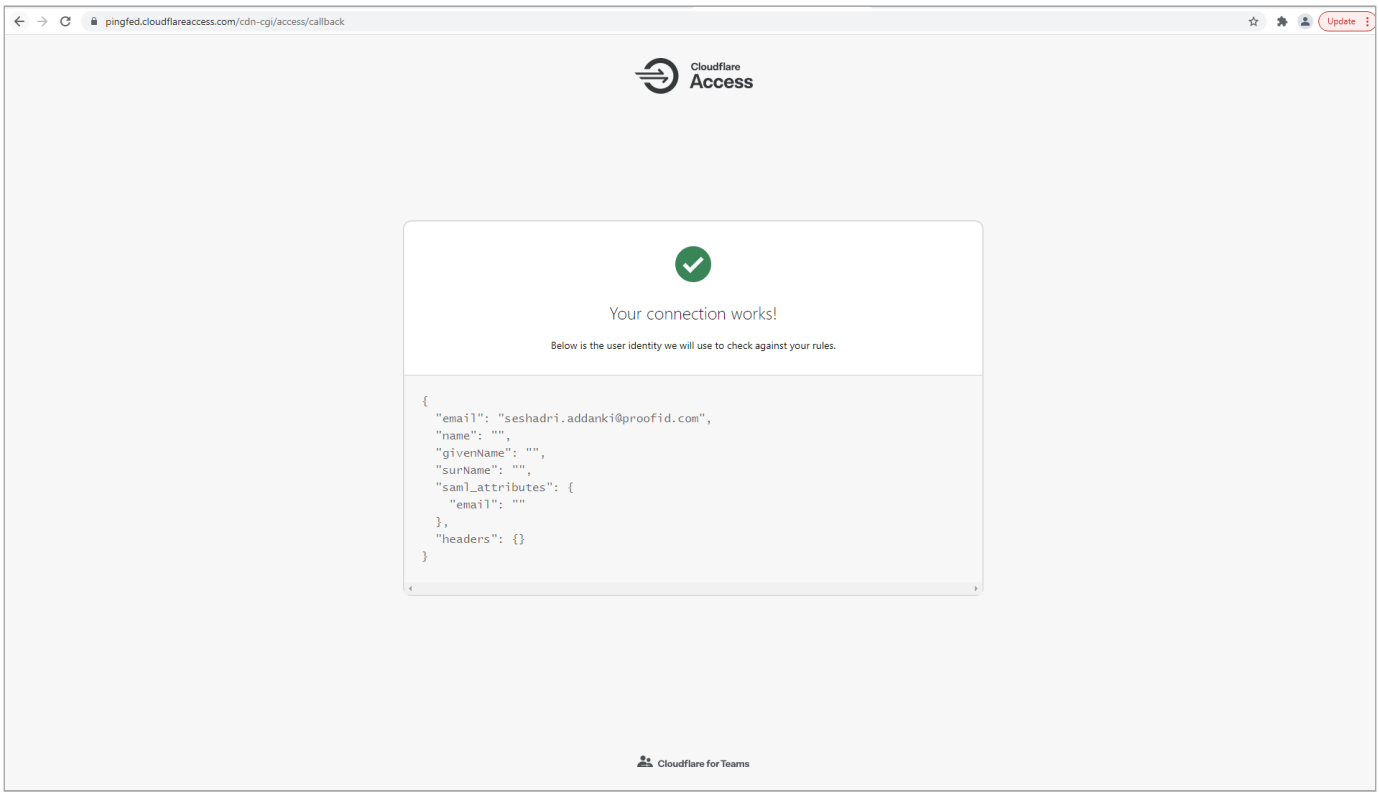
6. Click **Save** and close the **Login Method** page.
7. On the **Teams** dashboard, go to **Settings → Authentication**.
8. In the **Login methods** section, select **SAML + Pingfed**.



The Cloudflare connection configuration is now complete.

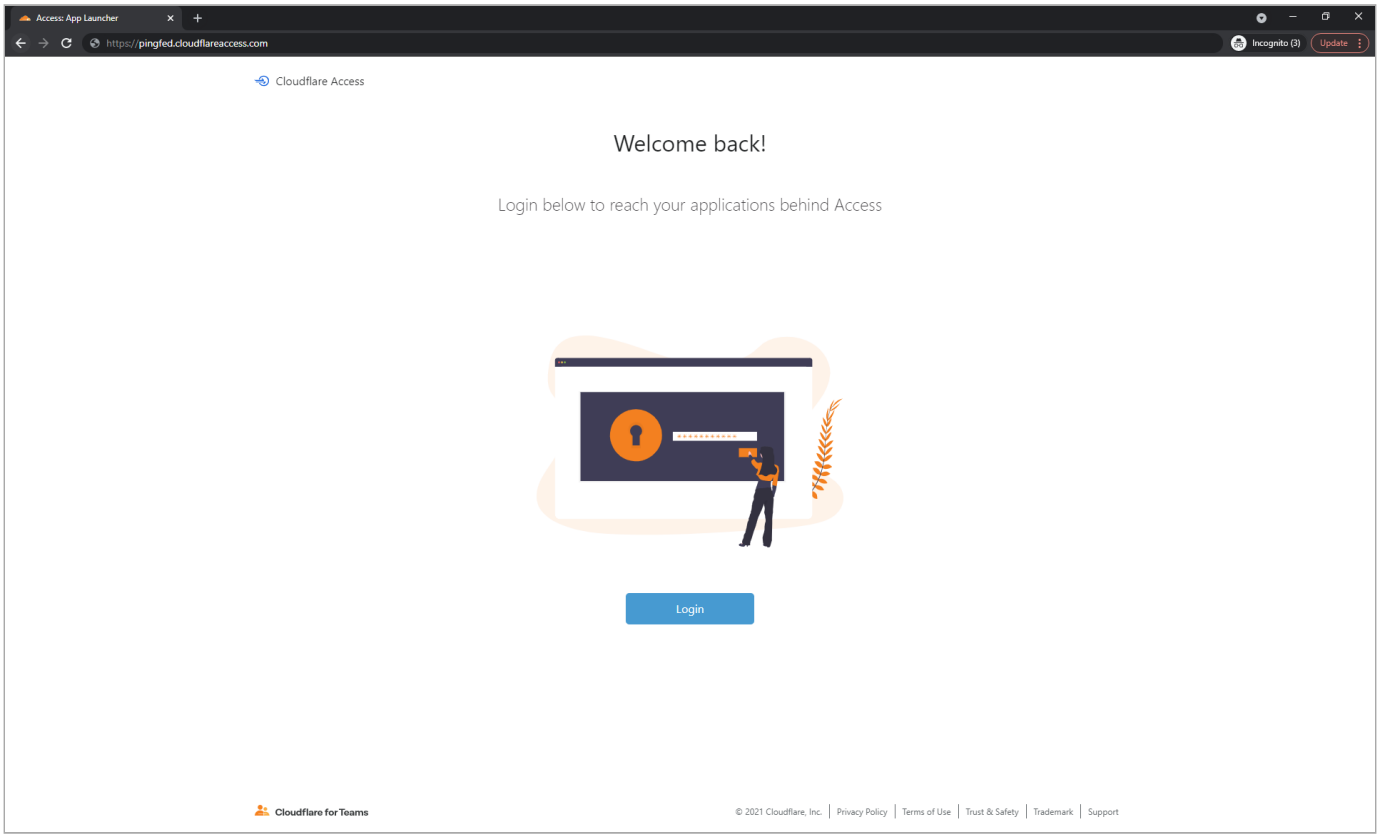
9. Click **Test**.
10. After the Cloudflare application redirects to PingFederate, enter the credentials.



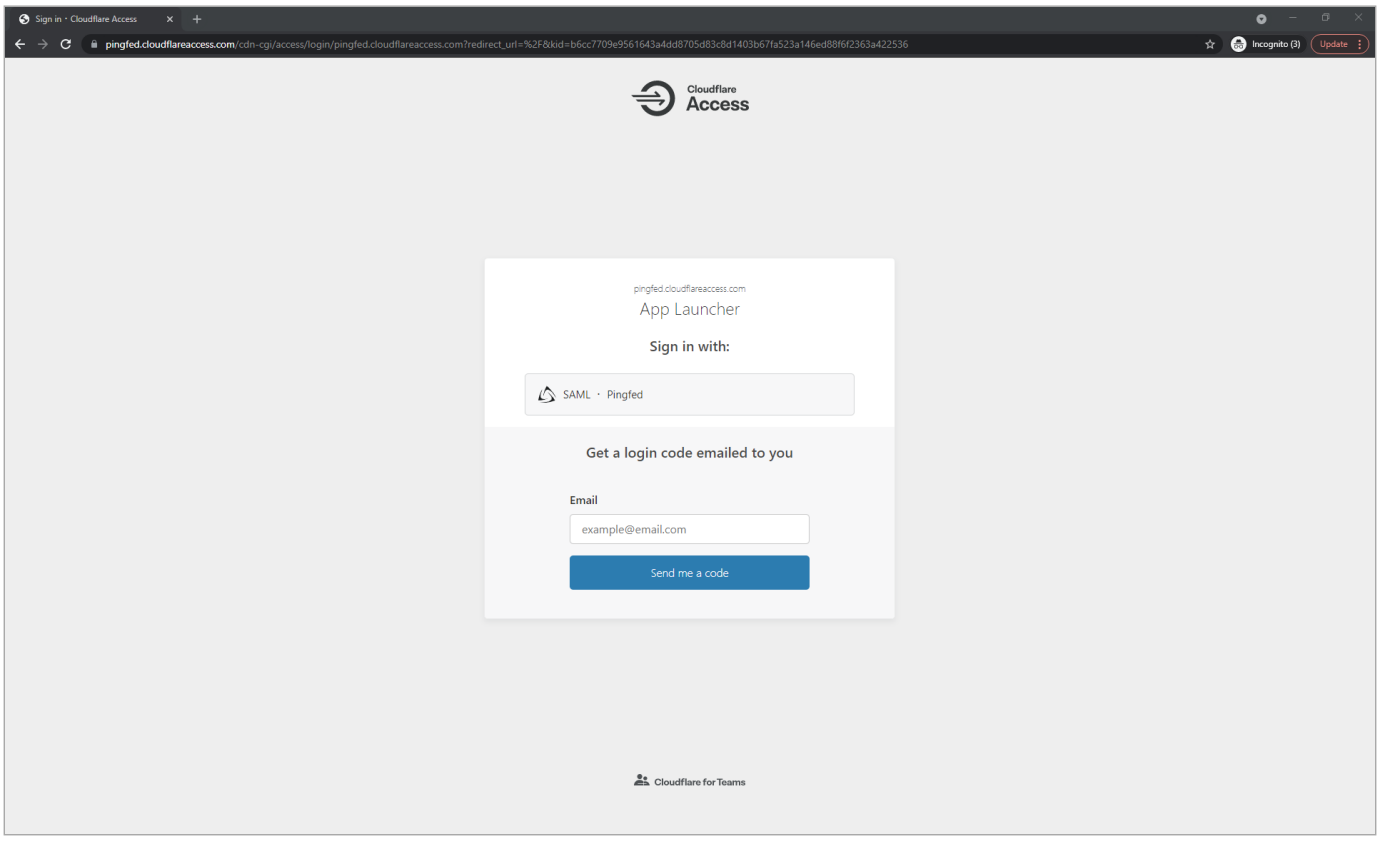


Test the PingFederate SP-initiated SSO integration

1. Go to your **Cloudflare Authentication Request URL** (for example, https://pingfed.cloudflareaccess.com/) and click **Login**.



2. Click **SAML– PingFed**.



3. After you're redirected to PingFederate, enter your PingFederate username and password.

   After successful authentication, you're redirected back to Cloudflare.

Coupa

Configuring SAML SSO with Coupa and PingFederate

Learn how to enable Coupa sign-on from a PingFederate URL (IdP-initiated sign-on) and direct Coupa sign-on using PingFederate (SP-initiated sign-on).

Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate Coupa with at least one user to test access.
- You must have administrative access to PingFederate and Coupa.

Download the Coupa metadata

1. Sign on to your Coupa Admin organization as an administrator.
2. Go to `https://your_site.coupahost.com/administration/security`.
3. Select the **Sign in using SAML** check box.
4. Click the **Download and import SP metadata** link.
5. Save the Coupa metadata.

Create a PingFederate SP connection for Coupa

1. Sign on to the PingFederate administrative console.
2. Create an SP connection for Coupa in PingFederate using the Coupa metadata:
    1. Configure using **Browser SSO** profile **SAML 2.0**.
        - Enable the following **SAML Profiles**:
            - **IdP-Initiated SSO**
            - **SP-Initiated SSO**
        - In **Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment**, map **SAML_SUBJECT** to the attribute containing a user's email address.
        - In **Protocol Settings: Allowable SAML Bindings**, enable **POST**.
        - In **Credentials: Digital Signature Settings** select the PingFederate signing certificate.
3. Save the configuration.

4. Export the signing certificate.
5. Export the metadata file.

Add the PingFederate IdP Connection to Coupa

1. Sign on to your Coupa Admin organization as an administrator.
2. Go to `https://your_site.coupahost.com/administration/security`.
3. Make sure that the **Sign in using SAML** check box is selected.
4. In the **Upload IdP metadata** section, click **Choose File**.
5. Select the PingFederate metadata file and import it.
6. In the **Certificate** field, upload the PingFederate signing certificate.
7. Click **Save**.
8. Click the **Users** tab and edit the users who will use SAML authentication.
9. Set **Single Sign-On ID** to the value users will use to sign on, for example, their email address.
10. Set **Authentication method** to **SAML**.
11. Click **Save**.

Test the PingFederate IdP-initiated SSO integration

1. Go to the PingFederate SSO application endpoint for the Coupa SP connection.
2. Complete PingFederate authentication.

   You're redirected to your Coupa domain.

Test the PingFederate SP-initiated SSO integration:

1. Go to your Coupa URL.
2. After you're redirected to PingFederate, enter your PingFederate username and password.

   You're redirected back to Coupa.

Configuring SAML SSO with Coupa and PingOne for Enterprise

Learn how to enable Coupa sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct Coupa sign-on using PingOne for Enterprise (SP-initiated sign-on).

Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate Coupa with at least one user to test access.

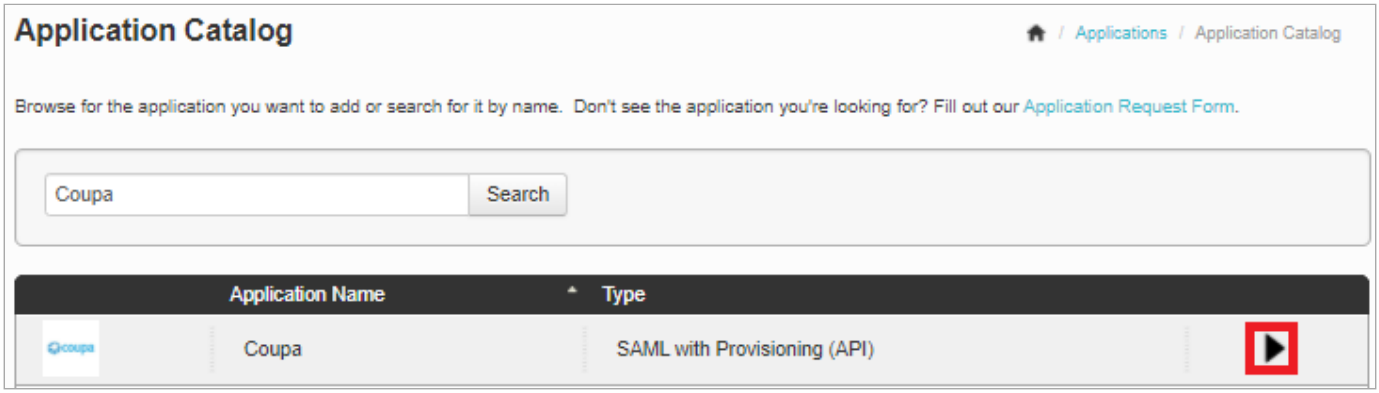
- You must have administrative access to PingOne for Enterprise and Coupa.

Download the Coupa metadata

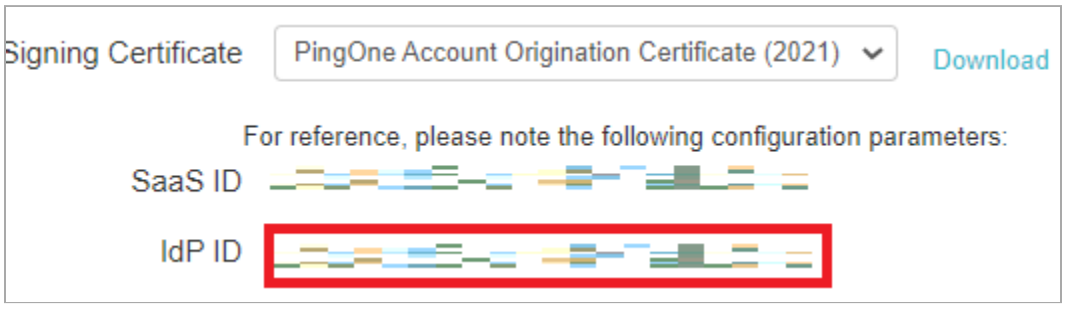
1. Sign on to your Coupa Admin organization as an administrator.
2. Go to `https://your_site.coupahost.com/administration/security`.
3. Select the **Sign in using SAML** check box.
4. Click the **Download and import SP metadata** link.
5. Save the Coupa metadata.

Set up the Coupa application in PingOne for Enterprise and extract the metadata

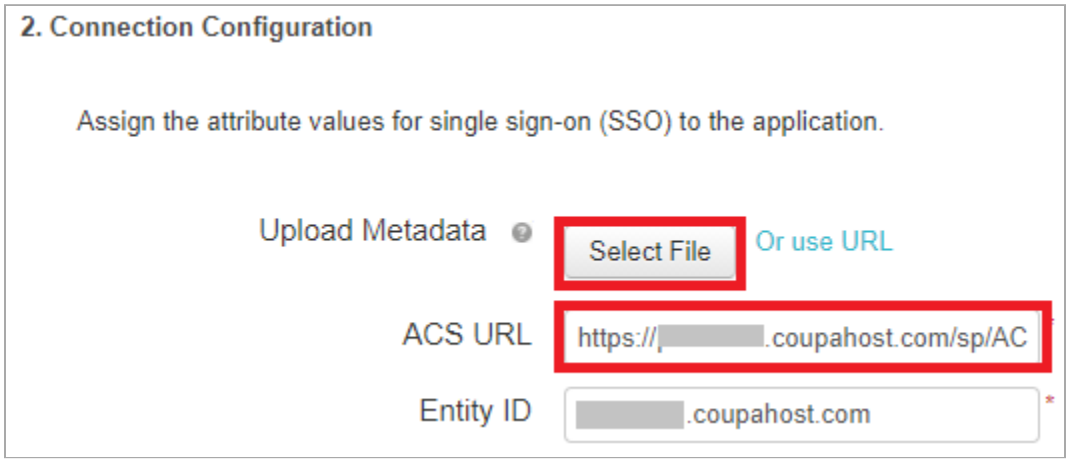
1. Sign on to PingOne for Enterprise for Enterprise and go to **Applications → Application Catalog**.
2. Search for `Coupa`.
3. Expand the Coupa entry and click the **Setup** icon.



4. Copy the **IdP ID** value.



5. Click **Continue to Next Step**.
6. Click **Select File** and upload the Coupa metadata file.

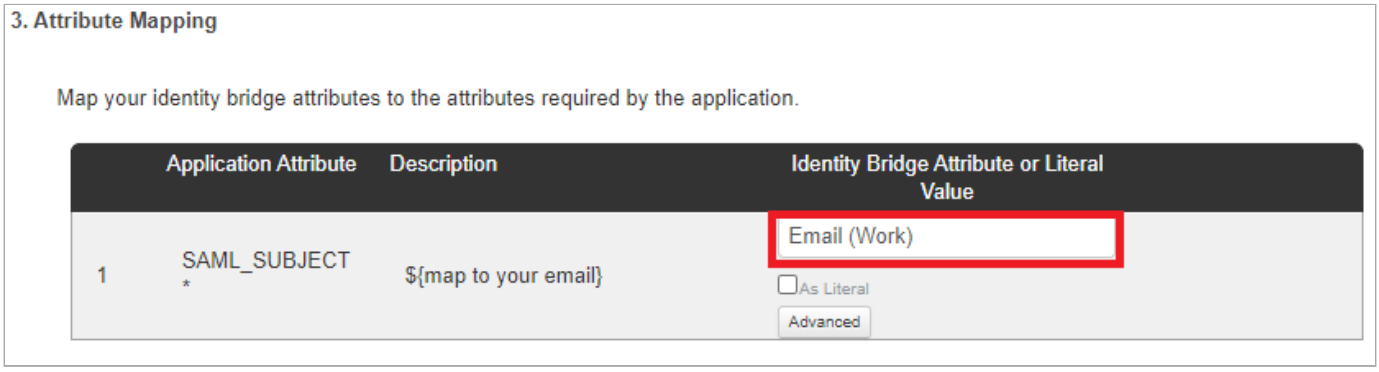


7. Edit the ACS URL to add a relay state parameter to enable IdP initiated sign-on.

   `https://your-environment.coupahost.com/sp/ACS.saml2?RelayState=https://your-environment.coupahost.com/sessions/saml_post`

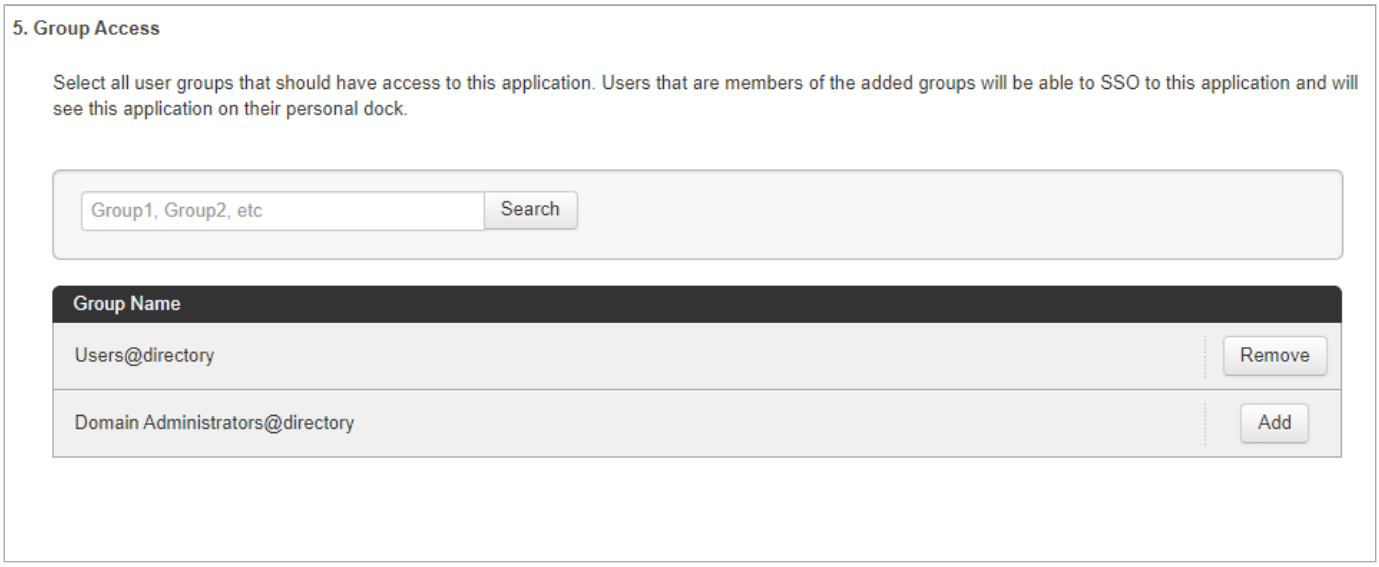
8. Click **Continue to Next Step**.

9. Ensure **SAML_SUBJECT** is mapped to the field containing a user's email address.

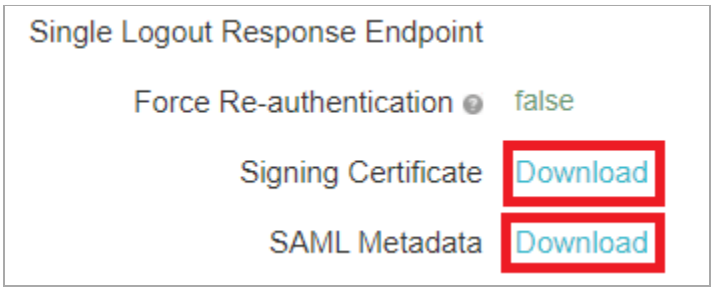


10. Click **Continue to Next Step** twice.

11. Click **Add** for all user groups that should have access to Coupa.



12. Click **Continue to Next Step**.
13. Download the PingOne for Enterprise SAML metadata and signing certificate.



14. Click **Finish**.

Add the PingOne for Enterprise IdP connection to Coupa

1. Sign on to your Coupa Admin organization as an administrator.
2. Go to `https://your_site.coupahost.com/administration/security`.
3. Ensure the **Sign in using SAML** check box is selected.
4. In the **Upload IdP metadata** section, click **Choose File**, select the PingOne for Enterprise metadata, and import the file.
5. Confirm that the **Login Page URL** field has the **IdP ID** value from PingOne for Enterprise.

   ```
   https://your site.coupahost.com/sp/startSSO.ping?PartnerIdpId=PingOne for Enterprise IdP ID value&TARGET=https://your site.coupahost.com/sessions/saml_post
   ```

6. In the **Certificate** field, upload the PingOne for Enterprise signing certificate.
7. Click **Save**.
8. Click the **Users** tab and edit the users who will use SAML authentication.
9. Set **Single Sign-On ID** to the value users will use to sign on, for example, their email address.

10. Set **Authentication method** to SAML.
11. Click **Save**.

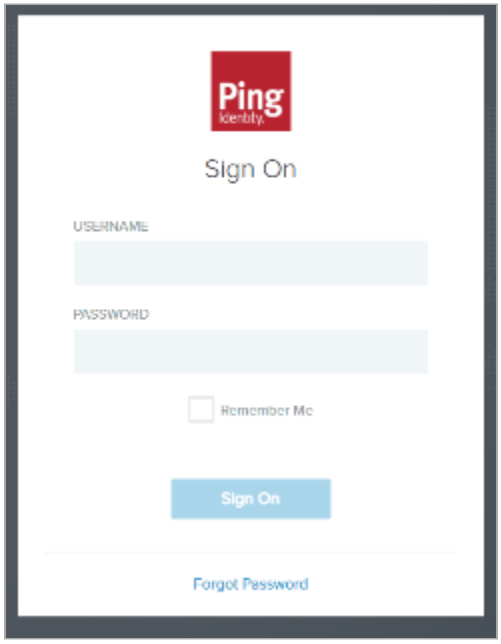
Test the PingOne for Enterprise IdP-initiated SSO integration:

1. Go to your Ping desktop as a user with Coupa access.

> **Note**
>
> To find the Ping desktop URL in the Admin console, go to **Setup → Dock → PingOne Dock URL**.

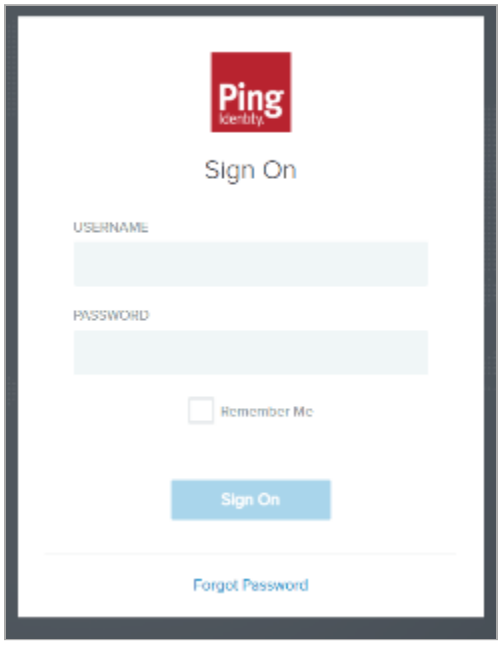
2. Complete PingOne for Enterprise authentication.

   You're redirected to your Coupa domain.



Test the PingOne for Enterprise SP-initiated SSO integration

1. Go to your Coupa URL.
2. After you're redirected to PingOne, enter your PingOne for Enterprise username and password.



You’re redirected back to Coupa.

Datadog

Configuring SAML SSO with Datadog and PingOne

Learn how to enable SAML SSO with Datadog and PingOne

Before you begin

To enable SSO within Datadog, you must have an administrator account.

About this task

> **Note**
>
> This is a tested integration.

Set up the integration

1. Sign on to your PingOne SSO admin account and go to **Connections → Applications** and click the plus icon (+).
2. On the **New Application** page, click **Advanced Configuration**, and on the **SAML** line, click **Configure**.
3. On the **Create App Profile** page, enter the following:
    1. **Application Name**
    2. **Optional: Description**
    3. **Optional: Icon**
4. Click **Next**.
5. On the corresponding **Configure SAML Connection** page, click **Manually Enter** to begin configuring Datadog with PingOne.
6. In a new tab, sign on to your Datadog admin account. In the lower left hand corner, click on your account name and then **Configure SAML**, which will contain information for the next step.
7. In PingOne, enter the following information for the required fields:
    1. The **ACS URL(s)** of the application.

       You can find this on the Datadog admin console under **Assertion Consumer Service URL**.
    2. The **Entity ID** of the application. from the previous step.

       You can find this on the Datadog admin console under **Service Provider Entity ID**.
    3. Update the **SUBJECT NAMEID FORMAT** to `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`.

4. Enter the **Assertion Validity Duration (in seconds)**, for example, `3600`.
5. Configure the remaining options as needed.
6. Click **Save and Continue**.

8. On the **Attribute Mapping** page, enter the following attributes:
    1. Outgoing value: **User ID** = Application Attribute: **saml_subject** (required).
    2. Outgoing value: **Family Name** = Application Attribute: **sn**
    3. Outgoing value: **Given Name** = Application Attribute: **givenName**
    4. Outgoing value: **Username** = Application Attribute: **eduPersonPrincipalName**
    5. Click **Save and Close**.

    > **Note**
    >
    > You can add additional attributes to control roles. See the Datadog documentation for more information.

9. On the newly-created application, click the **Configuration** tab and click **Download Metadata**.
10. In your Datadog account, click **Choose File**, upload the IdP metadata that you downloaded in the previous step, and click **Upload File**.
11. After uploading the IdP metadata and configuring your IdP, click **Enable** to enable SAML and finalize the configuration.
12. If you're leveraging this integration for an IdP-initiated sign-on, in the **Additional Features** section of Datadog, make sure to select the **Identity Provider (IdP) Initiated Login** check box.

    The set up is now complete.

Create and assign identities

Before you test the integration, you must create and assign identities in PingOne.

> **Note**
>
> If you've already assigned identities and groups in PingOne, you can test the integration.

1. In PingOne, go to **Identities → Groups** and click the **+** icon next to **Groups.**
2. On the **Create New Group** page, enter values for the following:
    - **Group Name** (Required)
    - **Description** (Optional)
    - **Population** (Optional)
3. Click **Finish & Save**.
4. To add identities to the group, on the **Identities** tab, go to **Users → + Add User**.

5. On the **Add User**page, enter in all the necessary information for a user.

   > **Important**
   >
   > Verify the first name, last name, USER ID, and USERNAME are correct, as these are values passed in the SAML assertion.

6. Click **Save**.
7. Assign the user that you created to the group that you created previously.

   Locate the user you created and do the following:

   1. Expand the section for the user.
   2. Select the **Groups** tab.
   3. Click **+ Add**.

8. In the **Available Groups** section, select the group that you created and click the **+** icon to add it to the user's group memberships. Click **Save**.
9. On the **Connections** tab, for the Datadog application:
   - Click the **Access** tab
   - Click the **Pencil** icon to edit the configuration
10. Select the group that you created and add it to the **Applied Groups** section. Click **Save**.

Test the integration

1. In the PingOne admin console, go to **Dashboard → Environment Properties**.
2. Right-click on the **Application Portal URL** and open it in a private browser session.
3. Sign on as the test user that you created and click the Datadog tile.

   You're signed on to the user's Datadog account using SSO and testing is complete.

DocuSign

Configuring SAML SSO using DocuSign and PingFederate

Learn how to enable DocuSign sign on from a PingFederate URL (IdP-initiated sign-on) and direct DocuSign sign on using PingFederate (SP-initiated sign-on).

Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Make sure DocuSign has a valid domain, an organisation created, and is populated with at least one user to test access.
- You must have administrative access to PingFederate and DocuSign.

Create a PingFederate SP Connection for DocuSign

1. Sign on to PingFederate administration console.
2. Create an SP connection for DocuSign in PingFederate:
    - Configure using **Browser SSO** profile **SAML 2.0**.
    - Set **Partner's Entity ID** to `Placeholder`.

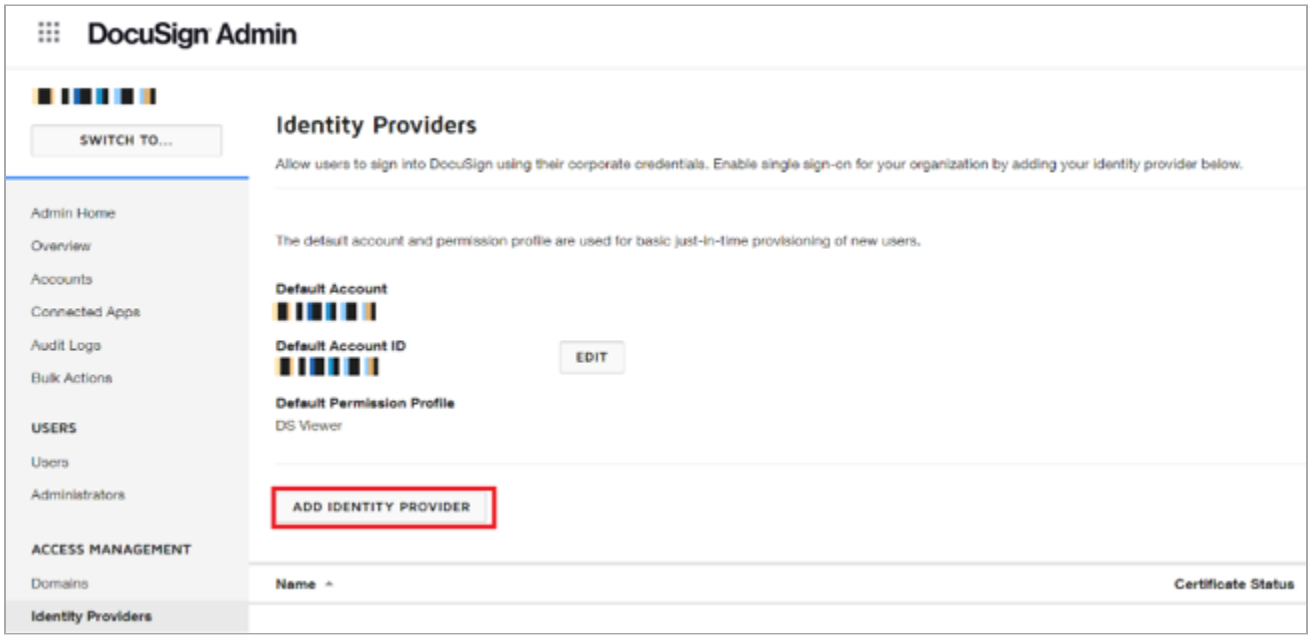
      You will update this value later.
    - Enable the following **SAML Profiles**:
        - **IdP-Initiated SSO**
        - **SP-Initiated SSO**
    - In **Assertion Creation: Attribute Contract**, extend the contract to add attributes named `SAML_NAME_FORMAT`, `surname`, `givenname` and `emailaddress`.
    - In **Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment**, map **SAML_SUBJECT**, **surname**, **givenname** and **emailaddress** and map **SAML_NAME_FORMAT** to `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`.
    - In **Protocol Settings: Assertion Consumer Service URL**, set **binding** to **POST**, and set **Endpoint URL** to `http://placeholder`.

      You will update the placeholder value later.
    - In **Protocol Settings: Allowable SAML Bindings**, enable **POST**.
    - In **Credentials: Digital Signature Settings**, select the PingFederate signing certificate.

3. Save the configuration.
4. Export the signing certificate.
5. Export and then open the metadata file, and copy the value of these properties:
    - `entityID`
    - `Location entry` (`https://your value/idp/SSO.saml2`)

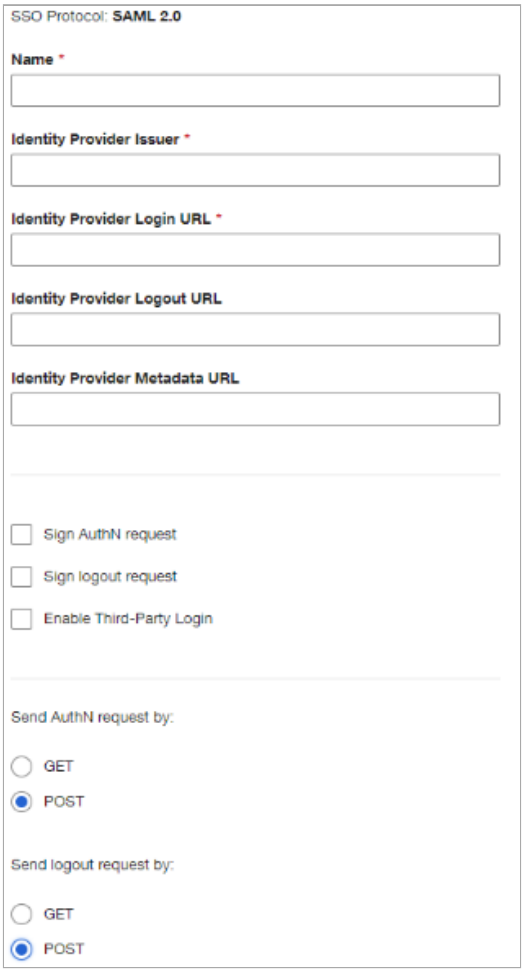
Add the PingFederate connection to DocuSign

1. Sign on to your DocuSign domain as an administrator.
2. In the left navigation pane, select **Identity Providers**, and then click **Add Identity Provider**.



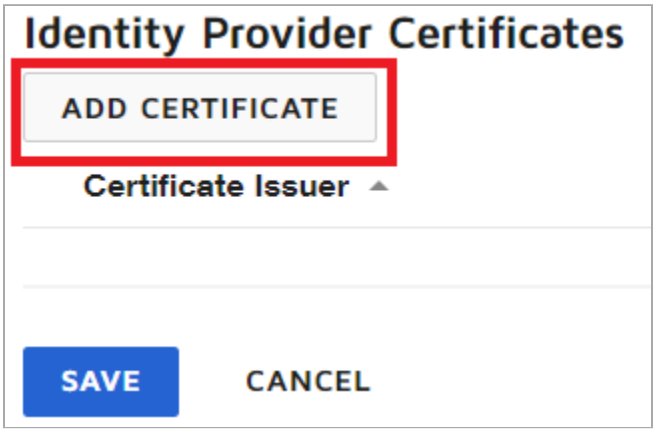
3. Configure the following fields.

Field	Value
Name	A name for the identity provider.
Identity Provider Issuer	Enter the **Issue** value from PingID.
Identity Provider Login URL	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=PingOne IdP ID value`
Send AuthN Request by	Click **POST**.
Select Send Logout Request by	Click **POST**.

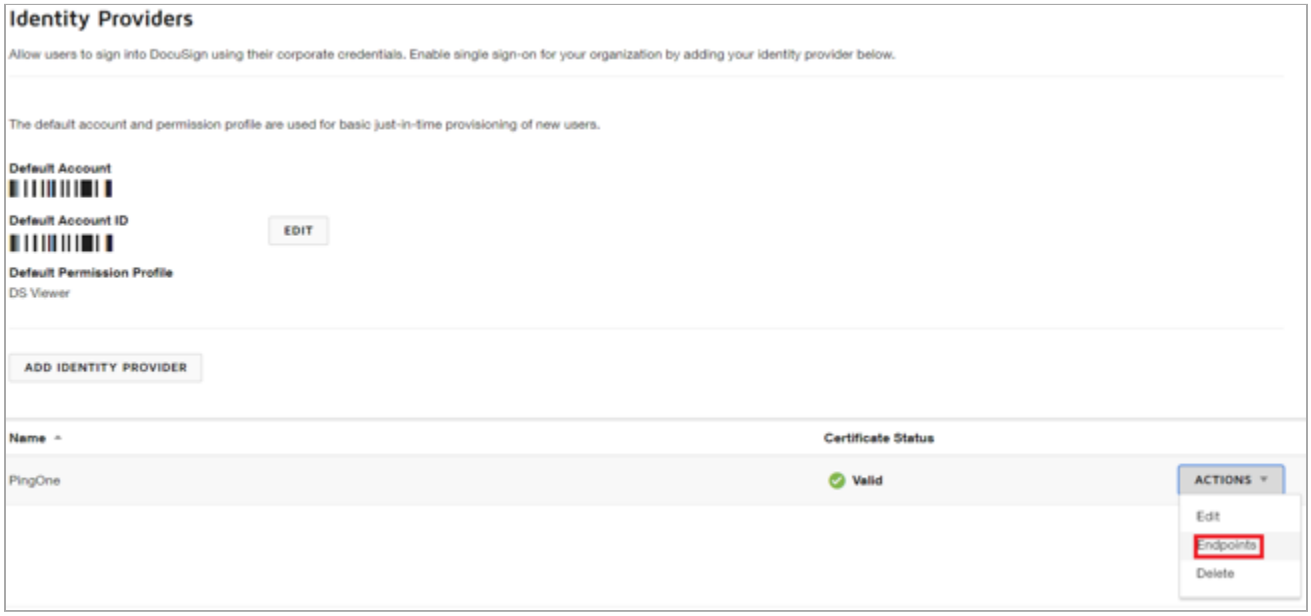


4. In the **Custom Attribute Mapping** section, click **Add New Mapping**, and then:
    - In the **Field** list, select **surname**, then enter `surname` in the **Attribute** field.
    - In the **Field** list, select **givenname**, then enter `givenname` in the **Attribute** field.
    - In the **Field** list, select **emailaddress**, then enter `emailaddress` in the **Attribute** field.
5. Click **Save**.
6. Click **Add New Certificate**.

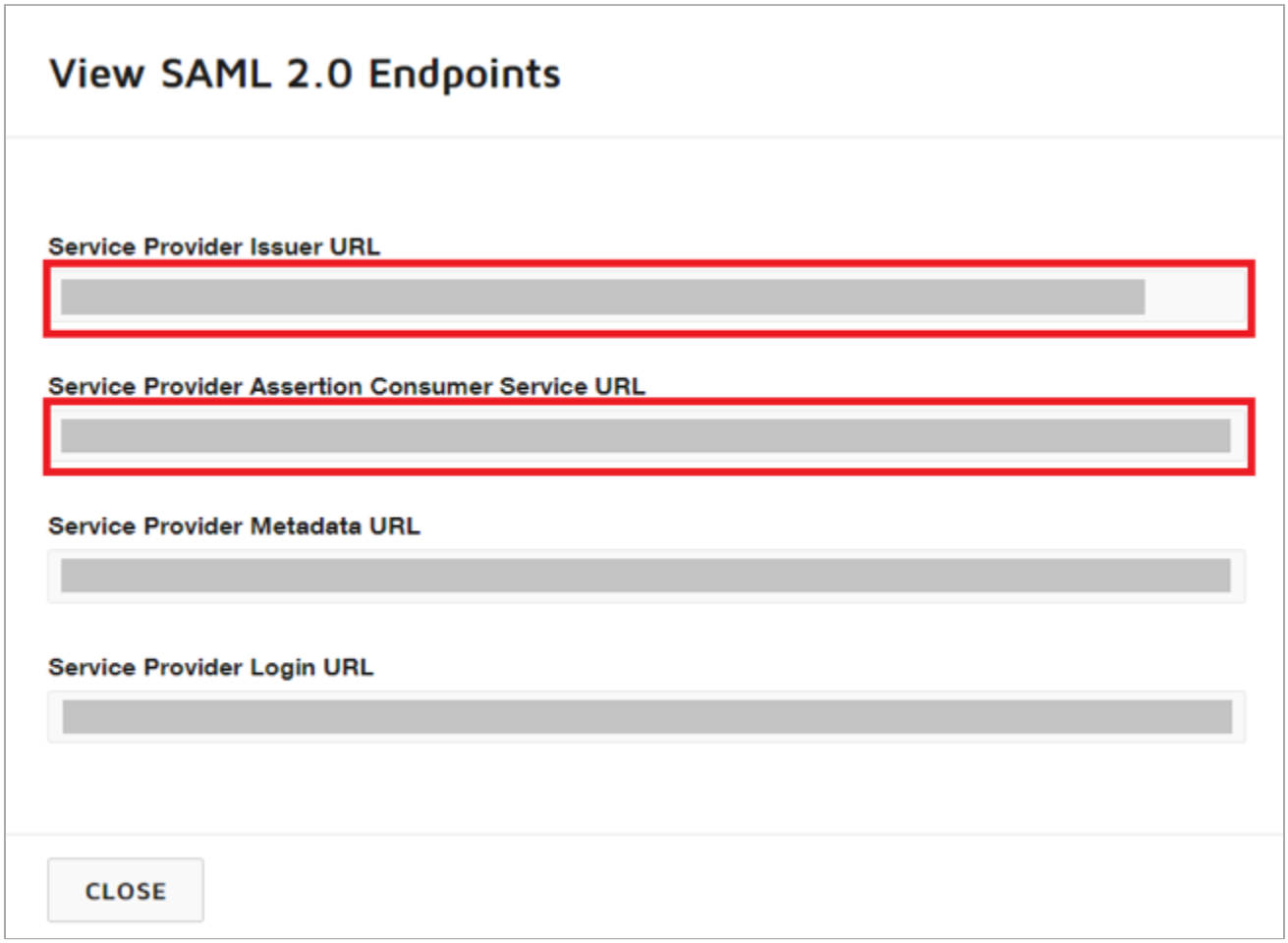
7. Click **Add Certificate**.



8. Select the signing certificate that downloaded from PingFederate. Click **Save**.
9. In the **Actions** list for the identity provider that you created, select **Endpoints**.



10. Copy the **Service Provider Issuer URL** and **Service Provider Assertion Consumer Service URL** values.



The DocuSign connection configuration is complete.

> **Note**
>
> After testing, you can set the domain to require IP authentication to remove the DocuSign sign-on screen.

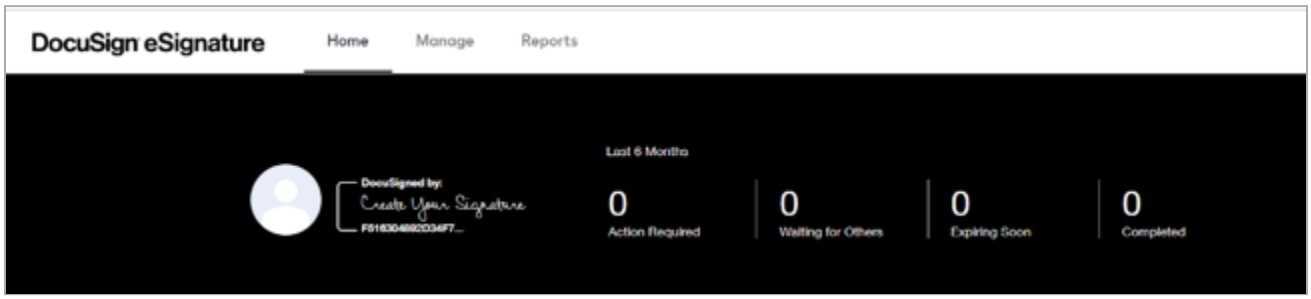
Update the EntityID and ACS URL values in PingFederate

1. Sign on to the PingFederate administrative console.
2. Edit the SP connection for DocuSign.
3. Set **Partner's Entity ID** to the DocuSign **Service Provider Issuer URL** value.
4. Set **Assertion Consumer Service URL Endpoint URL** to the **DocuSign Service Provider Assertion Consumer Service URL** value.
5. Save the changes.

Test the PingFederate IdP-initiated SSO integration

1. Go to the PingFederate SSO application endpoint for the DocuSign SP connection.
2. Complete PingFederate authentication.

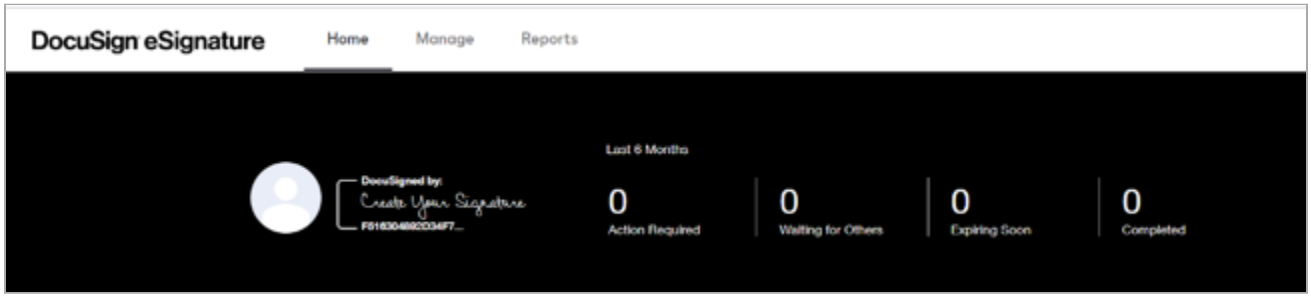
You're redirected to your DocuSign domain.



Test the PingFederate SP-initited SSO integration

1. Go to https://account.docusign.com.
2. Enter your email address.
3. Click **Use Company Login**.
4. After you're redirected to PingFederate, enter your PingFederate username and password.

   After successful authentication, you're redirected back to DocuSign.



Configuring SAML SSO with DocuSign and PingOne for Enterprise

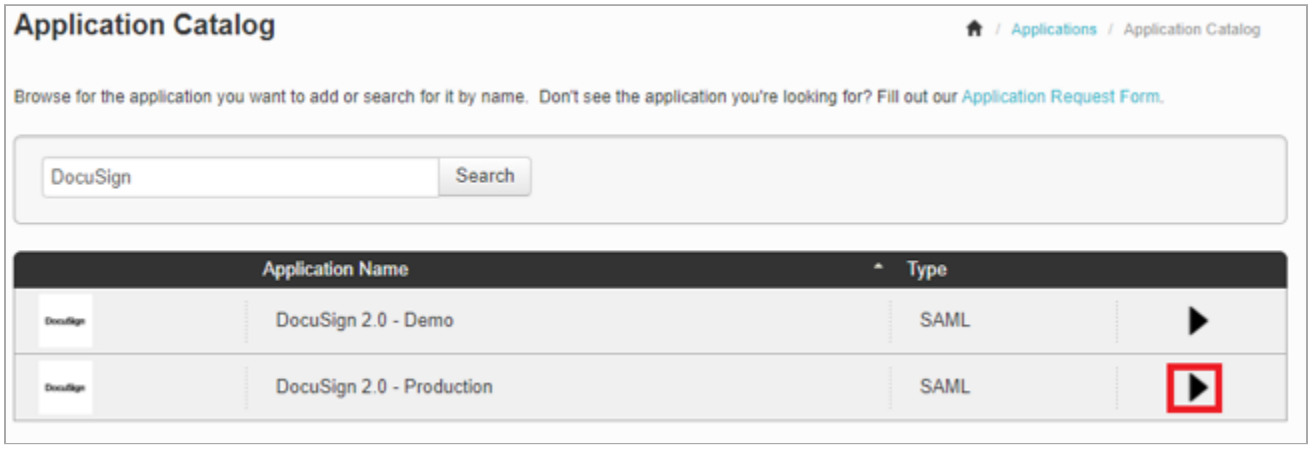
Learn how to enable DocuSign sign on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct DocuSign sign on using PingOne for Enterprise (SP initiated sign on).

Before you begin

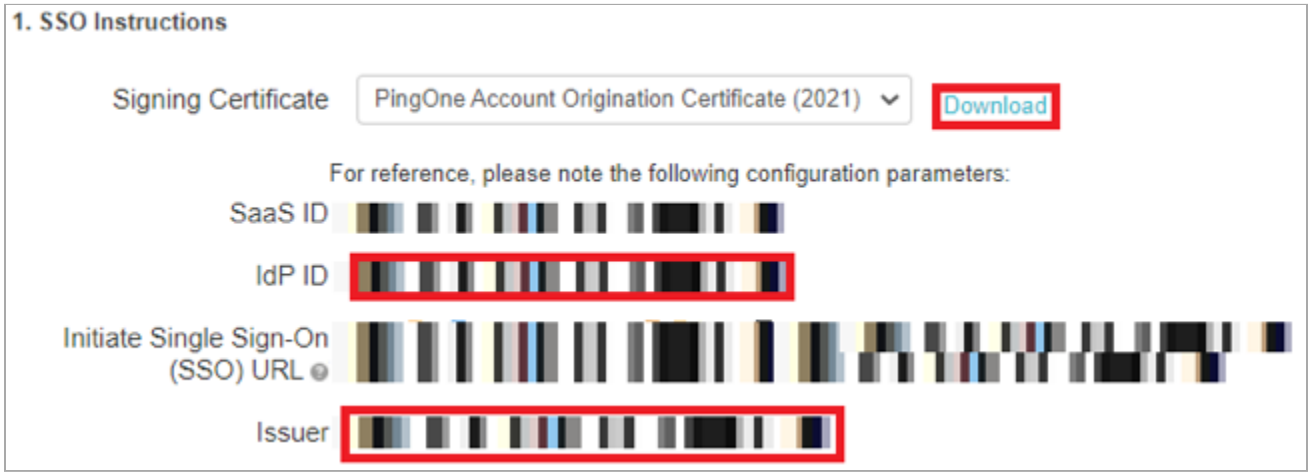
- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Make sure DocuSign has a valid domain, an organization created, and is populated with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and DocuSign.

Copy PingOne values for the Supplied DocuSign Application

1. Sign on to PingOne for Enterprise, go to **Applications → Application Catalog**, and search for DocuSign.

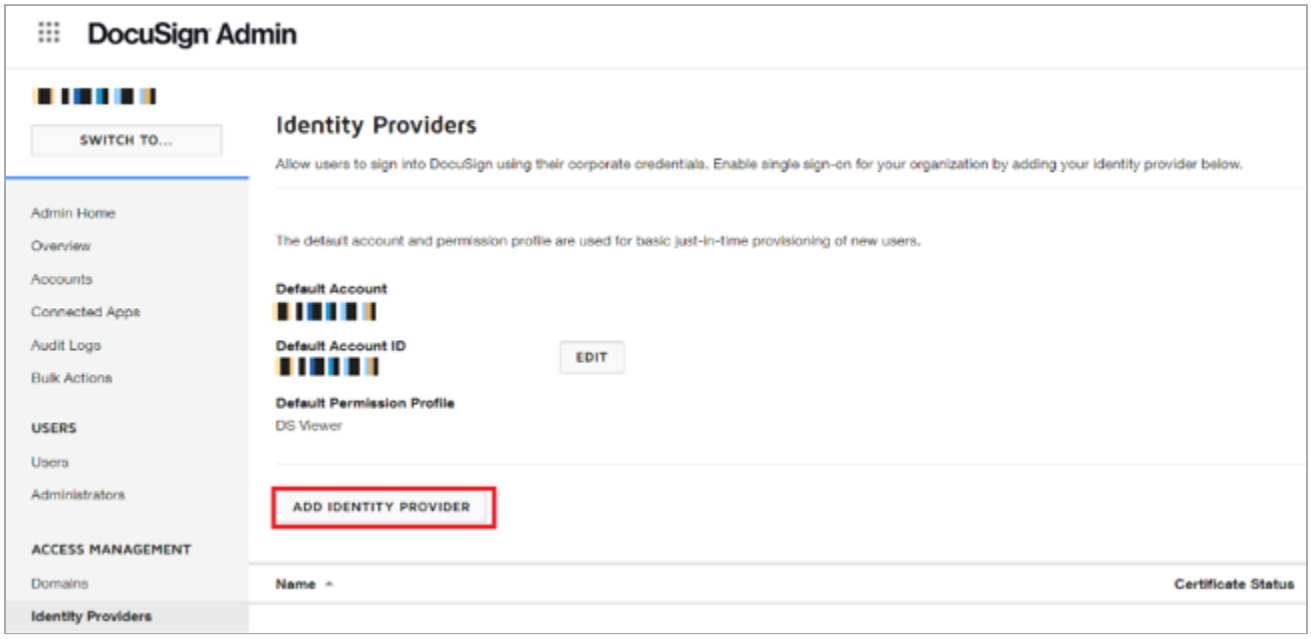


2. Expand the **DocuSign 2.0 - Production** entry and click the **Setup** icon.
3. Copy the **Issuer** and **IdP ID** values.
4. Download the **Signing Certificate**.



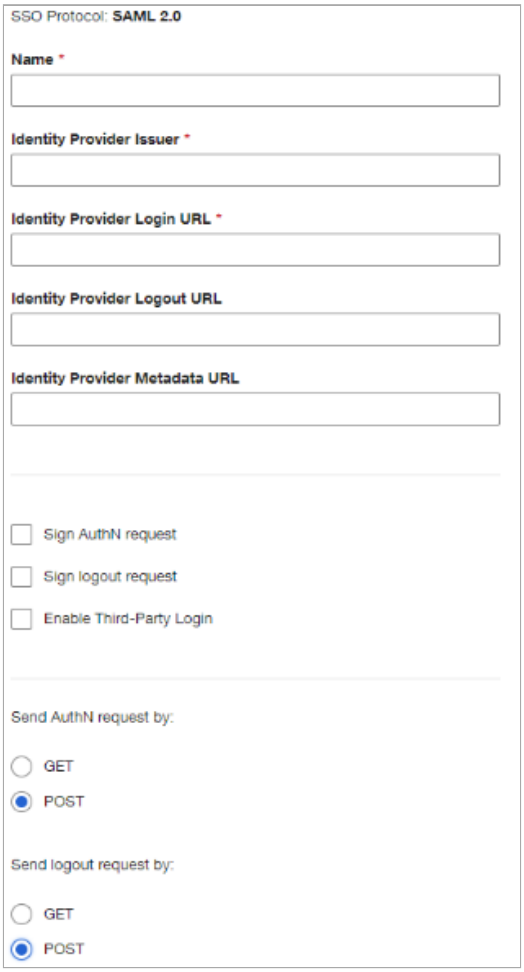
Add the PingOne for Enterprise IdP Connection to DocuSign

1. Sign on to your DocuSign Admin organization as an administrator.
2. In the left navigation pane, select **Identity Providers**, and then click **Add Identity Provider**.



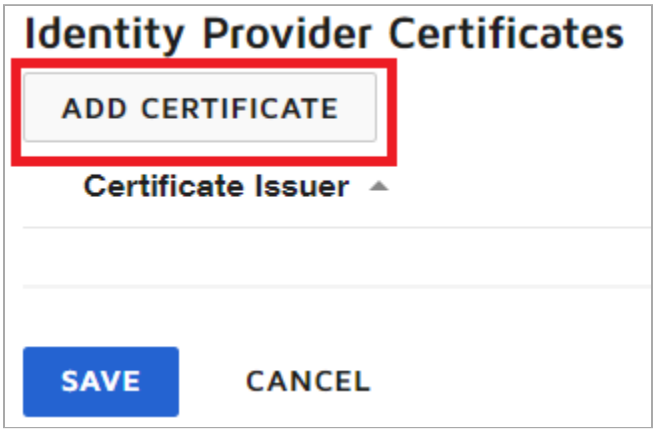
3. Configure the following fields

Field	Value
Name	A name for the identity provider
Identity Provider Issuer	The **Issue** value from PingID
Identity Provider Login URL	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=PingOne for Enterprise IdP ID value`
Send AuthN Request by	**POST**
Select Send Logout Request by	**POST**

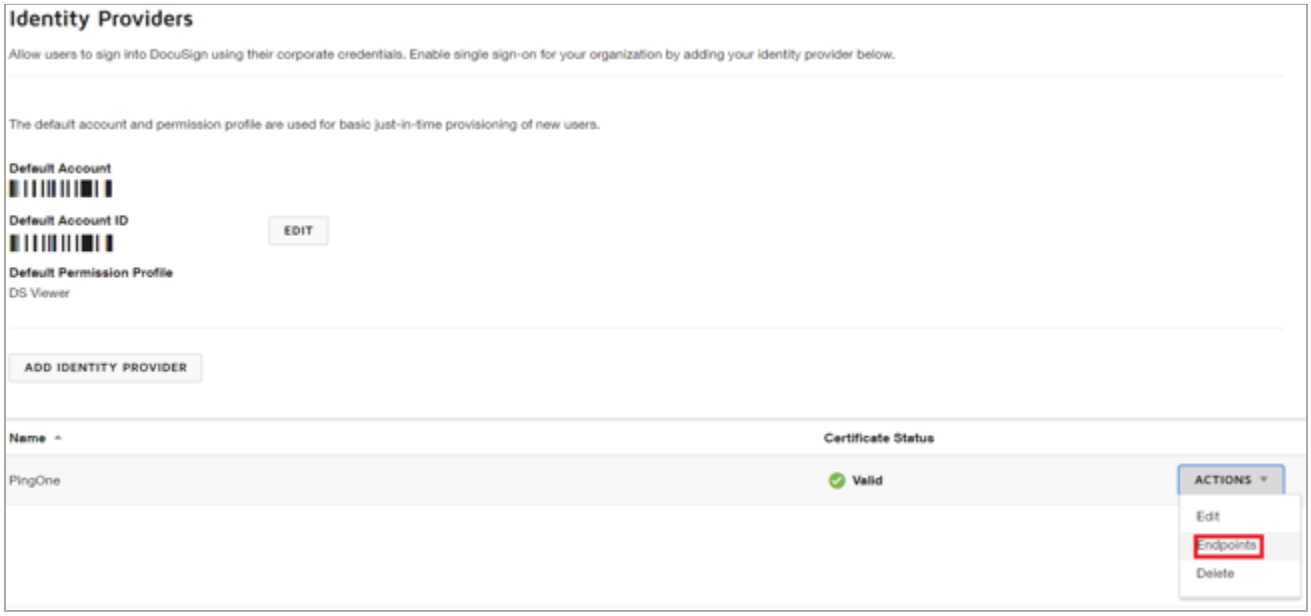


4. In the **Custom Attribute Mapping** section, click **Add New Mapping**, and then:
    - In the **Field** list, select **surname**, then enter `surname` in the **Attribute** field.
    - In the **Field** list, select **givenname**, then enter `givenname` in the **Attribute** field.
    - In the Field list, select **emailaddress**, then enter `emailaddress` in the **Attribute** field.
5. Click **Save**.
6. Click **Add New Certificate**.

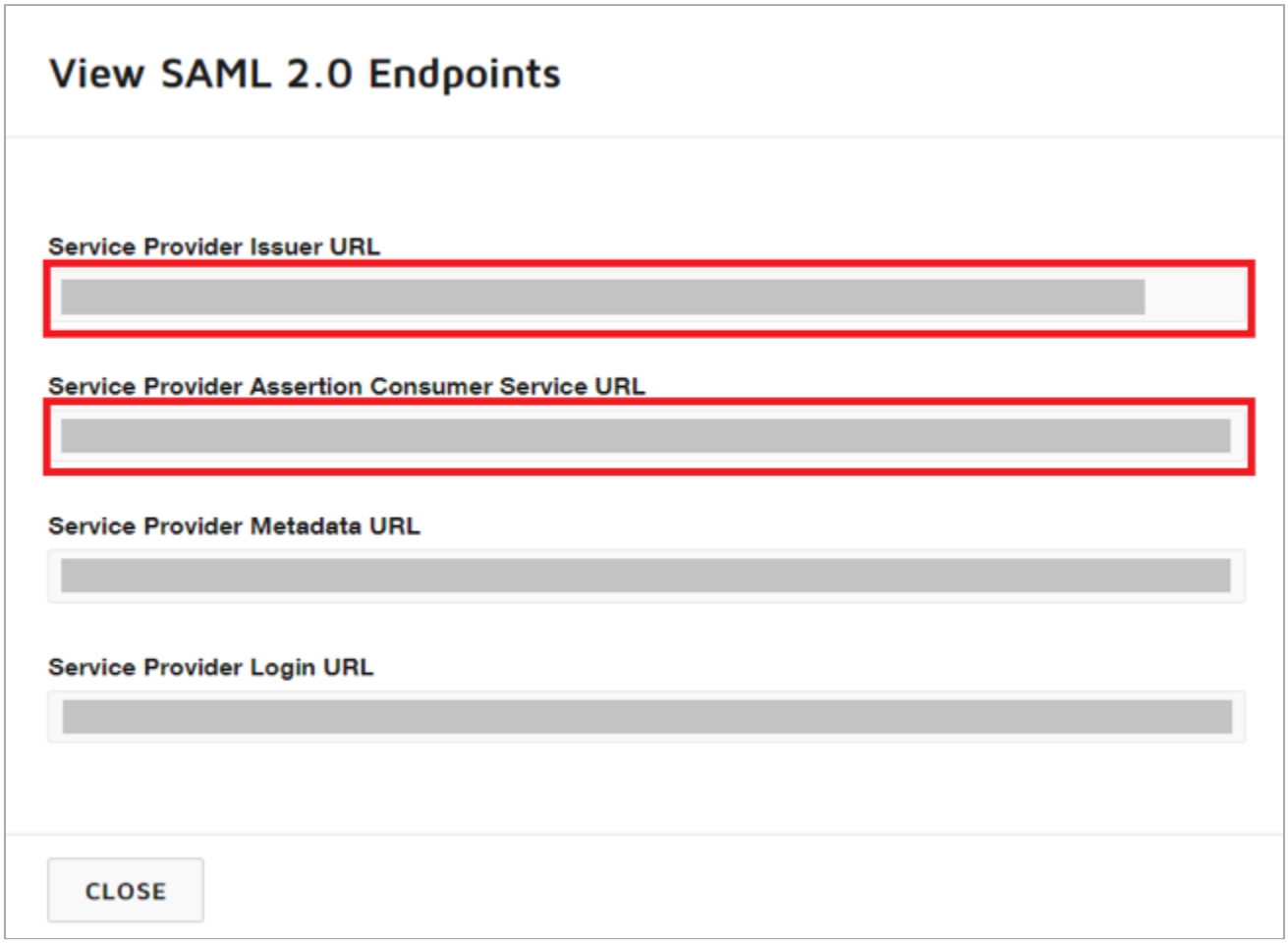
7. Click **Add Certificate**.



8. Select the signing certificate that you downloaded from PingOne for Enterprise. Click **Save**.
9. In the **Actions** list for the IdP that you created, select **Endpoints**.



10. Copy the **Service Provider Issuer URL** and**Service Provider Assertion Consumer Service URL** values.



The DocuSign connection configuration is complete.

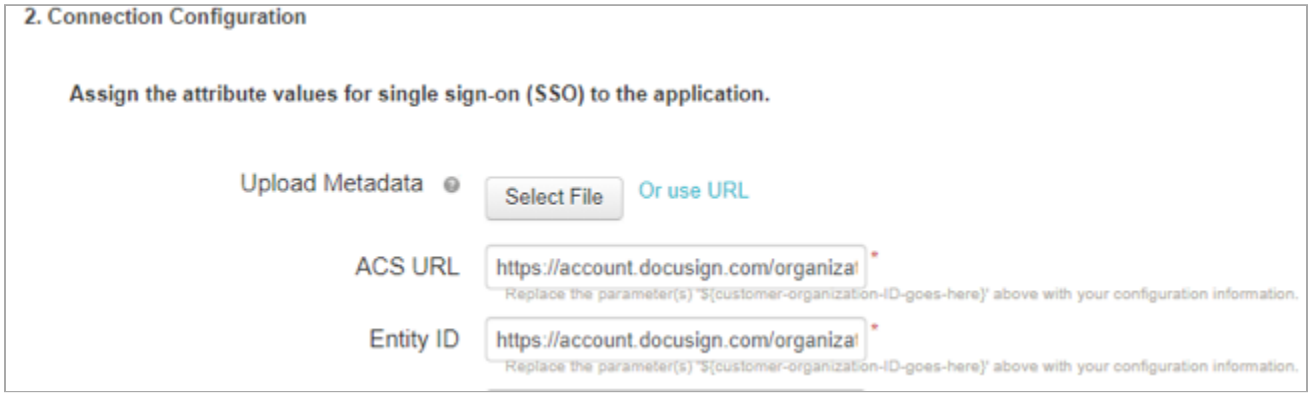
> **Note**
>
> After testing, you can set the domain to require IP authentication to remove the DocuSign sign-on screen.

Complete the DocuSign setup in PingOne for Enterprise

1. Continue editing the DocuSign entry in PingOne for Enterprise.

> **Note**
>
> If the session has timed out, complete the initial steps to the point of clicking **Setup**.

2. Click **Continue to Next Step**.
3. Set the **ACS URL** to the **DocuSign Service Provider Assertion Consumer Service URL** value.
4. Set the **Entity ID** to the **DocuSign Service Provider Issuer URL** value.

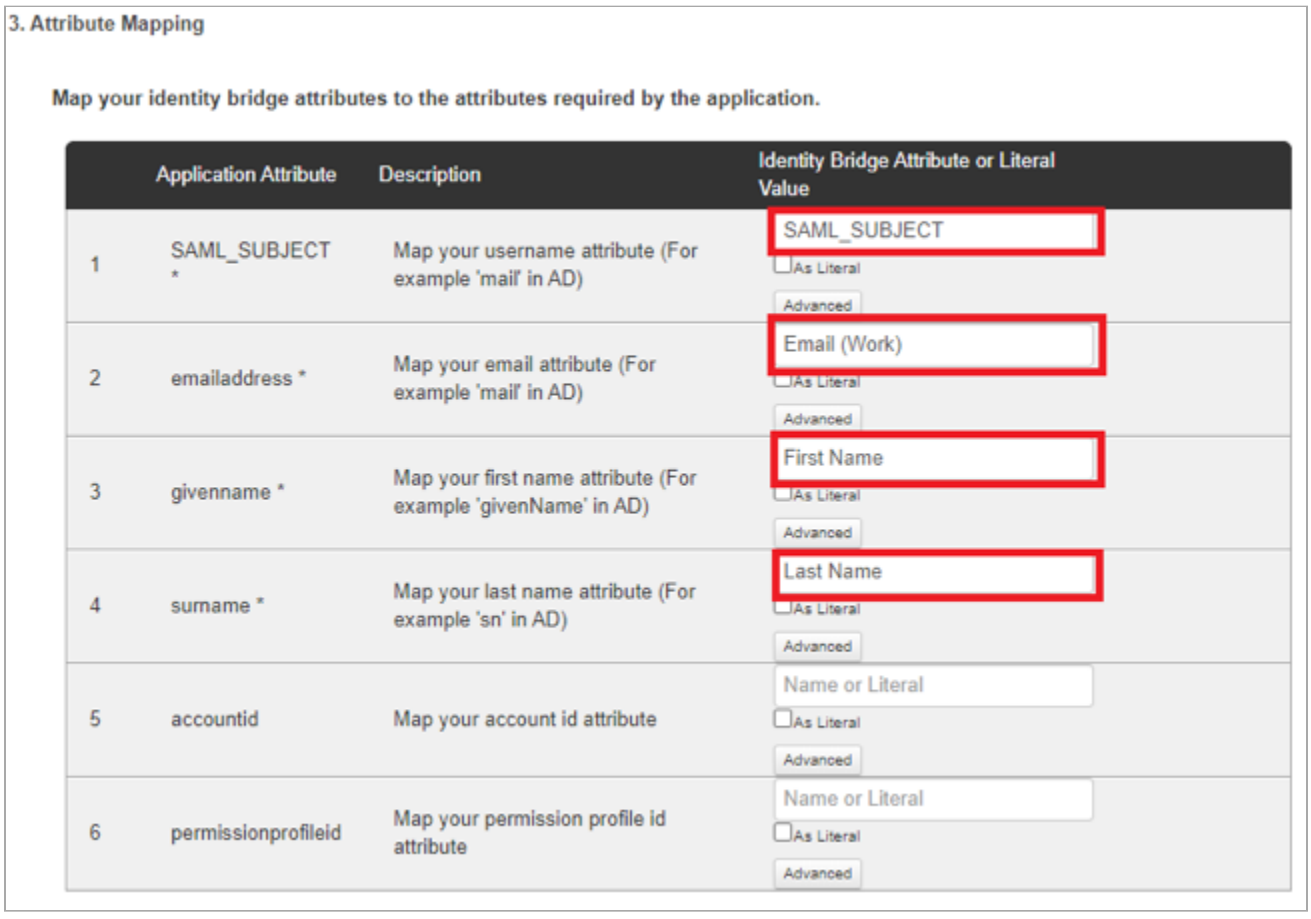


> **Note**
>
> Do not just update the organization ID.

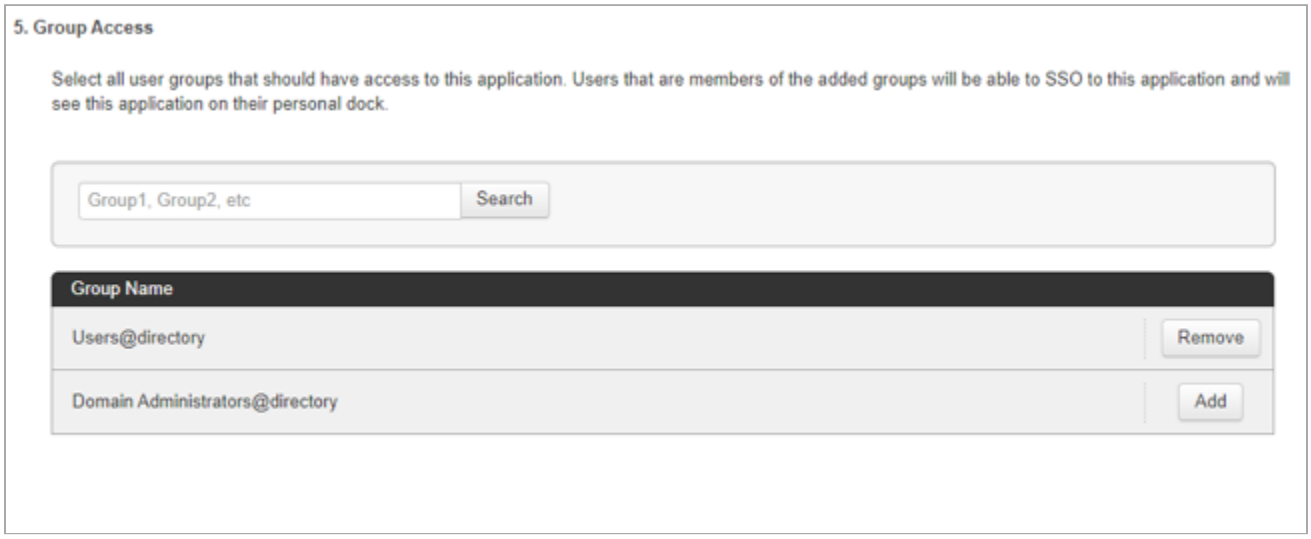
5. Click **Continue to Next Step**.

6. Map the required attributes to the corresponding attribute names in your environment.

> **Note**
>
> The corresponding attribute names might not be an exact match.



7. On the **SAML_SUBJECT** line, click **Advanced**, and change the name format you're sending to DocuSign to `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`.
8. Click **Continue to Next Step** twice.
9. Click **Add** for all user groups that should have access to DocuSign.



10. Click **Continue to Next Step**.
11. Click **Finish**.

    PingOne for Enterprise configuration is complete.

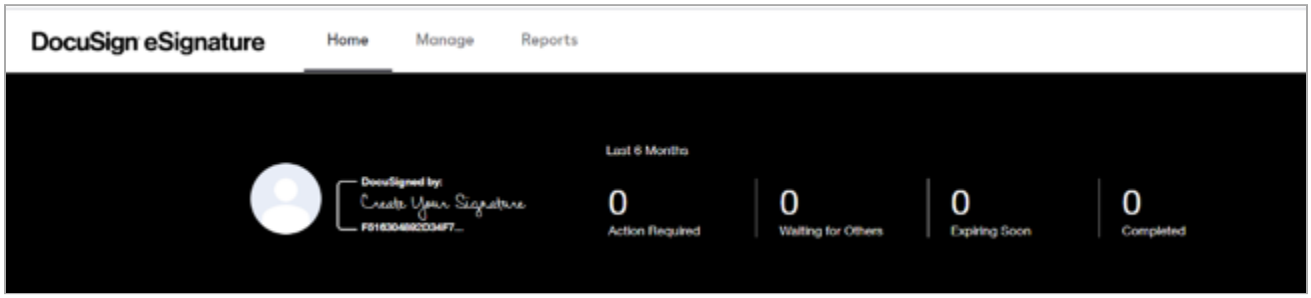
Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with DocuSign access.

> **Note**
>
> To find the Ping desktop URL in the Admin console, go to **Setup → Dock → PingOne Dock URL**.

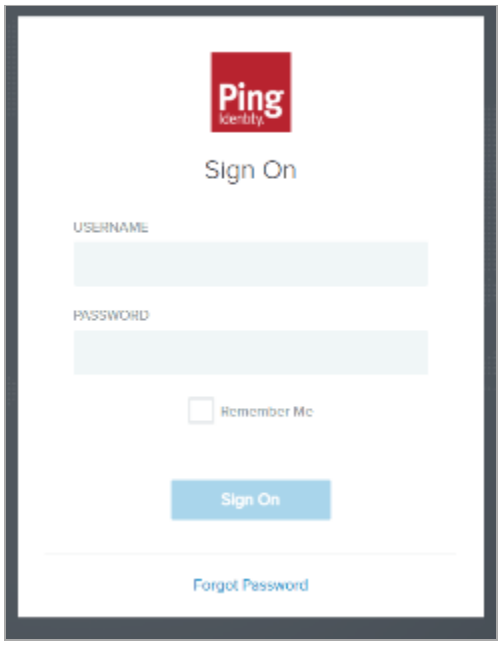
2. Complete the PingOne for Enterprise authentication.

   You're redirected to your DocuSign domain.

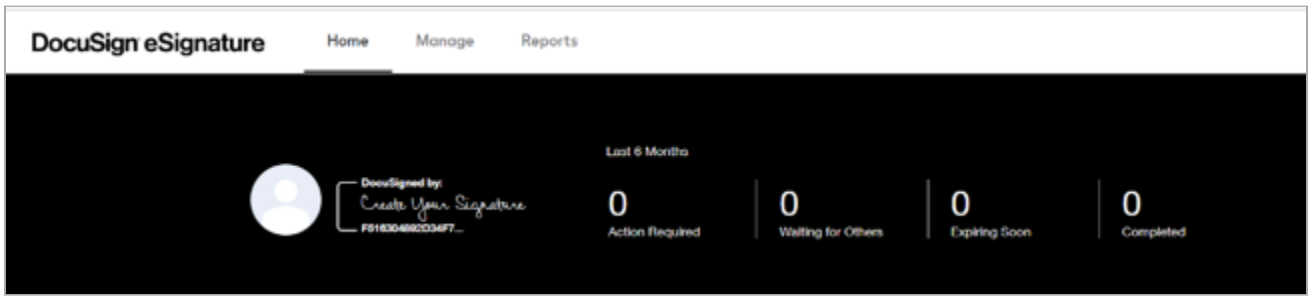


Test the PingOne for Enterprise SP-initiated SSO integration

1. Go to https://account.docusign.com.
2. Enter your email address.
3. Click **Use Company Login**.
4. When you're redirected to PingOne for Enterprise, enter your PingOne username and password.



After successful authentication, you're redirected back to DocuSign.



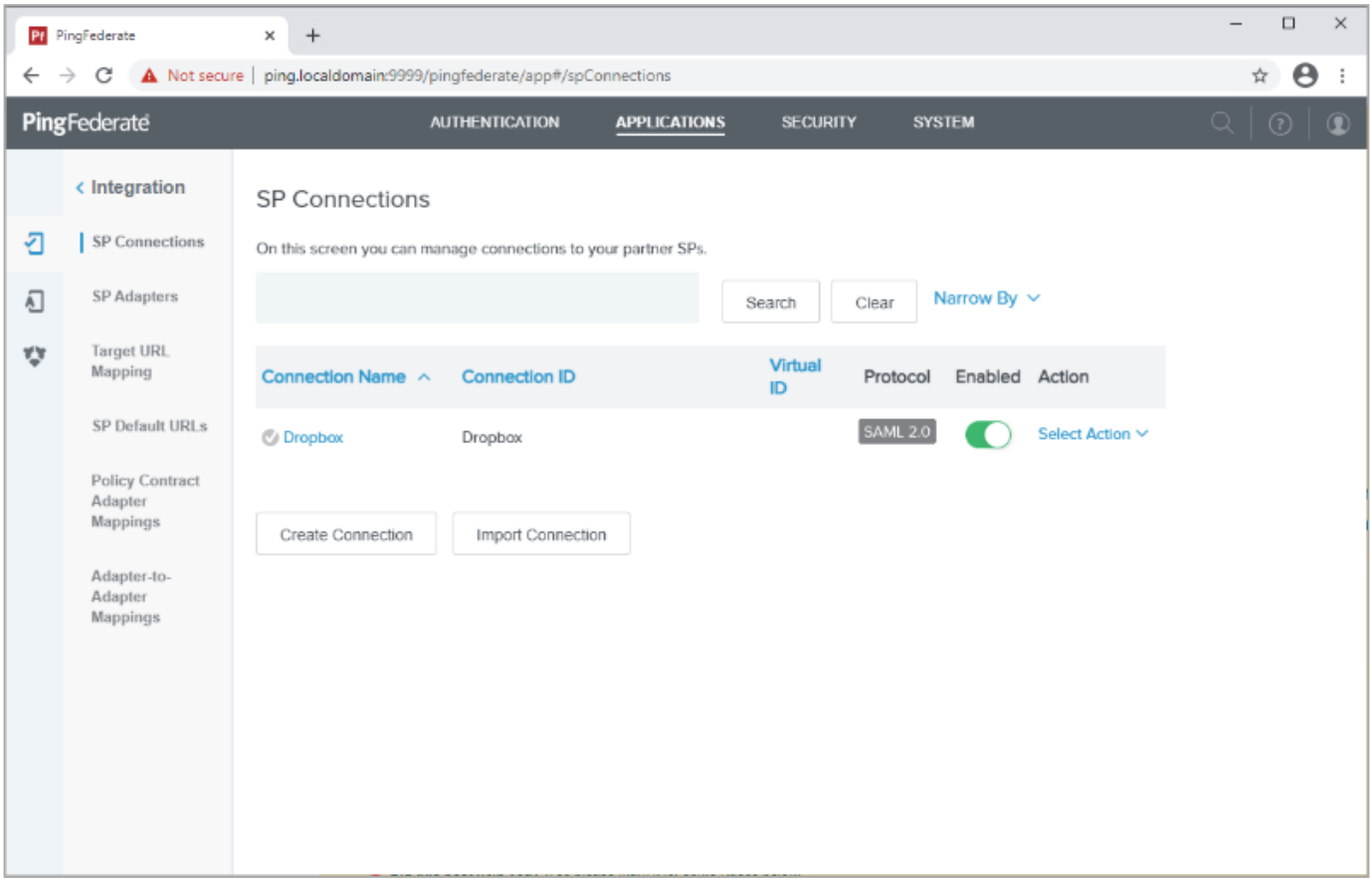
Dropbox

Configuring SAML SSO with Dropbox and PingFederate

Learn how to configure SAML SSO with Dropbox and PingFederate.

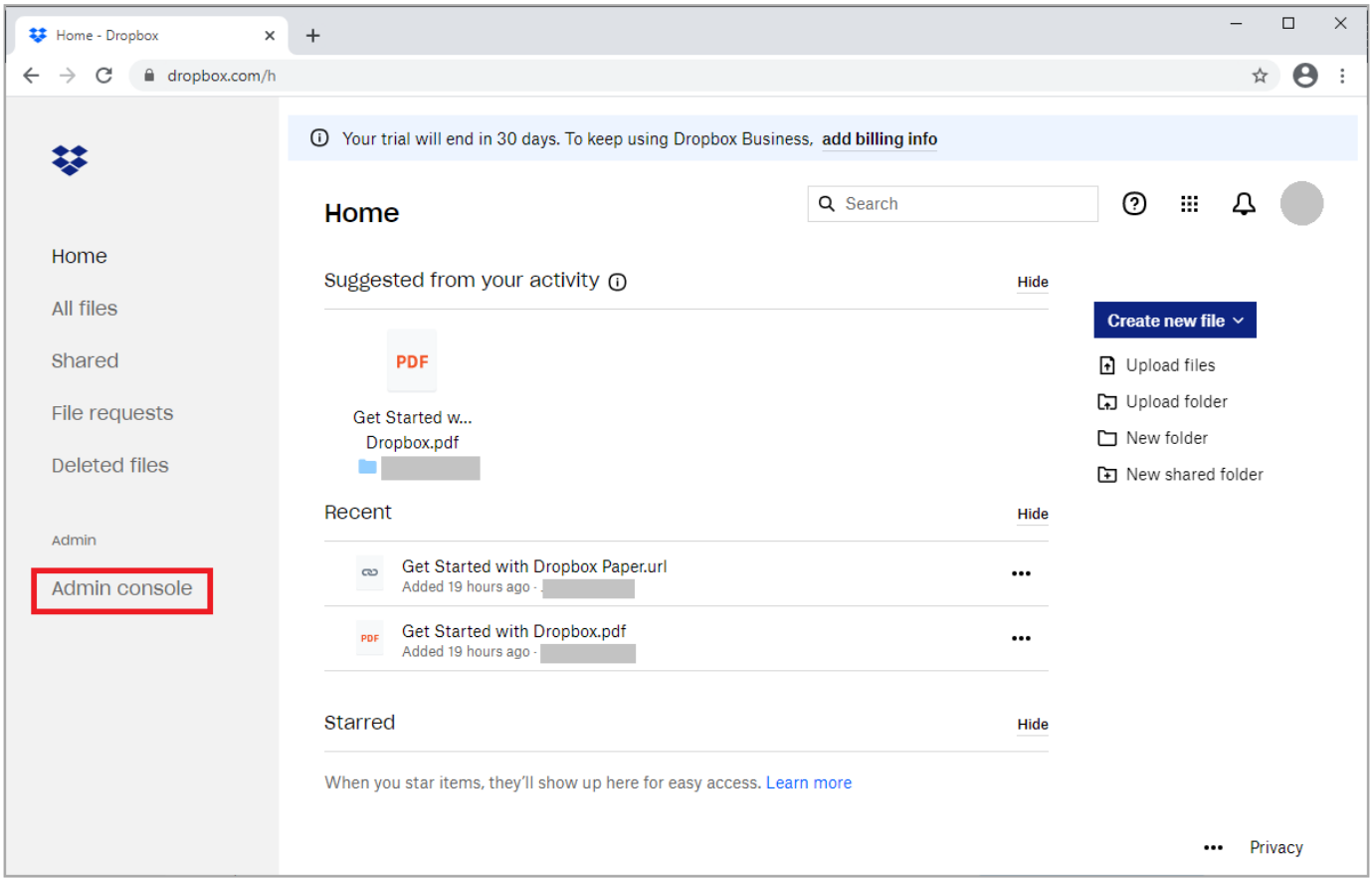
Create a PingFederate SP connection for Dropbox

1. Sign on to the PingFederate administrative console.
2. Create an SP connection in Ping Federate:
    1. Set **Partner's Entity ID** to **Dropbox**.
    2. Configure using **Browser SSO profile SAML 2.0**.
    3. Enable the following **SAML Profiles**:
        - **IDP-Initiated SSO**
        - **SP-Initiated SSO**
        - **IDP-Initiated SLO**
        - **SP-Initiated SLO**
    4. In **Assertion Creation: Attribute Contract**, set the **Subject Name Format** to `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`.
    5. In **Assertion Creation: Attribute Contract Fulfilment**, map attribute `SAML_SUBJECT` to the attribute `mail`.
    6. In **Protocol Settings**, set **Assertion Consumer Service URL:** to `https://www.dropbox.com/saml_login` and in **Allowable SAML Bindings**, enable **Redirect**.
3. Export the metadata for the newly-created SP connection.
4. Export the signing certificate public key.



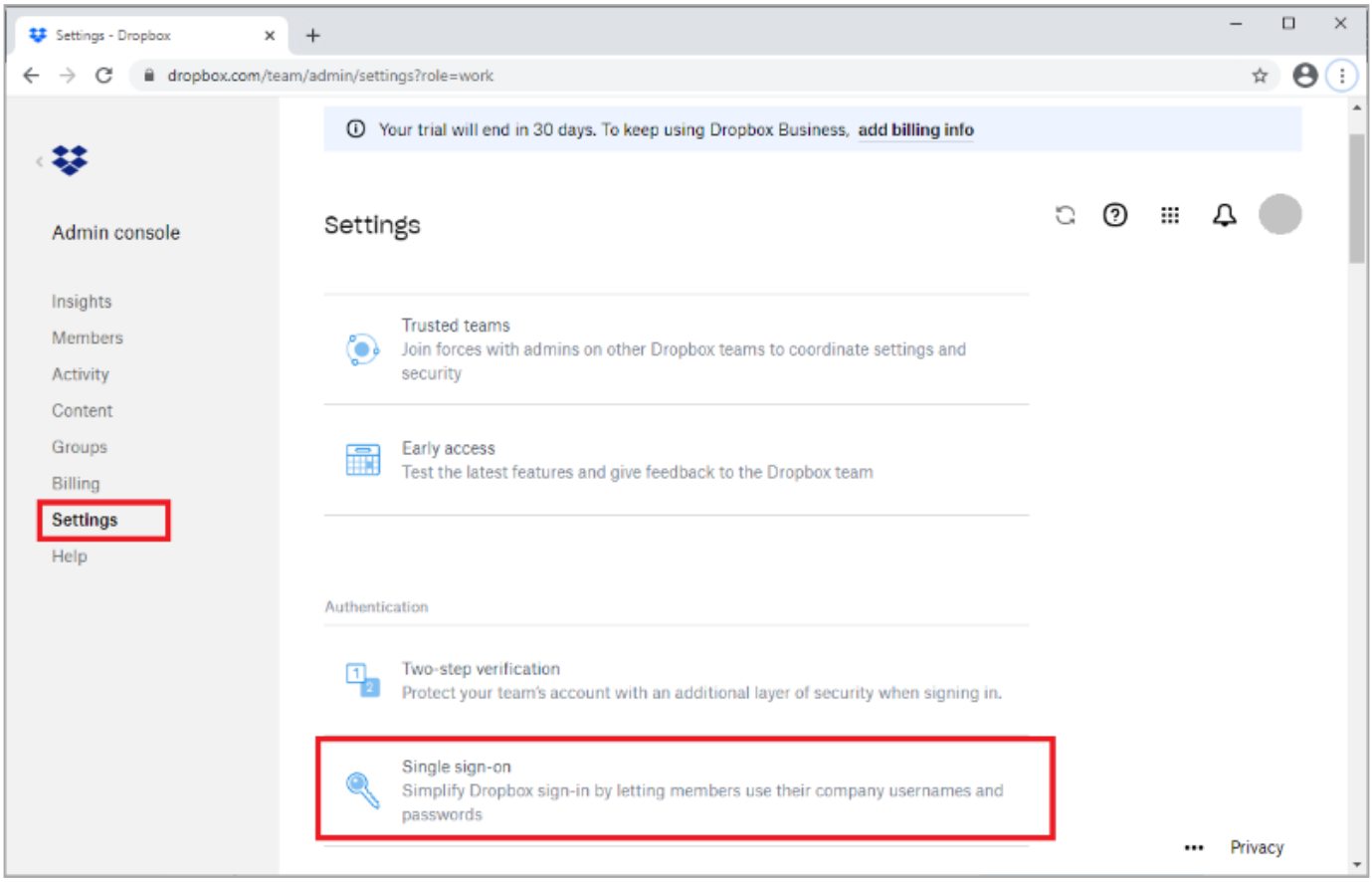
Configure the PingFederate IdP connection for Dropbox

1. Sign on to the Dropbox Admin Console as an administrator.

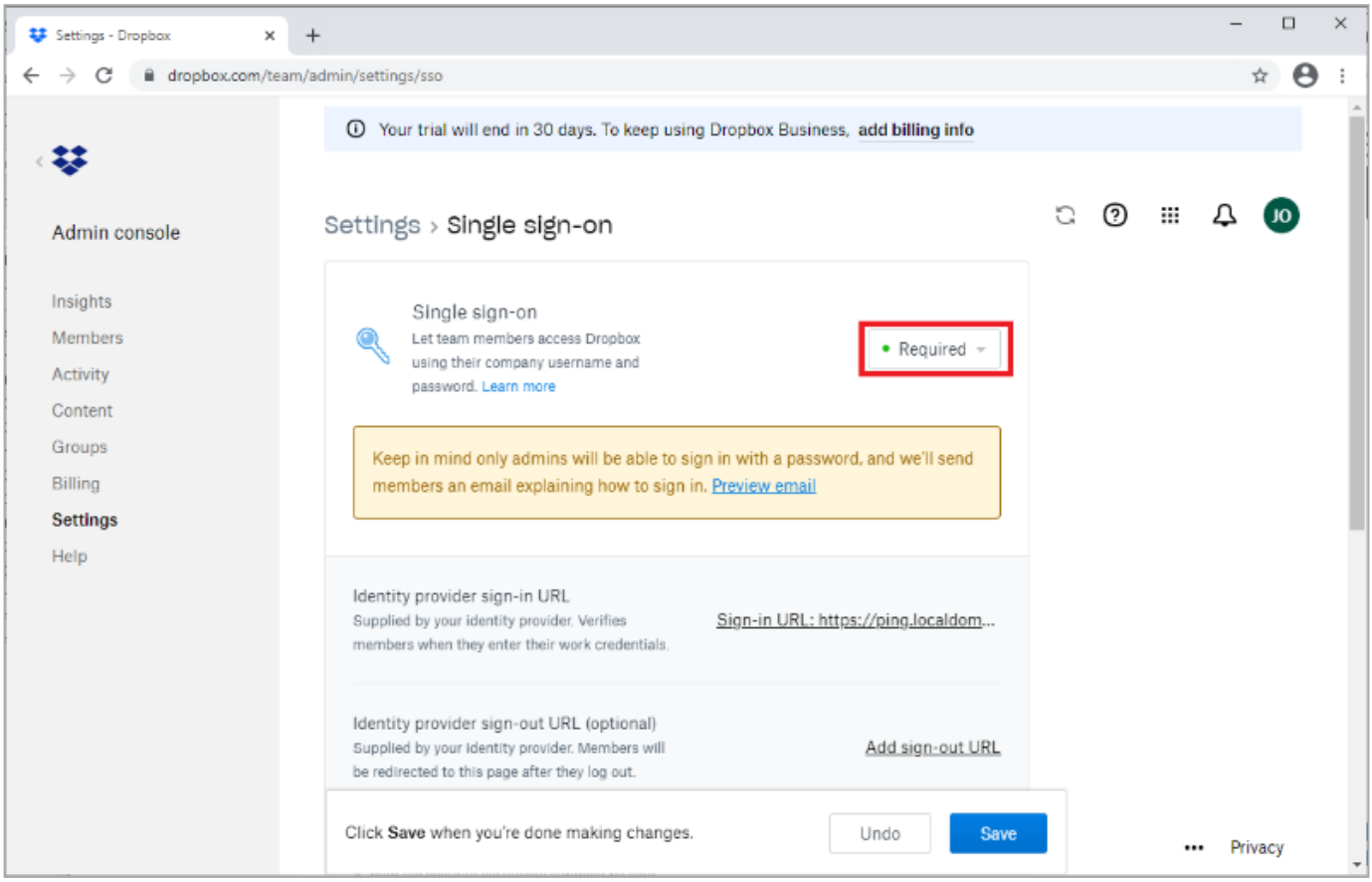


2. Click **Settings**.

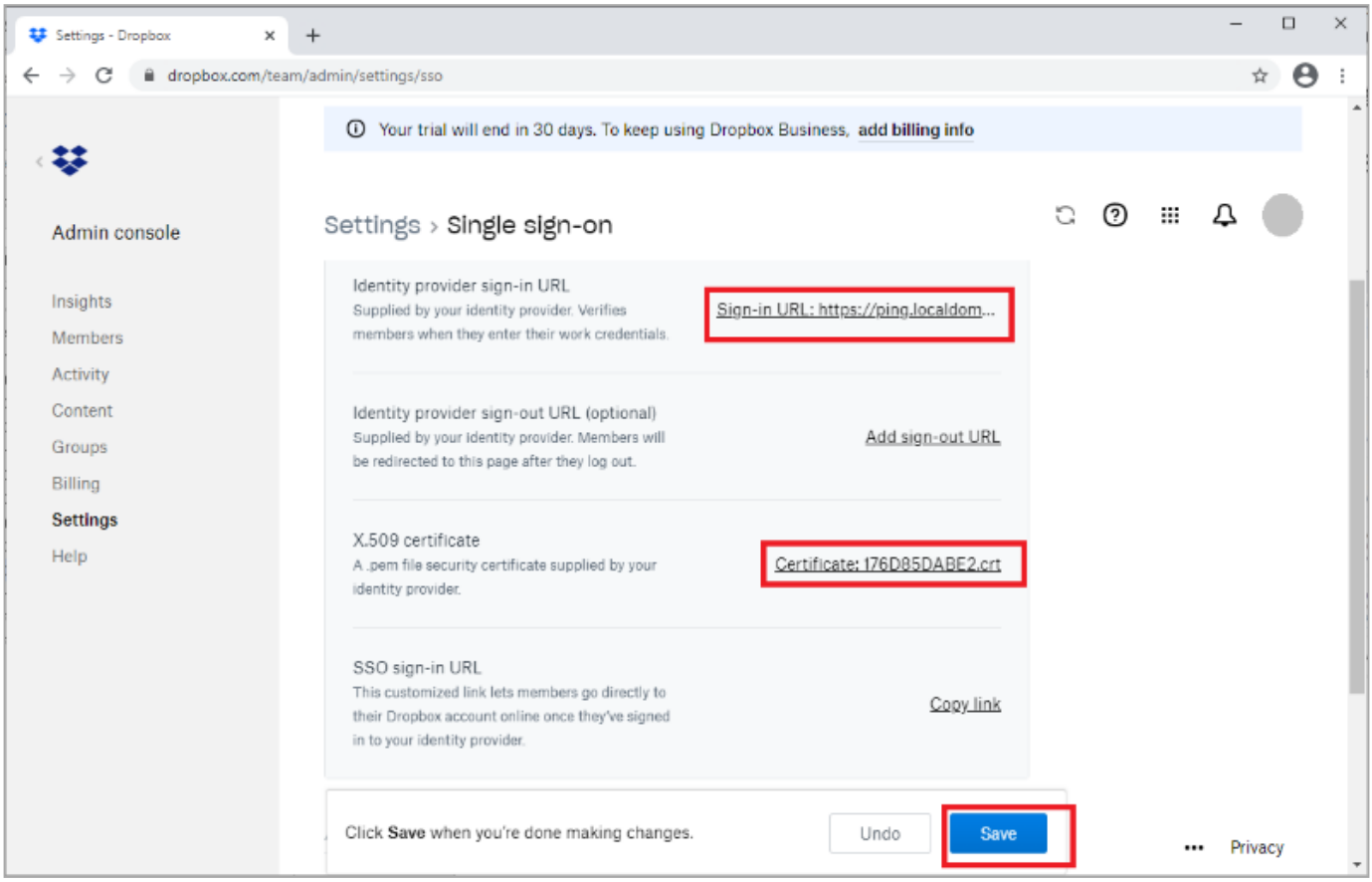
3. Click the **Single sign-on** section.



4. For **Single sign-on**, select **Required**.



5. In the **Identity provider sign-in URL** field, enter the **URL Location for SingleSignOnService Location** value that you retrieved from the PingFederate SP metadata that you downloaded.



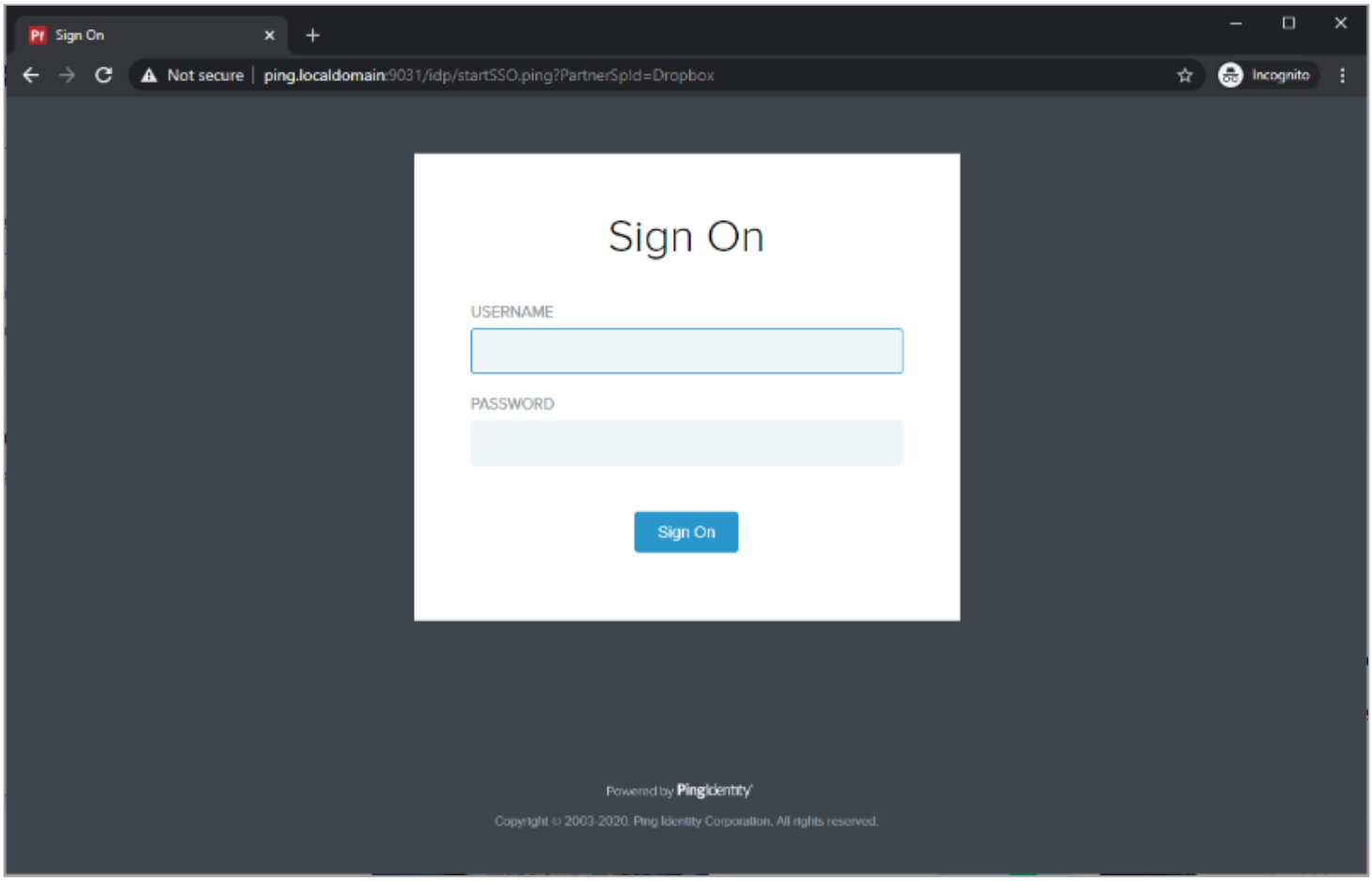
For example, `https://PingFederate-Hostname:PingFederate-Port/idp/SSO.saml2`.

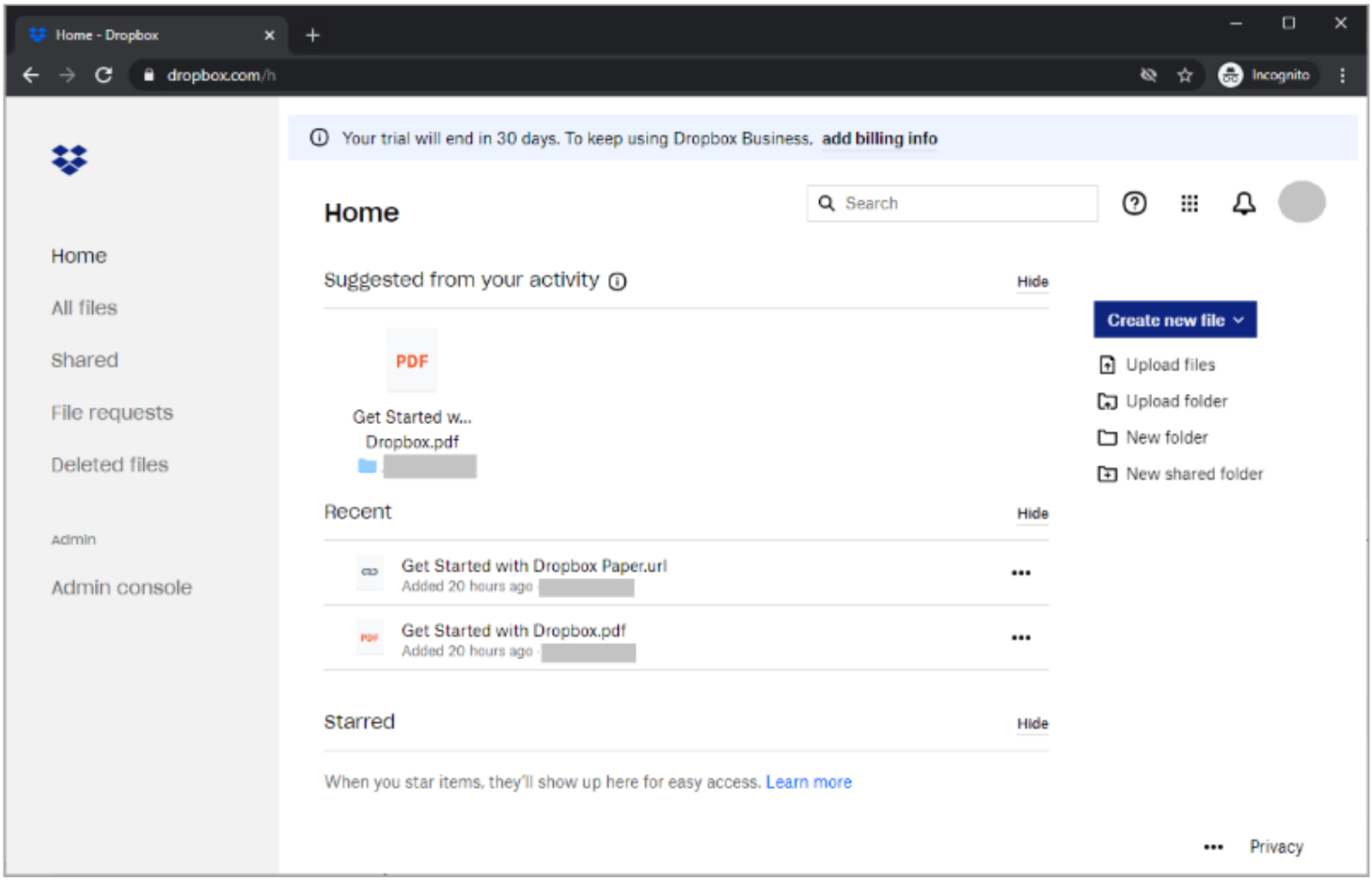
6. Upload the PingFederate signing certificate that you downloaded.
7. Click **Save**.

Test the PingFederate IdP-initiated SSO integration

Go to the **SSO Application Endpoint** value displayed in the PingFederate application configuration for the Dropbox configuration.

For example: `https://PingFederate-Hostname:PingFederate-Port/idp/startSSO.ping?PartnerSpId=Dropbox`



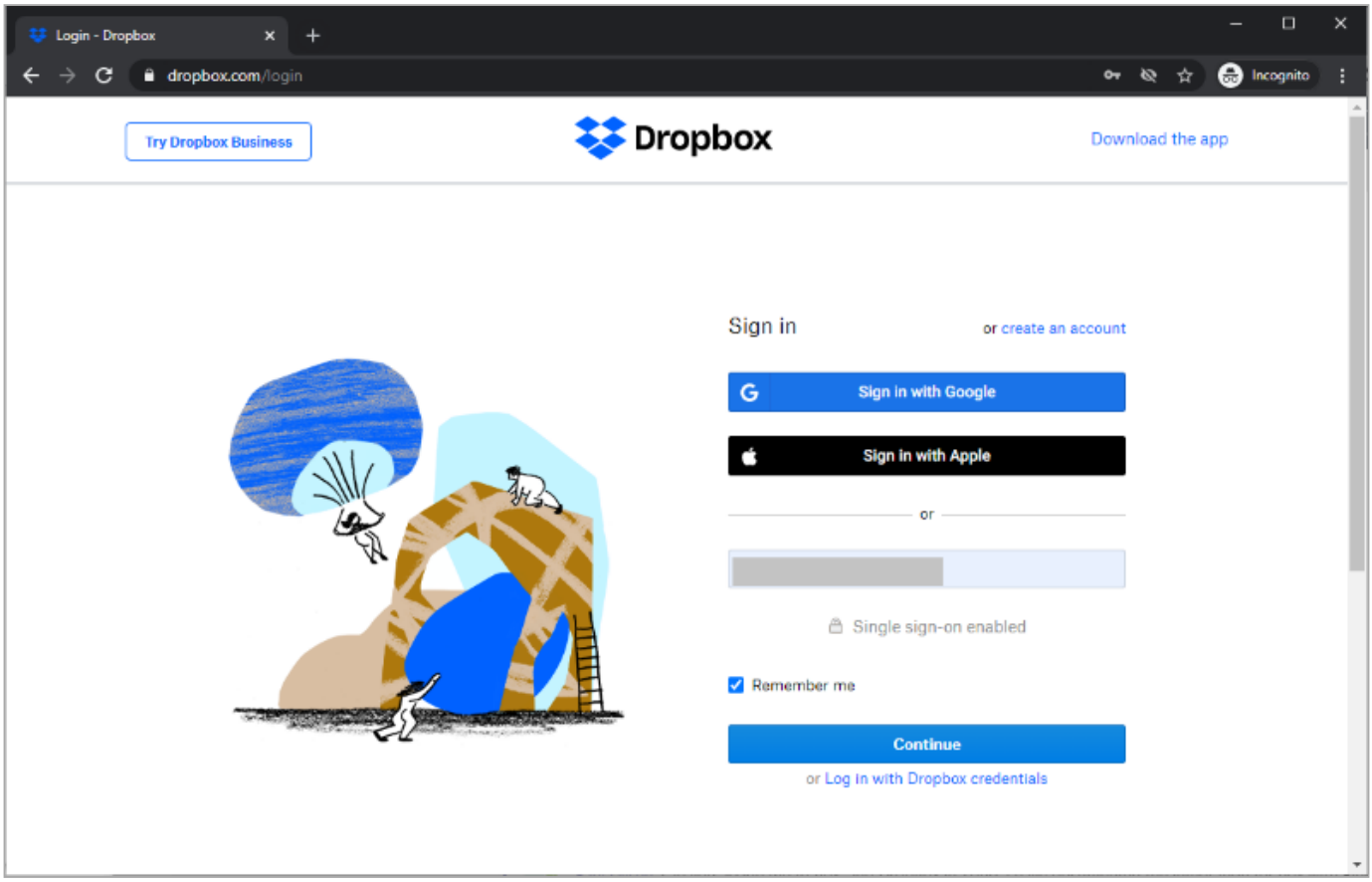


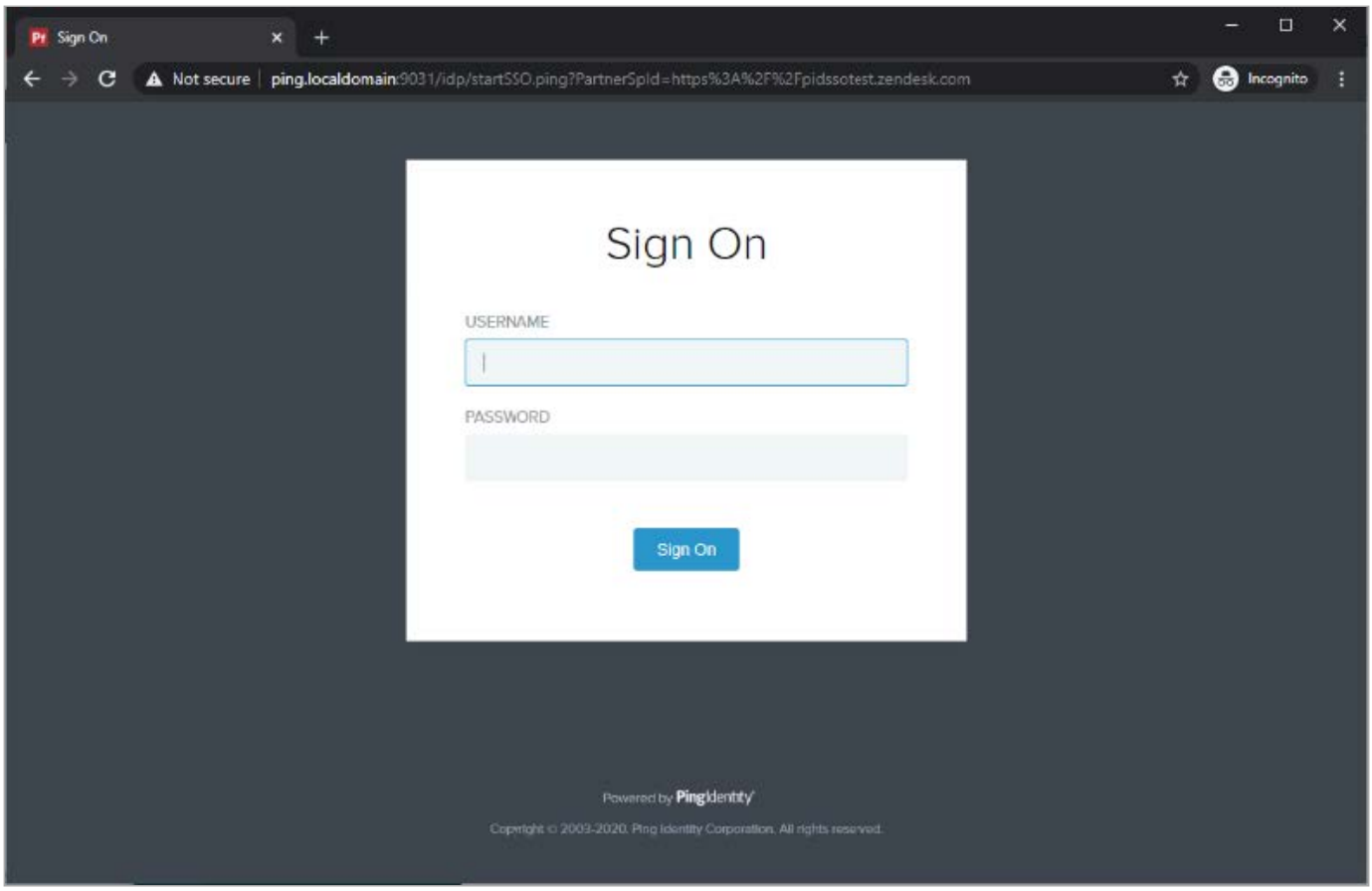
Test the PingFederate SP-initiated SSO integration

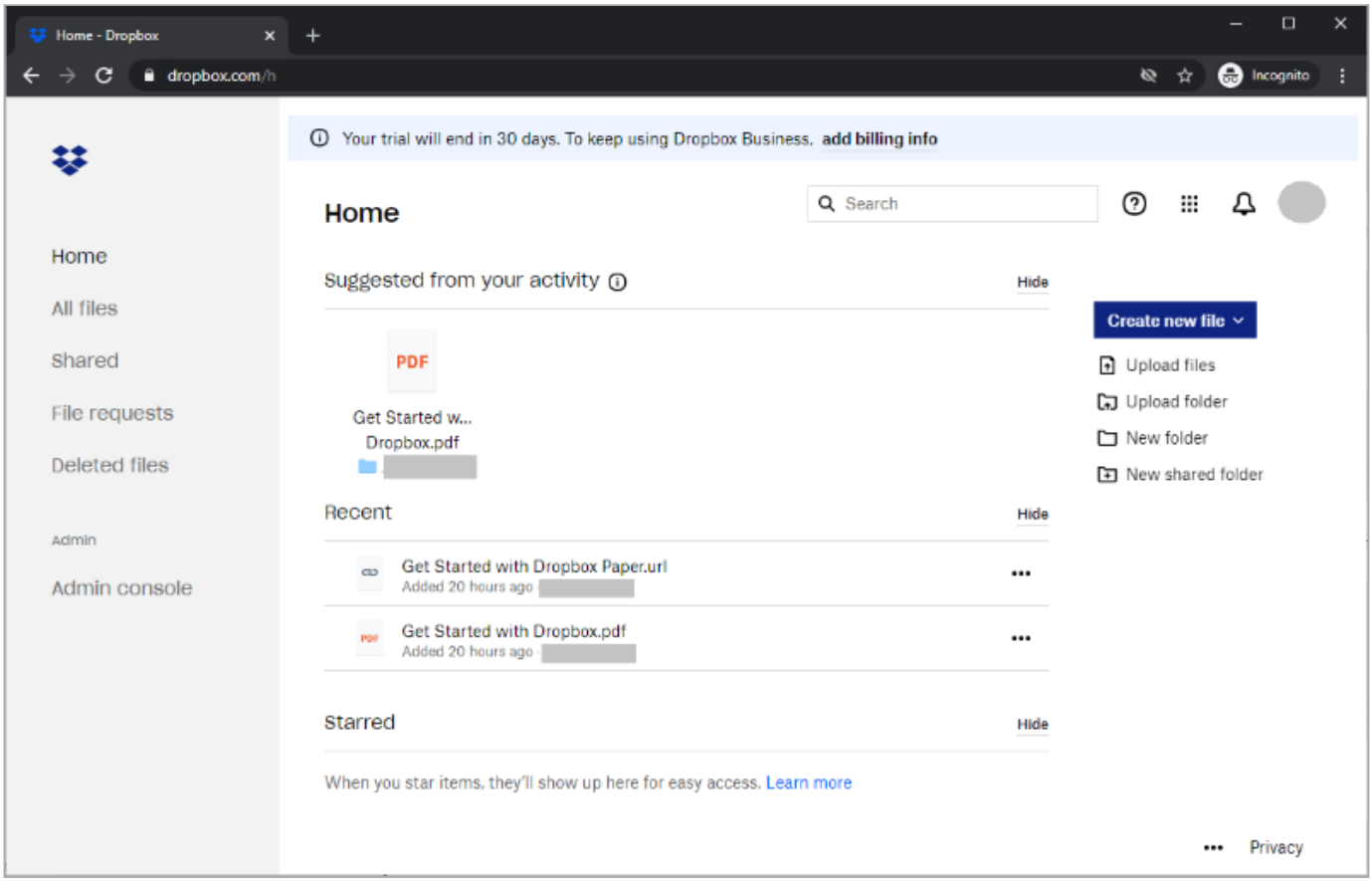
1. Go to `https://www.dropbox.com/login`.
2. Enter your email address.

   Dropbox will automatically detect that single sign-on is enabled based on the email used.
3. Click **Continue**.

   You're redirected to PingFederate for authentication.





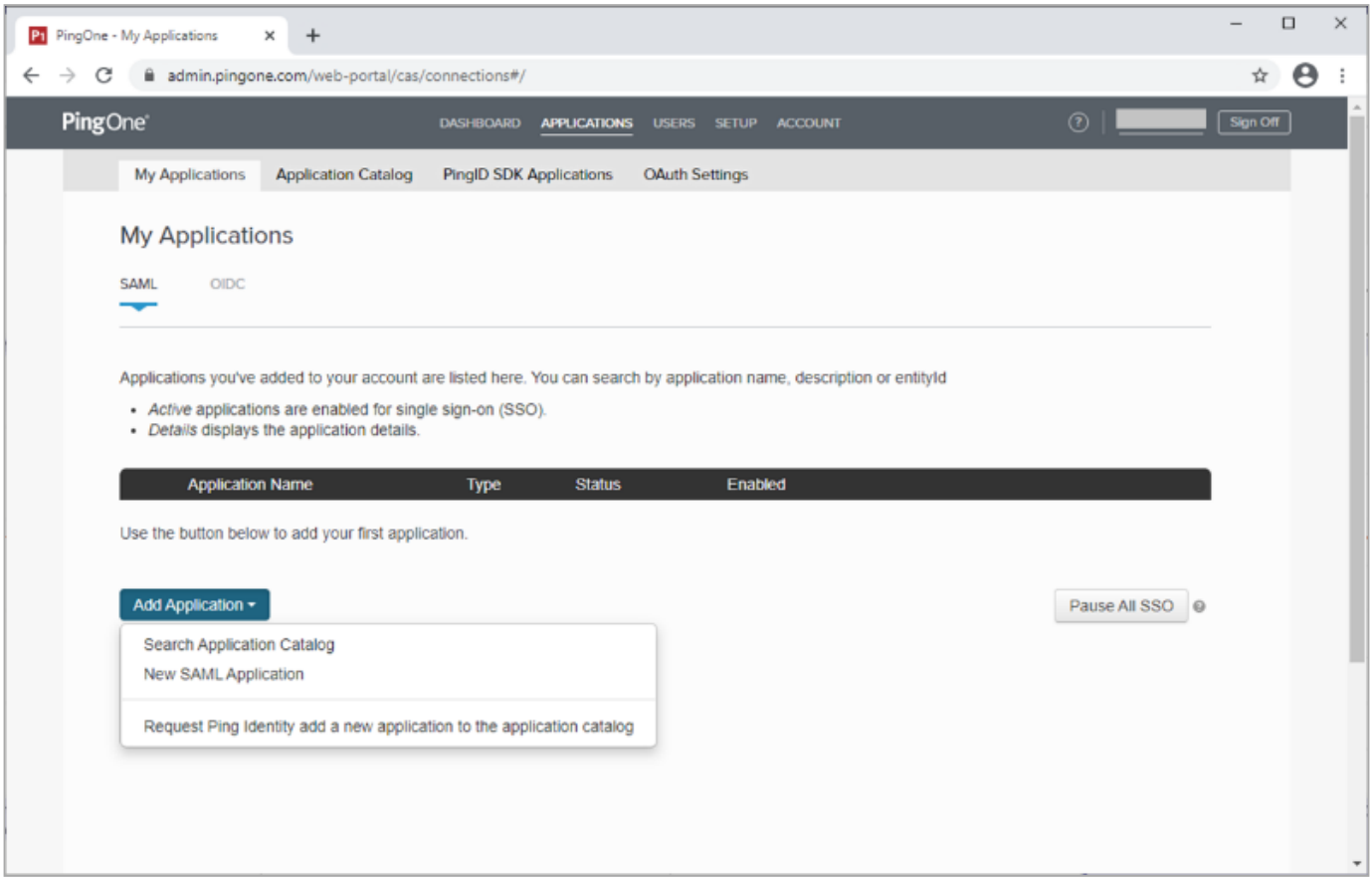


Configuring SAML SSO with Dropbox and PingOne for Enterprise

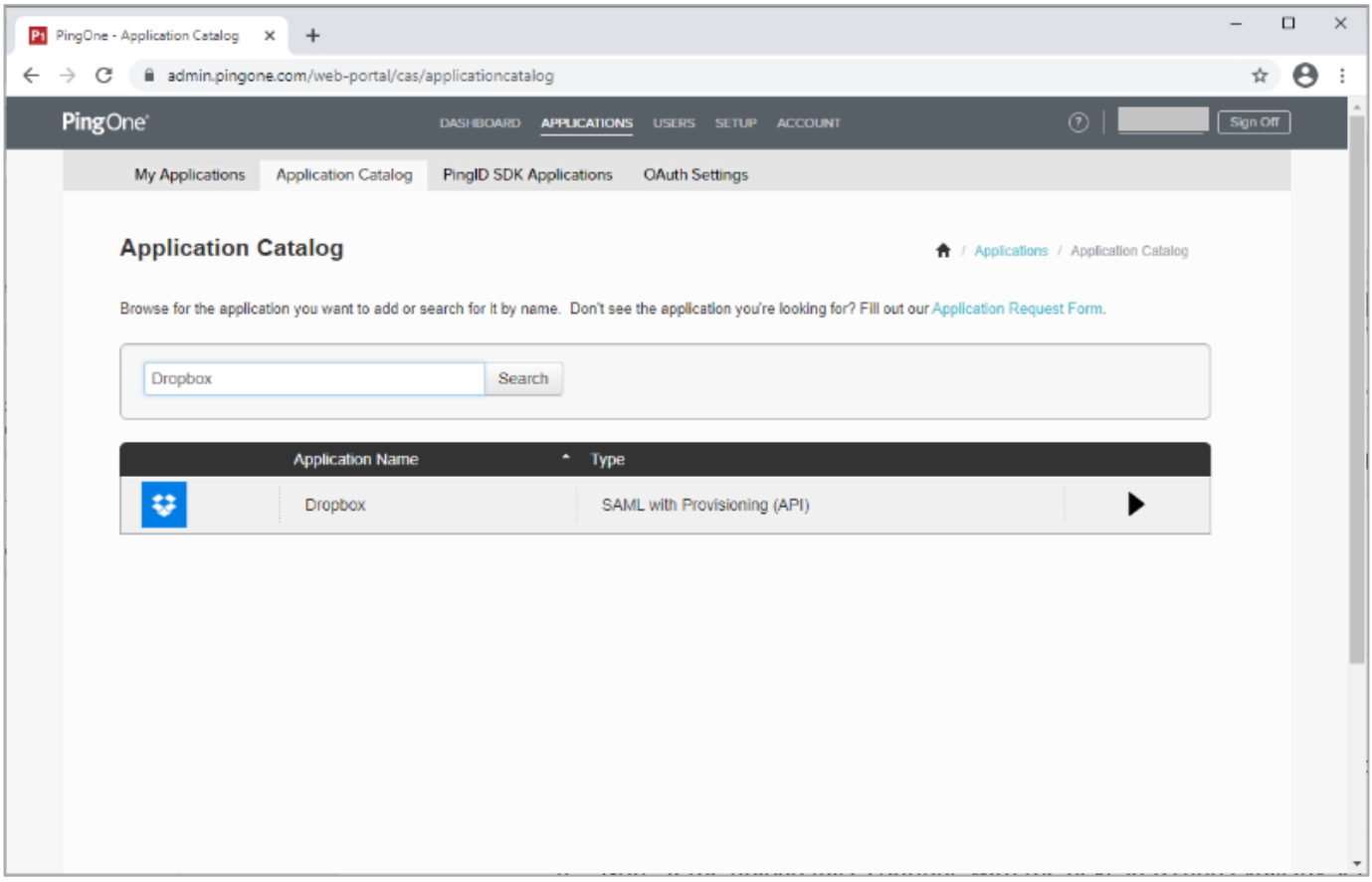
Learn how to configure SAML SSO with Dropbox and PingOne for Enterprise.

Create a PingOne for Enterprise application for Dropbox

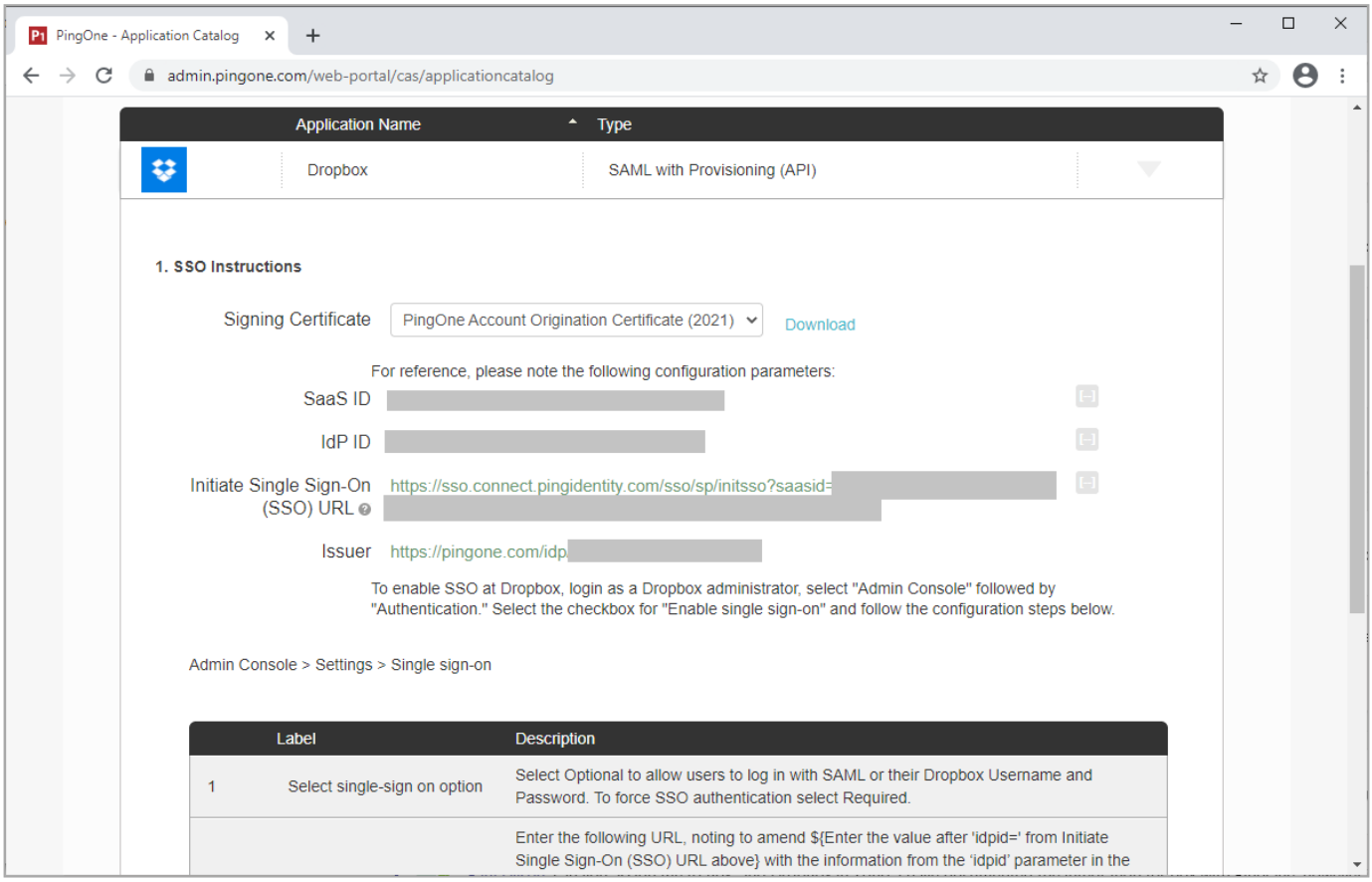
1. Sign on to PingOne for Enterprise and click **Applications**.
2. On the **SAML** tab, click **Add Application**.



3. Click **Search Application Catalog** and search for `Dropbox`.
4. Click the **Dropbox** row.

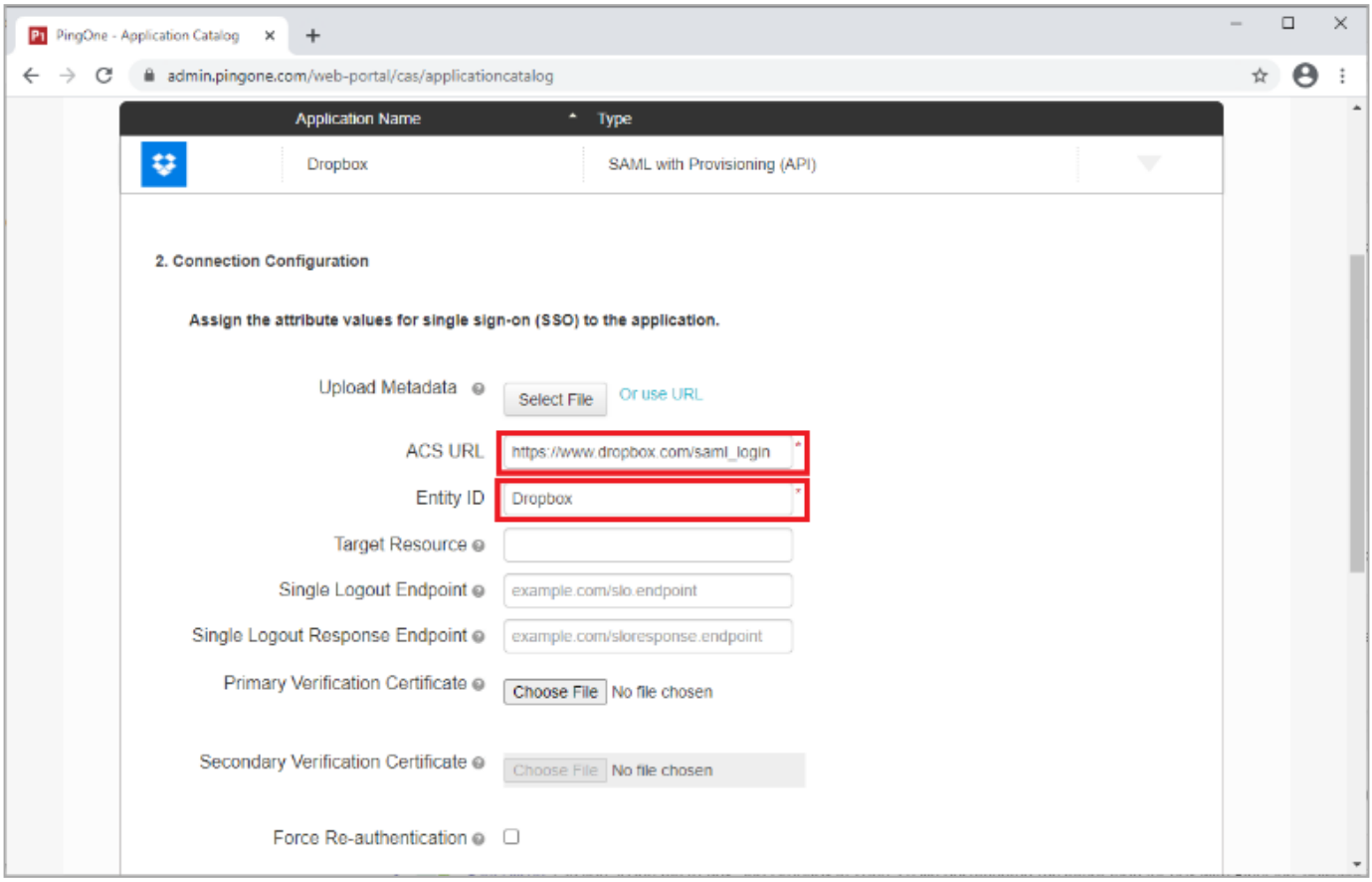


5. Click **Setup**.
6. Select the appropriate signing certificate.
7. Review the steps, and note the **PingOne for Enterprise SaaS ID**, **IdP ID**, **Initiate Single Sign-on (SSO) URL**, and **Issuer** values.

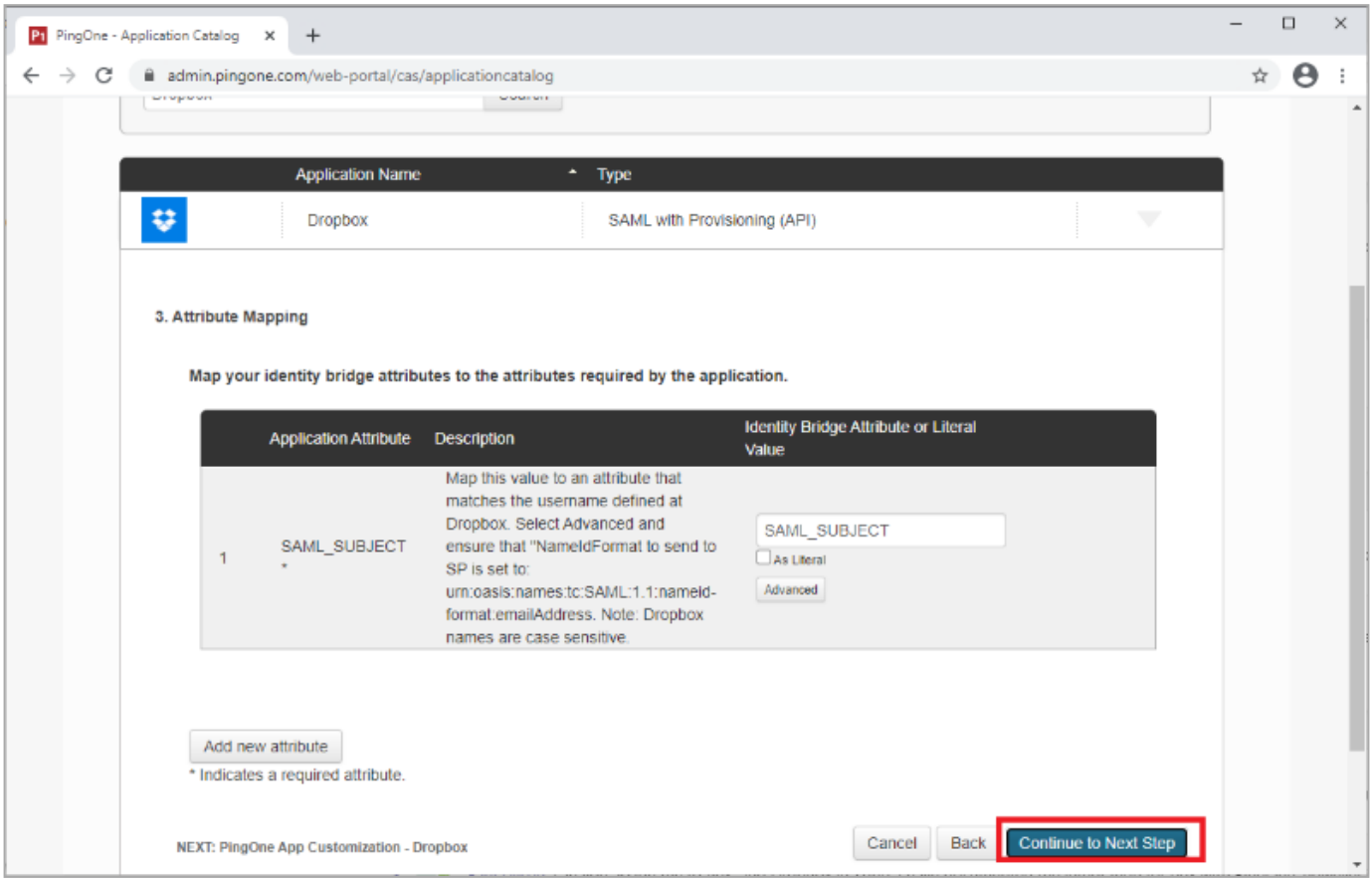


8. Click **Continue to Next Step**.

9. Ensure **ACS URL**is set to `https://www.dropbox.com/saml_login` and **Entity ID** is set to `Dropbox`.

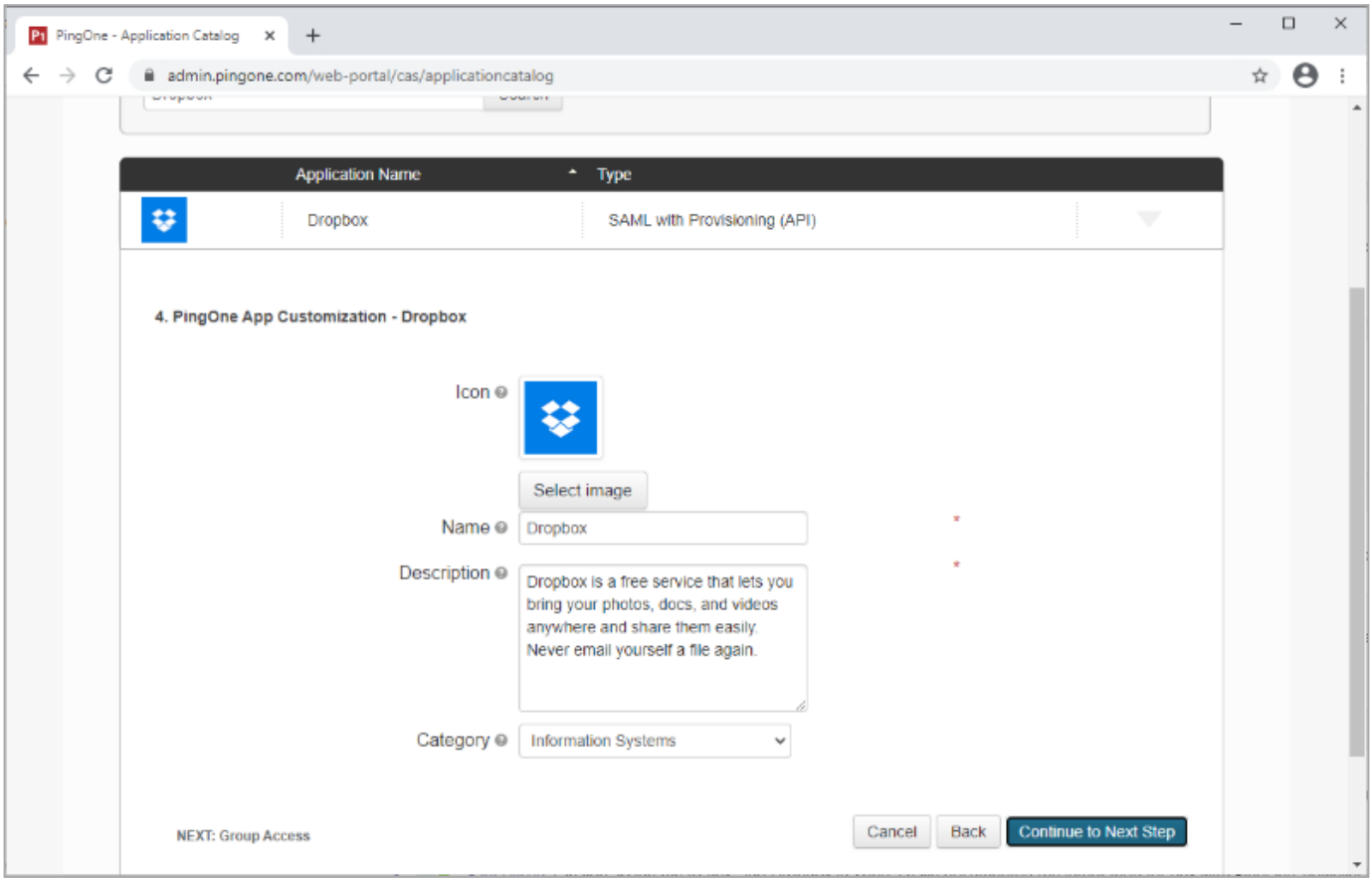


10. Click **Continue to Next Step**.
11. In the **Attribute Mapping** section, in the **Identity Bridge Attribute or Literal Value** column of the **SAML_SUBJECT** row, select the attribute **SAML_SUBJECT**.

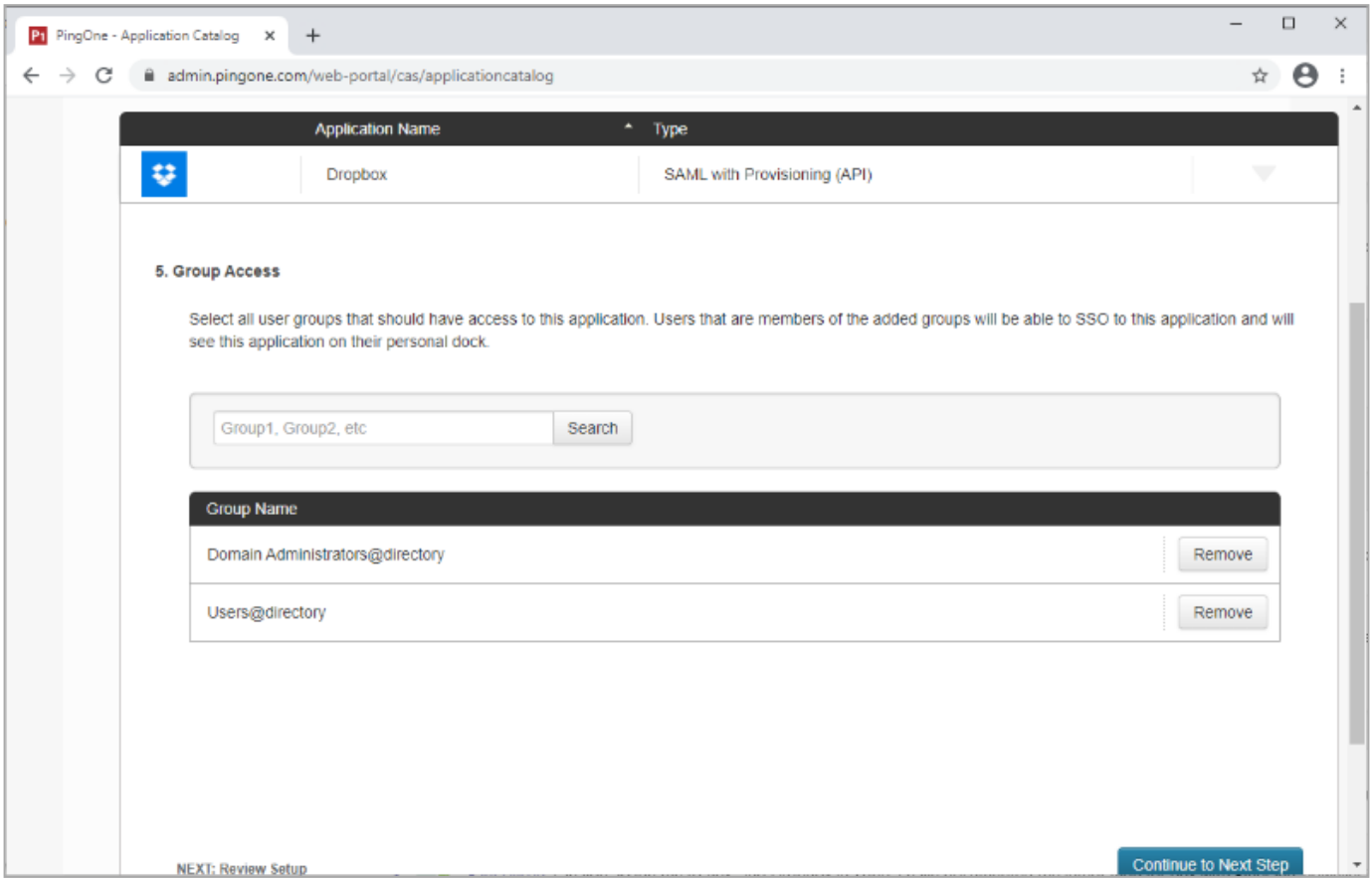


12. Click **Continue to Next Step**.

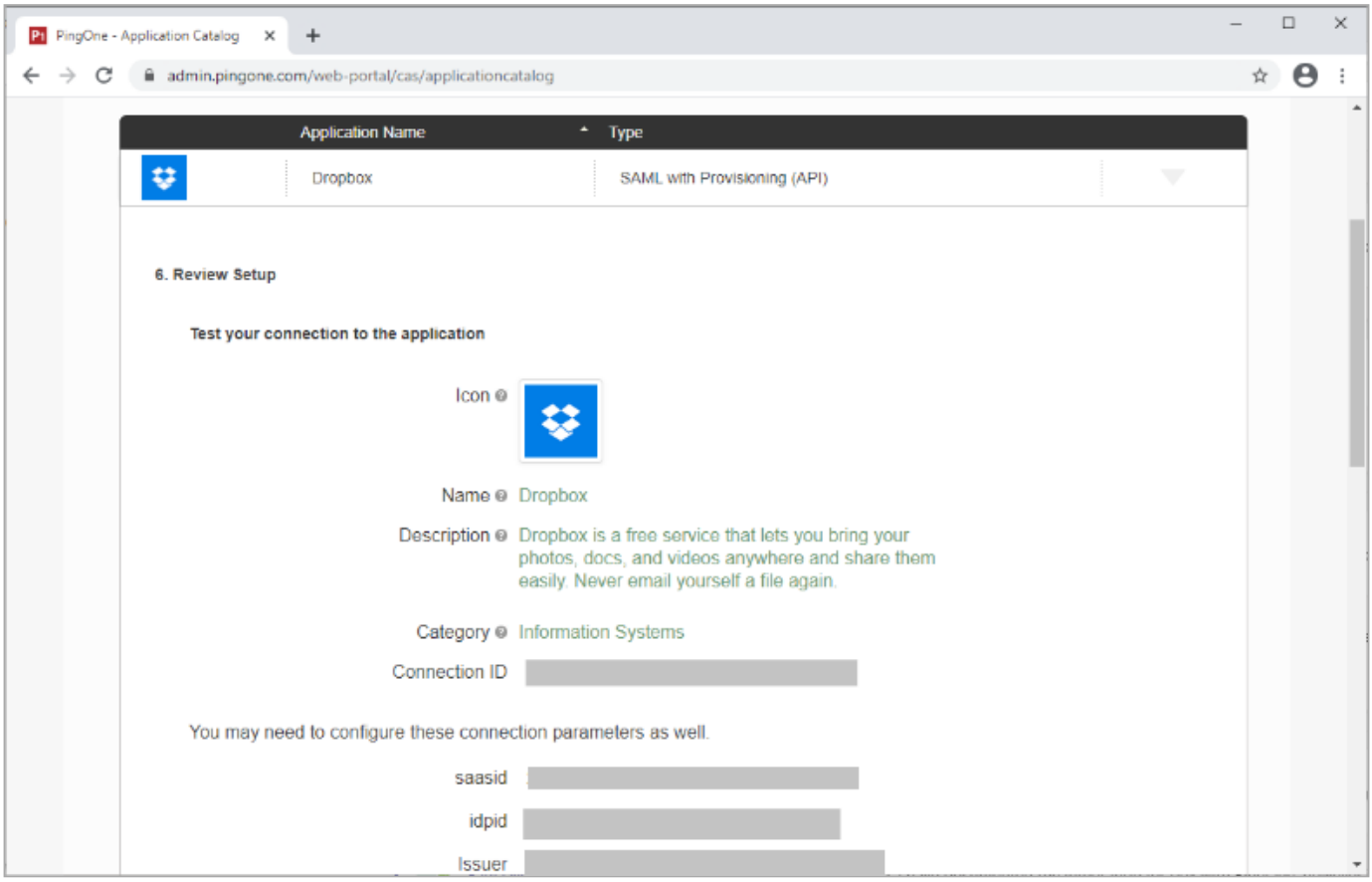
13. Update the **Name**, **Description**, and **Category** fields as required.

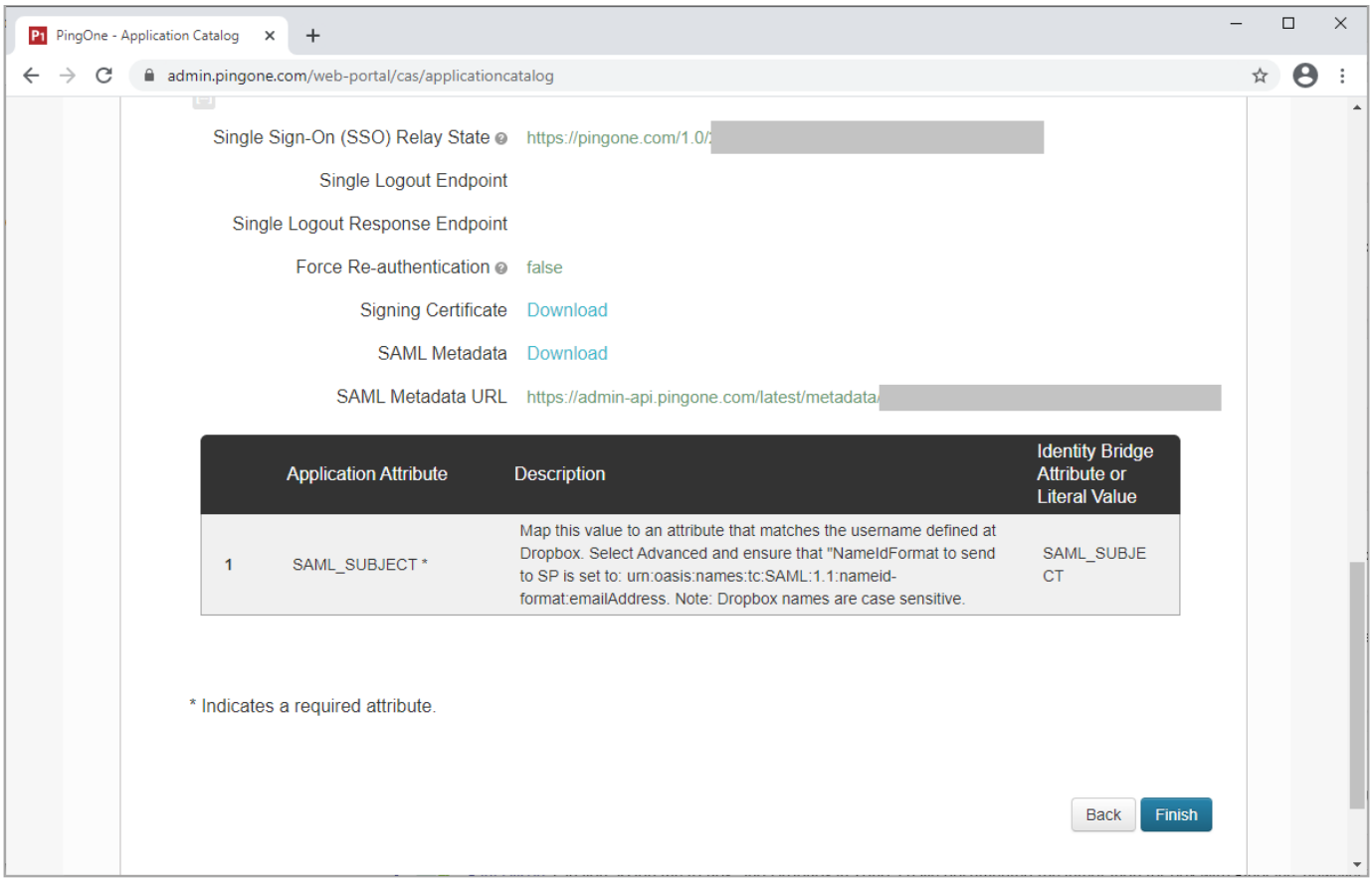


14. Click **Continue to Next Step**.
15. Add suitable user groups for the application.
16. Click **Continue to Next Step**.



17. Review the settings.





18. Copy the **Single Sign-On (SSO) URL** value to a temporary location.

    This is the IdP-initiated SSO URL that you can use for testing.

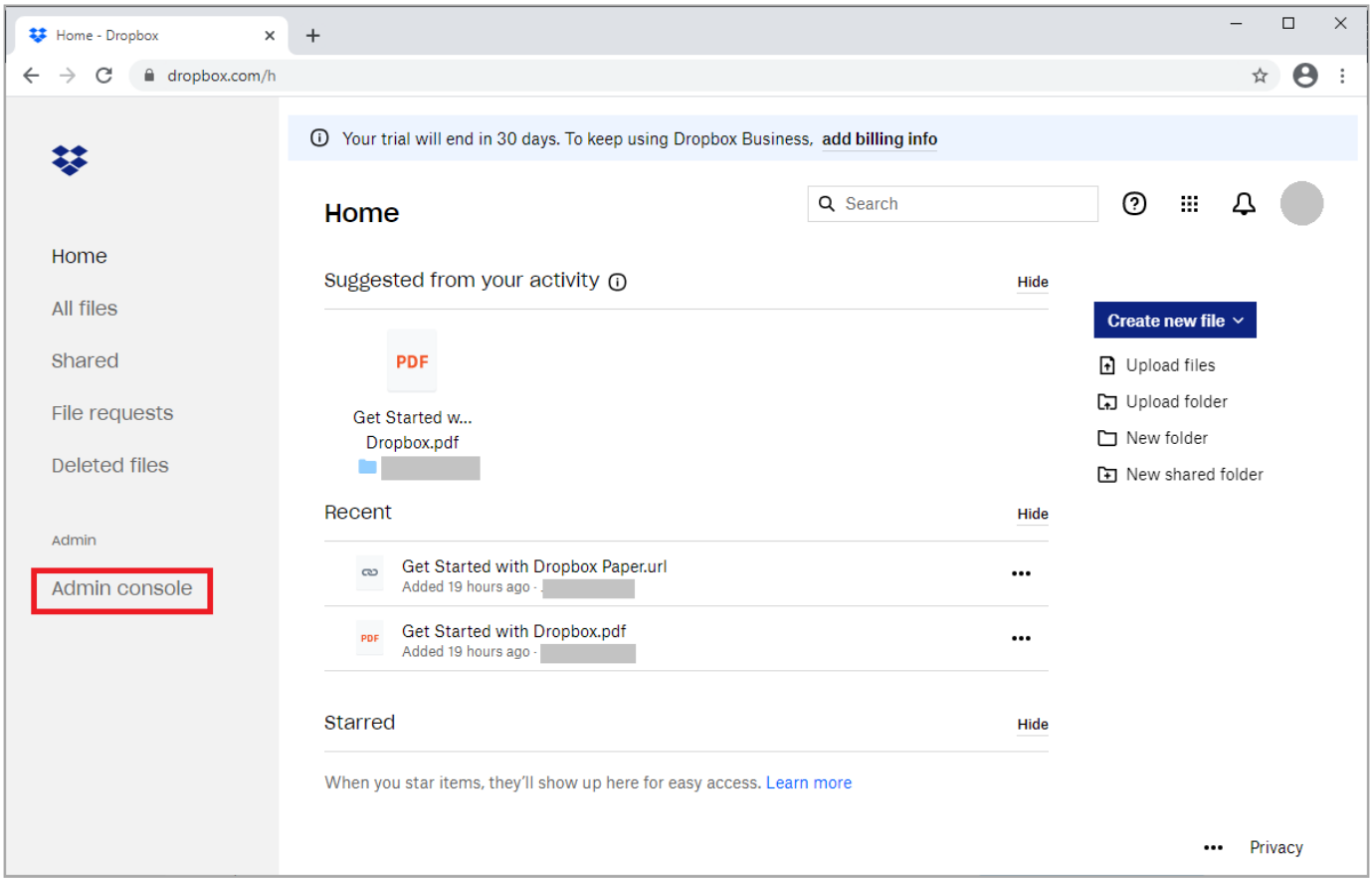
19. On the **Signing Certificate** row, click **Download** You will use this for the Dropbox configuration.

20. On the **SAML Metadata** row, click **Download**. You will use this for the Dropbox configuration.

21. Click **Finish**.

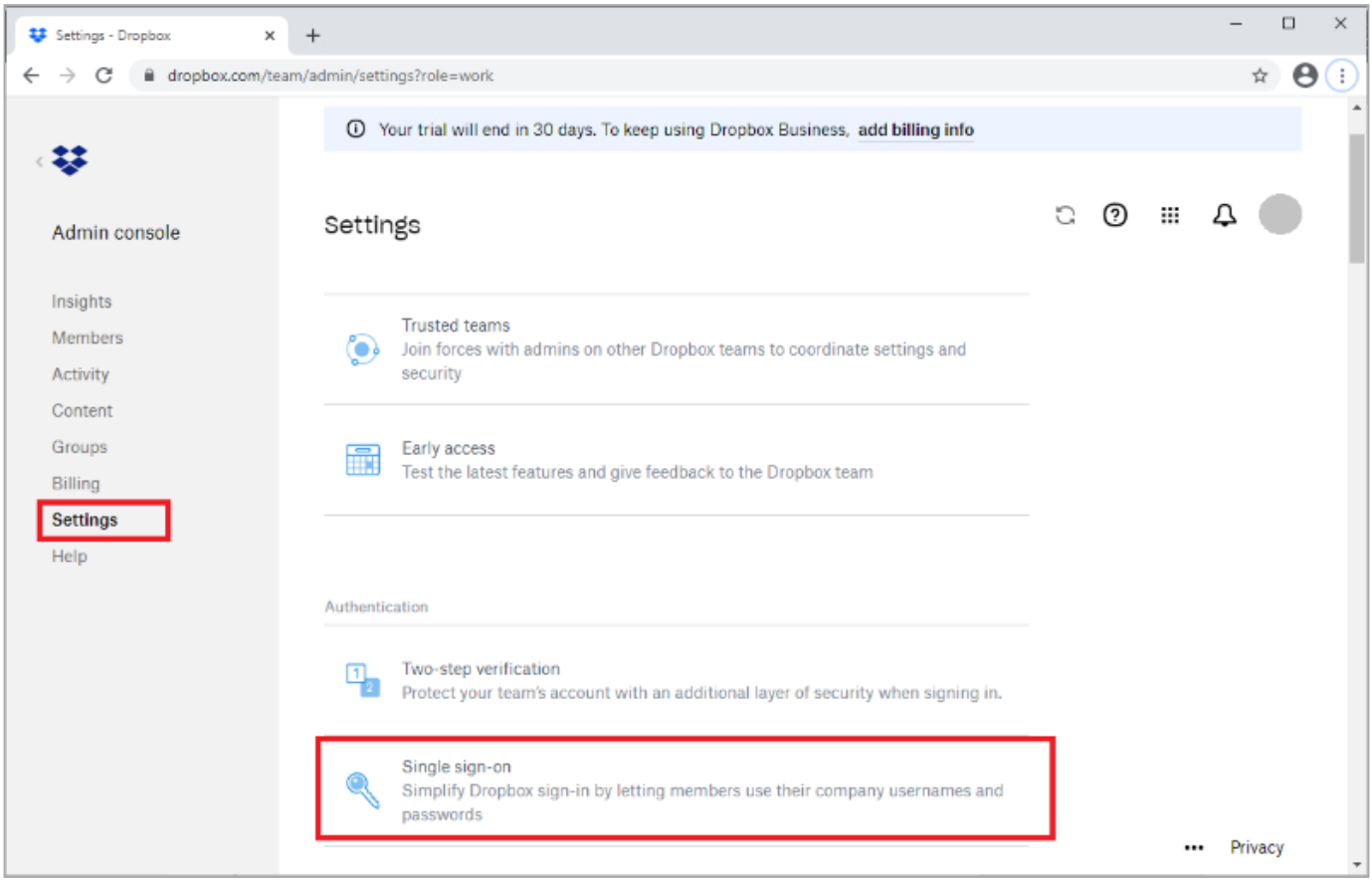
Configure a PingOne for Enterprise IdP connection for Dropbox

1. Sign on to the Dropbox Admin Console as an administrator.

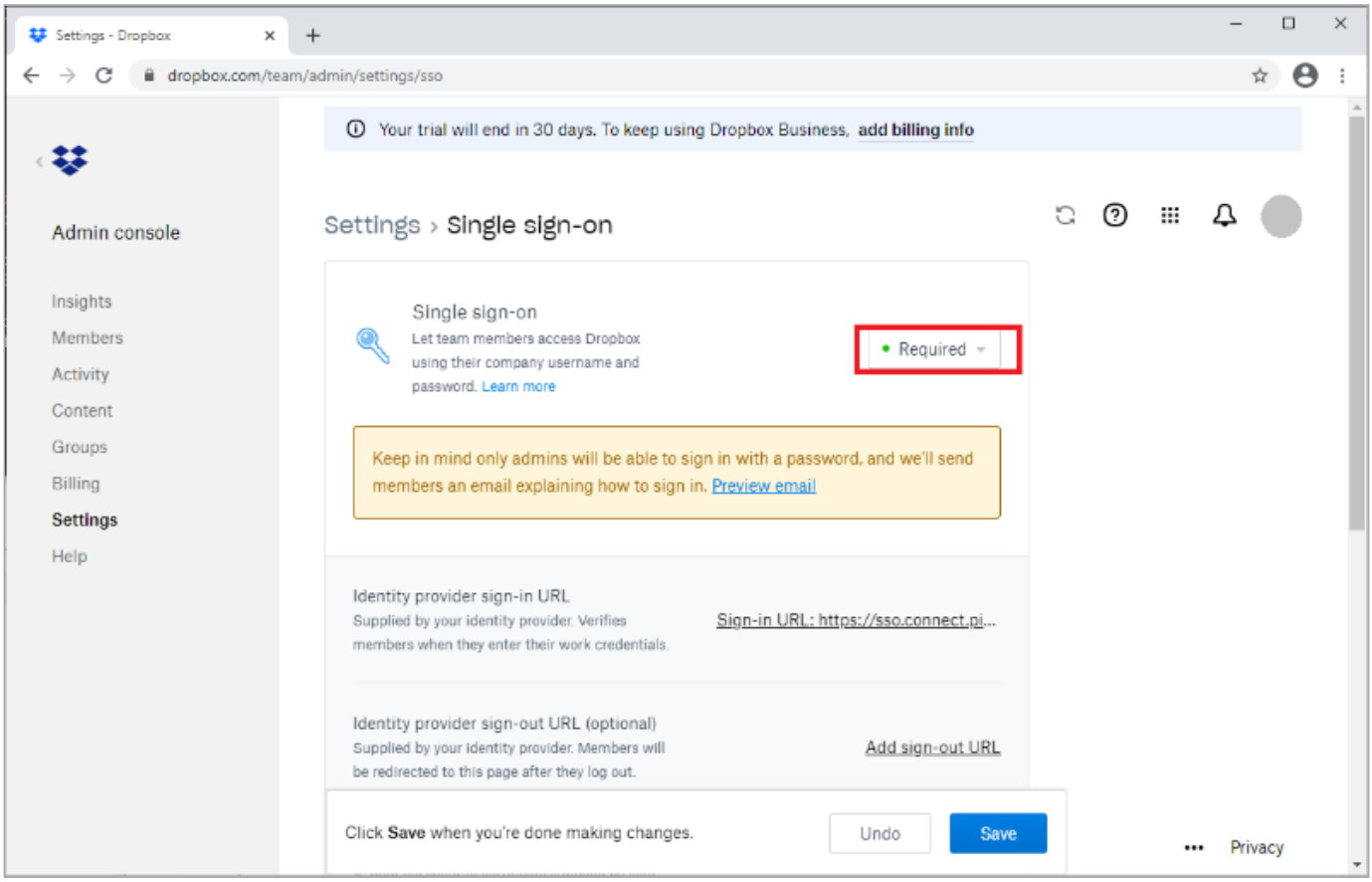


2. Click **Settings**.

3. Click the **Single sign-on** section.

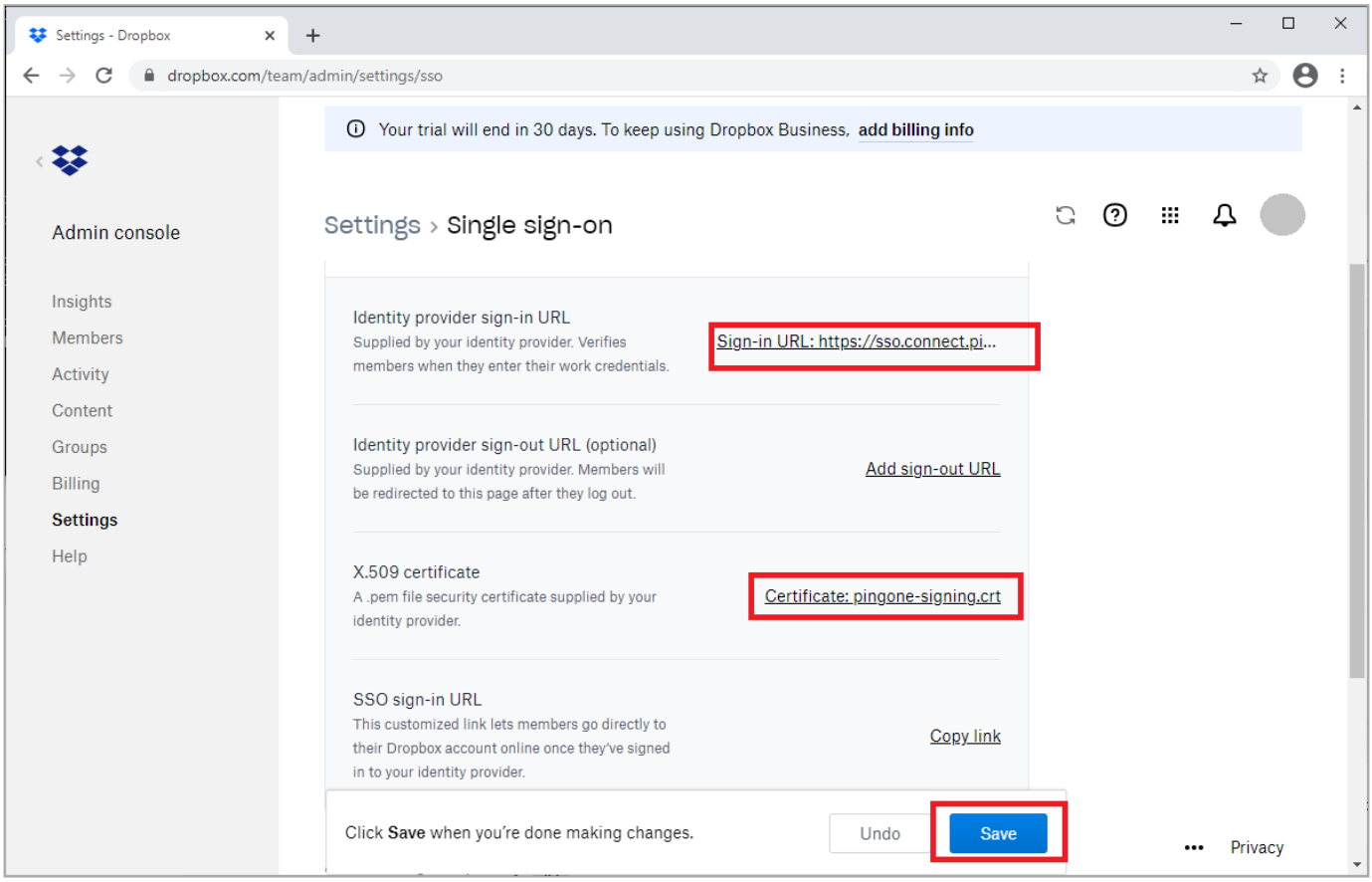


4. For **Single sign-on**, select **Required**.



5. In the **Identity provider sign-in URL** field, enter the **URL Location for SingleSignOnService Location** value that you retrieved from the PingOne for Enterprise SP metadata that you downloaded.

   For example, `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=idpid`

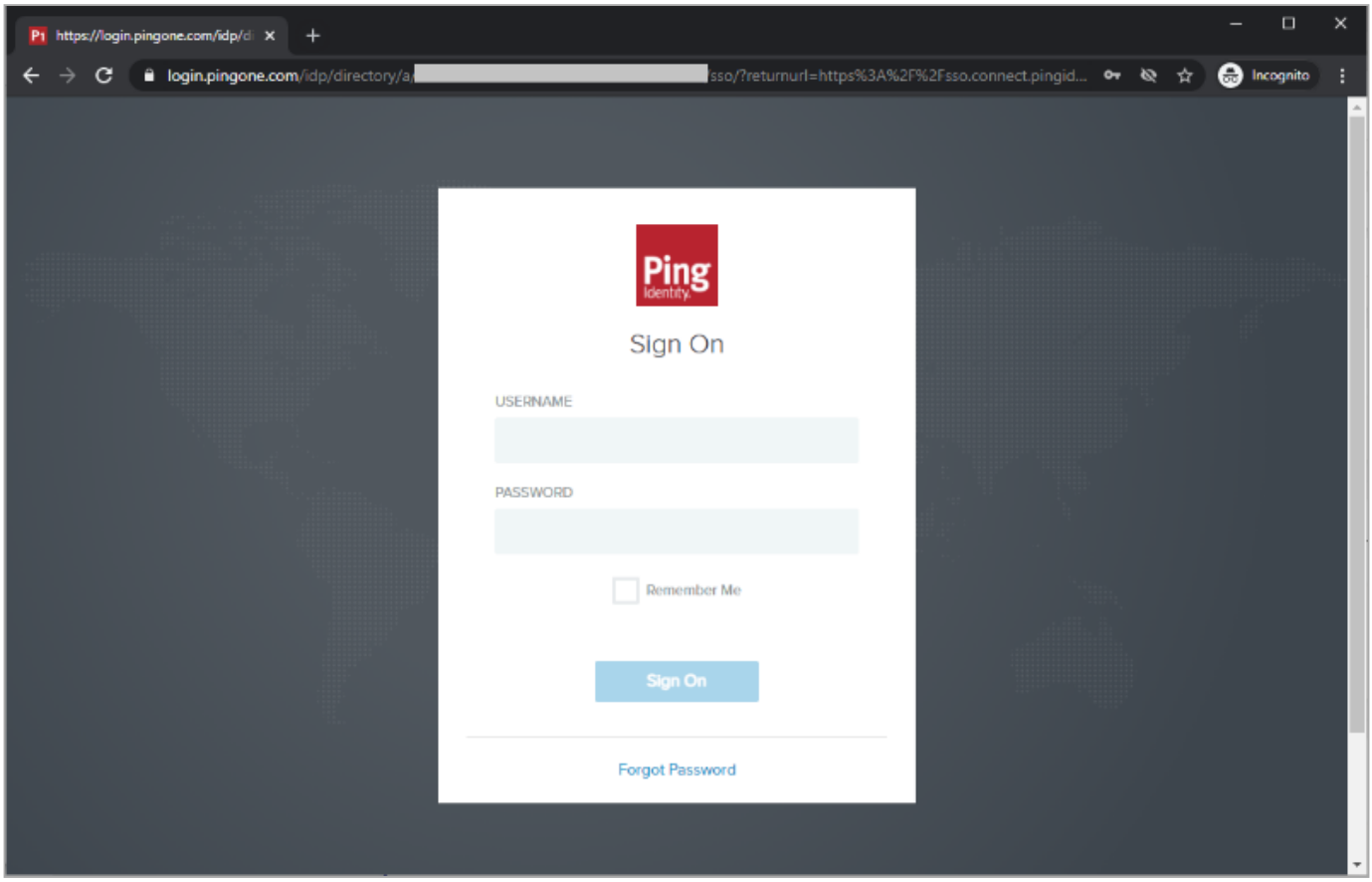


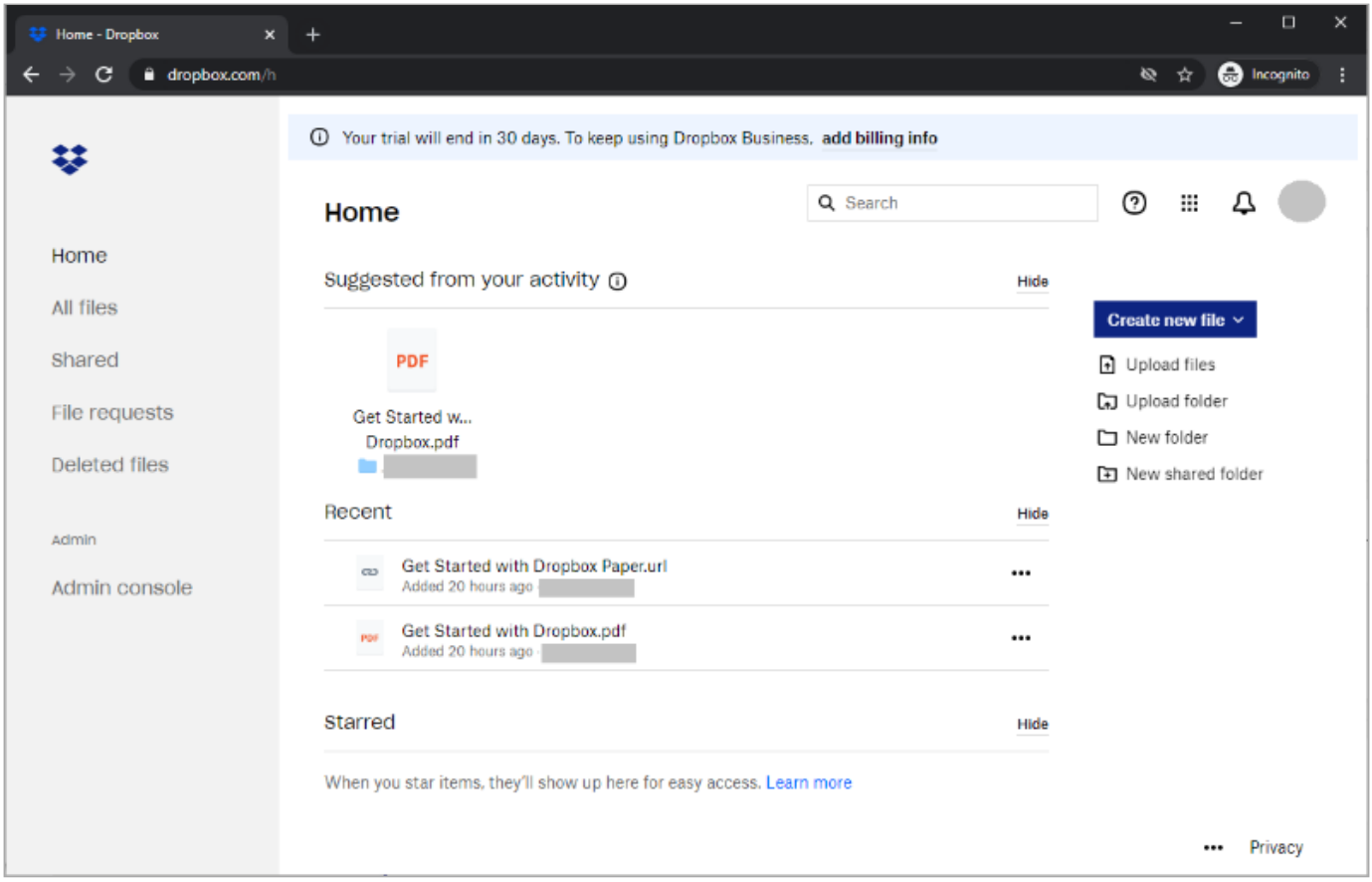
6. Upload the PingOne for Enterprise signing certificate that you downloaded.
7. Click **Save**.

Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to the **Single Sign-On (SSO) URL** in the PingOne for Enterprise Application configuration to perform IdP-initiated SSO.

   ```
   https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=saasid&idpid=idpid
   ```



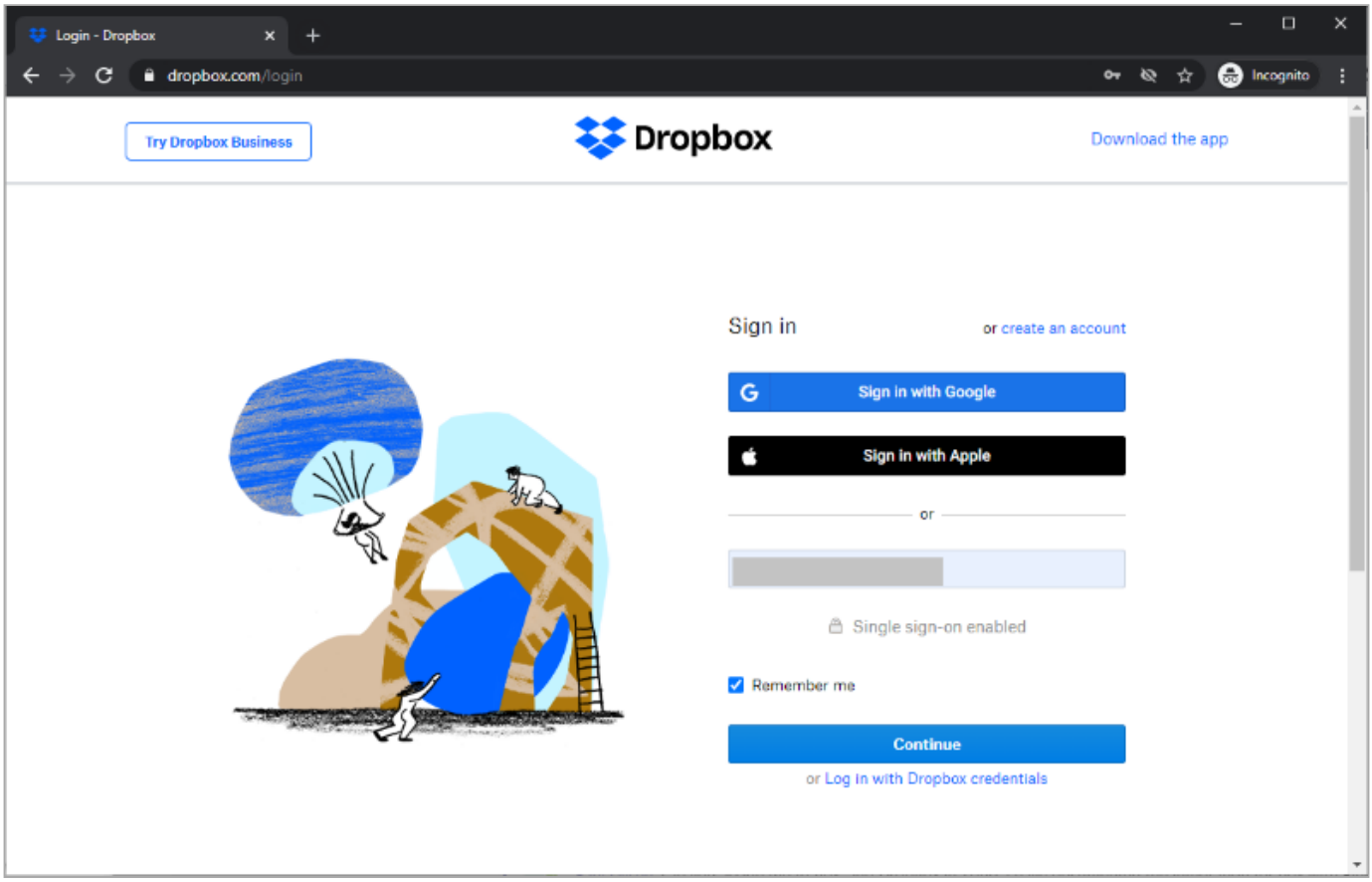


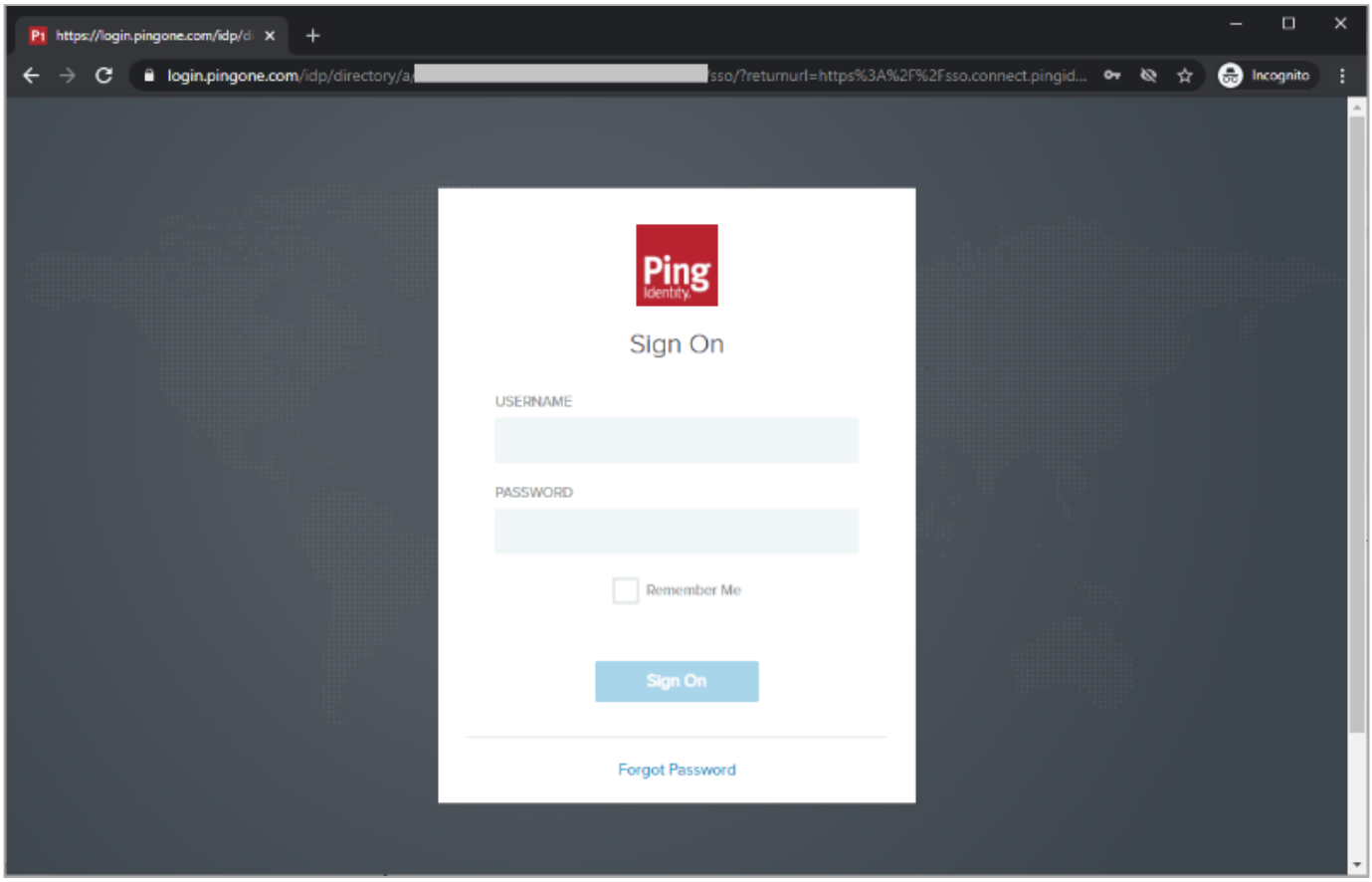
Test the PingOne for Enterprise SP-initiated SSO integration configuration

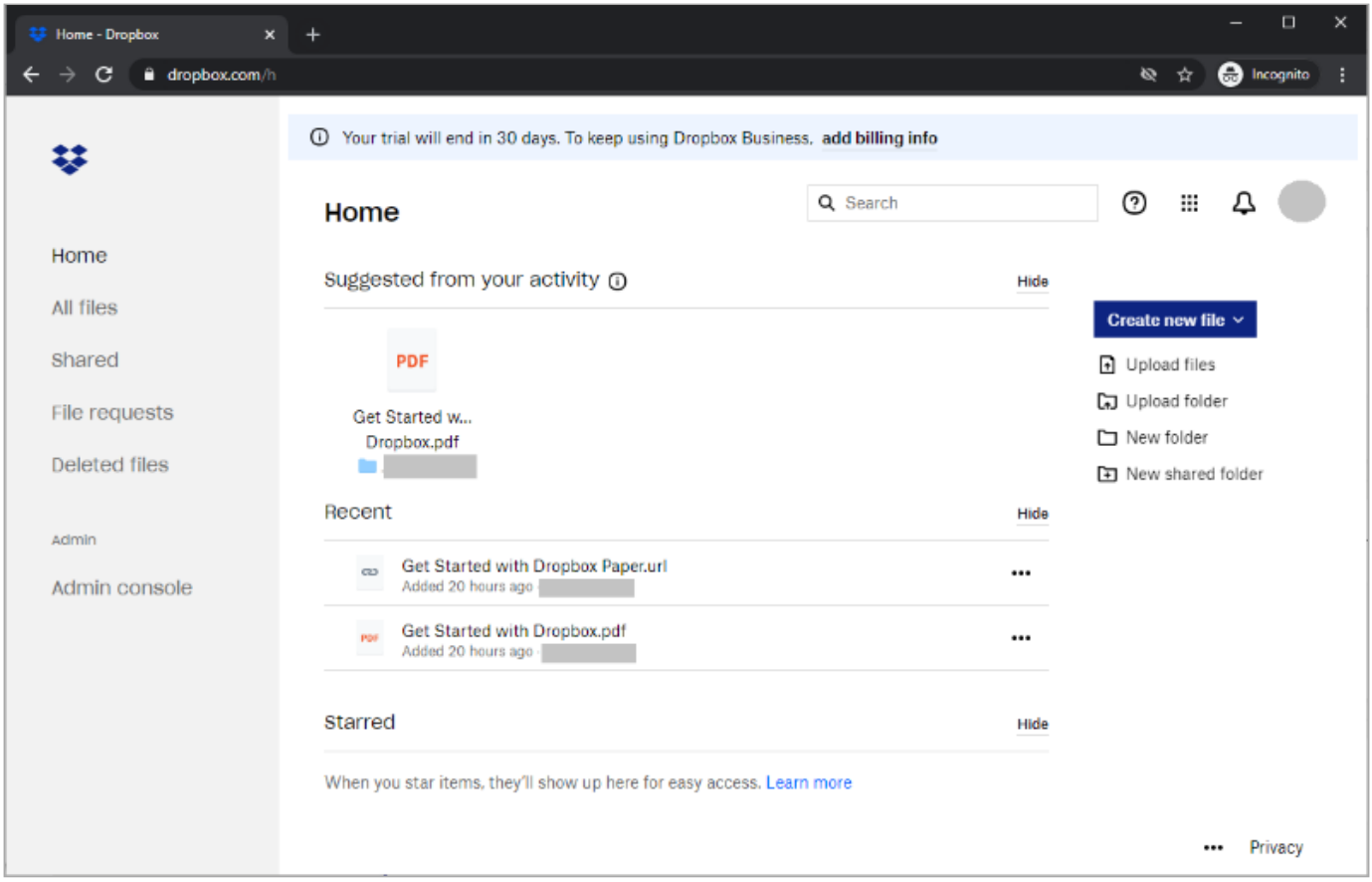
1. Go to `https://www.dropbox.com/login`.
2. Enter your email address.

   Dropbox automatically detects that single sign-on is enabled based on the email used.
3. Click **Continue**.

   You're redirected to PingOne for Enterprise for authentication.







Egnyte

Configuring SAML SSO with Egnyte and PingFederate

Learn how to enable Egnyte sign-on from a PingFederate URL (IdP-initiated sign-on) and direct Egnyte sign-on using PingFederate (SP-initiated sign-on).

Before you begin

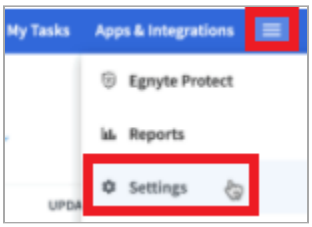
- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate Egnyte with at least one user to test access.
- You must have administrative access to PingFederate and Egnyte.

Create an SP connection for Egnyte

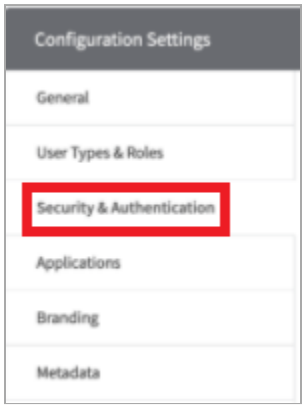
1. Sign on to the PingFederate administrative console.
2. Create an SP connection for Egnyte in PingFederate.
    1. Configure using **Browser SSO** profile **SAML 2.0**.
    2. Set **Partner's Entity ID** to `https://saml-auth.egnyte.com`.
    3. Enable the following **SAML Profiles**:
        - **IdP-Initiated SSO**
        - **SP-Initiated SSO**
    4. In **Assertion Creation → Authentication Source Mapping → Attribute Contract Fulfillment**, map the **SAML_SUBJECT** to the attribute containing the user's email address.
    5. In **Protocol Settings → Assertion Consumer Service URL**, set **Binding** to **POST** and set **Endpoint URL** to `https://your-Egnyte-domain.egnyte.com/samlconsumer/PingFederate`.
    6. In **Protocol Settings → Allowable SAML Bindings**, enable **POST**.
    7. In **Credentials → Digital Signature Settings**, select the **PingFederate Signing Certificate**.
3. Save the configuration.
4. Export the signing certificate.
5. Export and then open the metadata file and copy the value of the entityID and the Location entry (`https://your-value/idp/SSO.saml2`).

Add the PingFederate connection to Egnyte

1. Sign on to your Egnyte Admin organization as an administrator.
2. Click the menu icon and then click **Settings**.



3. Click the **Security and Authentication** tab.



4. In the **Single sign-on authentication** list, select **SAML 2.0**.
5. In the **Identity provider** list, select **Ping Identity**.
6. Set the following values:

Field	Value
Identity provider login URL	The Location value from the metadata that you exported.
Identity provider entity ID	The entityID value from the metadata that you exported.
Identity provider certificate	In a text editor, open the signing certificate that you downloaded in a text editor. Copy and paste the contents.
Default user mapping	Email address

7. Click **Save**.
8. Go to **Settings → Users and Groups**.
9. Select the appropriate users and set their **AuthType** to **SSO**.

Test the PingFederate IdP-initiated SSO integration

1. Go to the PingFederate **SSO Application Endpoint** for the Egnyte SP connection.
2. Complete the PingFederate authentication.

   You're redirected to your Egnyte domain.

Test the PingFederate SP-Initiated SSO integration

1. Go to `https://your-Egnyte-domain.Egnyte.com`.
2. Select the PingFederate sign-on option.
3. After you're redirected to PingFederate, enter your PingFederate username and password.

   You're redirected back to Egnyte.

Configuring SAML SSO with Egnyte and PingOne for Enterprise

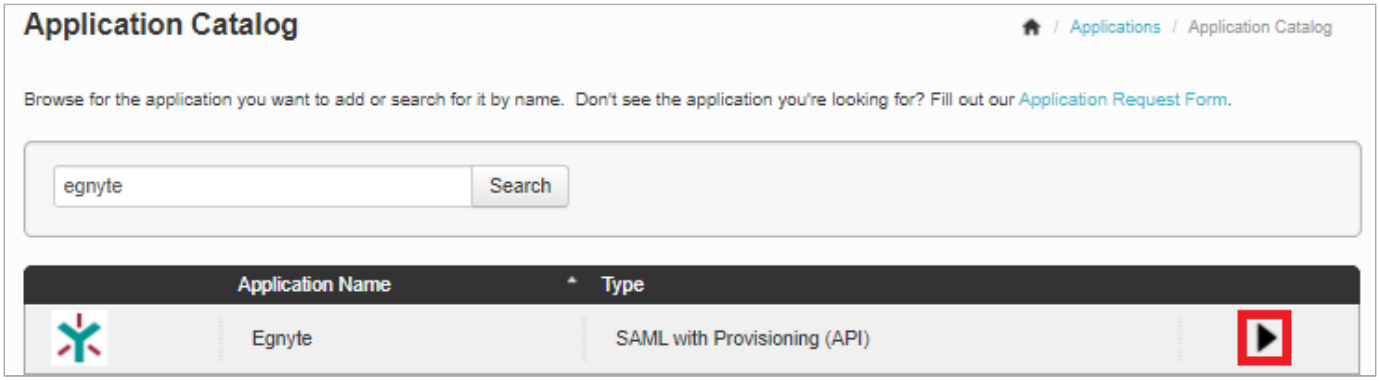
Learn how to enable Egnyte sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct Egnyte sign-on using PingOne for Enterprise (SP-initiated sign-on).

Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate Egnyte with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and Egnyte.

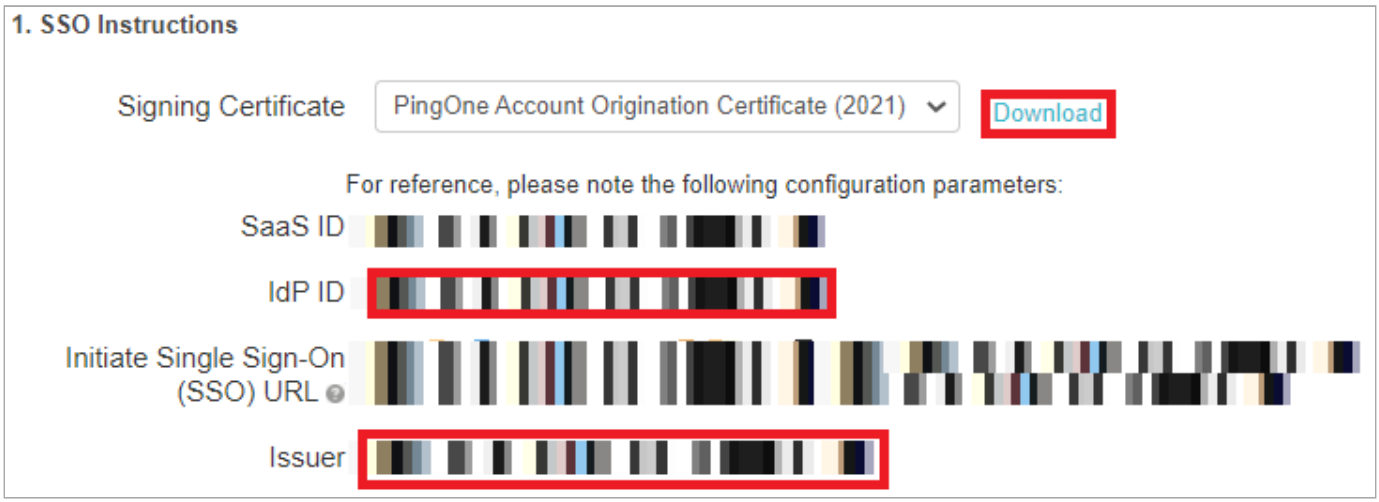
Update the supplied Egnyte application in PingOne for Enterprise

1. Sign on to PingOne for Enterprise and go to **Applications → Application Catalog**.
2. Search for `Egnyte`.

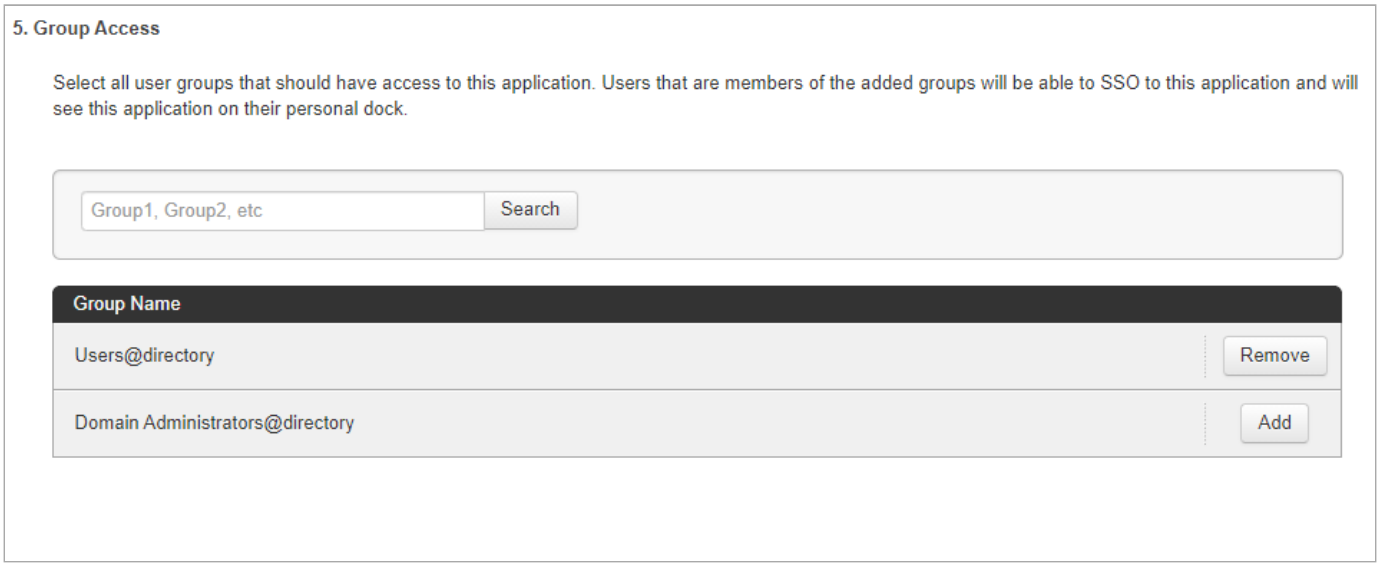


3. Expand the Egnyte entry and click the **Setup** icon.
4. Copy the **Issuer** and **IdP ID** values.

5. Download the signing certificate.



6. Click **Continue to Next Step**.
7. Set **ACS URL** to `https://Your-Egnyte-domain.egnyte.com/samlconsumer/PingIdentity`.
8. Click **Continue to Next Step** twice.
9. In the **Attribute Mapping** section, map **SAML_SUBJECT** to the attribute containing the user's email address.
10. Click **Continue to Next Step** twice.
11. Click **Add** for all user groups that should have access to Egnyte.

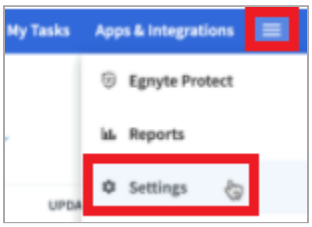


12. Click **Continue to Next Step**.
13. Click **Finish**.

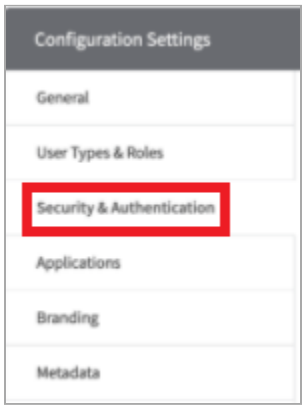
Add the PingOne for Enterprise IdP connection to Egnyte

1. Sign on to your Egnyte Admin organization as an administrator.

2. Click the menu icon and then click **Settings.**



3. Click the **Security and Authentication** tab.



4. In the **Single sign-on authentication** list, select **SAML 2.0**.
5. In the **Identity provider** list, select **Ping Identity**.
6. Set the following values:

Field	Value
Identity provider login URL	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=IdP-ID-value`
Identity provider entity ID	The **Issuer** value from above.
Identity provider certificate	In a text editor, open the signing certificate that you downloaded. Copy and paste the contents.
Default user mapping	Email address

7. Click **Save**.
8. Go to **Settings → Users and Groups**.
9. Select the appropriate users and set their **AuthType** to **SSO**.

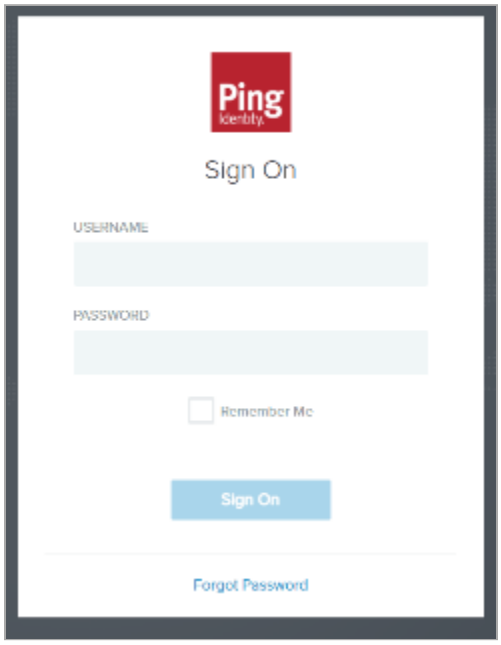
Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to our Ping desktop as a user with Egnyte access.

> **Note**
>
> To find the Ping desktop URL in the Admin console, go to **Setup → Dock → Dock URL**.

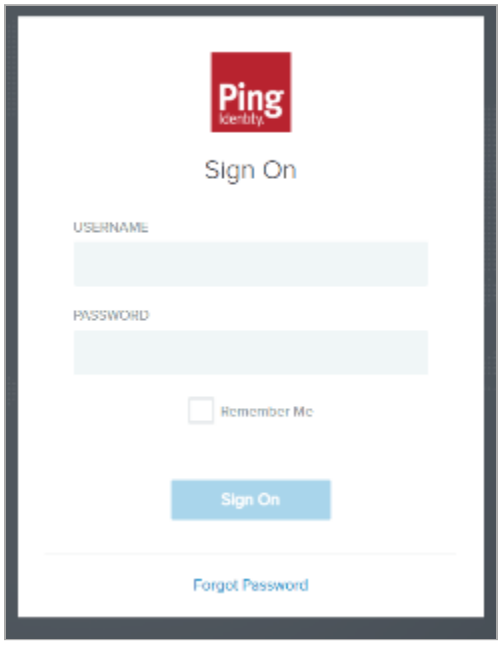
2. Complete the PingOne for Enterprise authentication.

   You're redirected to your Egnyte domain.



Test the PingOne for Enterprise SP-initiated SSO integration

1. Go to `https://Your-Egnyte-domain.Egnyte.com`.
2. Select the PingOne for Enterprise sign-on option.
3. After you're redirected to PingOne for Enterprise, enter your PingOne for Enterprise username and password.



You’re redirected back to Egnyte.

Evernote

Configuring SAML SSO with Evernote and PingFederate

Learn how to enable Evernote sign on from a PingFederate URL (IdP-initiated sign-on) and direct Evernote sign on using PingFederate (SP-initiated sign-on).

Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate Evernote with at least one user to test access.
- You must have administrative access to PingFederate and Evernote.

Create a PingFederate SP connection for Evernote

1. Sign on to the PingFederate administrative console.
2. Create an SP connection for Evernote in PingFederate:
    1. Configure using **Browser SSO** profile **SAML 2.0**.
    2. Set **Partner's Entity ID** to `https://www.evernote.com/saml2`.
    3. Enable the following **SAML Profiles**:
        - **IdP-Initiated SSO**
        - **SP-Initiated SSO**
    4. In **Assertion Creation → Authentication Source Mapping → Attribute Contract Fulfillment**, map **SAML_SUBJECT**.
    5. In **Protocol Settings → Assertion Consumer Service URL**, set **Binding** to **POST** and set **Endpoint URL** to `https://www.evernote.com/SamlConsumer.action`.
    6. In **Protocol Settings → Allowable SAML Bindings**, enable **POST**.
    7. In **Credentials → Digital Signature Settings**, select the **PingFederate Signing Certificate**.
3. Save the configuration.
4. Export the signing certificate.
5. Export the metadata, open the metadata file in a text editor, and copy the value of the Location entry (`https://your-value/idp/SSO.saml2`).

Add the PingFederate connection to Evernote

1. Sign on to your Evernote Admin organization as an administrator and go to the Evernote Business Admin Console.
2. Go to **Security → Single Sign-On**.
3. Set **SAML HTTP Request URL** to the Location value from the metadata file that you downloaded previously (`https://your-value/idp/SSO.saml2`).
4. In a text editor, open your PingFederate signing certificate file, copy the contents, and paste your signing certificate contents into the **X.509 Certificate** field.
5. Click **Save & Enable**.

Test the PingFederate IdP-initiated SSO integration

1. Go to the PingFederate **SSO Application Endpoint** for the Evernote SP connection.
2. Complete the PingFederate authentication.

   You're redirected to your Evernote domain.

Test the PingFederate SP-initiated SSO integration

1. Go to your Evernote URL.
2. Select the PingFederate sign-on option.
3. After you're redirected to PingFederate, enter your PingFederate username and password.

   You're redirected back to Evernote.

Configuring SAML SSO with Evernote and PingOne for Enterprise

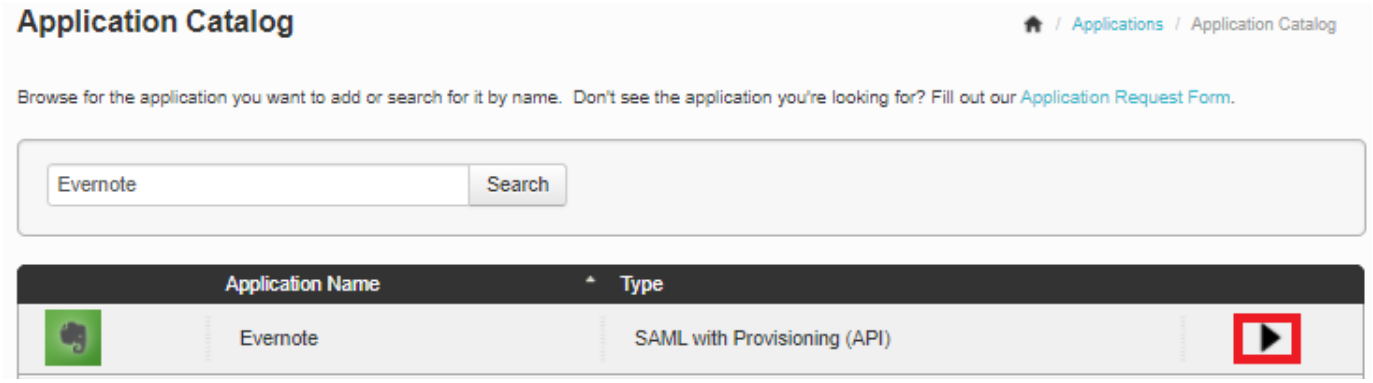
Learn how to enable Evernote sign on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct Evernote sign on using PingOne for Enterprise (SP-initiated sign-on).

Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate Evernote with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and Evernote.

Update the Evernote application in PingOne for Enterprise

1. Sign on to PingOne for Enterprise and go to **Applications → Application Catalog**.
2. Search for `Evernote`.

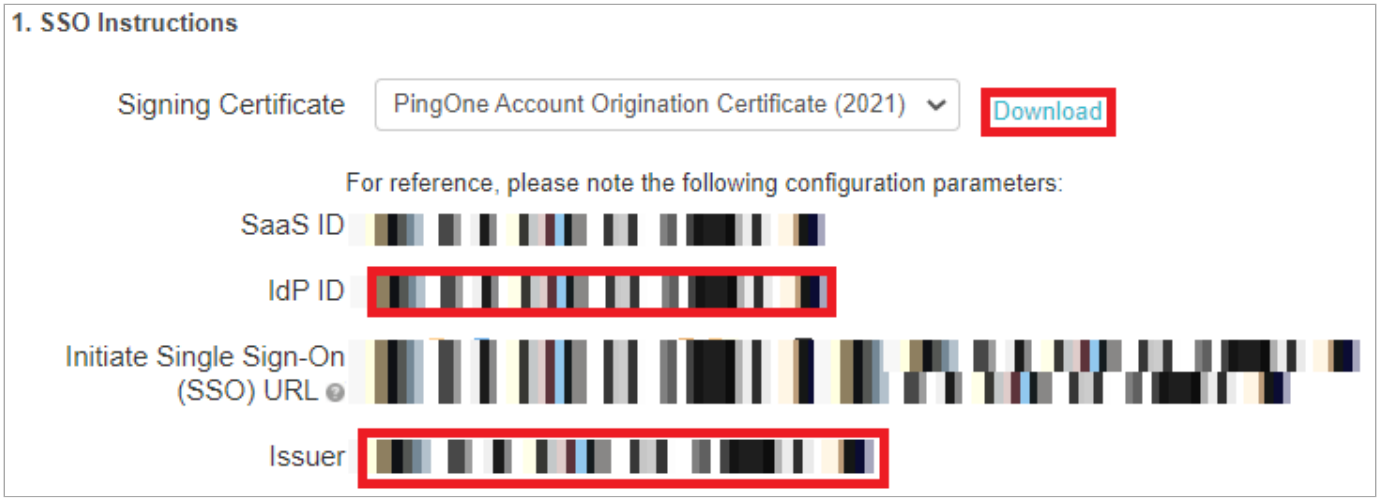


3. Expand the Evernote entry and click the **Setup** icon.

4. Copy the **IdP ID** value.

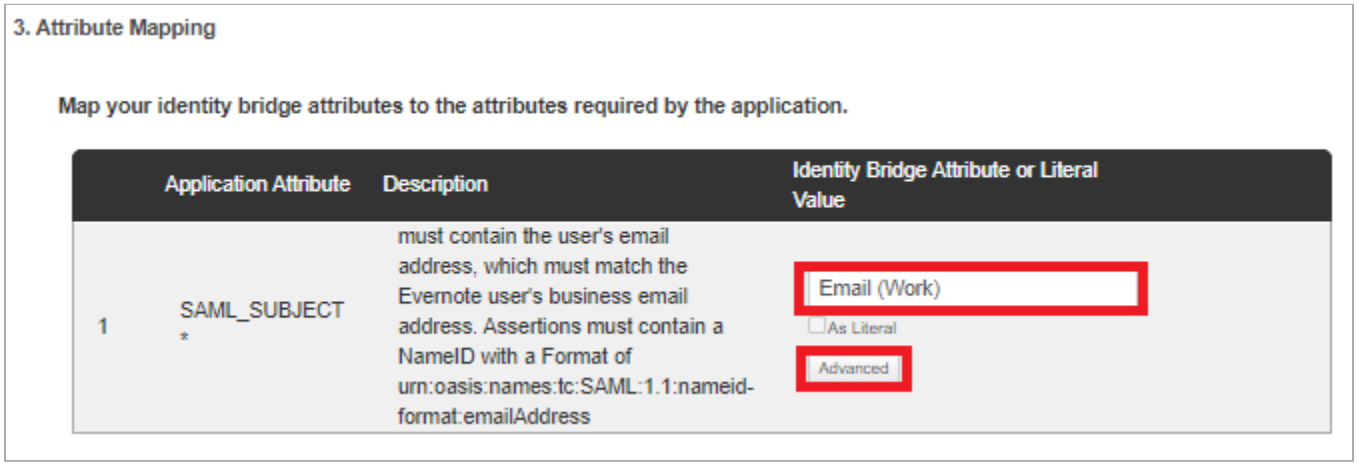
   You will need this wherever you see `IdP-ID-value` in the next procedure.

5. Download the signing certificate.

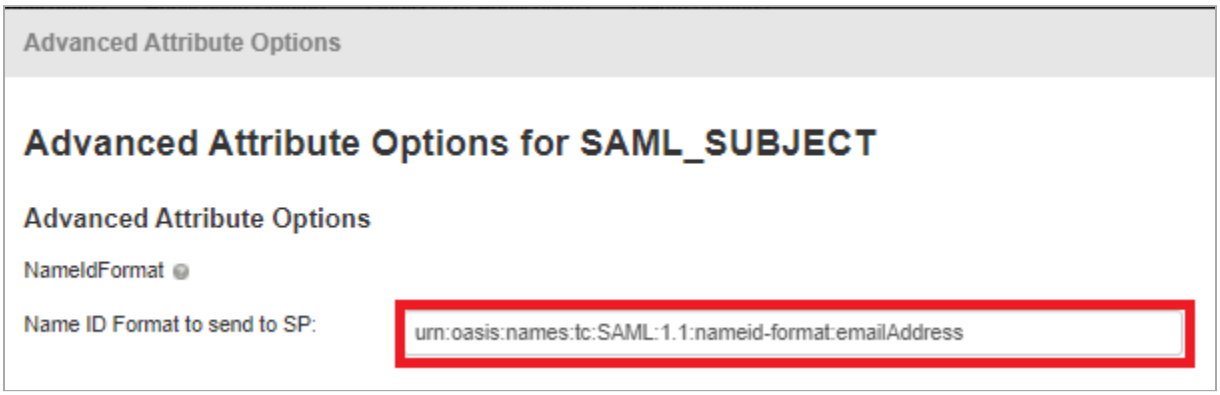


6. Click **Continue to Next Step** twice.

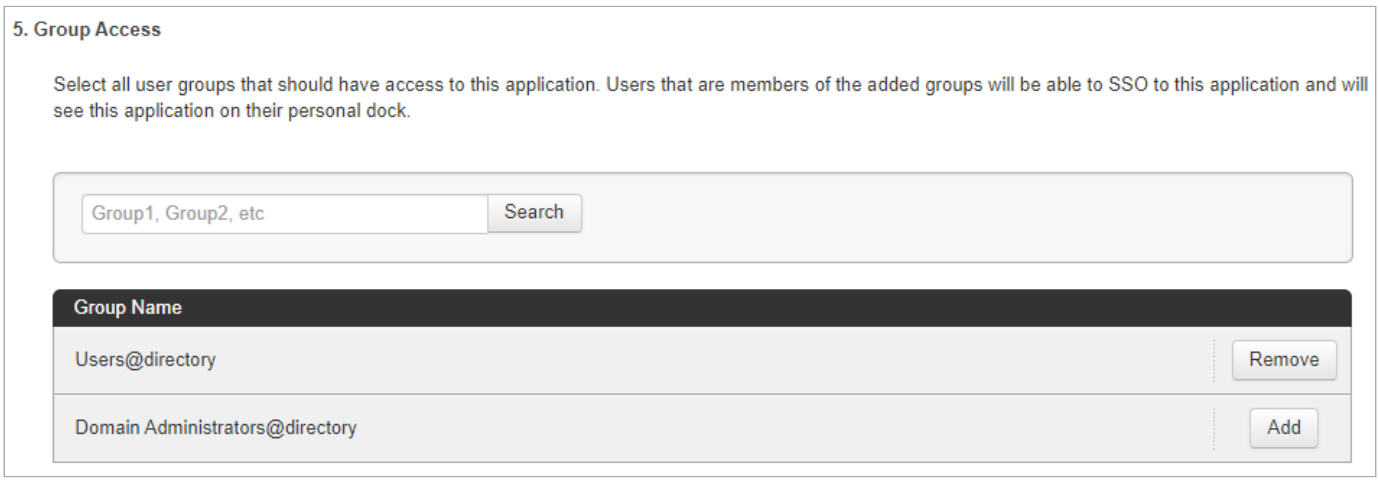
7. In the **Attribute Mapping** section, map **SAML_SUBJECT** to the attribute containing the user's email address.



8. Click **Advanced**.
9. In the **Name ID format to send to SP** field, enter `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`.



10. Click **Save**, then click **Continue to Next Step** twice.
11. Click **Add** for all user groups that should have access to Evernote.



12. Click **Continue to Next Step**.
13. Click **Finish**.

Add the PingOne for Enterprise IdP connection to Evernote

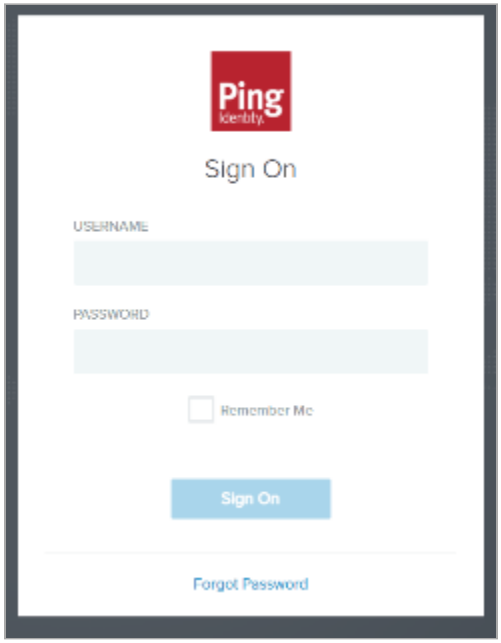
1. Sign on to your Evernote Admin organization as an administrator and go to the Evernote Business Admin Console.
2. Go to **Security → Single Sign-On**.
3. Set **SAML HTTP Request URL** to `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=IdP-ID-value`.
4. In a text editor, open your PingOne for Enterprise signing certificate.
5. Copy and paste your signing certificate contents into the **X.509 Certificate** field.
6. Click **Save & Enable**.

Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with Evernote access.

> **Note**
>
> To find the Ping desktop URL in the Admin console, go to **Setup → Dock → Dock URL**.

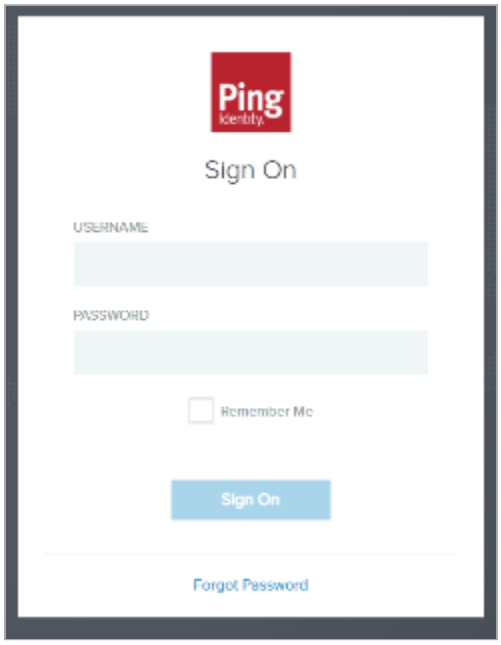
2. Complete the PingOne for Enterprise authentication.



You're redirected to your Evernote domain.

Test the PingOne for Enterprise SP-initiated SSO integration

1. Go to your Evernote URL.
2. Select the PingOne for Enterprise sign on option.
3. After you're redirected to PingOne for Enterprise, enter your PingOne for Enterprise username and password.



You’re redirected back to Evernote.

Freshworks

Configuring SAML SSO with Freshworks and PingOne

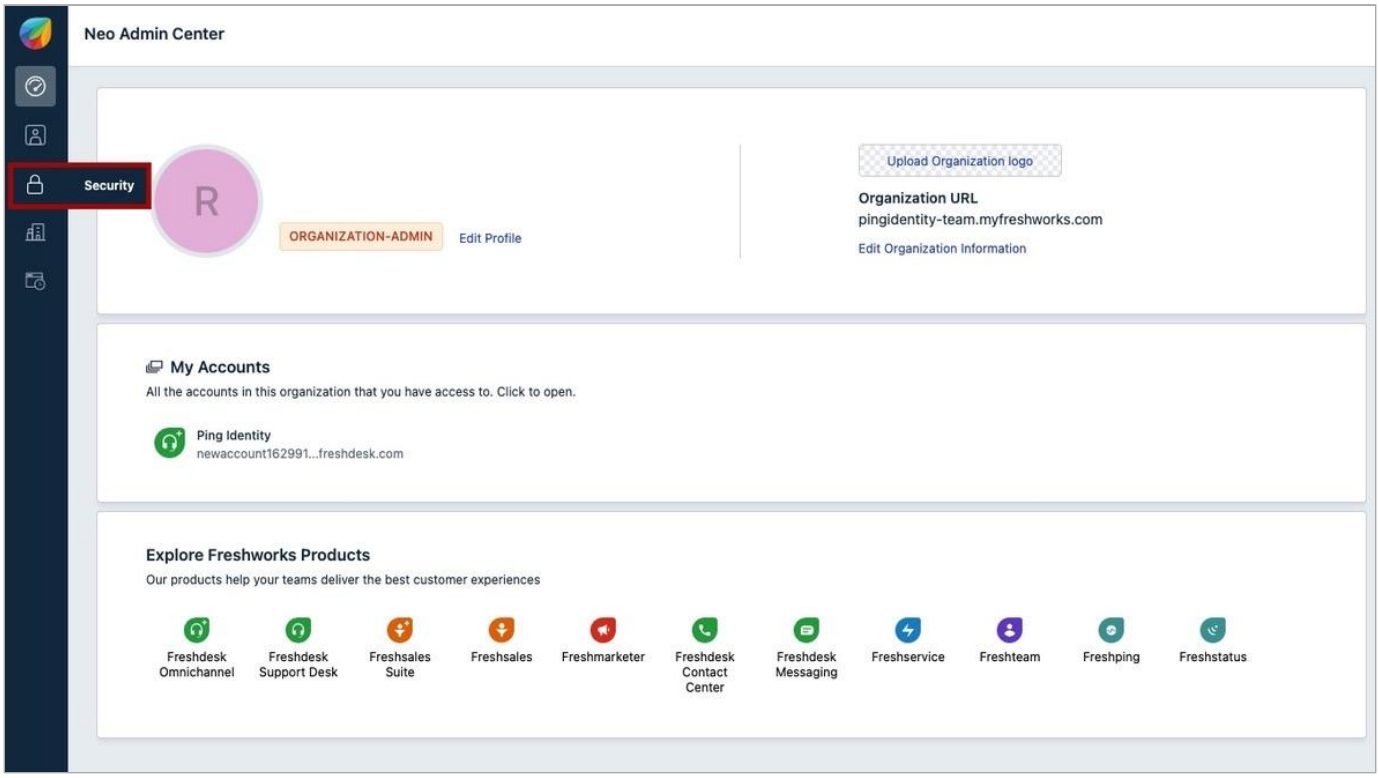
Learn how to configure SAML single sign-on (SSO) with Freshworks and PingOne.

Before you begin

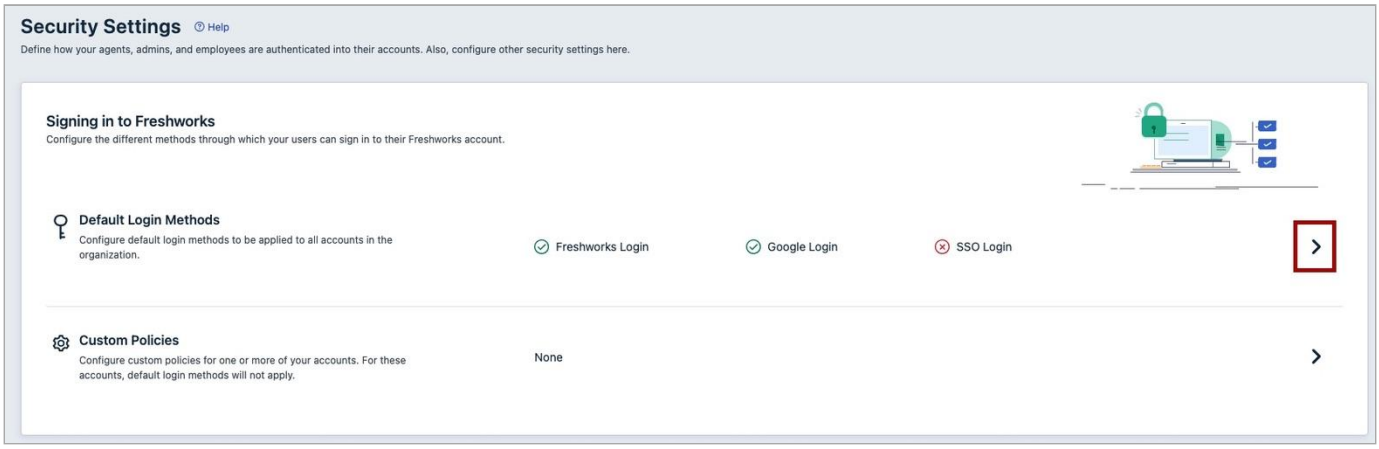
You must have a Business level or higher plan in Freshworks. Learn more at https://support.freshworks.com/support/solutions/articles/237923.

Configure SSO in Freshworks

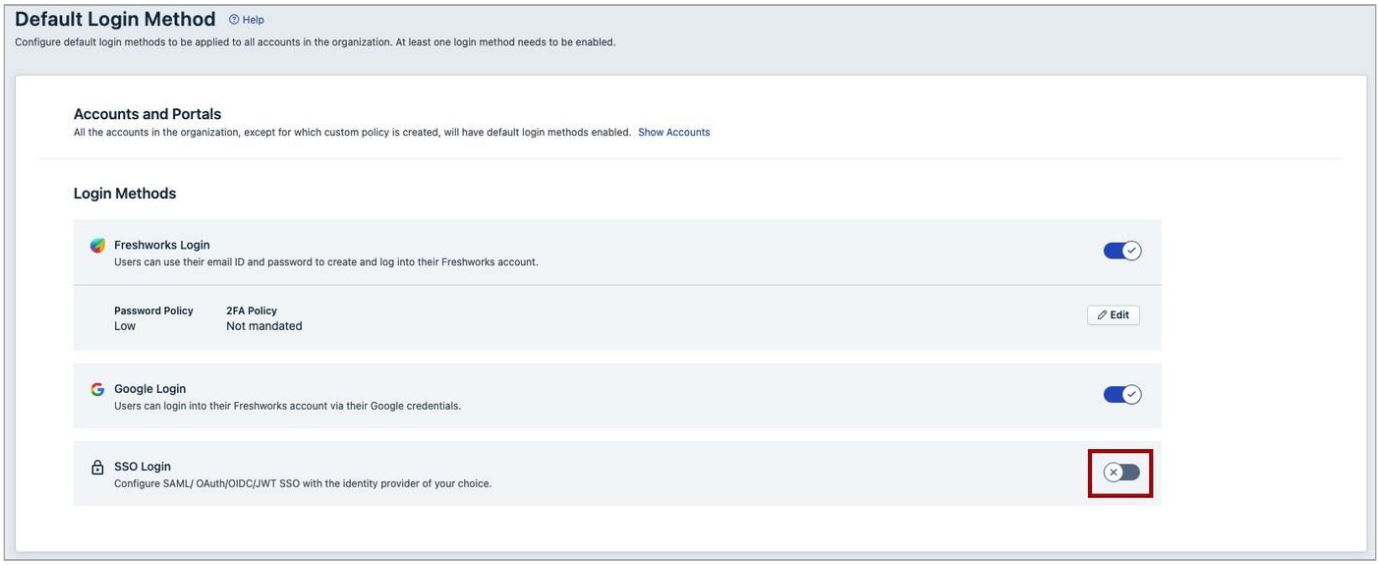
1. Sign on to your Freshworks Admin account homepage and go to the **Security** tab.



2. On the **Security Settings** page, in the **Default Login Methods** section, click the right arrow.

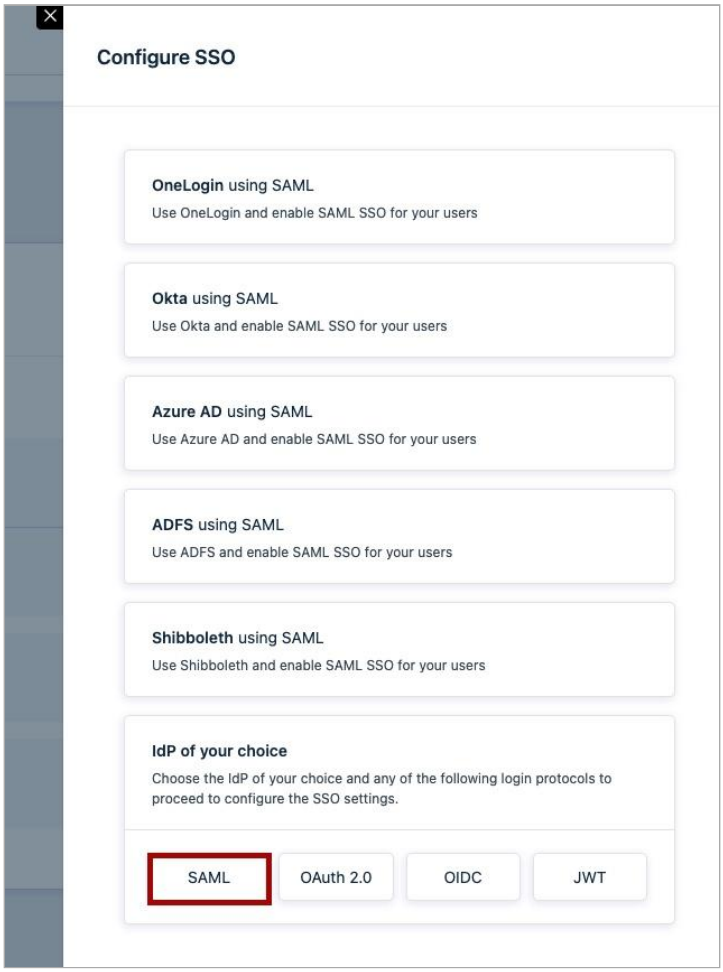


3. On the corresponding **Login Methods** page, click the **SSO Login** toggle.



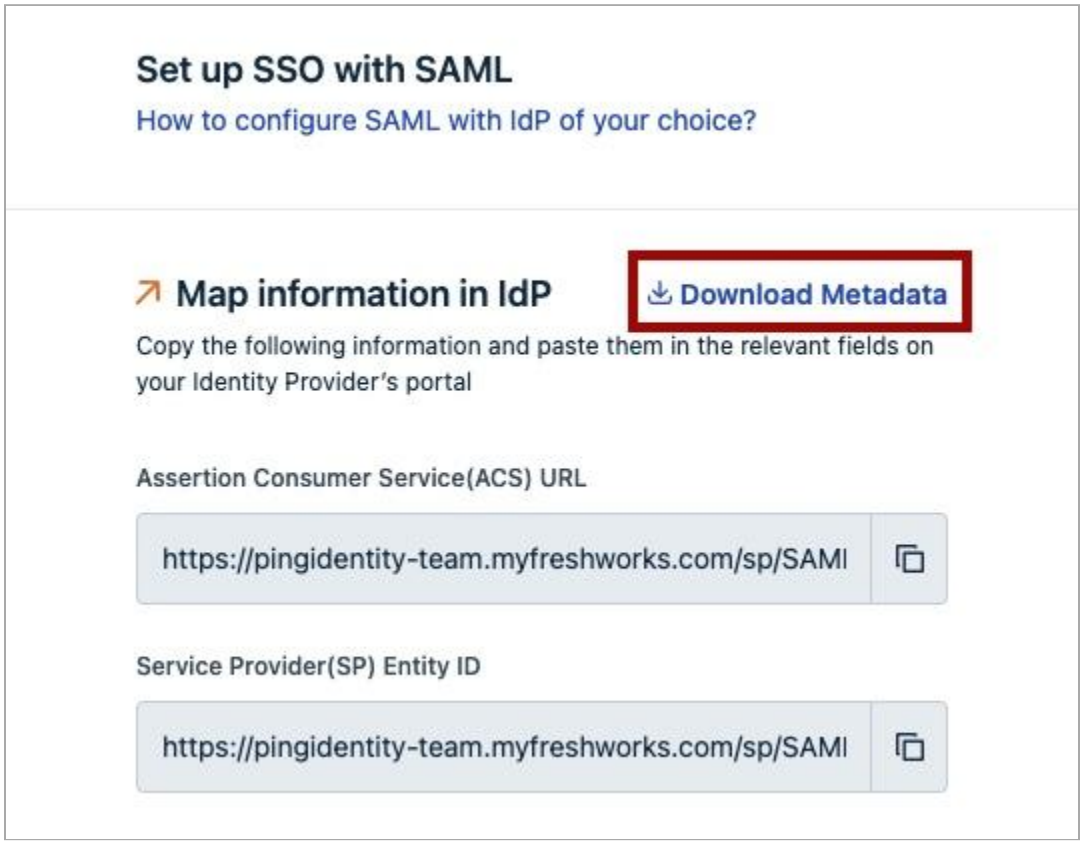
The **Configure SSO** panel opens.

4. On the **Configure SSO** panel, in the **IdP of your choice** section, click **SAML**.



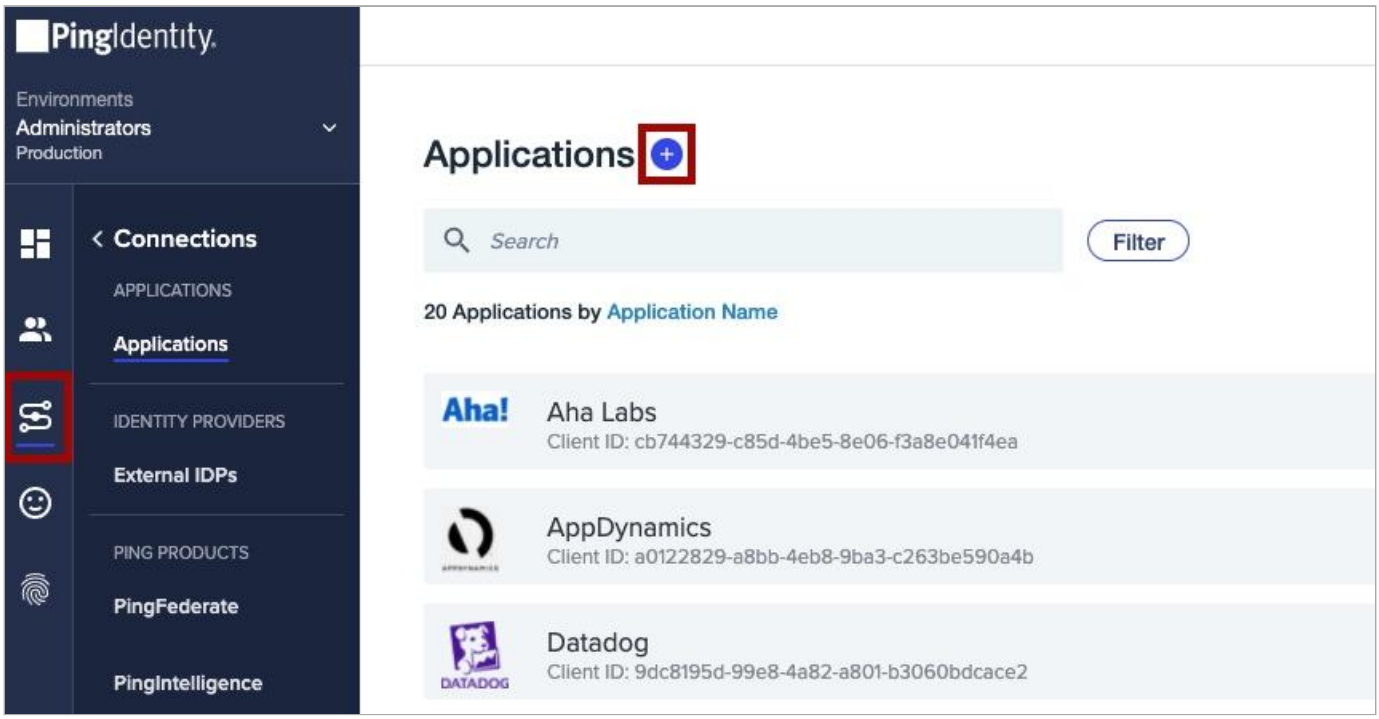
5. On the **Set up SSO with SAML** page, in the **Map information in IdP** section, make a note of the **Assertion Consumer Services (ACS) URL** and **Service Provider (SP) Entity ID** values. You will need them later.

   Click **Download Metadata**.



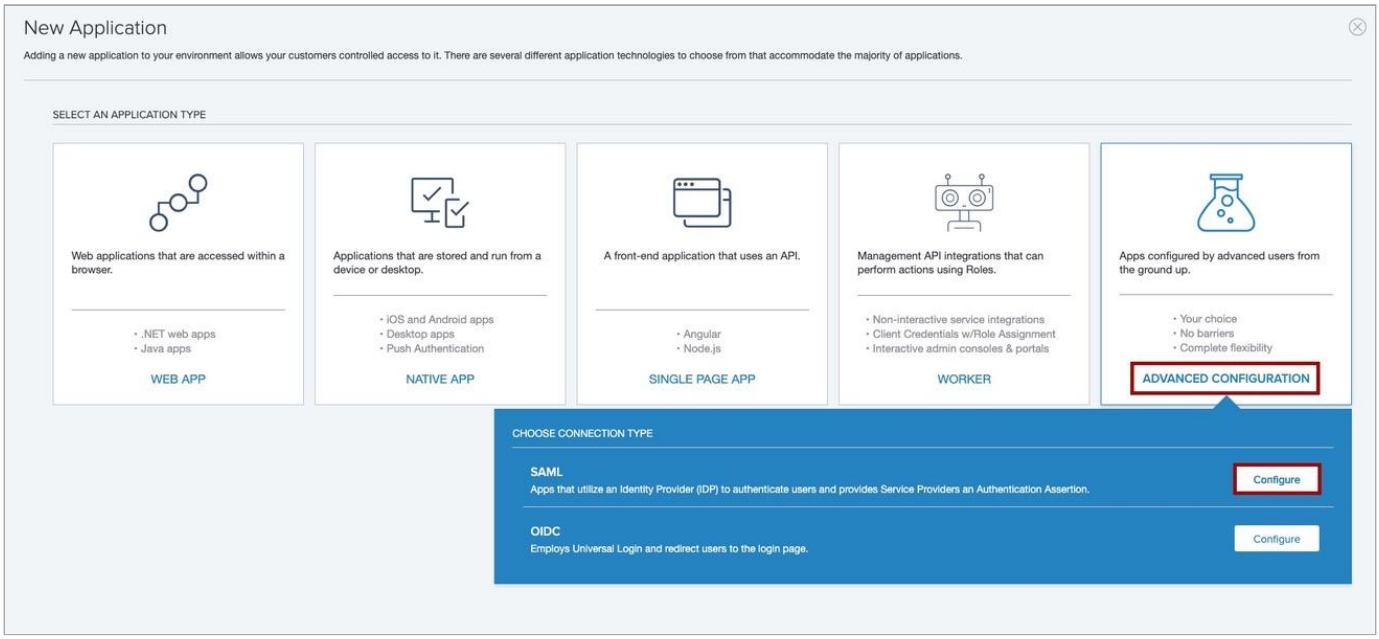
Configure SSO in PingOne

1. In PingOne, go to **Connections → Applications**.
2. Click the + icon next to **Applications**.

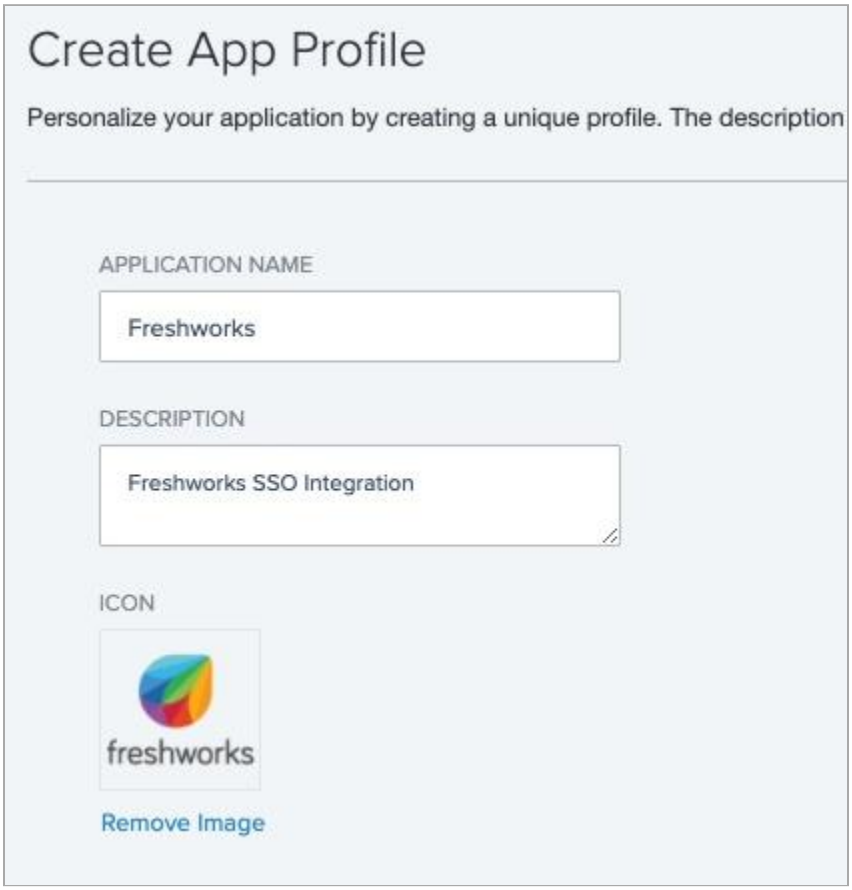


> **Important**
>
> You will use the settings displayed in Step 5 of the previous procedure to begin configuring Freshworks within PingOne.

3. On the **New Application** page, click **Advanced Configuration**.
4. In the **Choose Connection Type** list, on the **SAML** line, click **Configure**.

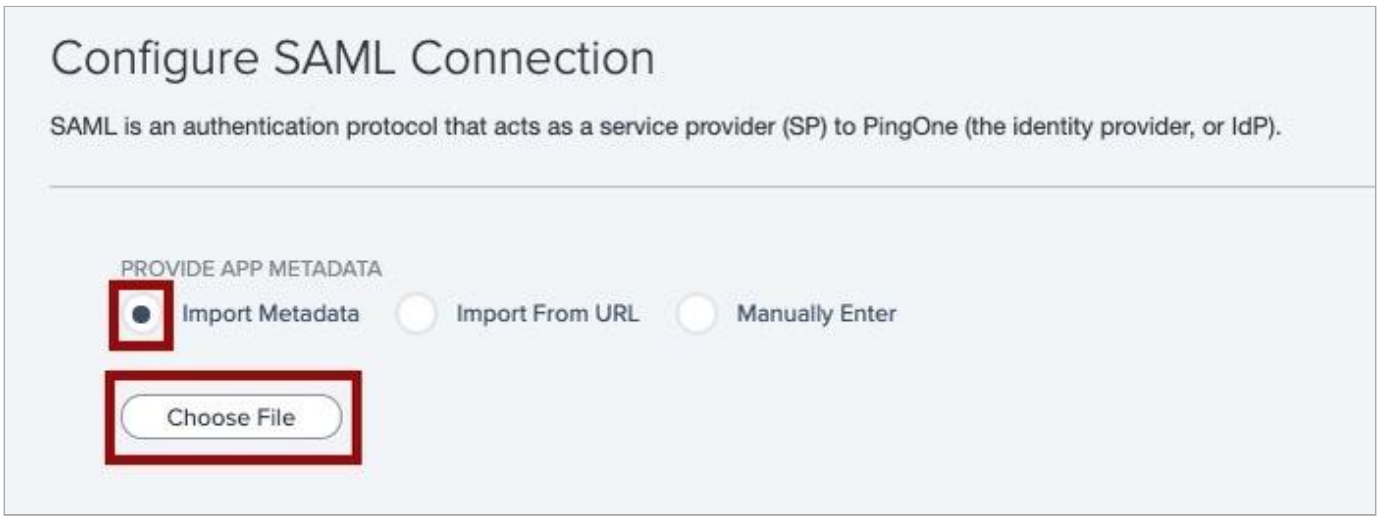


5. In **Create App Profile**, enter the values for:
    - **Application Name** (Required)
    - **Description** (Optional)
    - **Icon** (Optional)



6. On the **Configure SAML Connection** page, in the **Provide App Metadata** section, click **Import Metadata**.

   Upload the metadata downloaded previously and click **Import**.

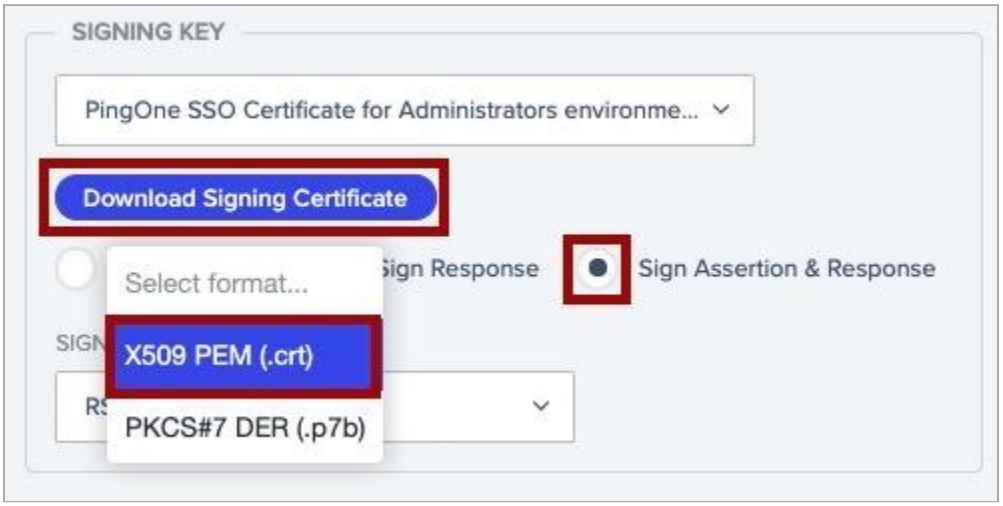


   After import, all necessary fields are populated automatically, except for the **Assertion Validity Duration**.

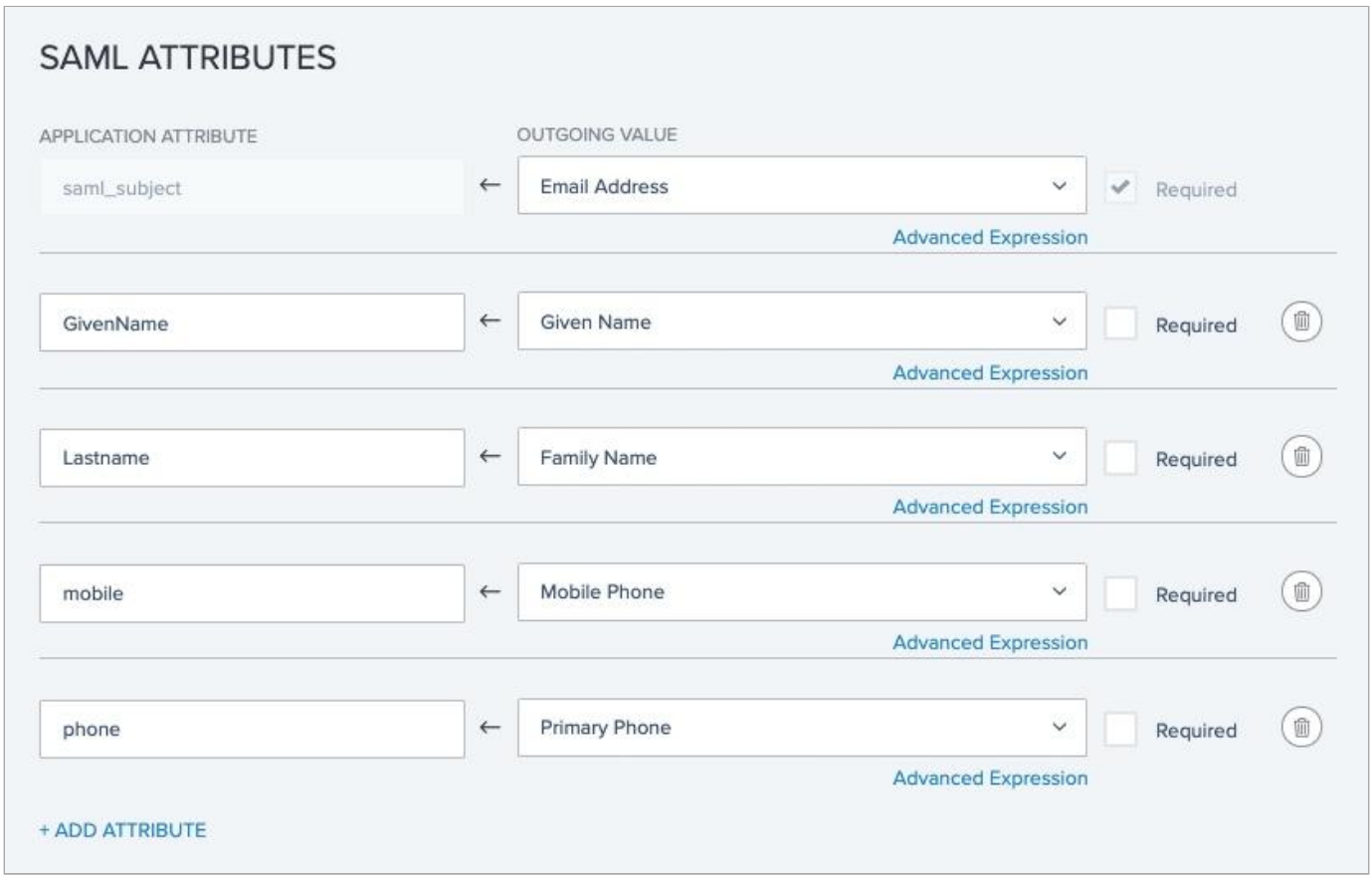
7. In the **Assertion Validity Duration** field, enter a valid duration value (in seconds), such as 3600.

8. In the **Signing Key** section, select **Download Signing Certificate** and download in the **X509 PEM (.crt)** format.

   Make sure that **Sign Assertion & Response** is selected, then click **Save and Continue**.

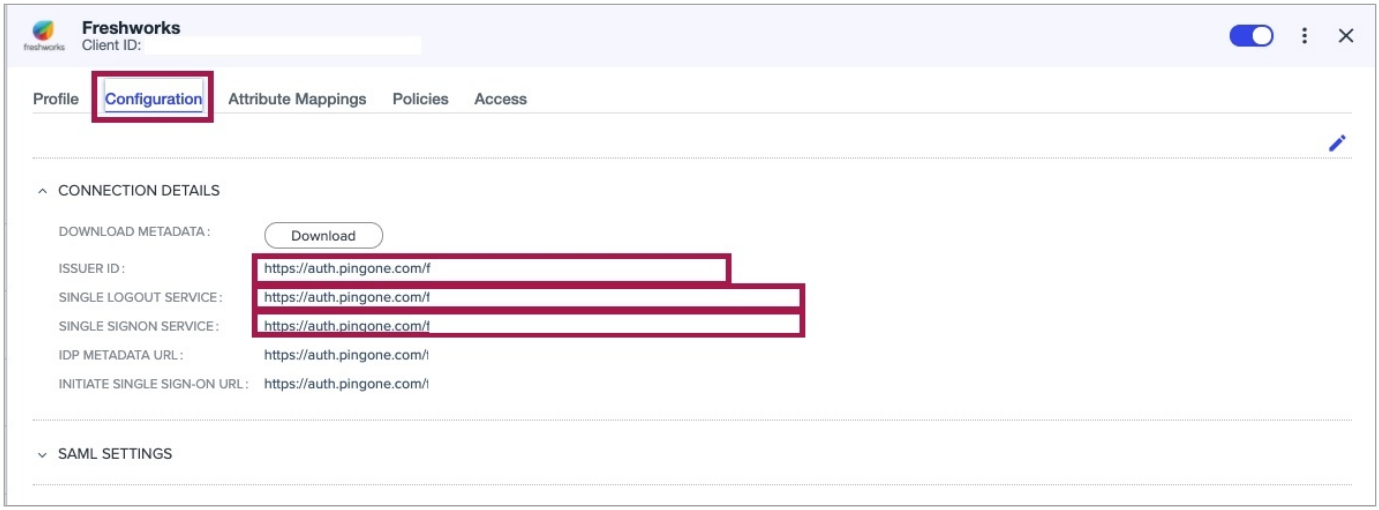


9. On the **Attribute Mapping** page, enter the values for the following attributes:
    - **Email Address** = saml_subject
    - **givenName**
    - **LastName**
    - **mobile**
    - **phone**



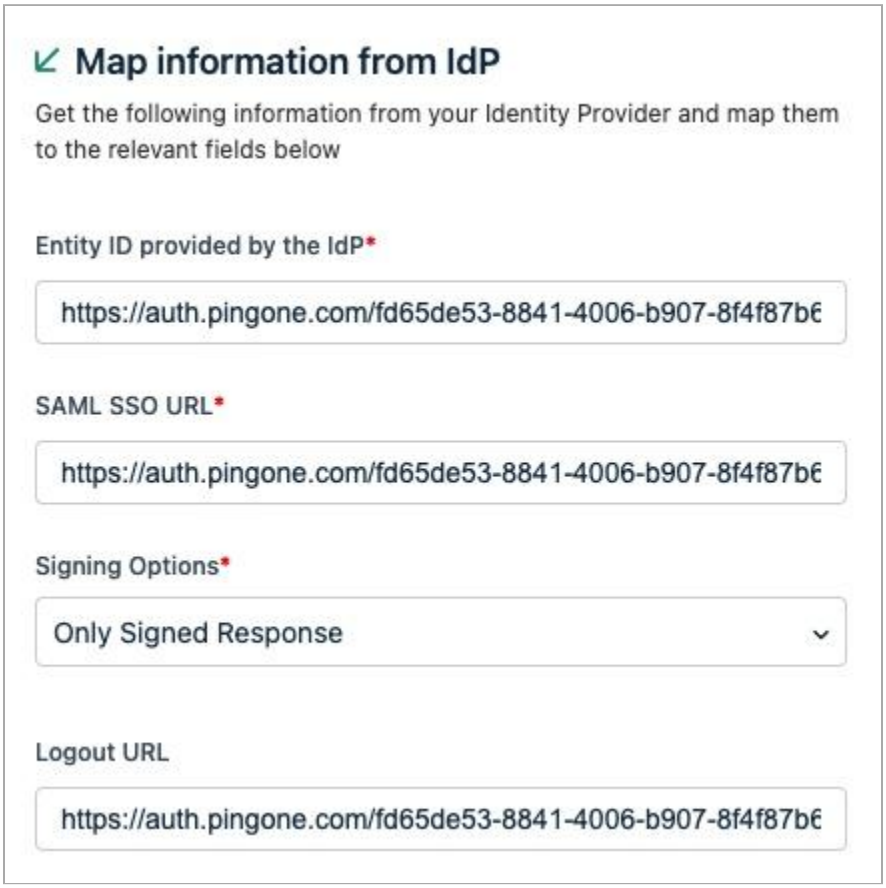
10. Click **Save and Close** to finalize the creation of the application.
11. After you create the application, click the toggle next to the application to enable it.

12. Select **Configuration** and copy the following values for later use.
    - **Issuer ID**
    - **Single Logout Service** (Optional)
    - **Single SignOn Service**



Integrate SAML SSO with Freshworks and PingOne

1. In Freshworks, go to **Set up SSO with SAML** and paste the information from the previous step into the below locations:
    - **Entity ID provided by the IdP** = the **Issuer ID** value from PingOne
    - **SAML SSO URL** = the **Single SignOn Service** value from PingOne
    - **Logout URL** = the **Single Logout Service** value from PingOne (Optional)

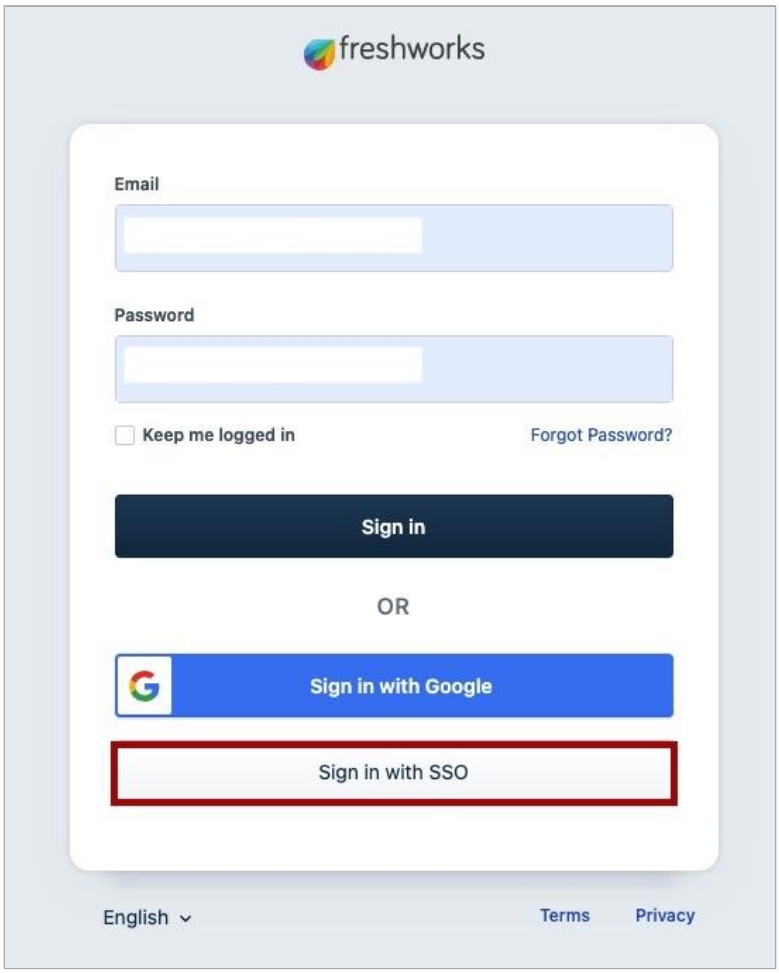


2. Upload the X509 certificate that you downloaded previously. Open the downloaded file with a text editor and copy and paste the certificate into the **Security certificate** field, then select **Configure SSO**.

> **Note**
>
> You must include the `BEGIN CERTIFICATE` and `END CERTIFICATE` text as part of the certificate upload.

3. Sign out of your Freshworks account, then click the **Sign in with SSO** to sign on.

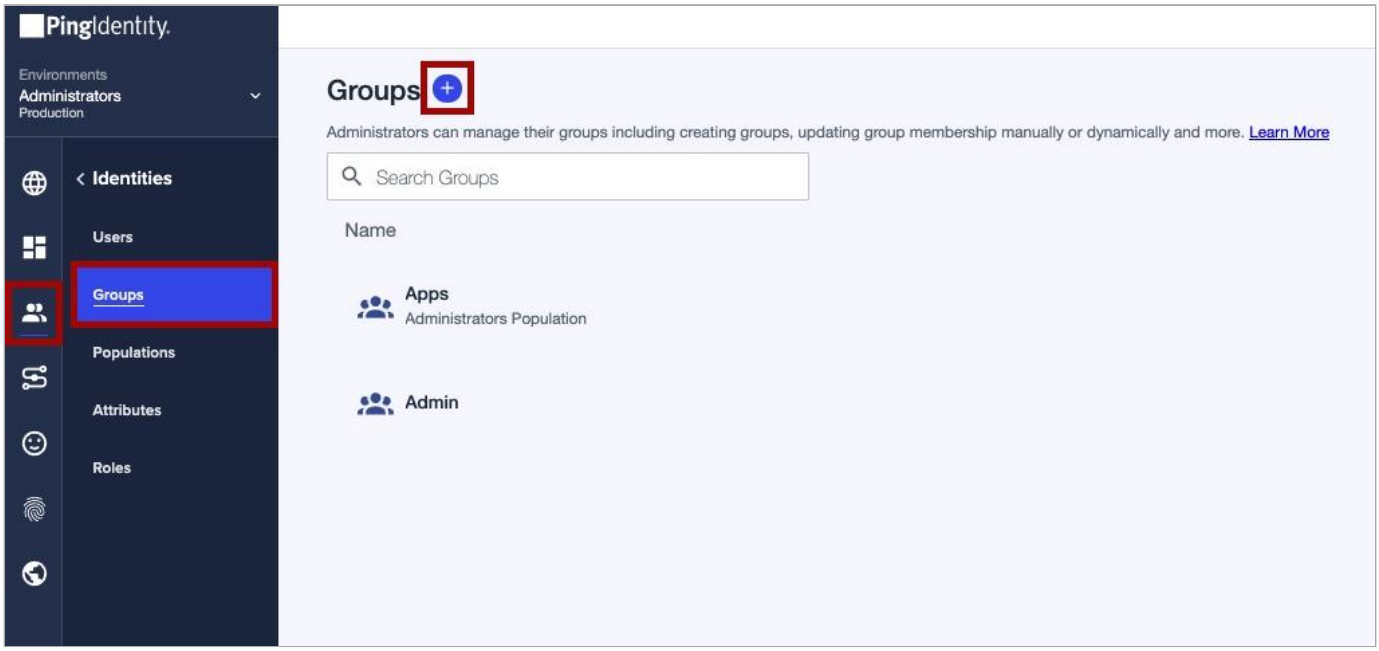
You're proxied into your account, finalizing the configuration.



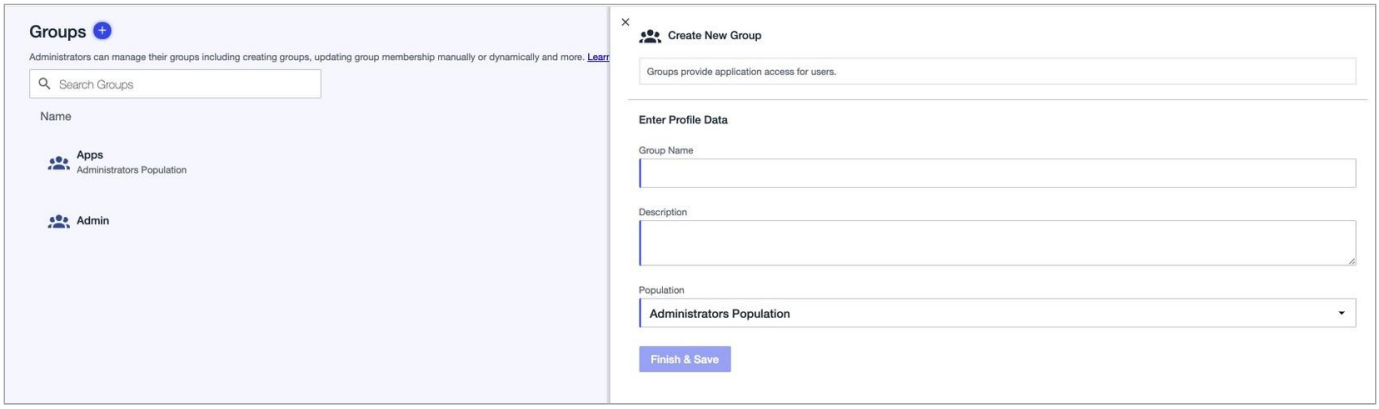
Create and assign identities in PingOne

Before you can test the integration, create and assign identities in PingOne. If you've already assigned identities and groups in PingOne, move on to Test the integration.

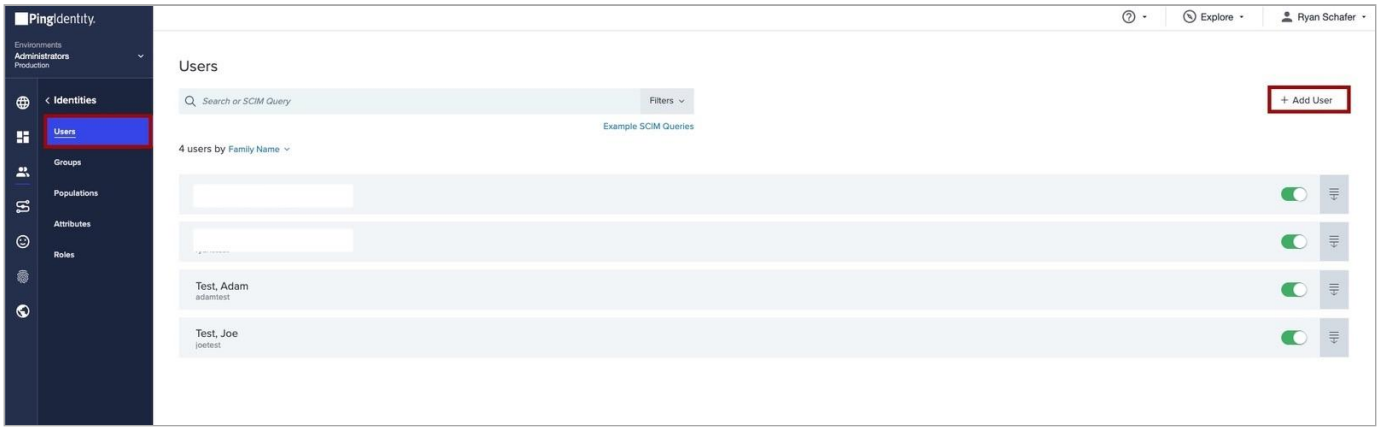
1. In PingOne, go to **Identities → Groups** and click the + icon next to **Groups**.



2. On the **Create New Group** page, enter values for the following:
    - **Group Name** (Required)
    - **Description** (Optional)
    - **Population** (Optional)
3. Click **Finish & Save**.



4. To add identities to the group, on the **Identities** tab, go to **Users → + Add User**.



5. On the **Add User** page, enter all the necessary information for a user.

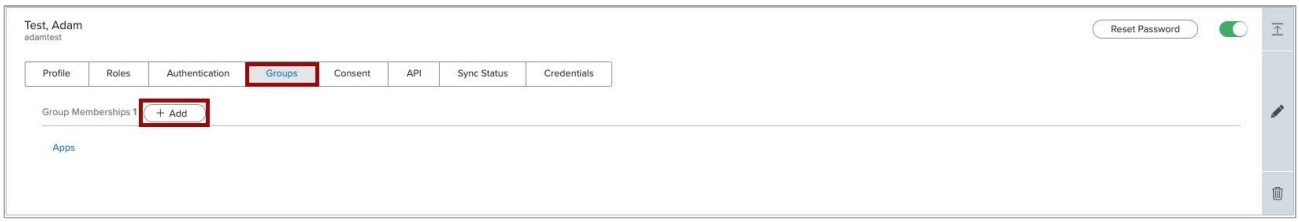
> **Important**
>
> Verify that the first name, last name, and email address are correct, as these are values passed in the SAML assertion.

6. Click **Save**.

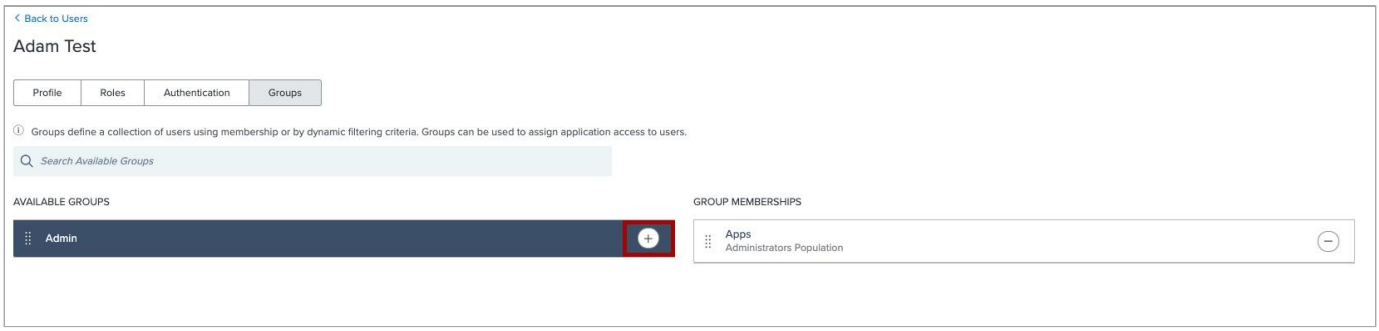
7. Assign the user that you created to the group that you created previously.

   Locate the user you created and do the following:

   1. Expand the section for the user.
   2. Select the **Groups** tab.
   3. Click **+ Add**.



8. In the **Available Groups** section, select the group that you created and click the **+** icon to add it to the user's group memberships. Click **Save**.

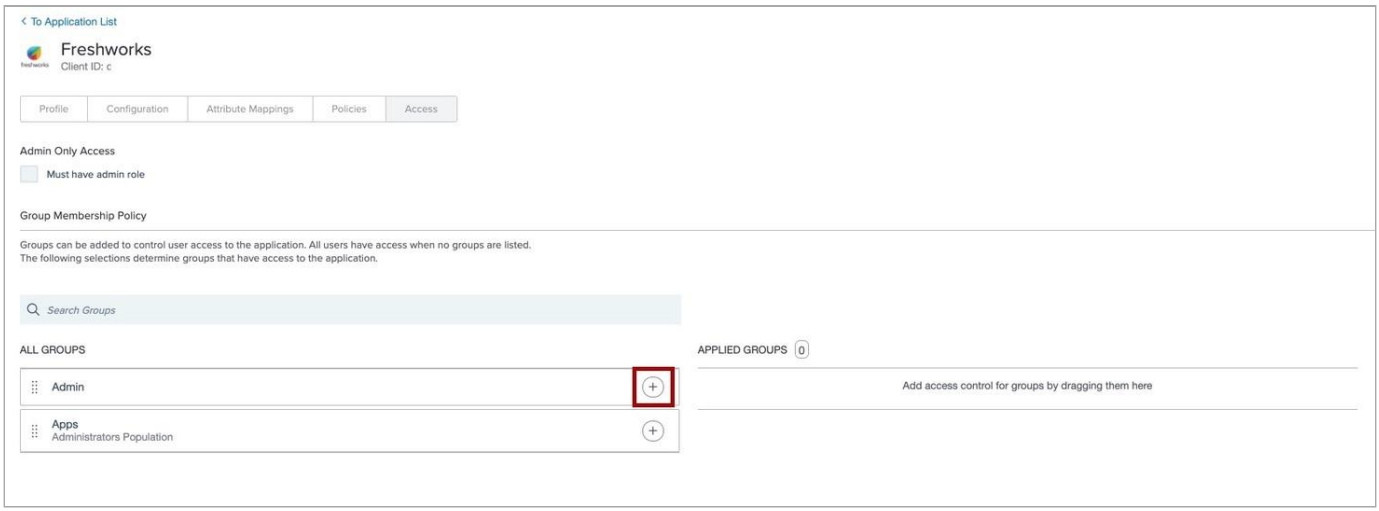


9. On the **Connections** tab for the Freshworks application do the following:

    1. Click the **Access** tab.

    2. Click the **Pencil** icon to edit the configuration.

10. Select the group that you created and add it to the **Applied Groups** section. Click **Save**.

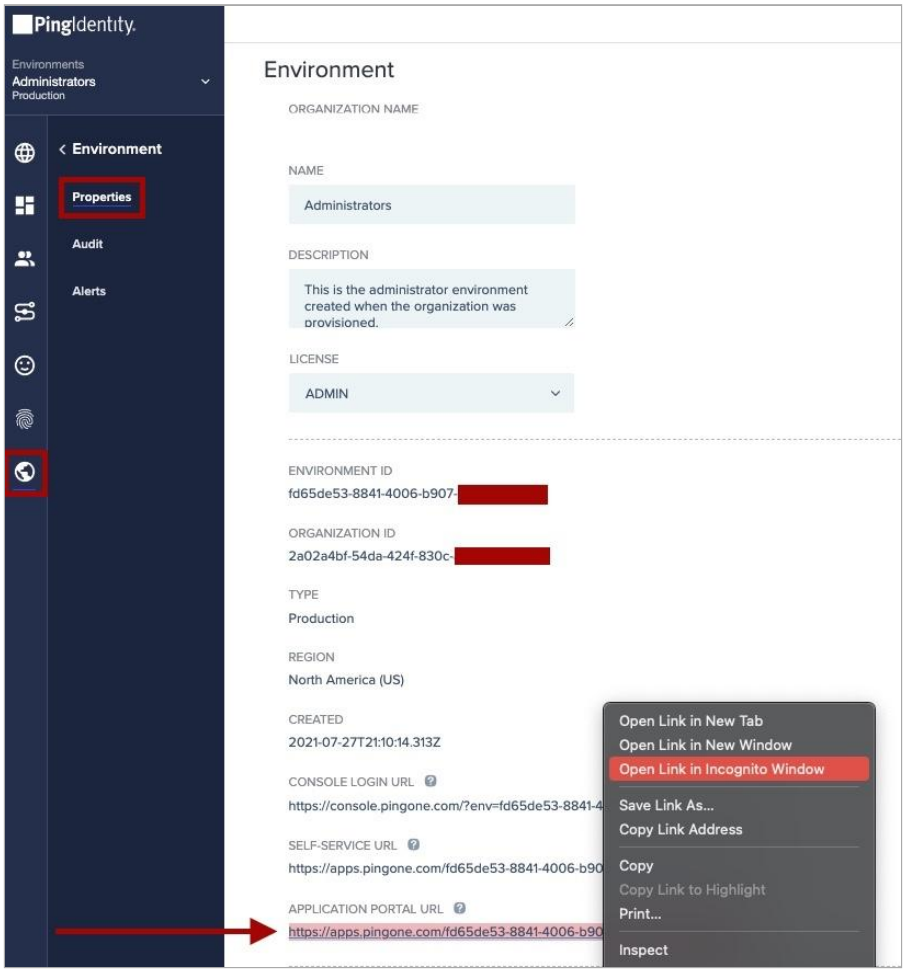


Test the integration

You're now ready to test the integration.

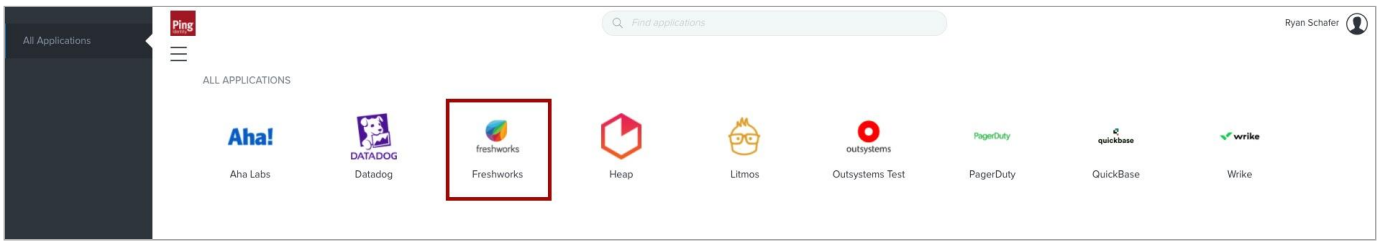
1. In the PingOne admin console, go to **Dashboard → Environment Properties**.

2. Right-click on the **Application Portal URL** and open it in a private browser session.



3. Sign on as the test user that you created and click the Freshworks tile.

   You're signed on to the user's Freshworks account using SSO and testing is complete.



GitHub

Configuring SAML SSO with GitHub Cloud and PingFederate

Learn how to enable GitHub sign-on from a PingFederate URL (IdP-initiated sign-on) and direct GitHub sign on using PingFederate (SP-initiated sign-on).

Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate GitHub with at least one user to test access.
- You must have administrative access to PingFederate and GitHub.

Create a PingFederate SP connection for GitHub

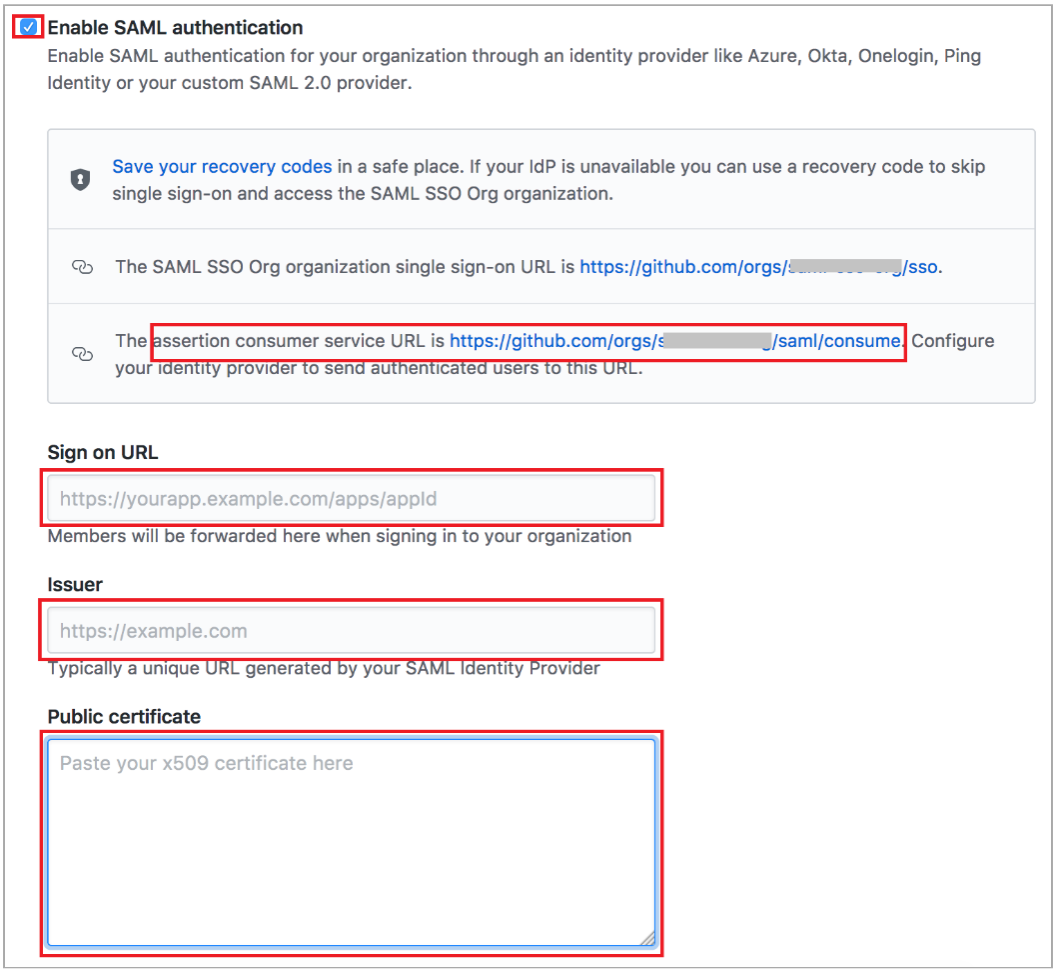
1. Sign on to the PingFederate administrative console.
2. Create an SP connection for GitHub in Ping Federate UI:
    1. Configure using **Browser SSO** profile **SAML 2.0**.
    2. Set **Partner's Entity ID** to `https://github.com/orgs/your-tenant`.
    3. Enable the following SAML Profiles:
        - **IdP-Initiated SSO**
        - **SP-Initiated SSO**
    4. In **Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment**, map **SAML_SUBJECT** to an attribute containing the user's email address.
    5. In **Protocol Settings: Assertion Consumer Service URL**, set **Binding** to **POST** and set **Endpoint URL** to `https://github.com/orgs/your-tenant/saml/consume`.
    6. In **Protocol Settings: Allowable SAML Bindings**, enable **POST**.
    7. In **Credentials: Digital Signature Settings**, select the **PingFederate Signing Certificate**.
3. Save the configuration.
4. Export the signing certificate.
5. Export and then open the metadata file.

   Copy the value of the entityID and the Location entry (`https://your-value/idp/SSO.saml2`).

Add the PingFederate IdP connection to GitHub

1. Sign on to GitHub as an administrator.
2. Select your GitHub organization.
3. Click **Organization settings**, then click **Security**.
4. Under **SAML single sign-on**, select **Enable SAML authentication**.

> **Note**
>
> The assertion consumer service URL displayed on this screen should match the value that you entered into the PingFederate **Endpoint URL** field.



5. Set the following values.

Field	Value
Sign on URL	The PingFederate Location value (`https://your-value/idp/SSO.saml2`)
Issuer	The PingFederate entityID value.

Field	Value
Public certificate	Paste in the contents of the PingFederate signing certificate.

6. Click **Save**.

Test the PingFederate IdP-initiated SSO integration

1. Go to the PingFederate **SSO Application Endpoint** for the GitHub SP connection.
2. Complete the PingFederate authentication.

   You're redirected to your GitHub domain.

Test the PingFederate SP-initiated SSO integration

1. Go to `https://github.com/orgs/your-tenant/sso`
2. After you're redirected to PingFederate, enter your PingFederate username and password.

   You're redirected back to GitHub.

Configuring SAML SSO with GitHub Cloud and PingOne for Enterprise

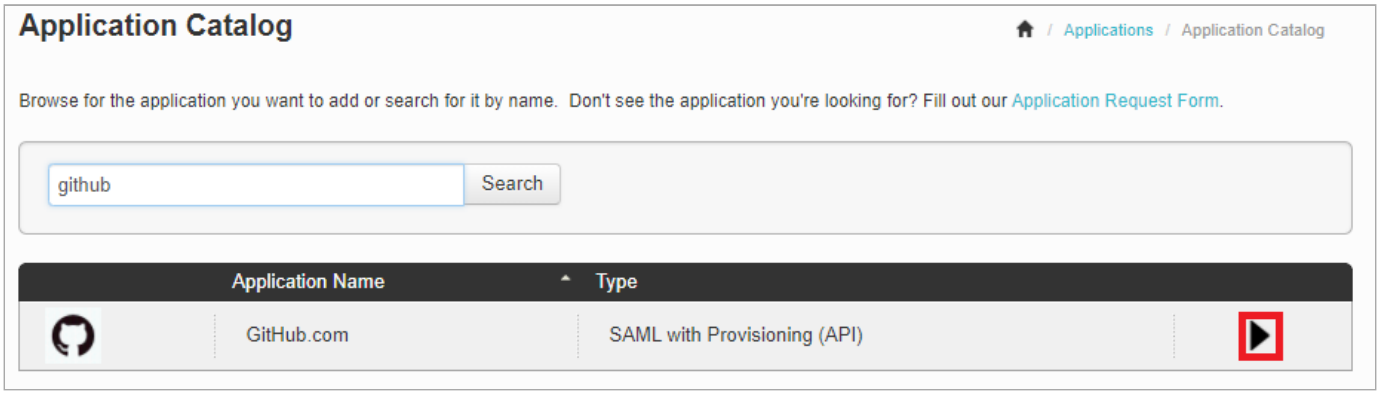
Learn how to enable GitHub sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct GitHub sign-on using PingOne for Enterprise (SP-initiated sign-on).

Before you begin

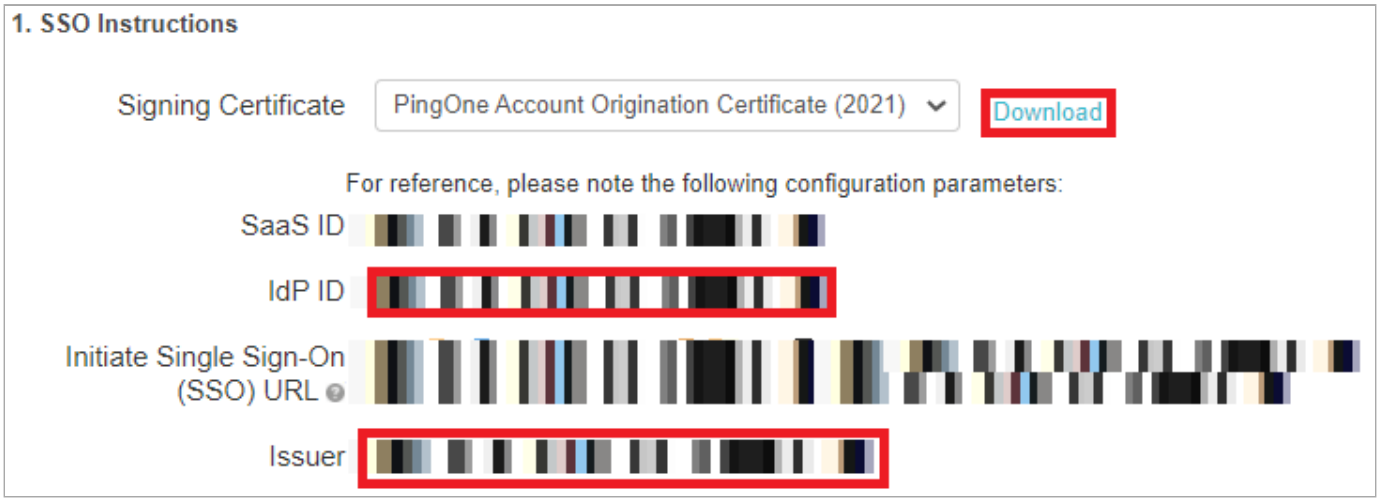
- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate GitHub with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and GitHub.

Set up the supplied GitHub application in PingOne for Enterprise

1. Sign on to PingOne for Enterprise for and go to **Applications → Application Catalog**.
2. Search for `GitHub`.
3. Expand the GitHub entry and click the **Setup** icon.

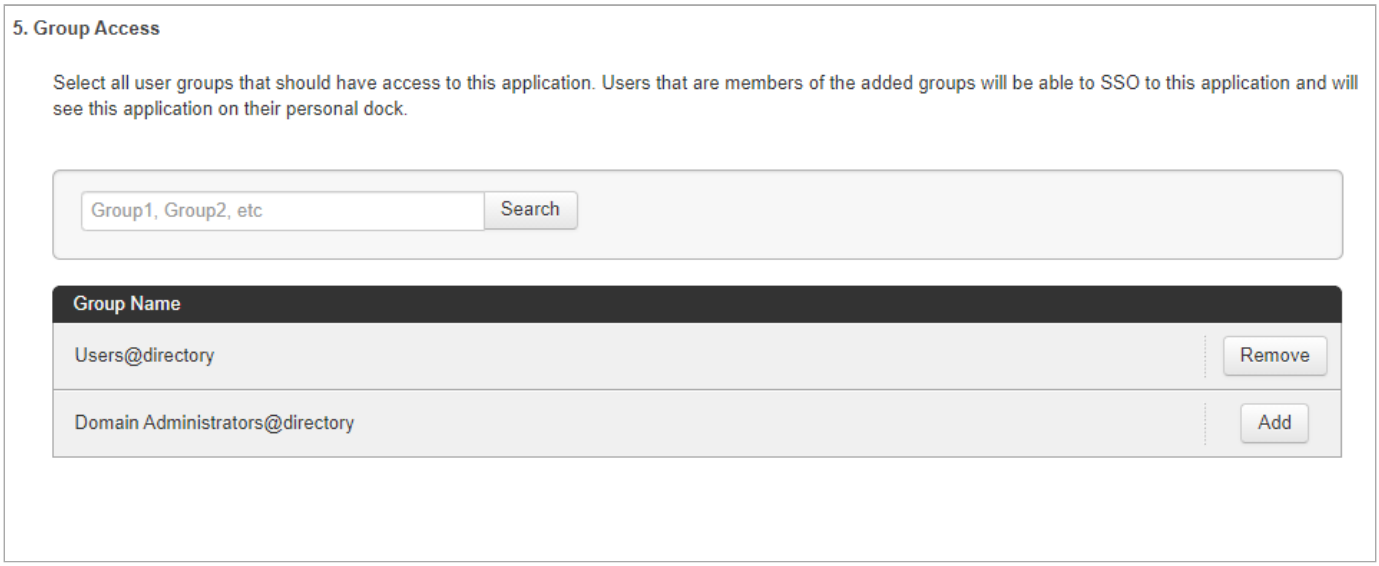


4. Copy the **Issuer** and **IdP ID** values.
5. Download the signing certificate.



6. Click **Continue to Next Step**.
7. Set **ACS URL** to `https://github.com/orgs/your-tenant/saml/consume`.

   Set **Entity ID** to `https://github.com/orgs/your-tenant`.
8. Click **Continue to Next Step**.
9. Ensure that **SAML_SUBJECT** is mapped to the field containing a user's email address.
10. Click **Continue to Next Step** twice.
11. Click **Add** for all user groups that should have access to GitHub.

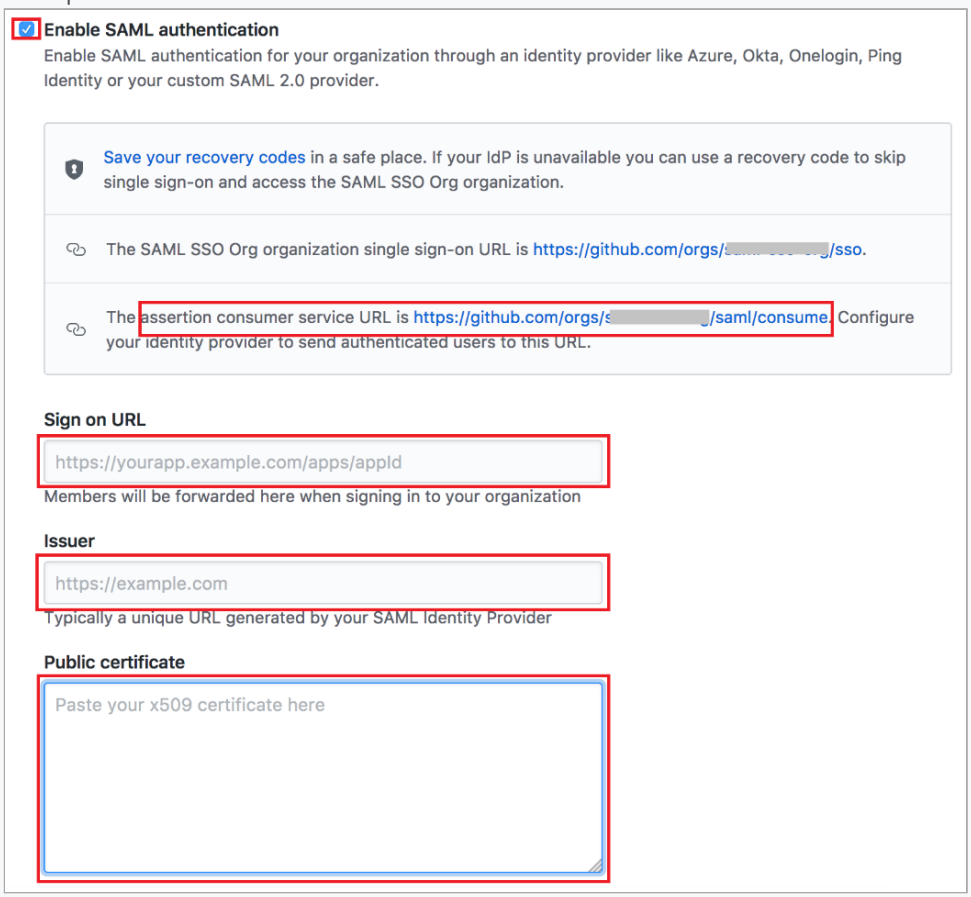


12. Click **Continue to Next Step**.
13. Click **Finish**.

Add the PingOne for Enterprise IdP connection to GitHub

1. Sign on to GitHub as an administrator.
2. Select your GitHub organization.
3. Click **Organization settings**, then click **Security**.
4. Under **SAML single sign-on**, select **Enable SAML authentication**.

> **Note**
>
> The assertion consumer service URL displayed on this screen should match the value that you entered into the PingOne for Enterprise **ACS URL** field.



5. Set the following values.

Field	Value
Sign on URL	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=`PingOne-IdP-ID-value
Issuer	PingOne for Enterprise **Issuer** value
Public certificate	Paste in the contents of the PingOne for Enterprise signing certificate.

6. Click **Save**.

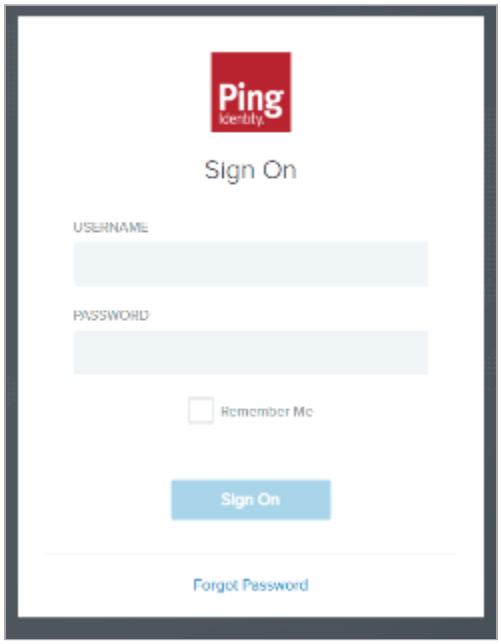
Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with GitHub access.

> **Note**
>
> To find the Ping desktop URL in the Admin console, go to **Setup → PingOne Dock**.

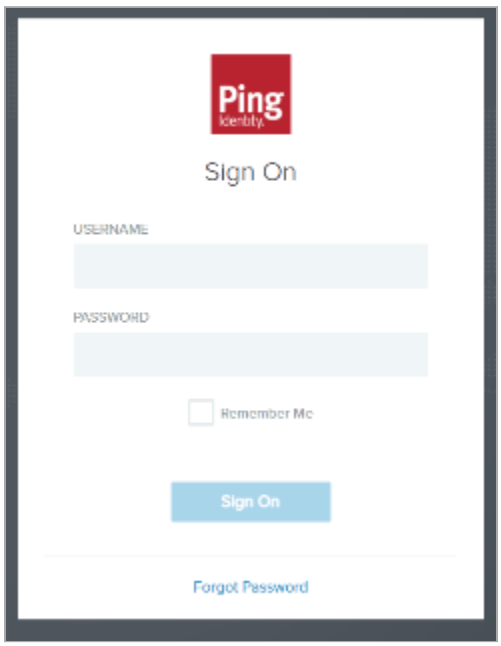
2. Complete the PingOne for Enterprise authentication.

   You're redirected to your GitHub domain.



Test the PingOne for Enterprise SP-initiated SSO integration

1. Go to `https://github.com/orgs/your-tenant/sso`.
2. After you're redirected to PingOne for Enterprise, enter your PingOne for Enterprise username and password.



You're redirected back to GitHub.

Configuring SAML SSO with GitHub Enterprise Server and PingFederate

Learn how to enable GitHub sign-on from a PingFederate URL (IdP-initiated sign-on) and direct GitHub sign-on using PingFederate (SP-initiated sign-on).

Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate GitHub with at least one user to test access.
- You must have administrative access to PingFederate and GitHub.

Download the GitHub metadata

1. Go to where your GitHub server publishes its metadata (`https://GitHub-hostname/saml/metadata`).
2. Save the metadata as an XML file.

Create a PingFederate SP connection for GitHub

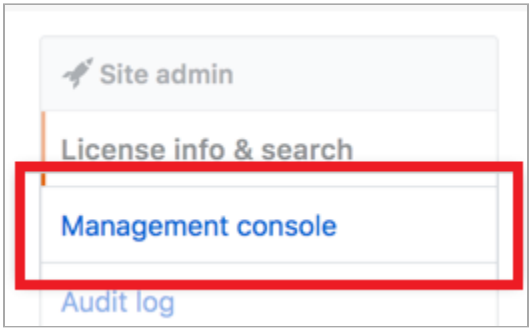
1. Sign on to the PingFederate administrative console.
2. Create an SP connection for GitHub in PingFederate using the GitHub metadata file:
    1. Configure using **Browser SSO** profile **SAML 2.0**.
    2. Enable the following **SAML Profiles**:
        - **IdP-Initiated SSO**
        - **SP-Initiated SSO**
    3. In **Assertion Creation: Attribute Contract**, if you want to have these values populated in GitHub, extend the contract to add attributes called **username** and **full_name.**
    4. In **Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment**, map **SAML_SUBJECT** to an attribute containing the user's email address.

       If added, map **username** and **full_name** to appropriate attributes.
    5. In **Protocol Settings: Allowable SAML Bindings**, enable **POST**.
    6. In **Credentials: Digital Signature Settings**, select the **PingFederate Signing Certificate**.
3. Save the configuration.
4. Export the signing certificate.
5. Export and then open the metadata file.

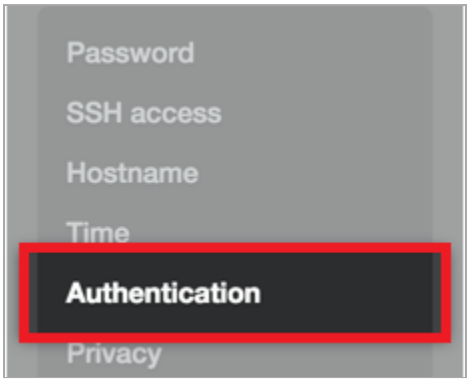
   Copy the value of the entityID and the Location entry (`https://your-value/idp/SSO.saml2`).

Add the PingFederate IdP Connection to GitHub

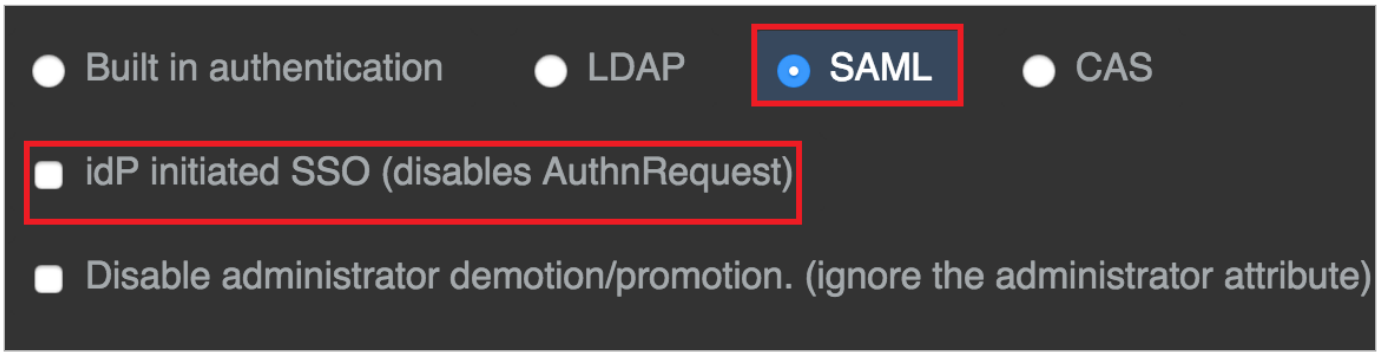
1. Sign on to GitHub Enterprise Server as an administrator.
2. Click the **Rocket** icon.
3. Click **Management Console**.



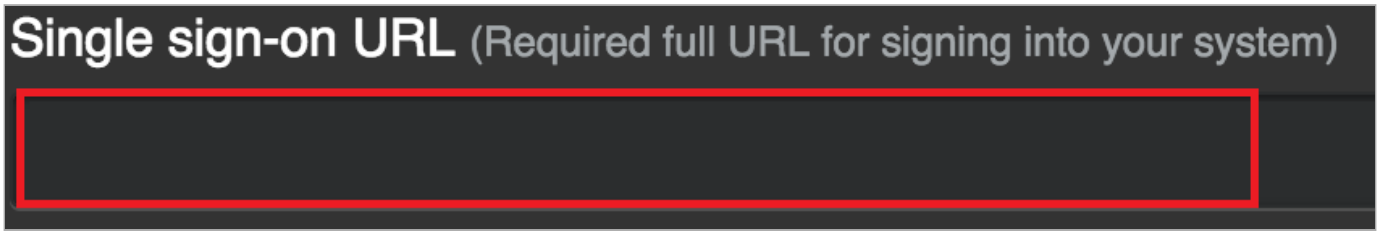
4. Click **Authentication**.



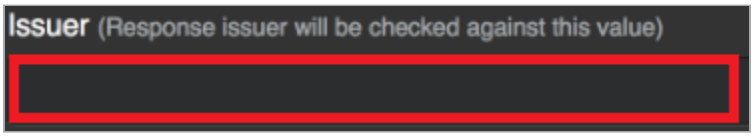
5. Click **SAML** and select the **idP initiated SSO (disables AuthnRequest)** check box.



6. In the **Single sign-on URL** field, enter the PingFederate Location value (`https://your-value/idp/SSO.saml2`).



7. In the **Issuer** field, enter the PingFederate **entityID** value.



8. Click **Choose File** for the **Verification Certificate** and upload the PingFederate signing certificate that you downloaded
9. Click **Save Settings**.

Test the PingFederate IdP-initiated SSO integration

1. Go to the PingFederate **SSO Application Endpoint** for the GitHub SP connection.
2. Complete the PingFederate authentication.

   You're redirected to your GitHub domain.

Test the PingFederate SP-initiated SSO integration

1. Go to your GitHub server.
2. After you're redirected to PingFederate, enter your PingFederate username and password.

   You're redirected back to GitHub.

Configuring SAML SSO with GitHub Enterprise Server and PingOne for Enterprise

Learn how to enable GitHub sign on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct GitHub sign on using PingOne for Enterprise (SP-initiated sign-on).

Before you begin

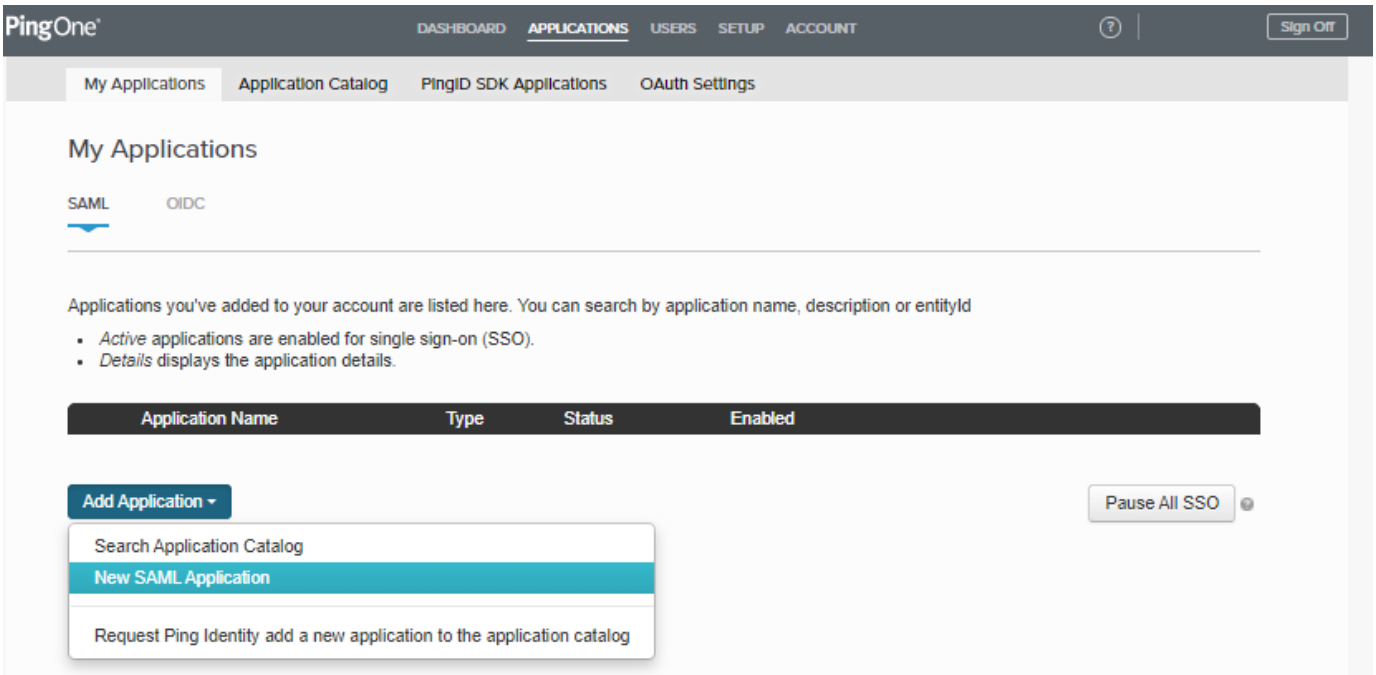
- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate GitHub with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and GitHub.

Download the GitHub metadata

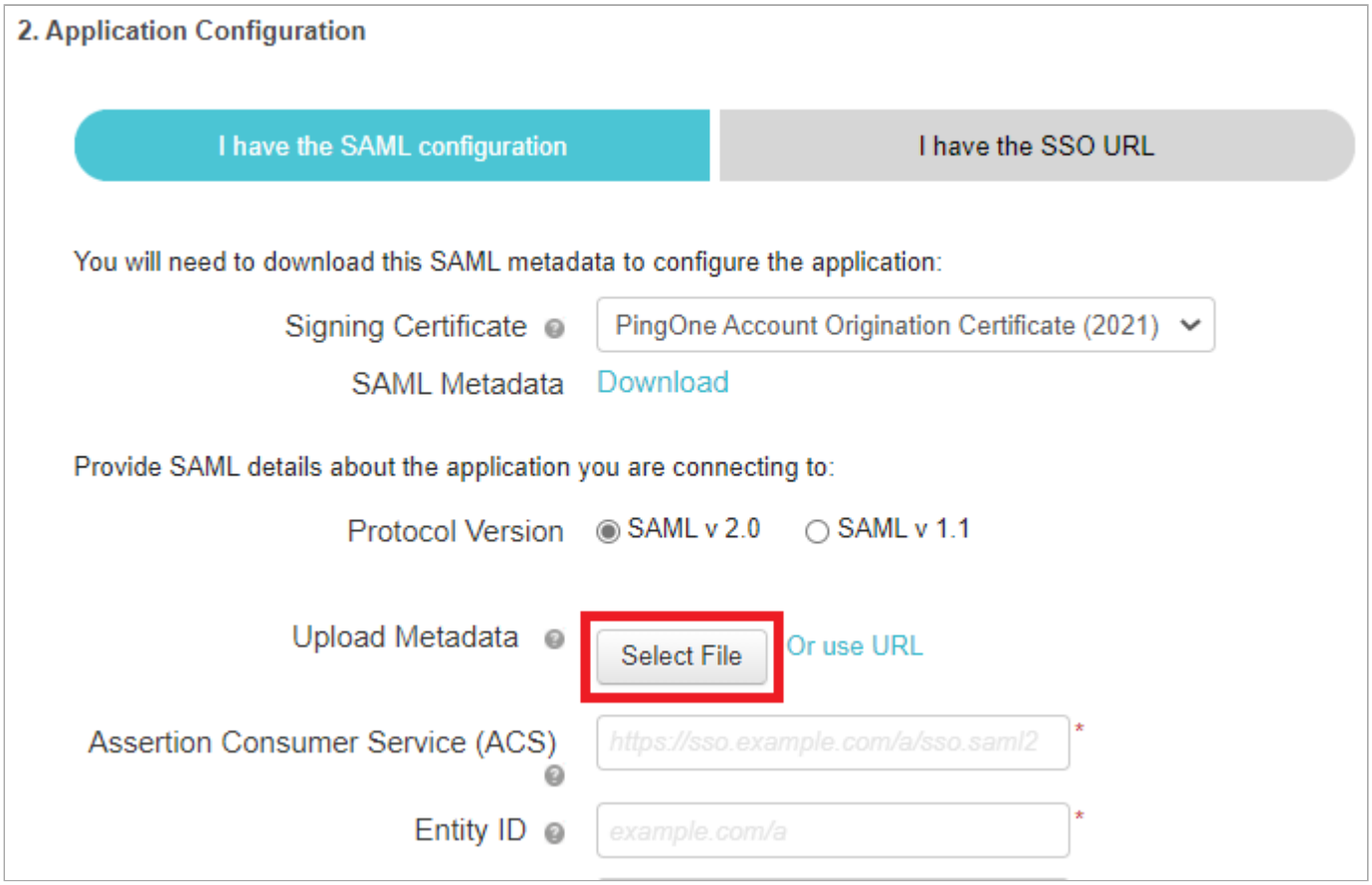
1. Go to where your GitHub server publishes its metadata (`https://GitHub-hostname/saml/metadata`).
2. Save the metadata as an XML file.

Set up the GitHub application in PingOne for Enterprise

1. Sign on to PingOne for Enterprise for Enterprise and go to **Applications → Application Catalog**.
2. On the **SAML** tab, click **Add Application**.



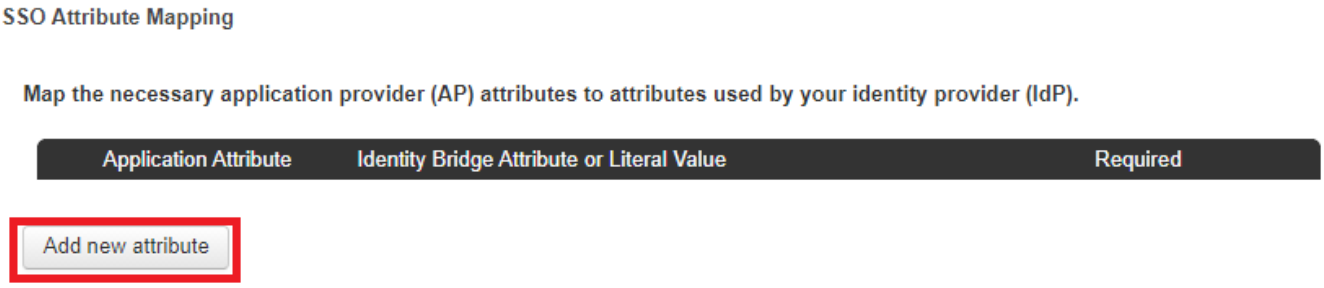
3. Enter **GitHub** as the application name.
4. Enter a suitable description.
5. Select **Collaboration** as the category.
6. Click **Continue to Next Step**.
7. In the **Upload Metadata** row, click **Select File** and upload the metadata file that you saved from GitHub.

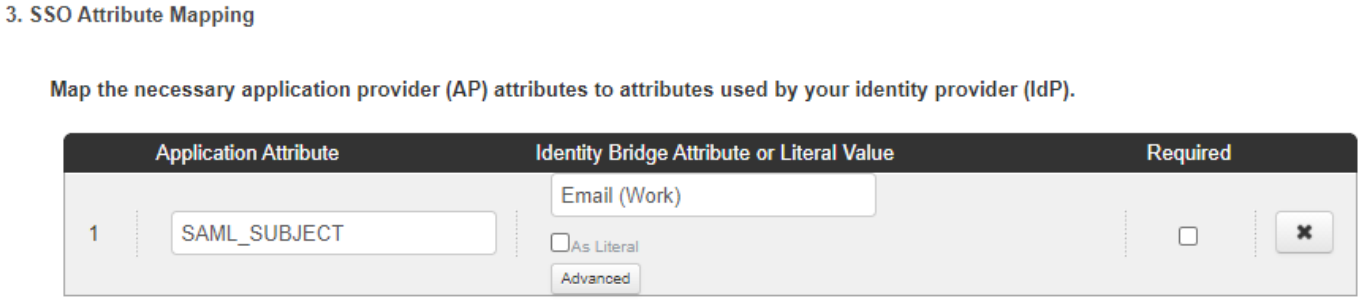


The following values should now be populated:

- **ACS URL**: `https://github.com/orgs/your-tenant/saml/consume`
- **Entity ID**: `https://github.com/orgs/your-tenant`

8. Click **Continue to Next Step**.
9. Click **Add new attribute** and map **SAML_SUBJECT** to the attribute containing the user's email address.



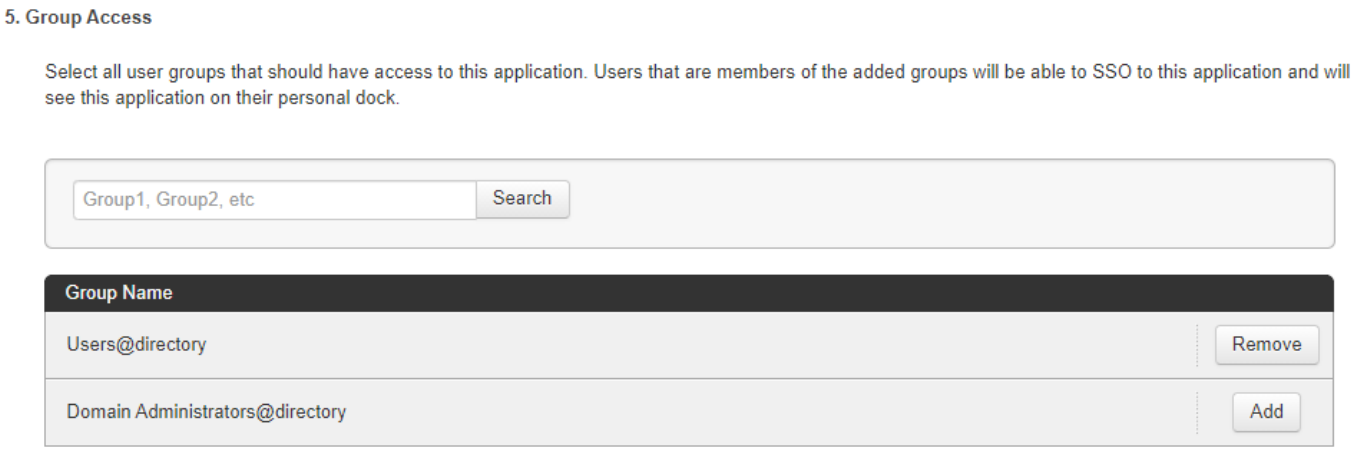


10. **Optional:** Add the **username** and **full_name** attributes, then map these to appropriate attributes.

    This populates these values in GitHub when a new user signs on.

11. Click **Continue to Next Step**.

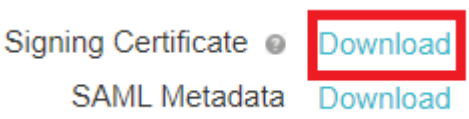
12. Click **Add** for all user groups that should have access to GitHub.



13. Click **Continue to Next Step**.

14. Copy the **Issuer** and **idpid** values.

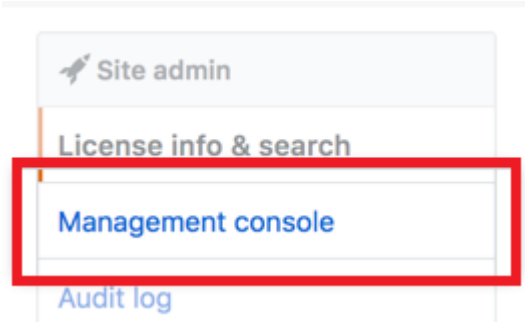
15. Download the signing certificate.



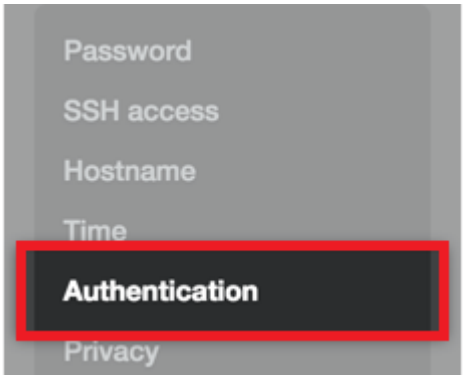
16. Click **Finish**.

Add the PingOne for Enterprise IdP Connection to GitHub

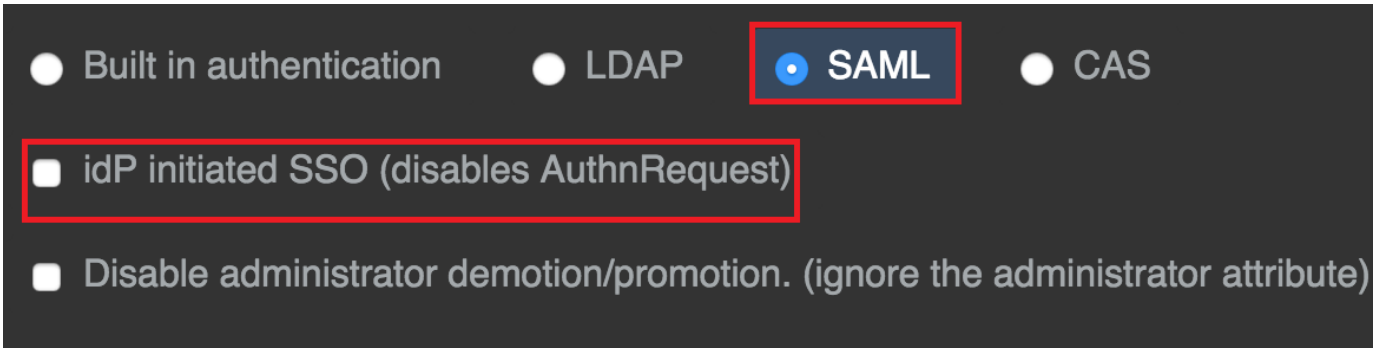
1. Sign on to GitHub Enterprise Server as an administrator.
2. Click the **Rocket** icon.
3. Click **Management Console**.



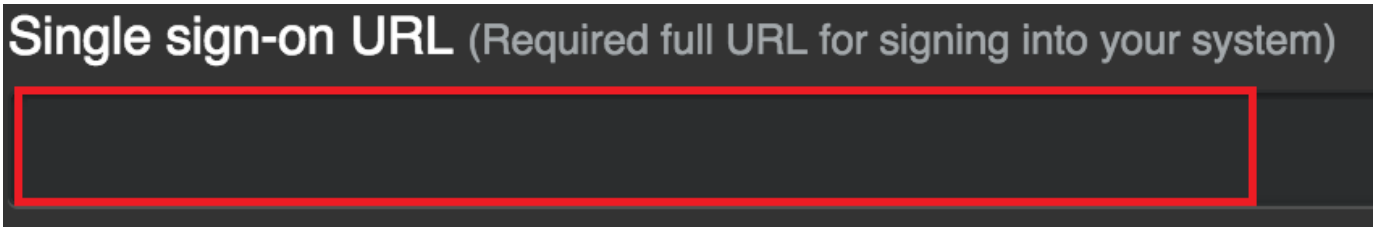
4. Click **Authentication**.



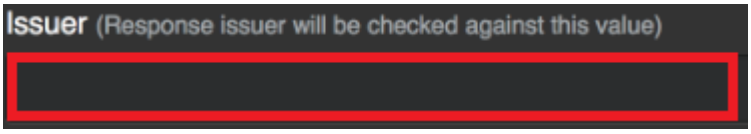
5. Click **SAML** and select the **idP initiated SSO (disables AuthnRequest)** check box.



6. In the **Single sign-on URL** field, enter `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=idpid-value-from-PingOne`.



7. In the **Issuer** field, enter the PingOne for Enterprise **Issuer** value.



8. Click **Choose File** for the **Verification Certificate** and upload the PingOne signing certificate that you downloaded.
9. Click **Save Settings**.

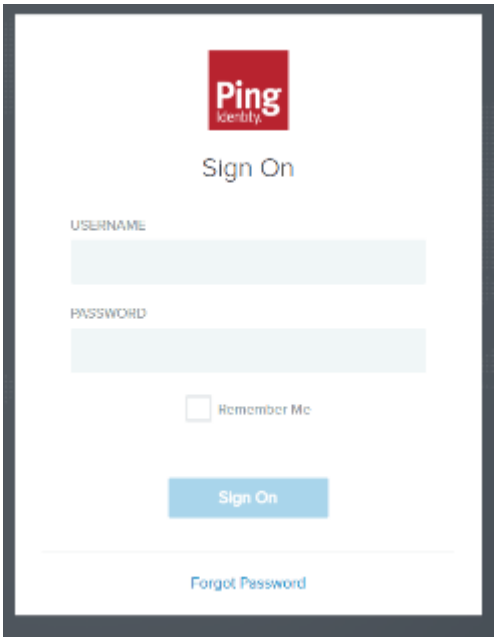
Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with GitHub access.

> **Note**
>
> To find the Ping desktop URL in the Admin console, go to **Setup → Dock → PingOne Dock URL**.

2. Complete the PingOne for Enterprise authentication.

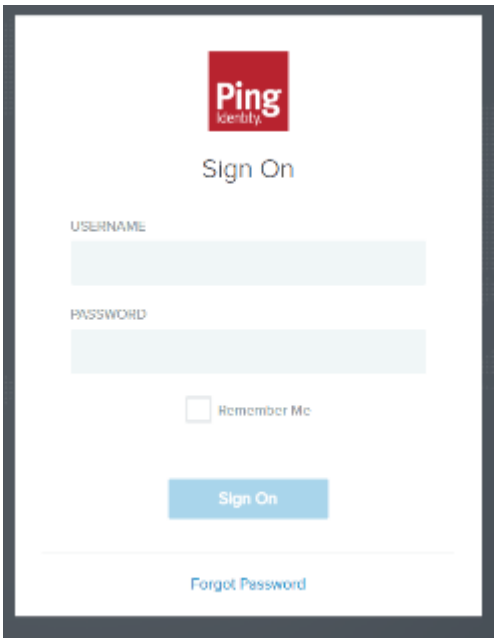
   You're redirected to your GitHub server.



Test the PingOne SP-initiated SSO integration

1. Go to your GitHub server.

2. After you're redirected to PingOne for Enterprise, enter your PingOne username and password.



You're redirected back to GitHub.

Greenhouse

Configuring SAML SSO with Greenhouse and PingOne

Learn how to configure SAML single sign-on (SSO) with Greenhouse and PingOne.

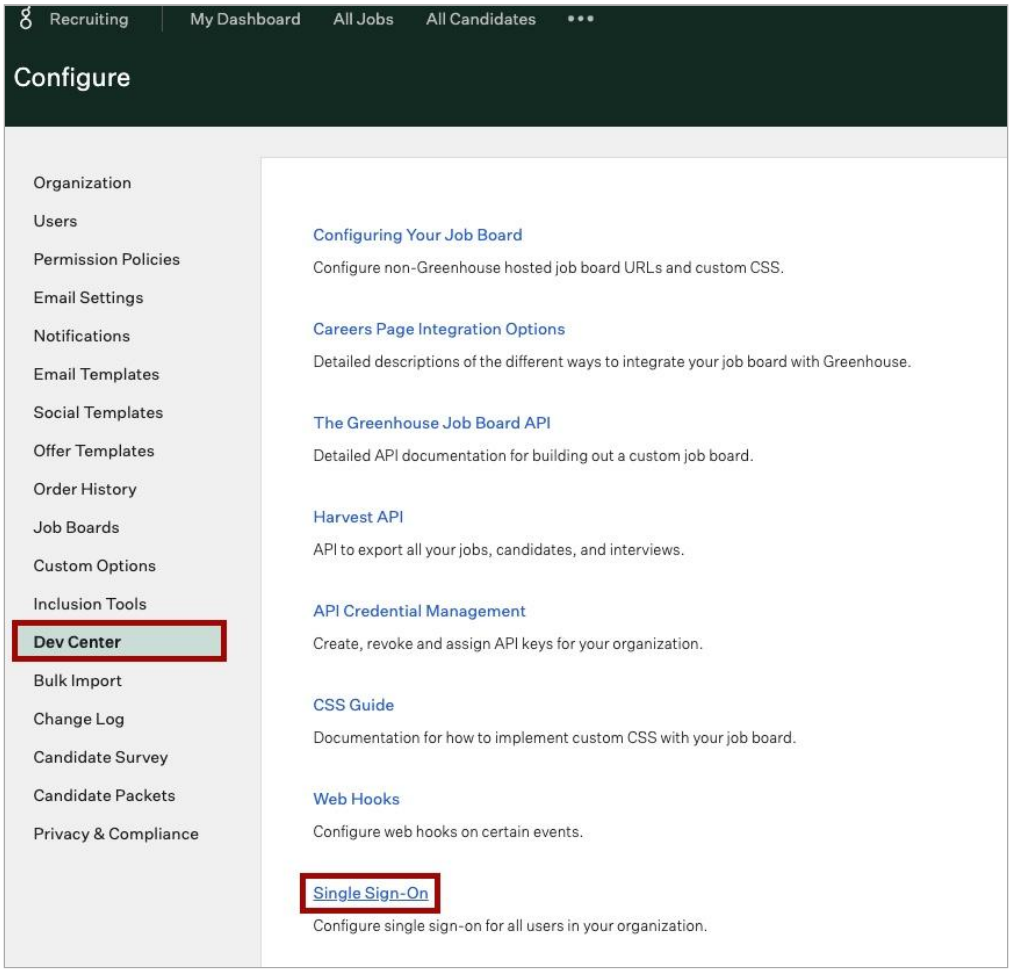
Before you begin

You must have an Advanced or Expert subscription tier to configure SAML. Learn more in see https://support.greenhouse.io/hc/en-us/articles/210259723-Single-Sign-On-overview.

> **Note**
>
> This is a tested integration.

Configure SSO in Greenhouse

1. Sign on to your Greenhouse portal and select the **Gear** icon (⚙) in the upper right hand corner.
2. In the left navigation pane, go to **Dev Center → Single Sign-On** to begin configuring SSO.



> **Note**
>
> If you don't see **Single Sign-On**, you'll need to contact Greenhouse customer support to update your permissions.

3. On the following page, click **Begin Configuration**.

   The configuration page opens.

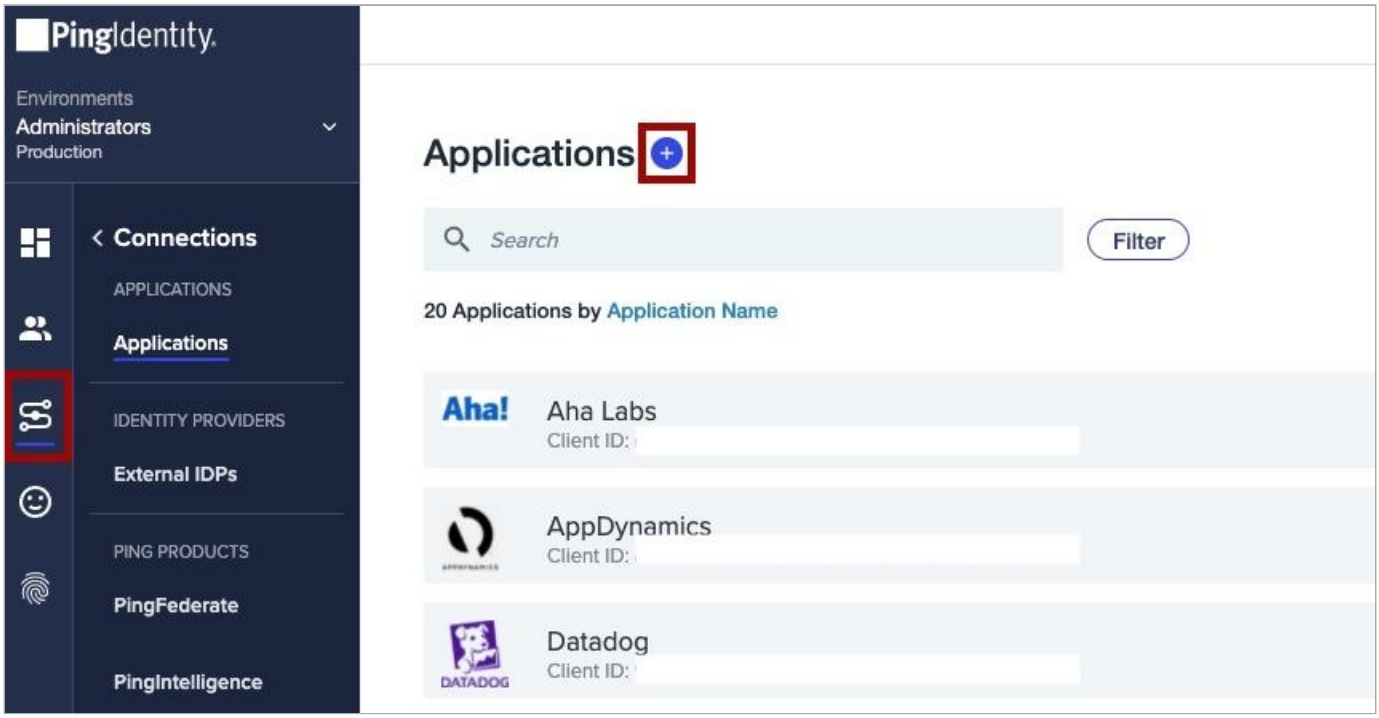
4. In the **Add Greenhouse to your Single Sign-on provider** section, note the **SSO Assertion Consumer URL**. You'll need this later.

Configure Greenhouse in PingOne

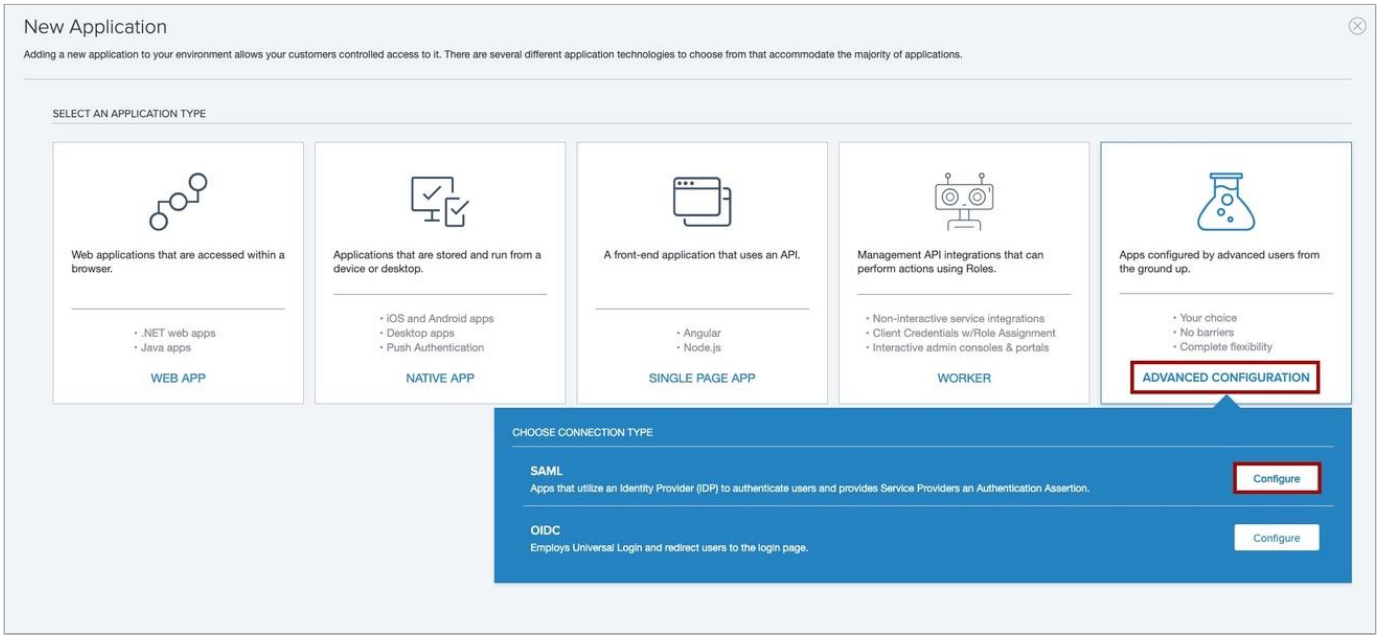
1. On a new tab, sign on to your PingOne SSO admin account.

You'll use the settings from the previous procedure to start configuring Greenhouse in PingOne.

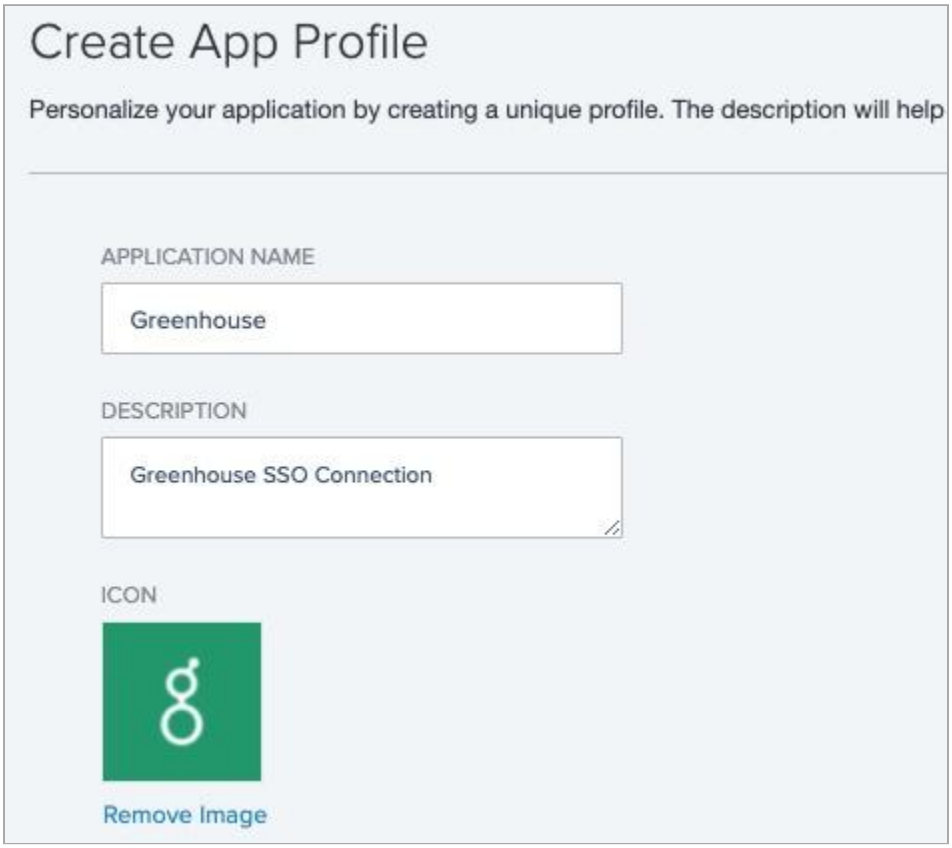
2. Go to **Connections → Applications** and click the + icon.



3. On the **New Application** page, click **Advanced Configuration**, and on the **SAML** line, click **Configure**.



4. On the **Create App Profile** page, enter:
    - **Application Name** (Required)
    - **Description** (Optional)
    - **Icon** (Optional)



5. Click **Save and Continue**.

6. On the **Configure SAML Connection** page, in the **Provide App Metadata** section, click **Manually Enter**.

7. Input the service provider (SP) data:

    - In the **ACS URLS** field, paste in the **SSO Assertion Consumer URL** that you copied from Greenhouse in the previous procedure.

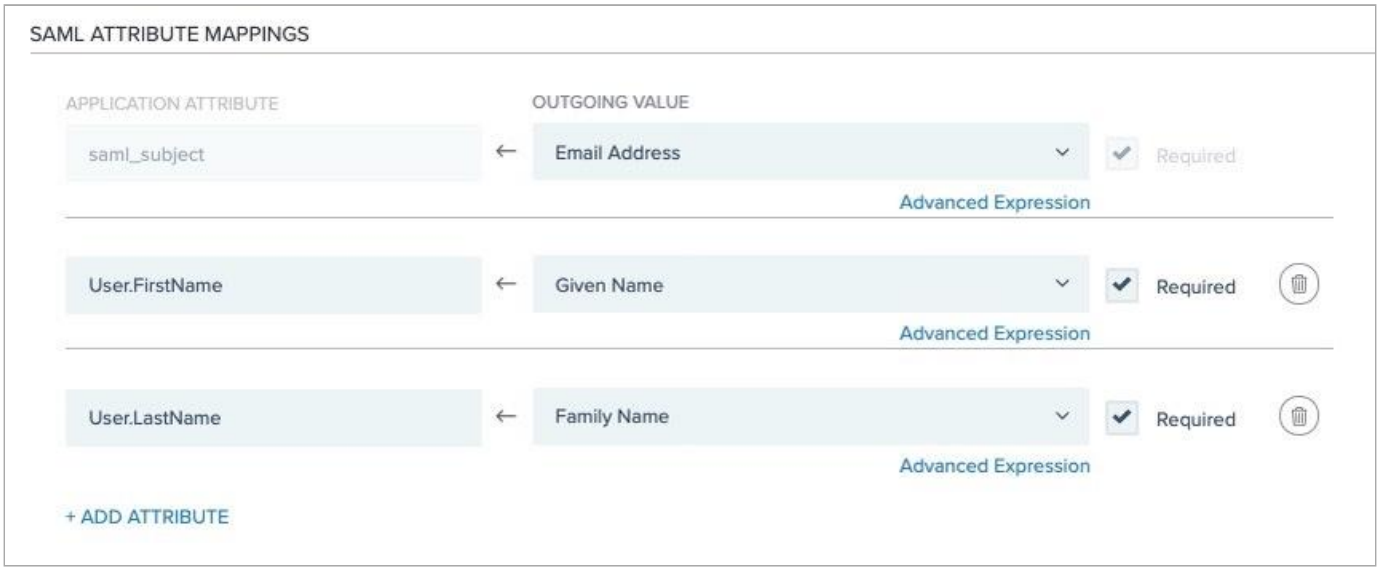
- In the **Entity ID** field, enter `greenhouse.io`.

- In the **Assertion Validity Duration (In Seconds)**, enter a value, for example, `3600`.

8. Click **Save and Continue**.
9. On the **Attribute Mapping** page, add the following attributes, selecting the **Required** check box for each attribute.
   - **saml_subject** = **Email Address**

     > **Note**
     >
     > This is automatically assigned to User ID, but will need to be updated.

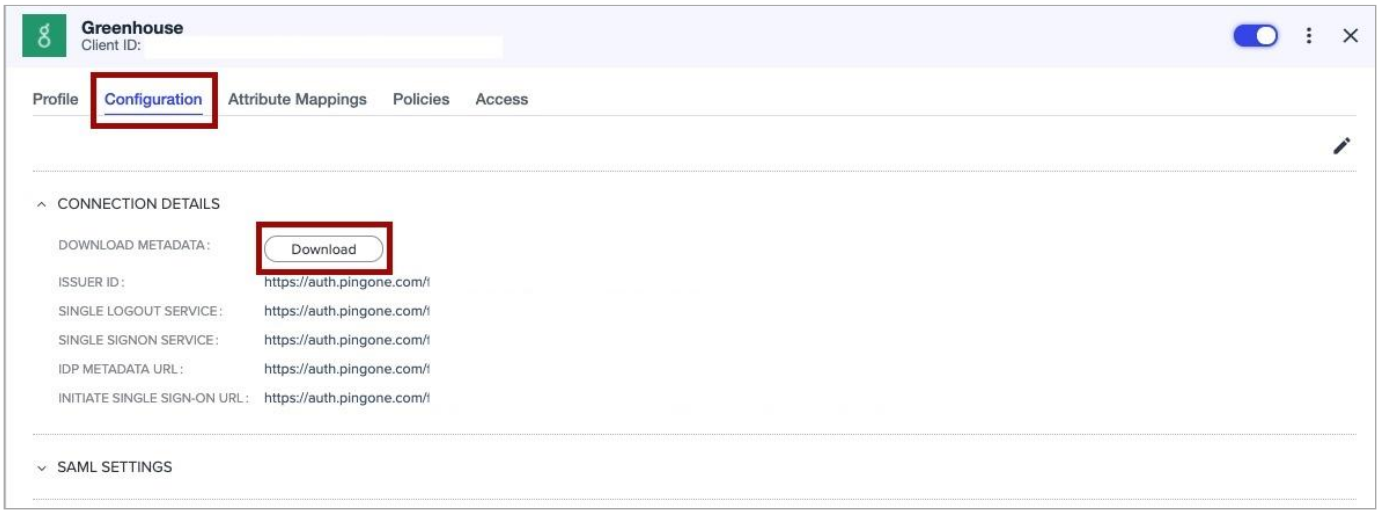
   - **User.FirstName** = **Given Name**
   - **User.LastName** = **Family Name**



10. Click **Save and Close**.
11. On the **Applications** page, enable the connection by toggling the slider:

12. Click on the newly created application to open it.
13. On the **Configuration** tab, in the **Connection Details** section, click **Download** to download the IdP metadata.

    You'll need this to complete the next step.

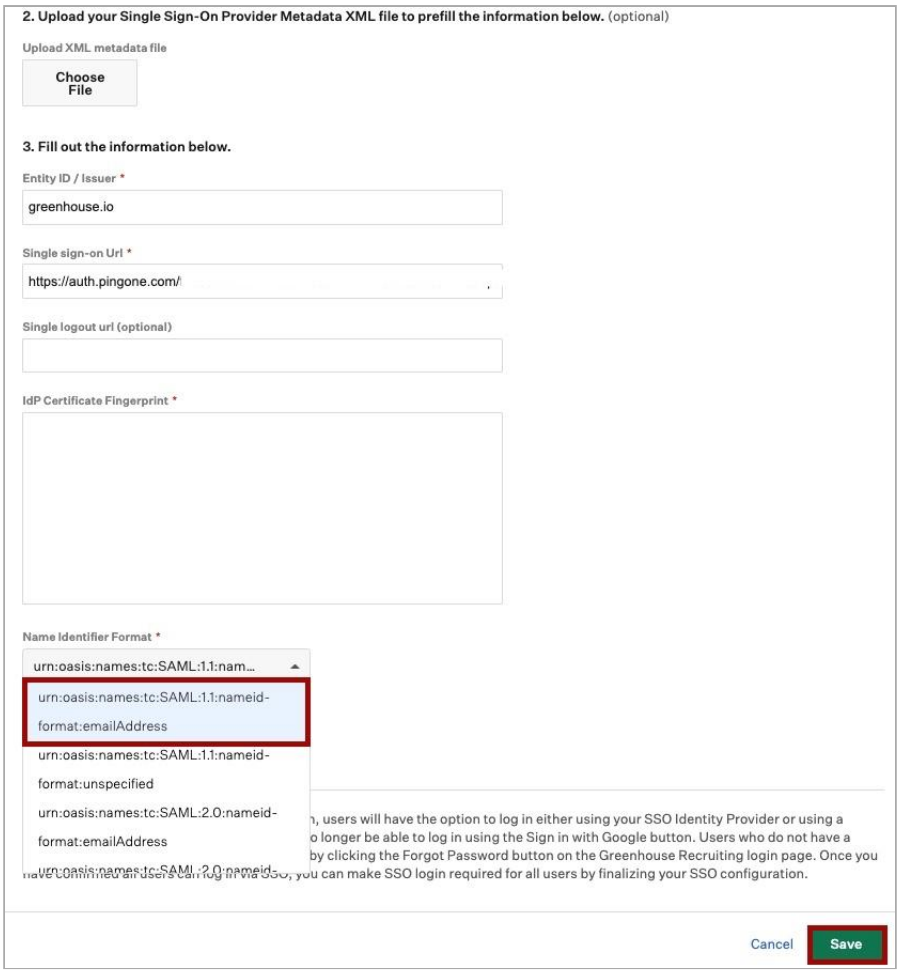


14. Return to Greenhouse and, in the **Upload your Single Sign-On Provider** section, click **Choose File** and upload the IdP metadata that you downloaded in the previous step.

All required fields will be populated automatically, except for the **Name Identifier Format**.

15. Update the **Name Identifier Format** to `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`.

    Click **Save**.

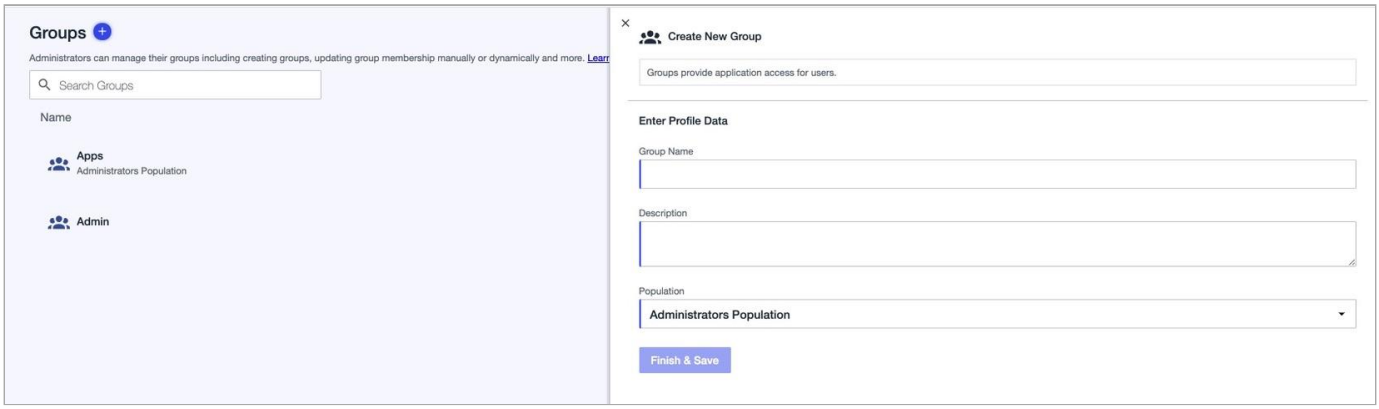


Create and assign identities

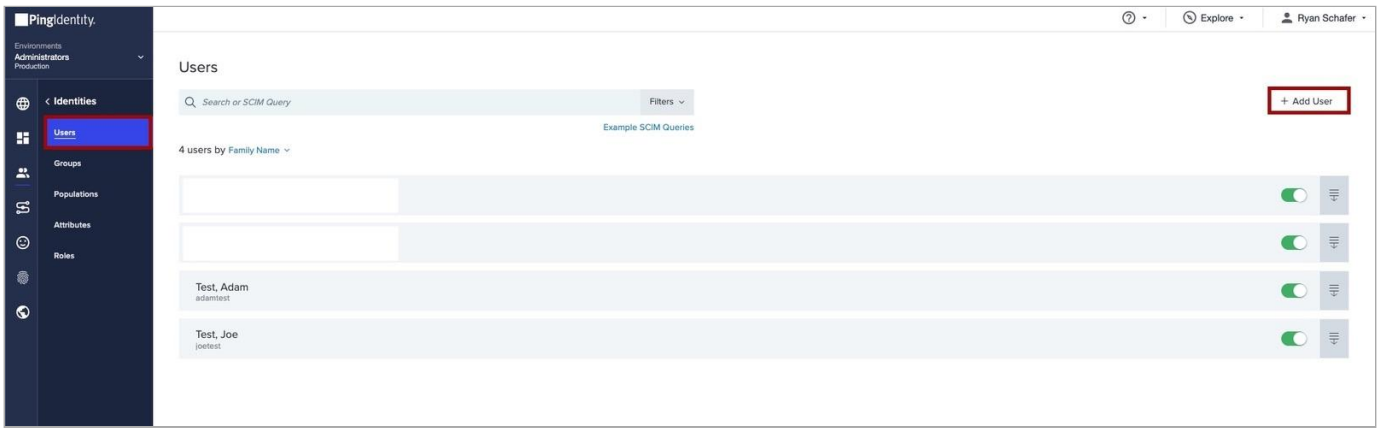
Before you can test the integration, you must create and assign identities in PingOne. If you've already assigned identities and groups in PingOne, move on to Test the integration.

1. In PingOne, go to **Identities Groups** and click the + icon next to **Groups.**

2. On the **Create New Group** page, enter values for the following:
    - **Group Name** (Required)
    - **Description** (Optional)
    - **Population** (Optional)
3. Click **Finish & Save**.



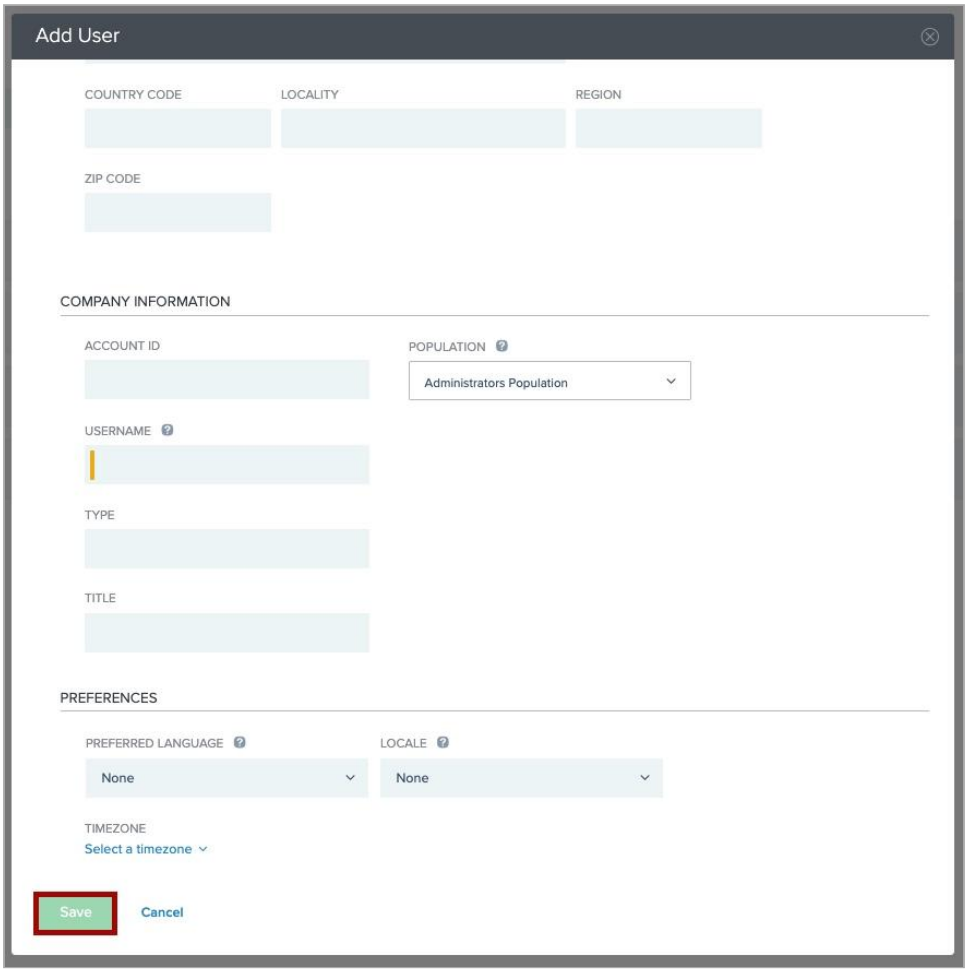
4. To add identities to the group, on the **Identities** tab, go to **Users → + Add User**.



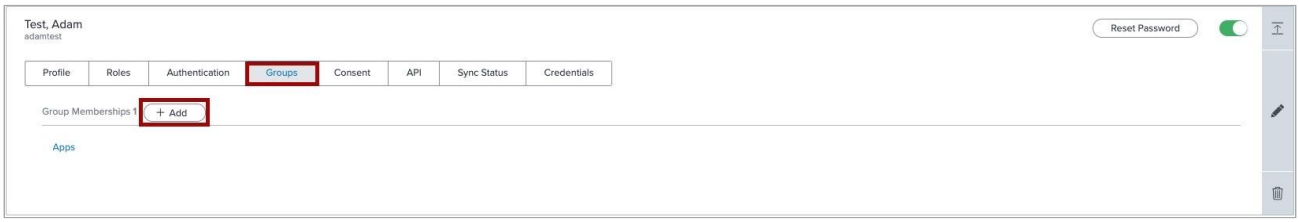
5. On the **Add User** page, enter all the necessary information for a user.

> **Important**
>
> Verify that the first name, last name, and email address are correct, as these are values passed in the SAML assertion.

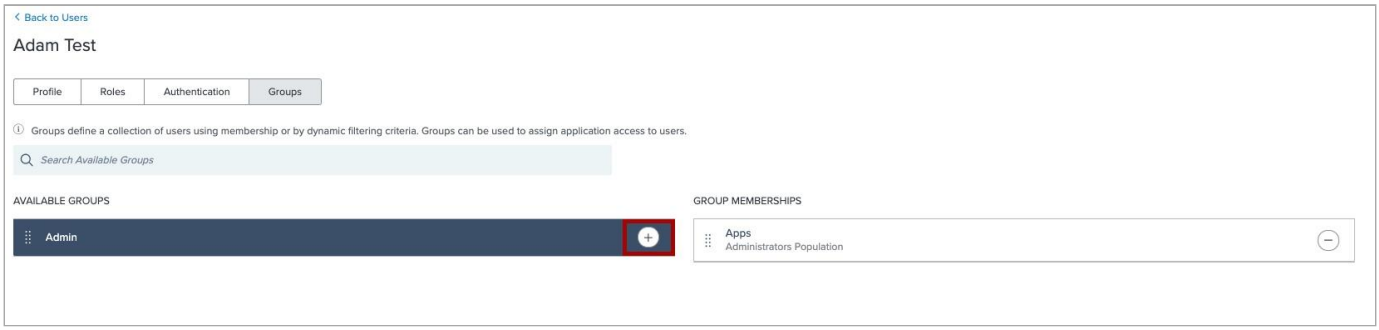
6. Click **Save**.



7. Assign the user that you created to the group that you created previously. Locate the user you created and do the following:
    - Expand their section.
    - Select the **Groups** tab.
    - Click **+ Add**.

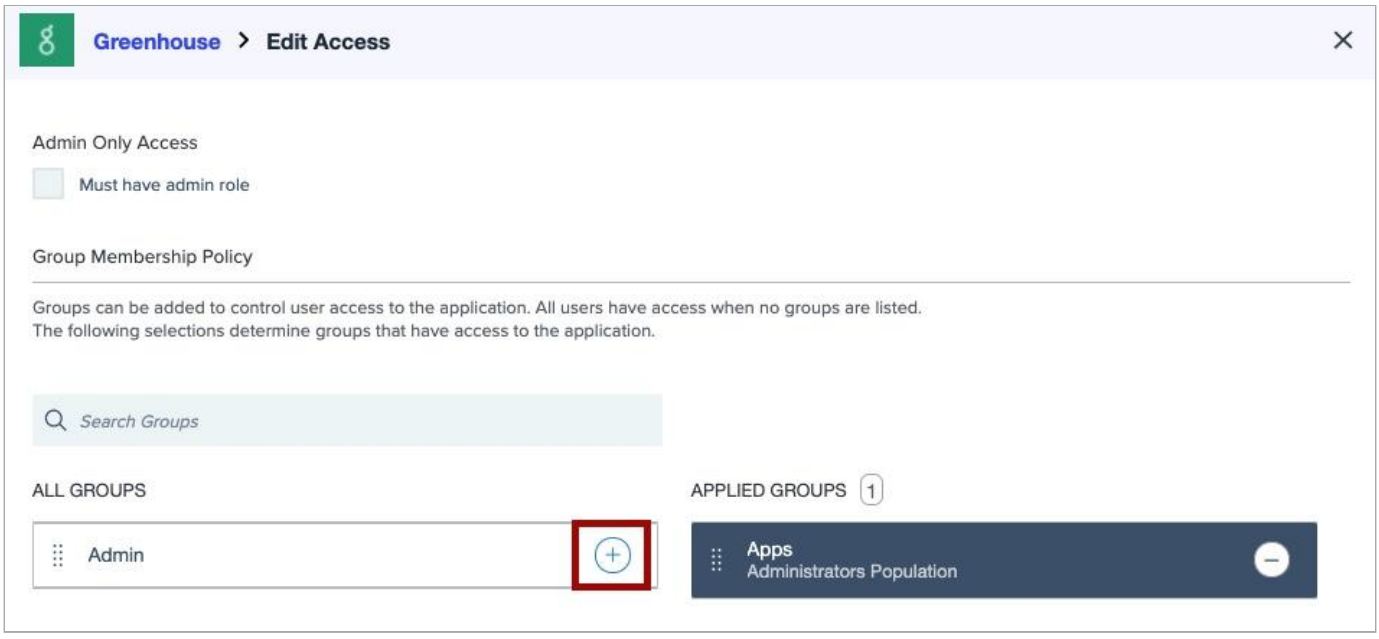


8. In the **Available Groups** section, select the group that you created and click the **+** icon to add it to the user's group memberships. Click **Save**.



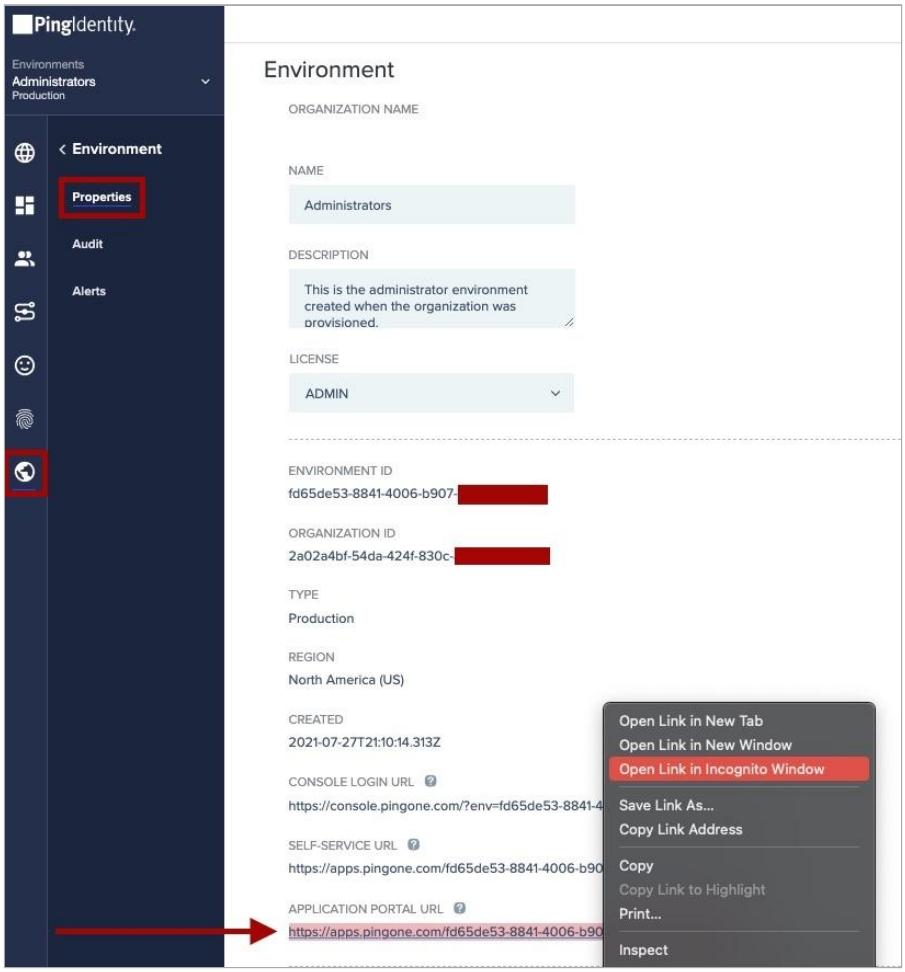
9. On the **Connections** tab, for the Greenhouse application, do the following:
    - Click the **Access** tab.
    - Click the **Pencil** icon to edit the configuration.

10. Select the group that you created and add it to the **Applied Groups** section. Click **Save**.

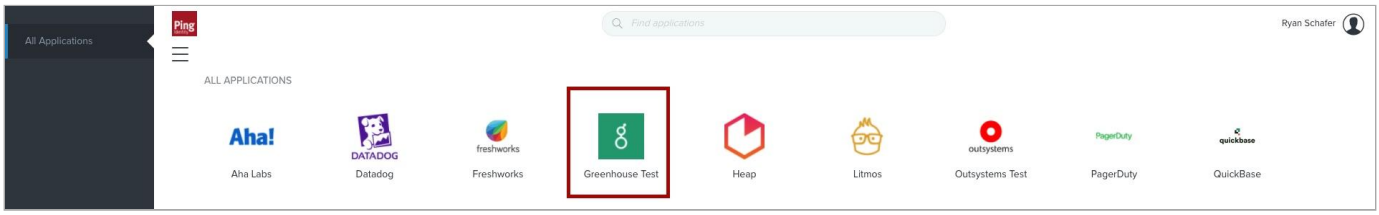


Test the integration

1. In the PingOne admin console, go to **Dashboard → Environment Properties**.
2. Right-click on the **Application Portal URL** and open it in a private browser session.

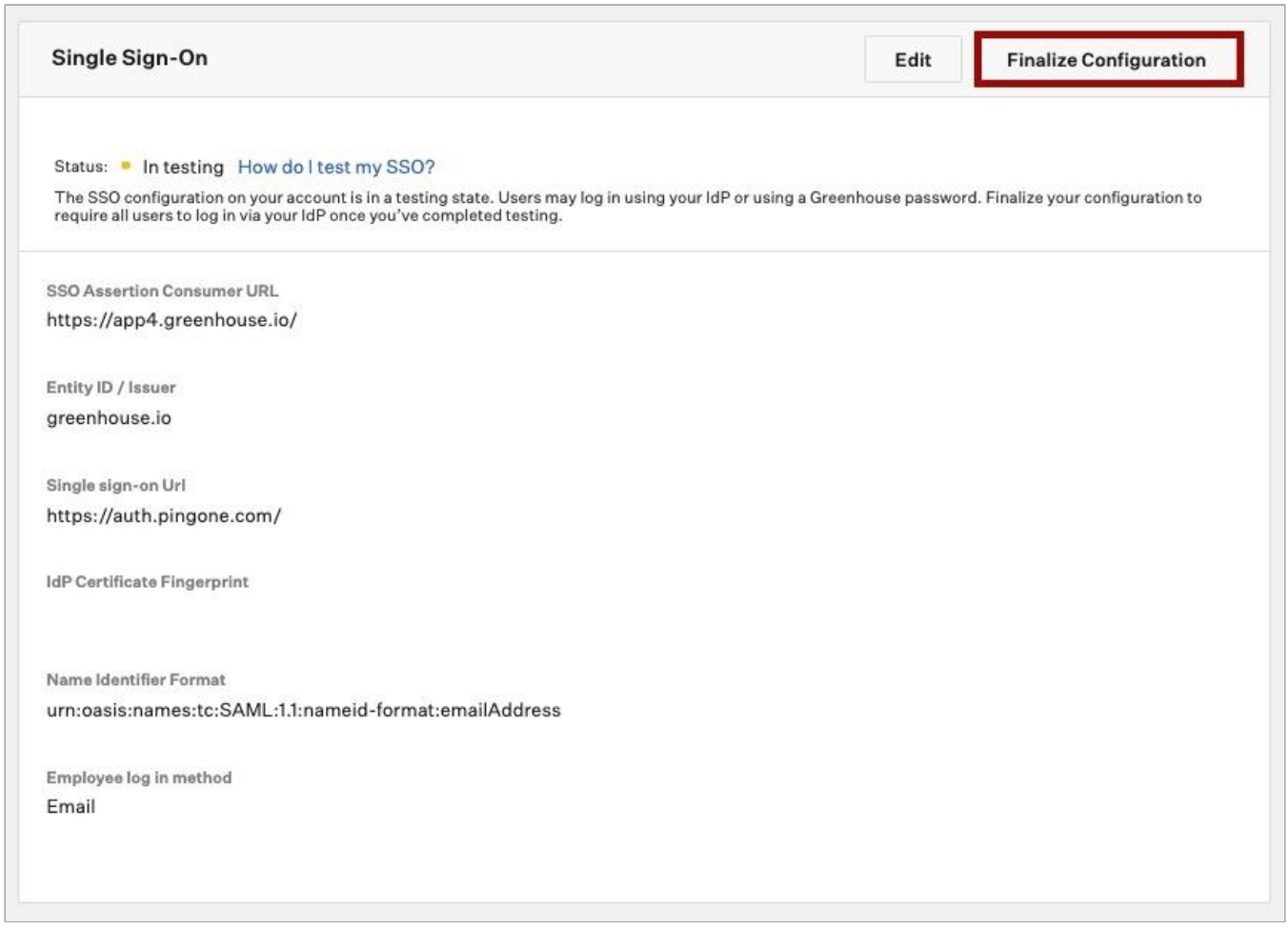


3. Sign on as the test user that you created and click the Greenhouse tile.

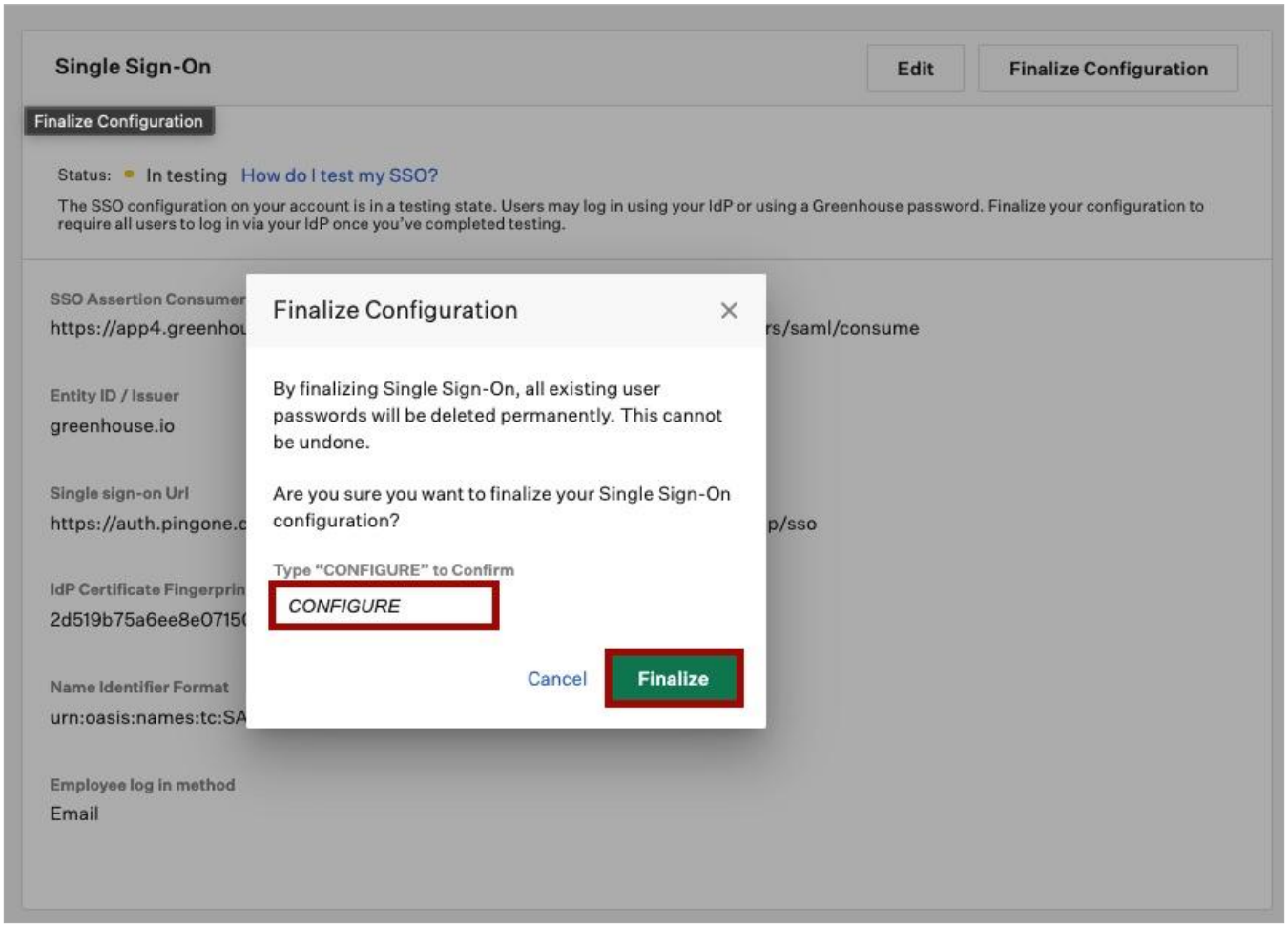


You're signed on to the user's Greenhouse account.

4. On the SSO configuration page in Greenhouse, click **Finalize Configuration**.



5. When prompted, enter `Configure`. Click **Finalize** to complete the connection.



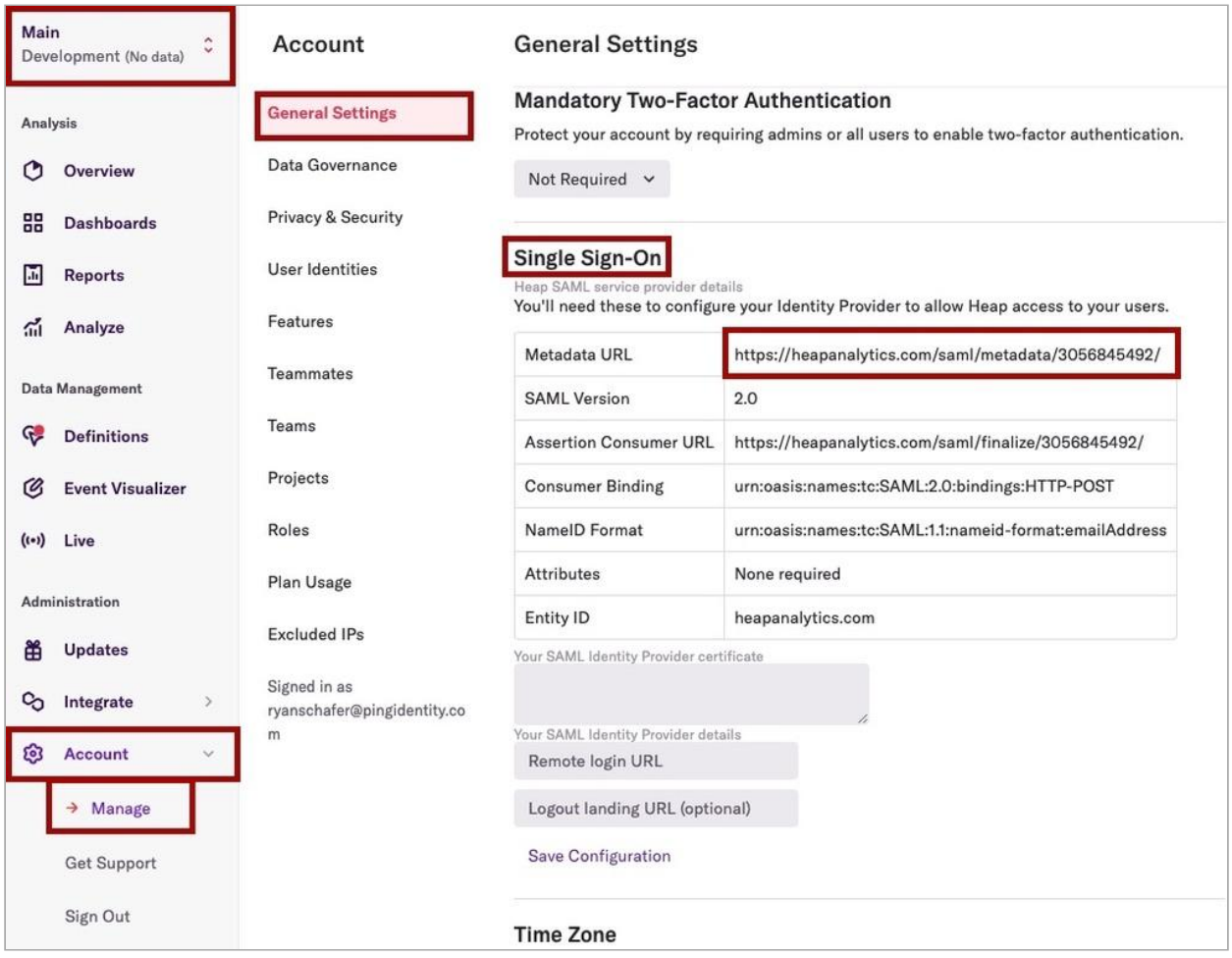
Heap

Configuring SAML SSO with Heap and PingOne

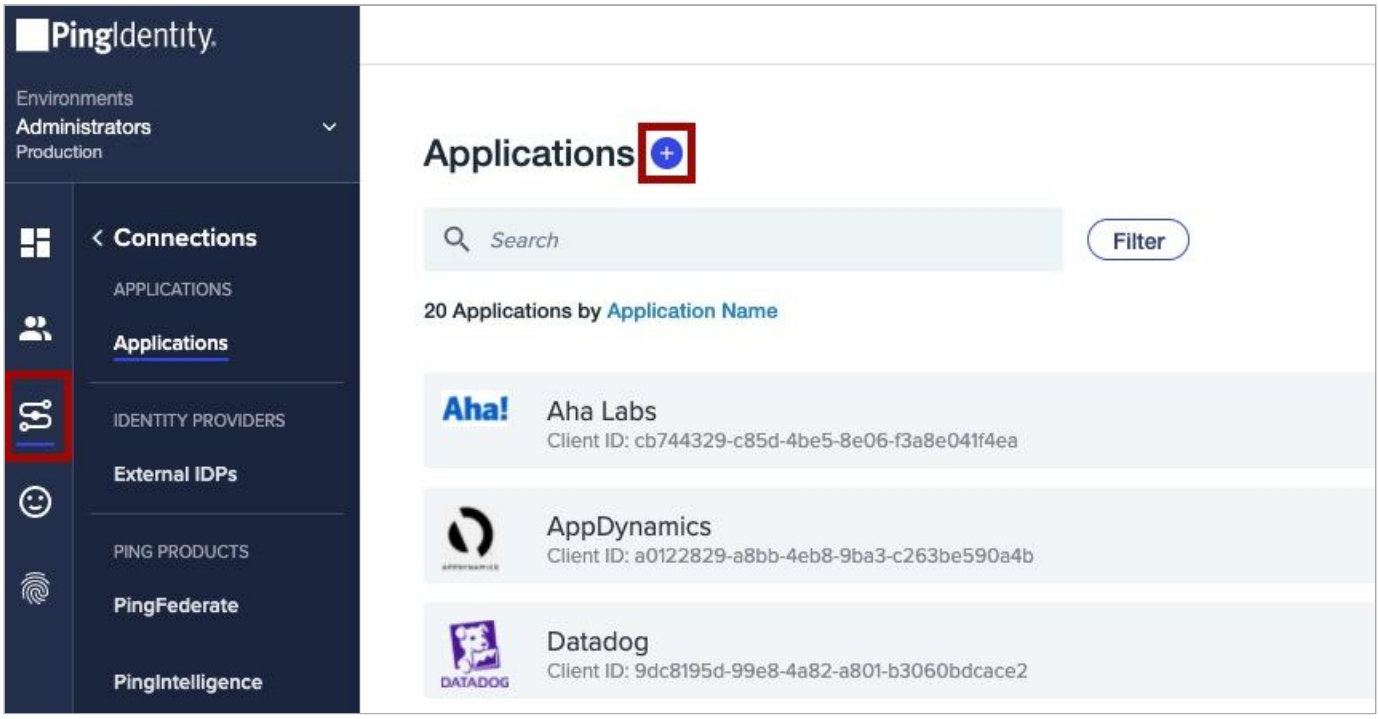
Learn how to configure SAML single sign-on (SSO) with Heap and PingOne.

Configure SSO with Heap

1. Sign on to your Heap admin portal and make sure that you're in the **Development** section.
2. In the left hand pane, go to **Account → Manage → General Settings**.
3. In the **Single Sign-On** section, copy the **Metadata URL**. You'll need this later.

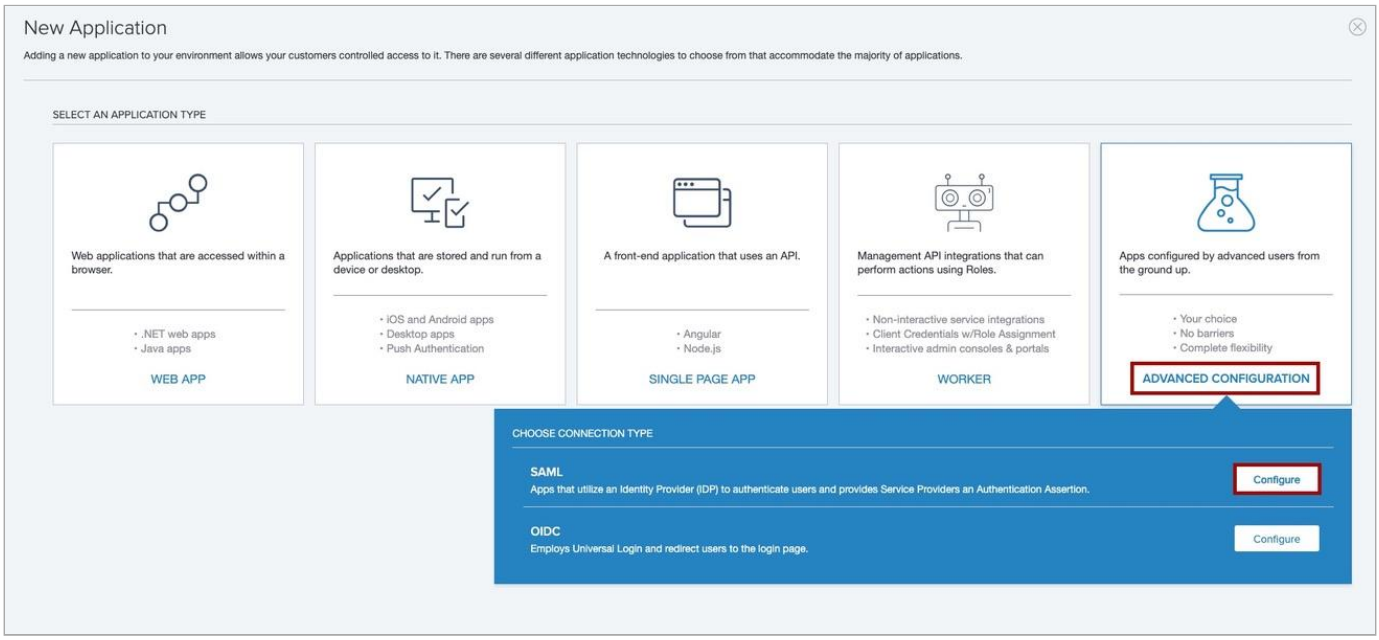


4. In a new tab, sign on to your PingOne admin account and go to **Connections → Applications**.
5. Click the + icon next to **Applications**.



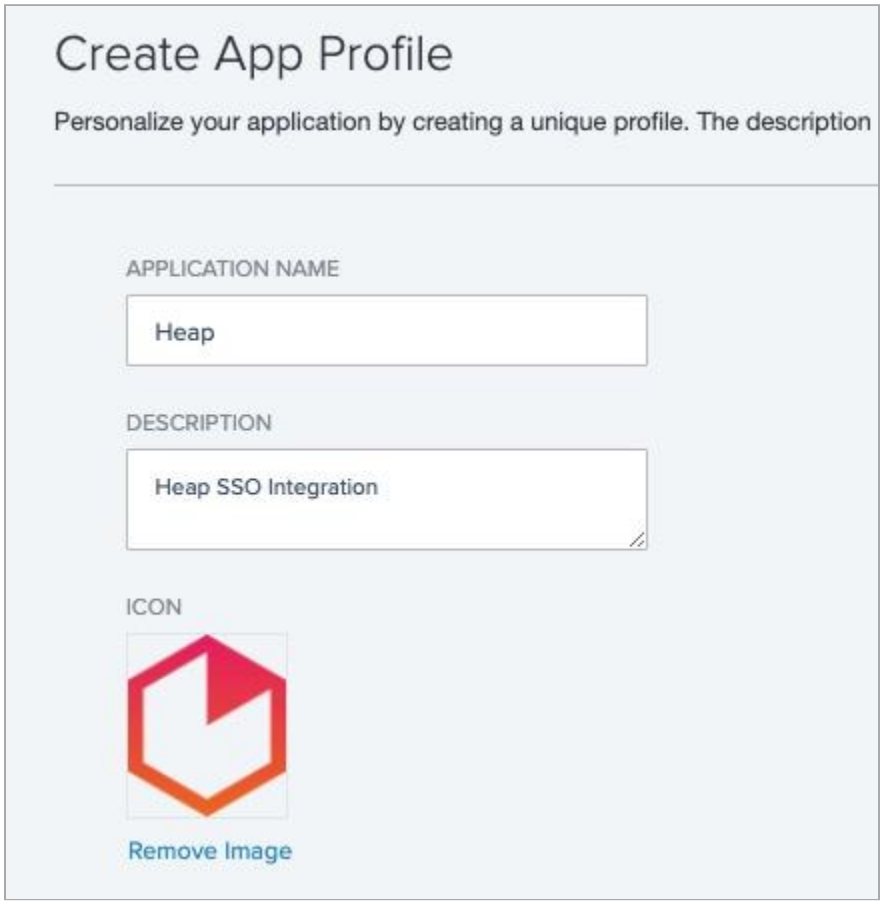
6. On the **New Application** page, click **Advanced Configuration**.

7. In the **Choose Connection Type** list, on the **SAML** line, click **Configure**.



8. On the **Create App Profile** page, enter the values for:

   - **Application Name** (Required)
   - **Description** (Optional)
   - **Icon** (Optional)



9. On the **Configure SAML Connection** page, in the **Provide App Metadata** section, click **Import From URL**.

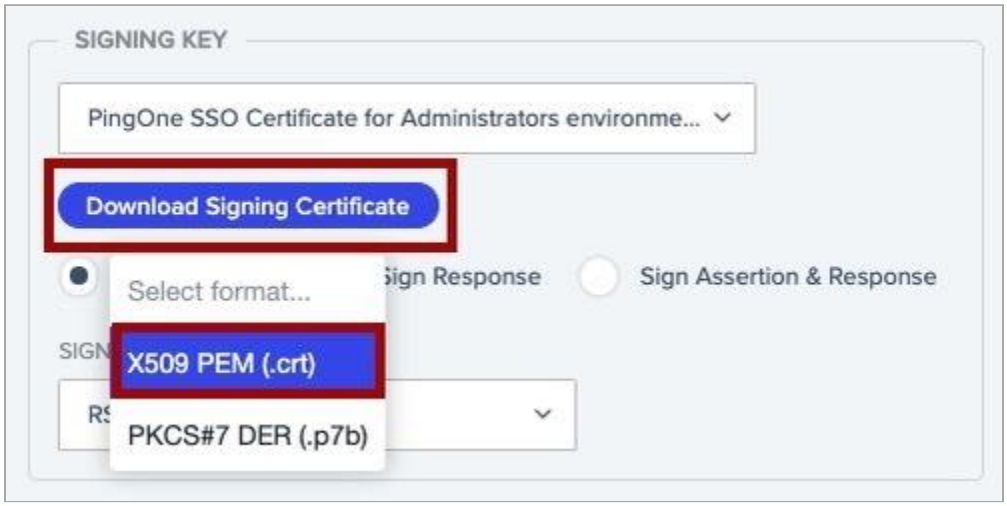
   Paste in the URL that you copied previously and click **Import**.

   After import, all necessary fields are auto-populated except for the **Assertion Validity Duration**.

10. In the **Assertion Validity Duration** field, enter a valid duration value (in seconds), such as 3600.
11. Update the **SUBJECT NAMEID FORMAT** section to `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`.

> **Note**
>
> If you don't update this section, you'll get an error for the integration. **SUBJECT NAMEID FORMAT** does not automatically update when you upload the service provider metadata.

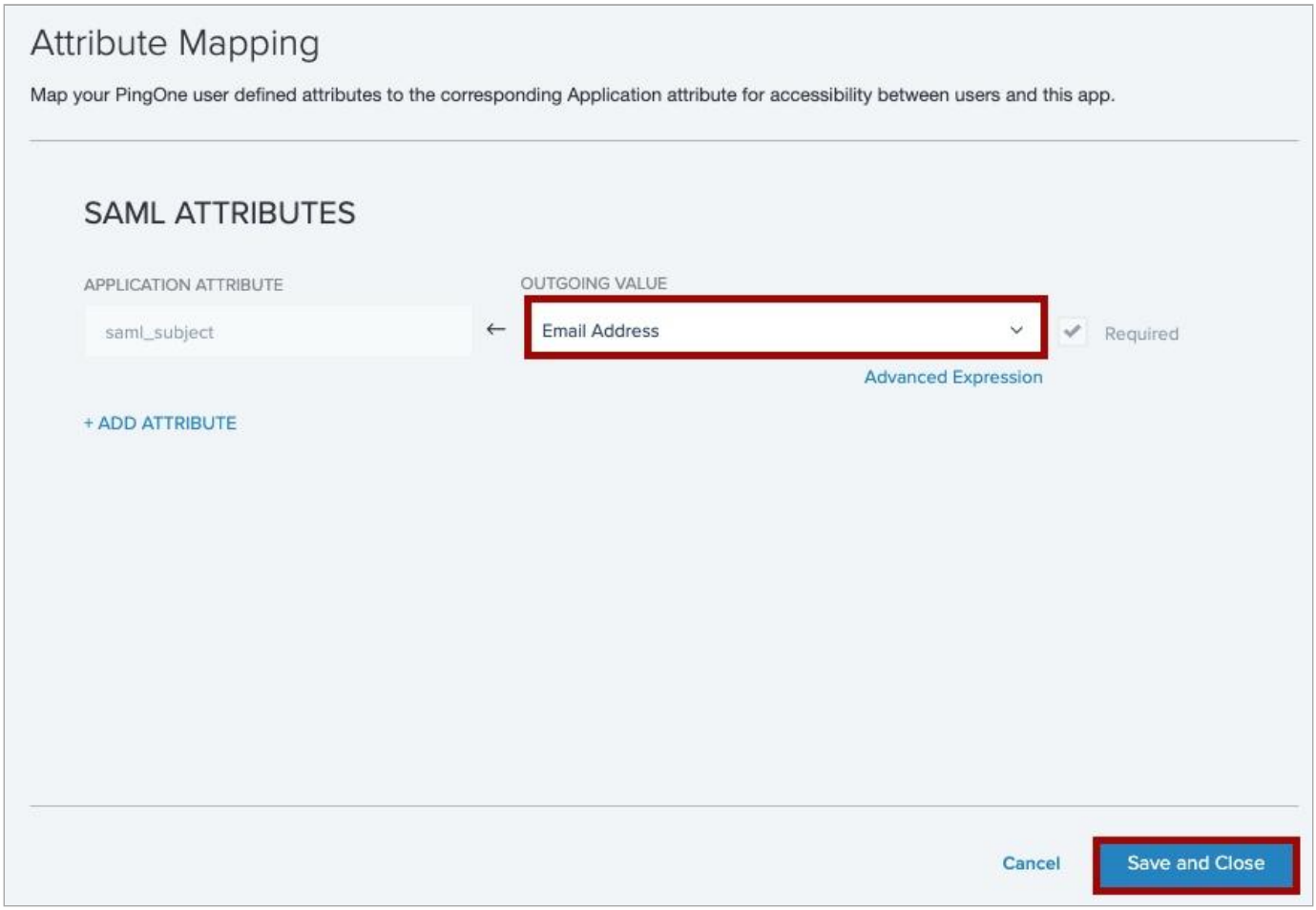
12. In the **Signing Key** section, select **Download Signing Certificate** and download in the **X509 PEM (.crt)** format. Click **Save and Continue**.



13. On the **Attribute Mapping** page, update the **Outgoing Value** to **Email Address** for the **saml_subject** application attribute.

> **Note**
>
> No other attributes are required.

14. Click **Save and Close** to finalize the creation of the application.

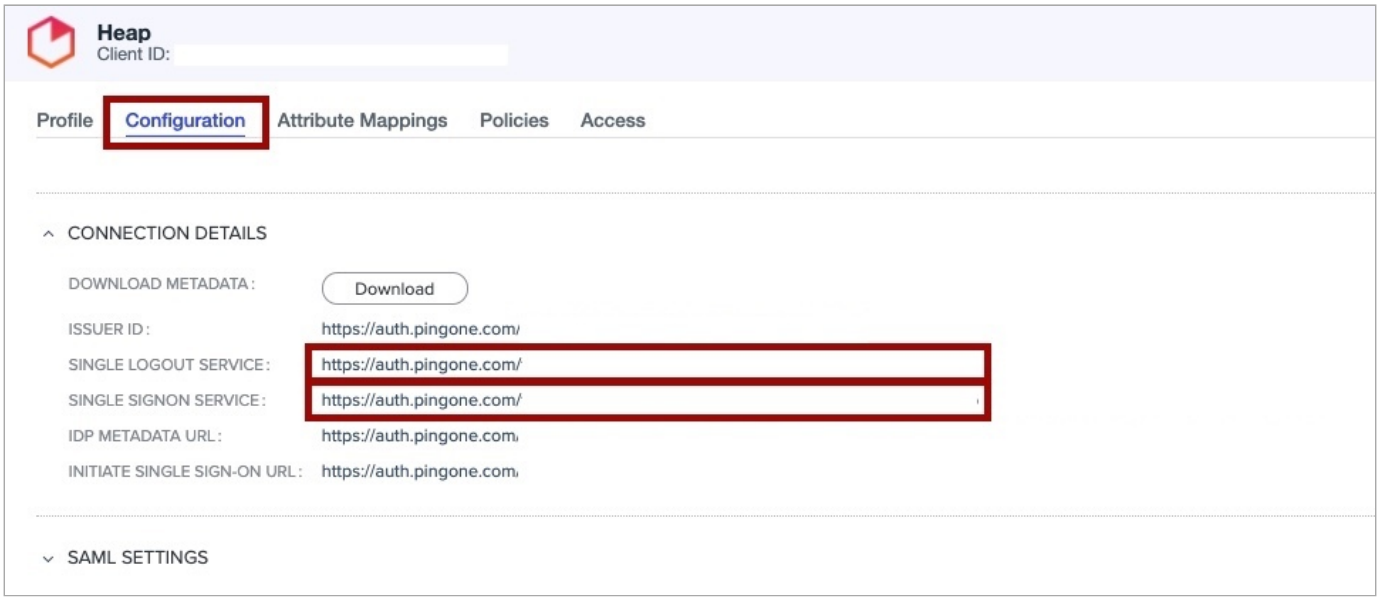


15. After you create the application, click the toggle next to the application to enable it.

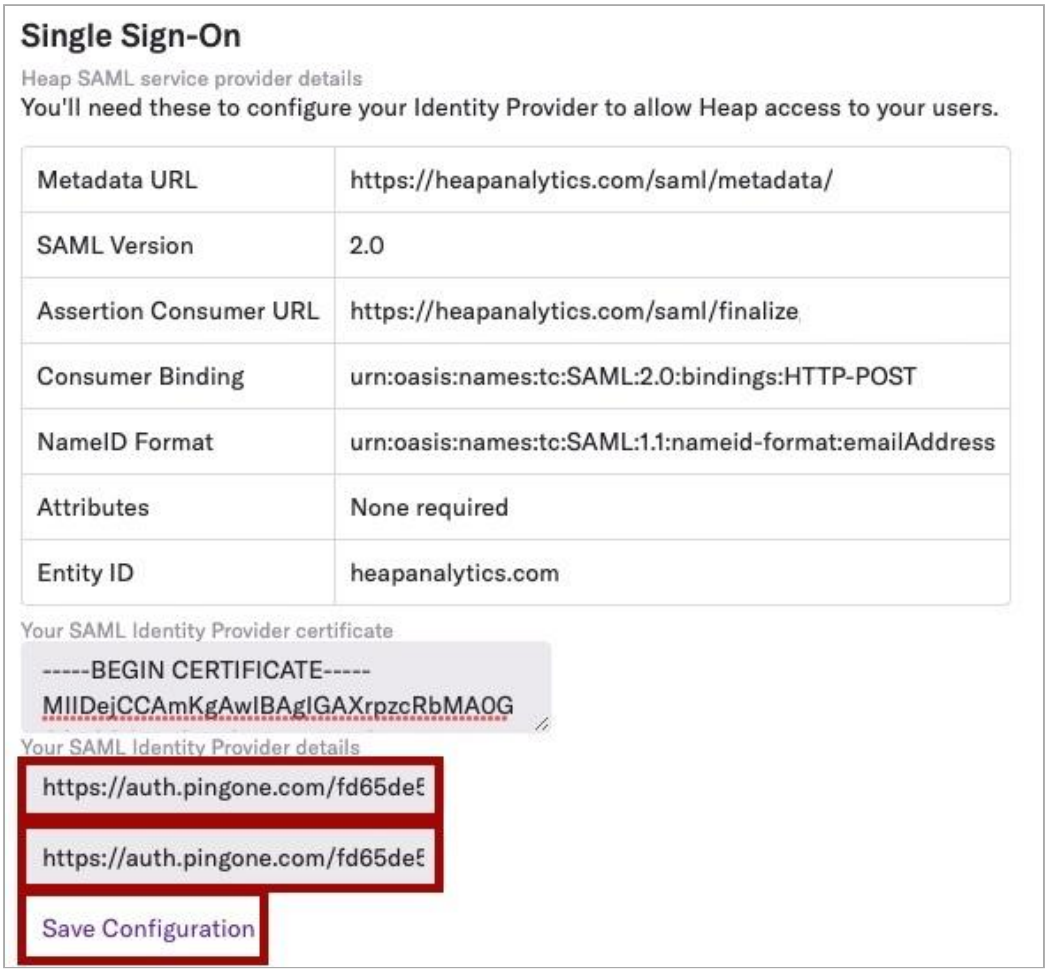
16. Select **Configuration** and copy the following values. You'll need these later.
    - **Single Logout Service**
    - **Single SignOn Service**

17. In your Heap account, go to the **Your SAML Identity Provider certificate** section and paste in the Ping X509 certificate that you downloaded previously.

> **Note**
>
> You must include the `BEGIN CERTIFICATE` and `END CERTIFICATE` text as part of the certificate upload.



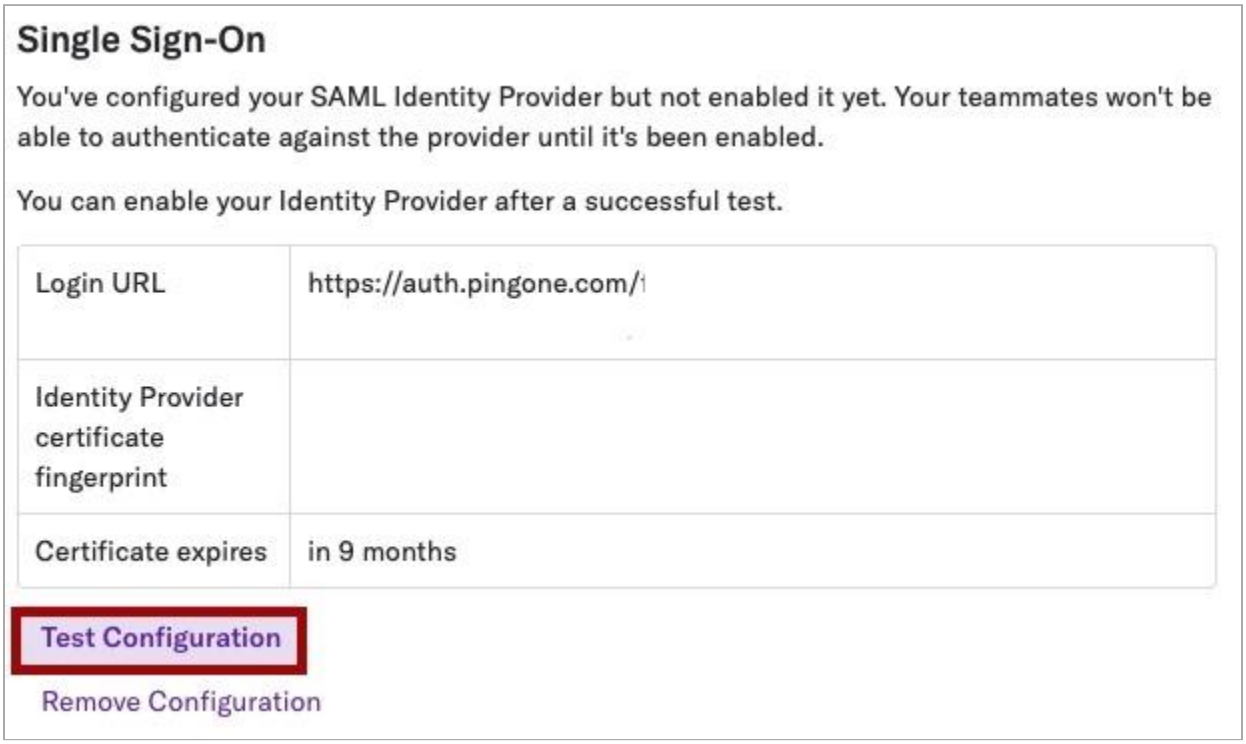
18. Paste the URLs that you copied previously into the corresponding fields:
    - **Single SignOn Service**= **Remote login URL**
    - **Single Logout Service**= **Logout landing URL** (optional)
19. Click **Save Configuration**.



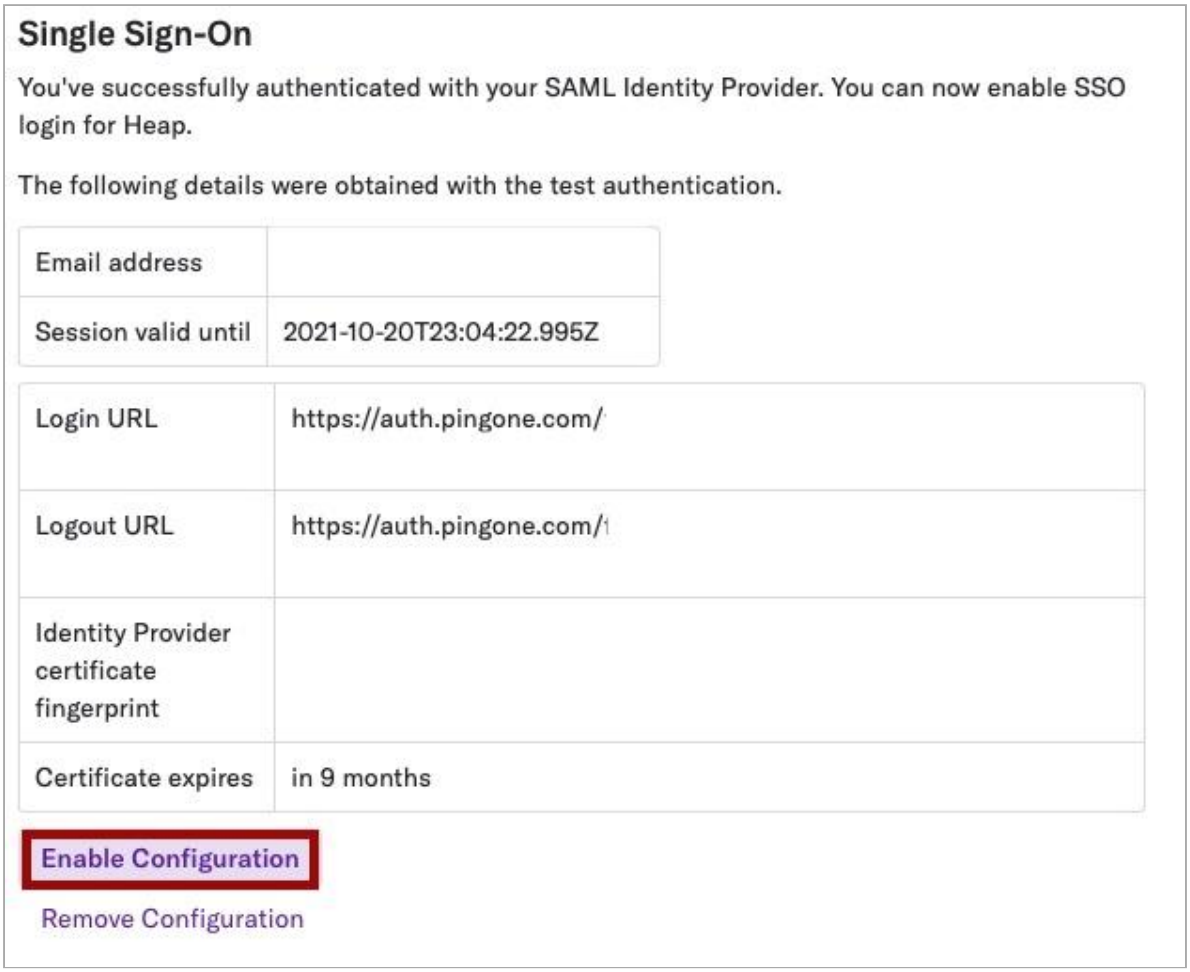
After saving the configuration, a **Test Configuration** button appears.

20. Click **Test Configuration**.

    You're signed out and then prompted to sign on with your username and password.



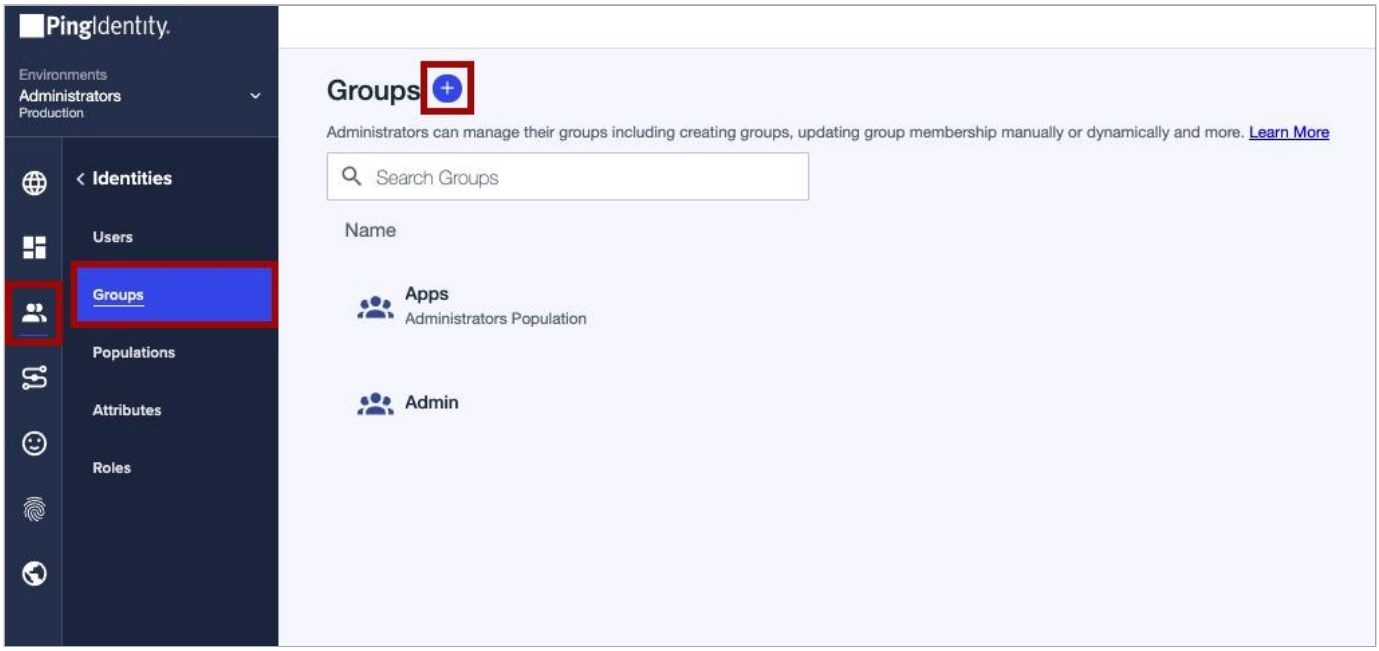
21. After signing on to your Heap account, go to the **Single Sign-On** settings section and select **Enable Configuration** to finalize the SSO connection.



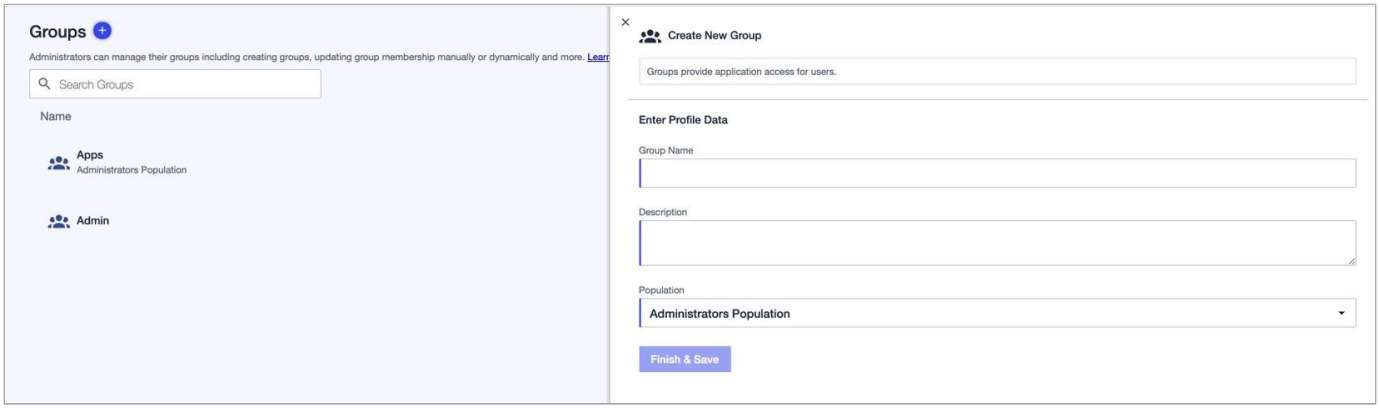
Create and assign identities

Before testing your integration, you must create and assign identities in PingOne. If you've already assigned identities and groups in PingOne, move on to Test your integration.

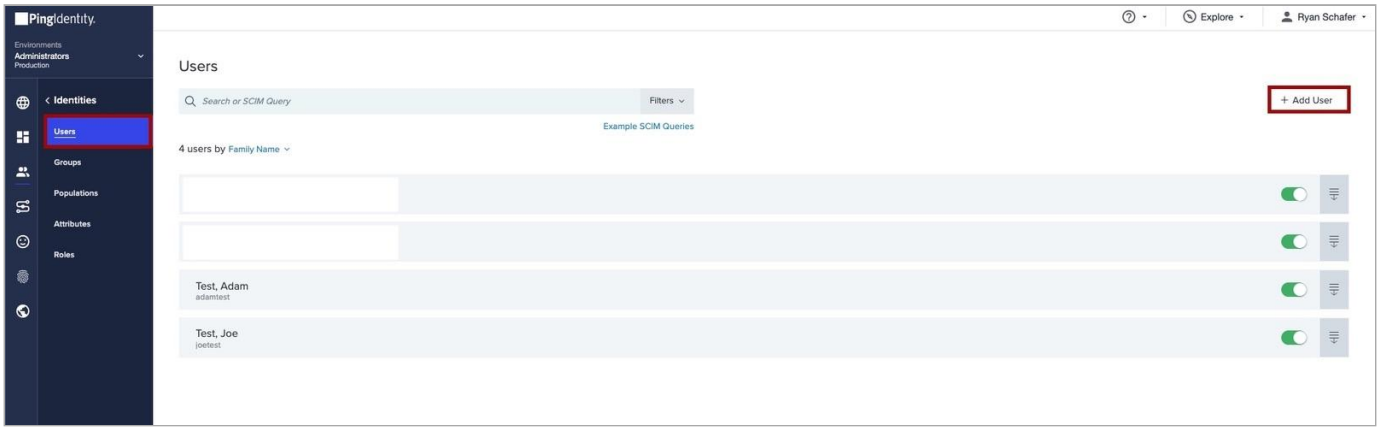
1. In PingOne, go to **Identities → Groups** and click the + icon next to **Groups.**



2. On the **Create New Group** page, enter values for the following:
    - **Group Name** (Required)
    - **Description** (Optional)
    - **Population** (Optional)
3. Click **Finish & Save**.



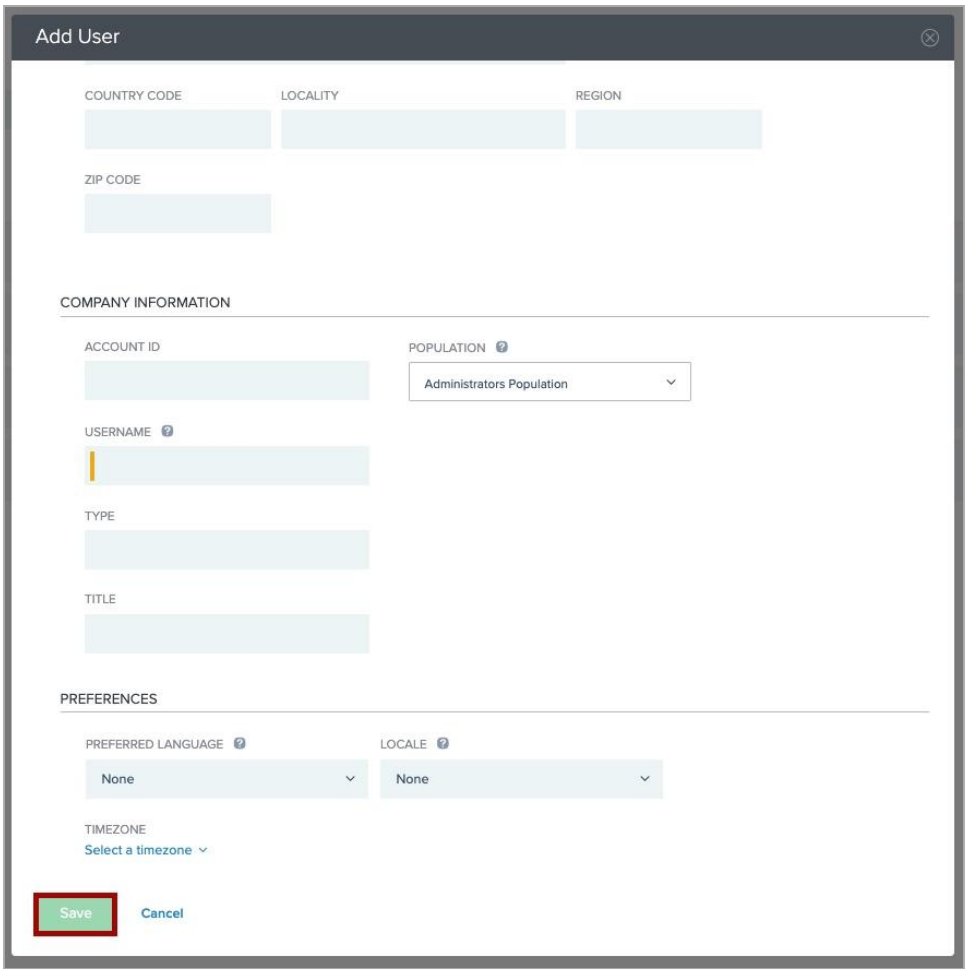
4. To add identities to the group, on the **Identities** tab, go to **Users → + Add User**.



5. On the **Add User** page, enter in all the necessary information for a user.

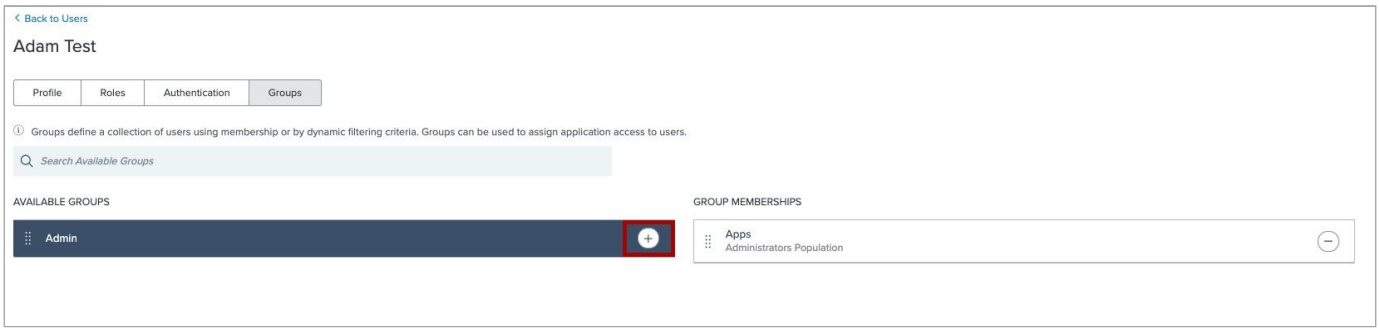
> **Important**
>
> Verify that the first name, last name, and email address are correct, as these are values passed in the SAML assertion.

6. Click **Save**.



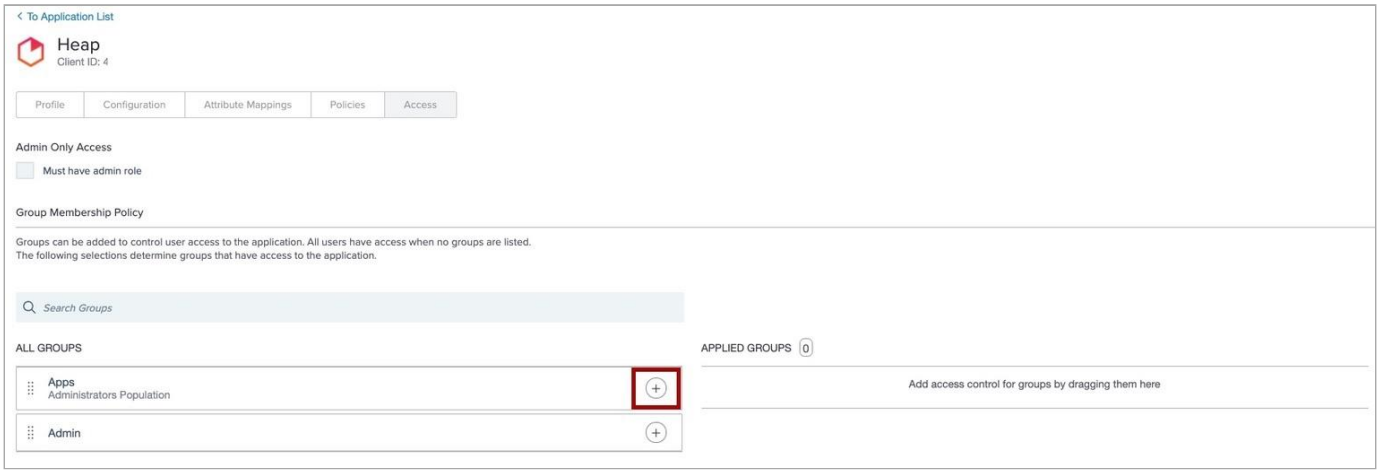
7. Assign the user that you created to the group that you created previously. Locate the user you created and do the following:
    1. Expand the section for the user.
    2. Select the **Groups** tab.
    3. Click **+ Add**.

8. In the **Available Groups** section, select the group that you created and click the **+** icon to add it to the user's group memberships. Click **Save**.



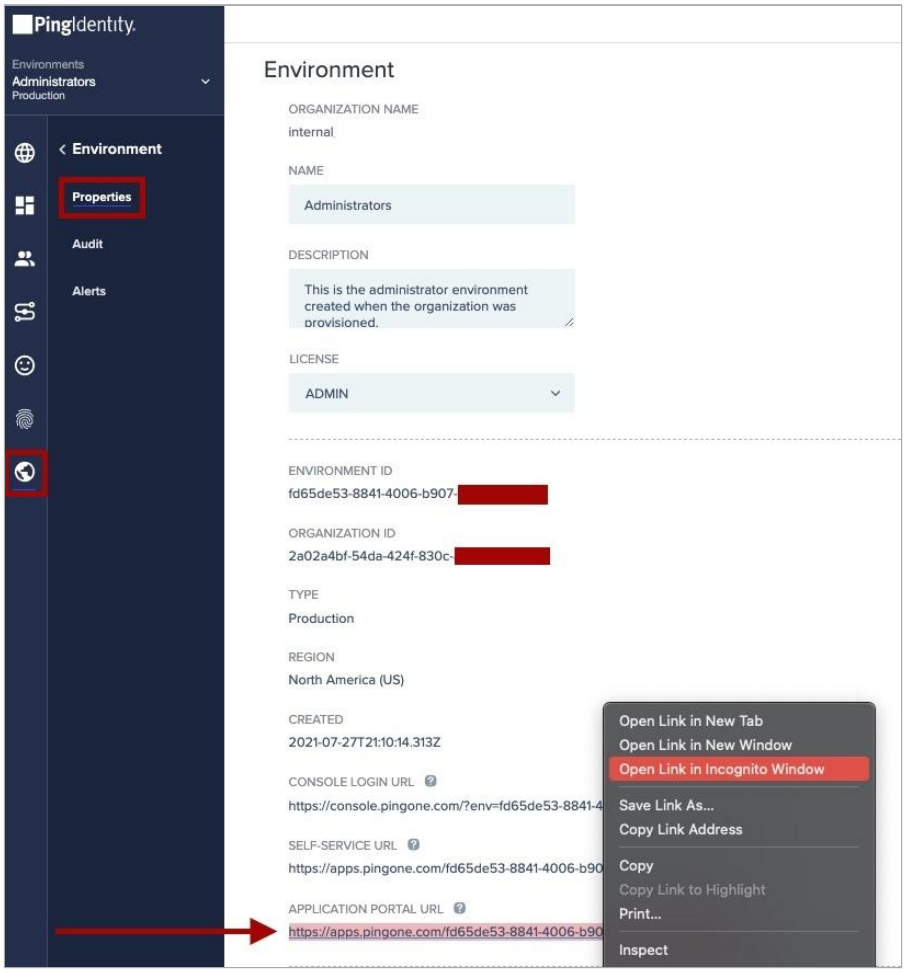
9. On the **Connections** tab, for the Heap application:
    - Click the **Access** tab
    - Click the **Pencil** icon to edit the configuration

10. Select the group that you created and add it to the **Applied Groups** section. Click **Save**.



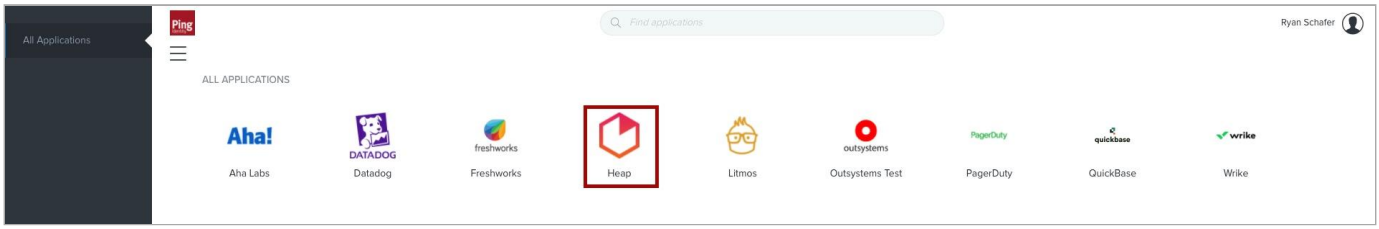
Test your integration

1. In the PingOne admin console, go to **Dashboard → Environment Properties**.
2. Right-click on the **Application Portal URL** and open it in a private browser session.



3. Sign on as the test user that you created and click the Heap tile.

   You're signed on to the user's Heap account using SSO and testing is complete.



HubSpot

Configuring SAML SSO with HubSpot and PingFederate

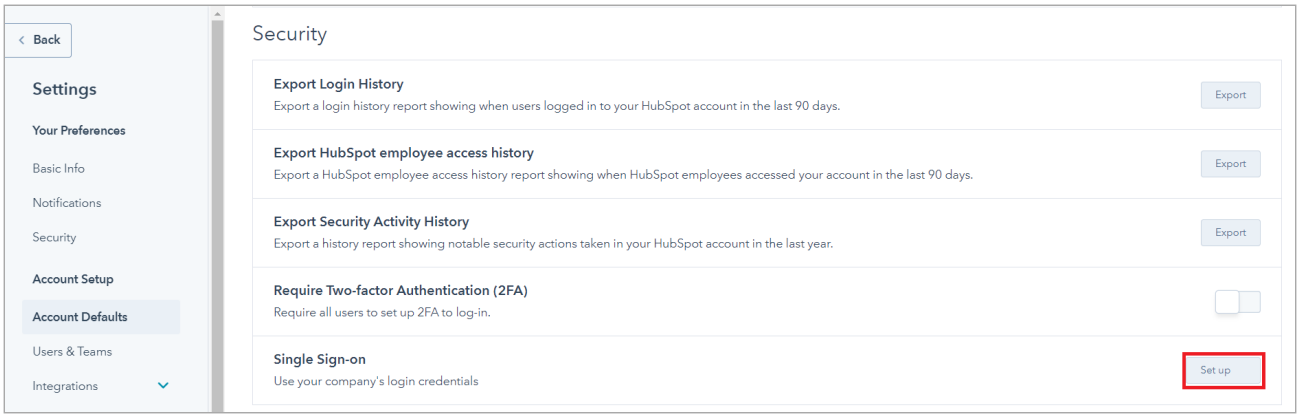
Learn how to enable HubSpot sign-on from a PingFederate URL (IdP-initiated sign-on) and direct HubSpot sign-on using PingFederate (SP-initiated sign-on).

Before you begin

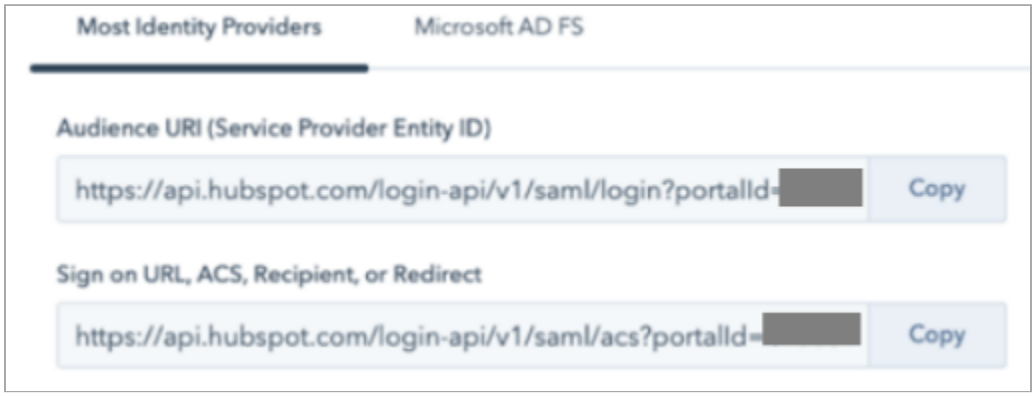
- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate HubSpot with at least one user to test access.
- You must have administrative access to PingFederate and HubSpot.

Create a PingFederate SP connection for HubSpot

1. Obtain the HubSpot SSO details.
    1. Sign on to HubSpot, click the **Gear** icon (⚙), and select **Account Details** from the **Settings** menu.
    2. In the **Single Sign-on** section, click **Set up**.



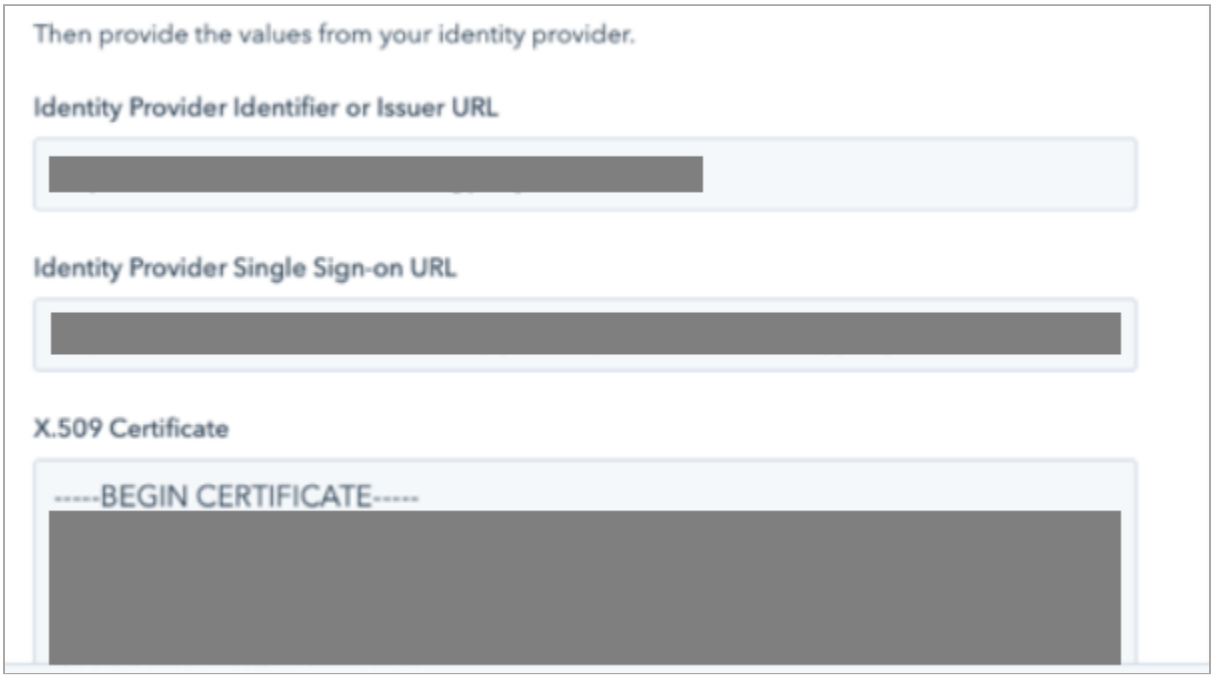
    3. Copy the **Audience URI** and **Sign on URL, ACS, Recipient, or Redirect** values.



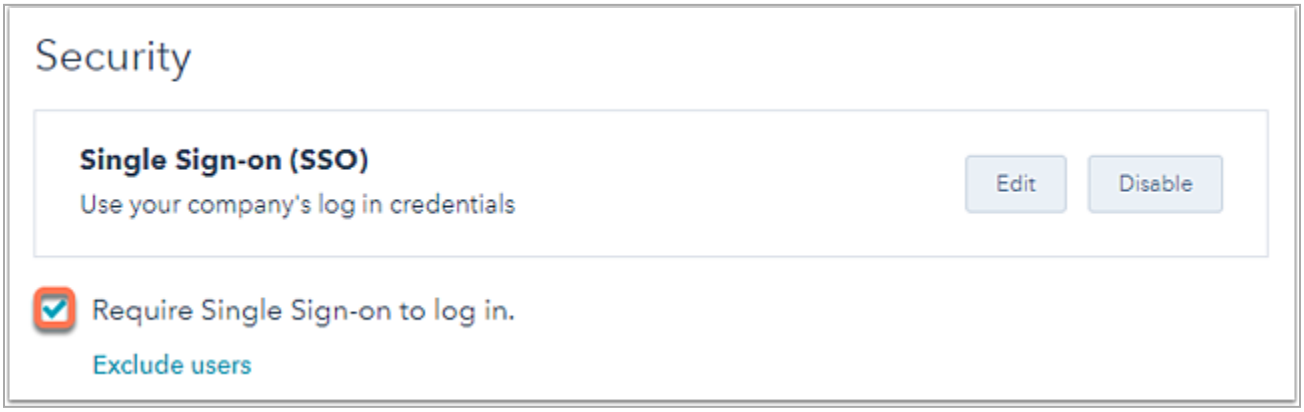
2. Sign on to the PingFederate administrative console.
3. Create an SP connection for HubSpot in PingFederate.
    1. Configure using Browser SSO profile SAML 2.0.
    2. Set **Partner's Entity ID** to the HubSpot **Audience URI** value.
    3. Enable **IdP-Initiated SSO** and **SP Initiated SSO.**
    4. In **Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment**, map the SAML_SUBJECT to the email attribute.
    5. In **Protocol Settings: Assertion Consumer Service URL**, set **Binding** to **POST** and set **Endpoint URL** to the HubSpot **Sign on URL, ACS, Recipient, or Redirect** value.
    6. In **Protocol Settings: Allowable SAML Bindings**, enable **POST**.
    7. In **Credentials: Digital Signature Settings**, select the PingFederate signing certificate.
4. Export the metadata for the newly-created HubSpot SP connection.
5. Export the signing certificate.
6. Open the metadata file and copy the values of the entityID and the Location entry (`https://your-value/idp/SSO.saml2`).

Add the PingFederate connection to HubSpot

1. Sign on to HubSpot, click the **Gear** icon (⚙), select **Account Details**, and access the **Single Sign-on** settings.
2. Paste the entityID value that you copied previously to the **Identity Provider Identifier or Issuer URL** field.
3. Paste the Location value you copied previously to the **Identity Provider Single Sign-on URL** field.
4. Paste the PingFederate certificate into the **X.509 Certificate** field.



5. Click **Verify**.
6. In the left sidebar menu, click **Account Defaults**.
7. In the **Single Sign-on (SSO)** section, select the **Require Single Sign-on to log in** check box.

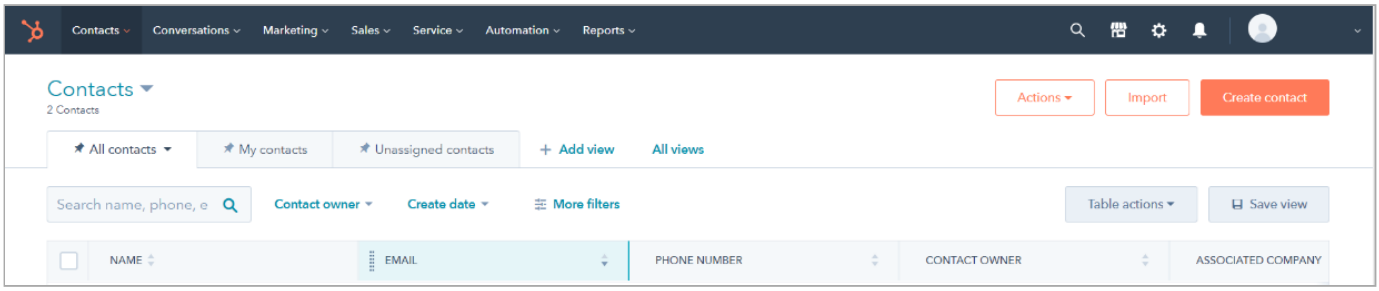


> **Note**
>
> The user setting this up is automatically excluded to ensure their access is not lost in case of setup issues.

Test the PingFederate IdP-initiated SSO integration

1. Go to the PingFederate SSO Application Endpoint for the HubSpot SP connection.
2. Complete PingFederate authentication.

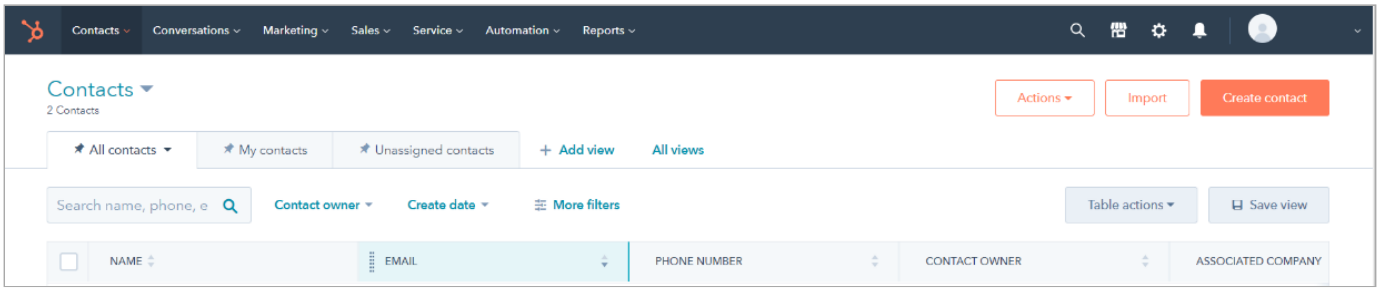
   You're redirected to your HubSpot domain.



Test the PingFederate SP-initiated SSO integration

1. Go to https://app.hubspot.com/login/sso.
2. When you are redirected to PingFederate, enter your PingFederate username and password.

   After successful authentication, you're redirected back to HubSpot.



Configuring SAML SSO with HubSpot and PingOne for Enterprise

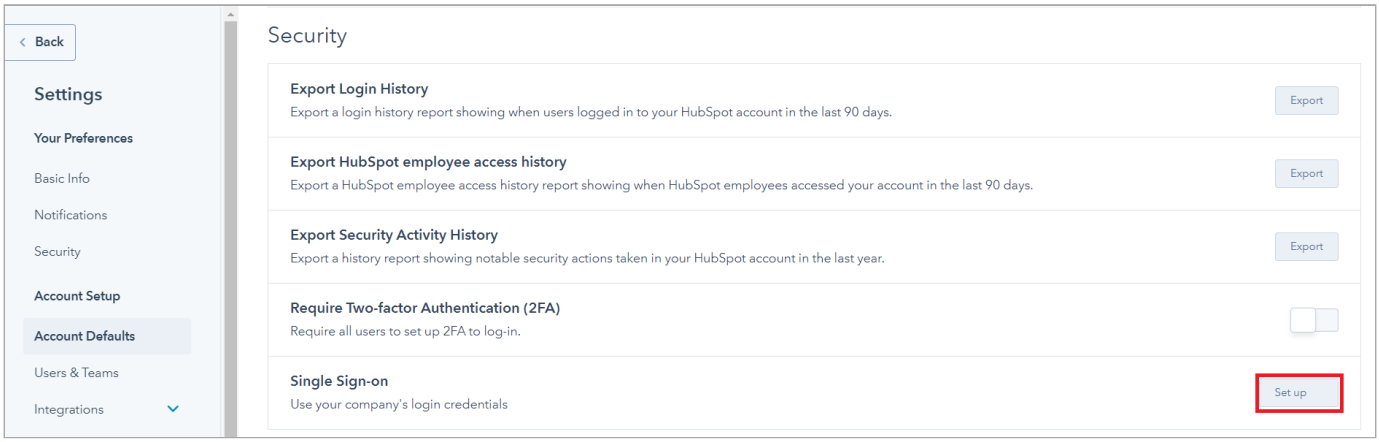
Learn how to enable HubSpot sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct HubSpot sign-on using PingOne for Enterprise (SP-initiated sign-on).

Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate HubSpot with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and HubSpot.

Obtain the HubSpot SSO details

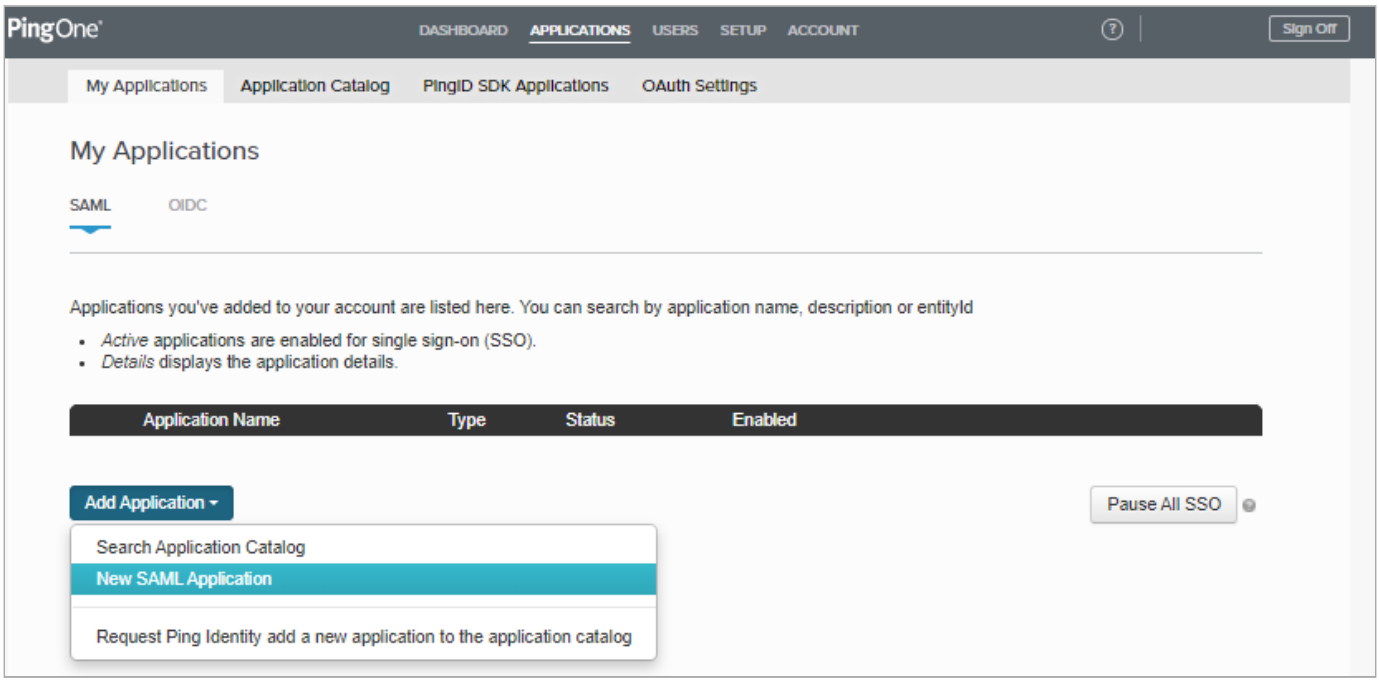
1. Sign on to HubSpot, click the **Gear** icon (⚙), and select **Account Details** in the **Settings** menu.
2. In the **Single Sign-on** section, click **Set up**.



3. Copy the **Audience URI** and **Sign on URL, ACS, Recipient, or Redirect** values.

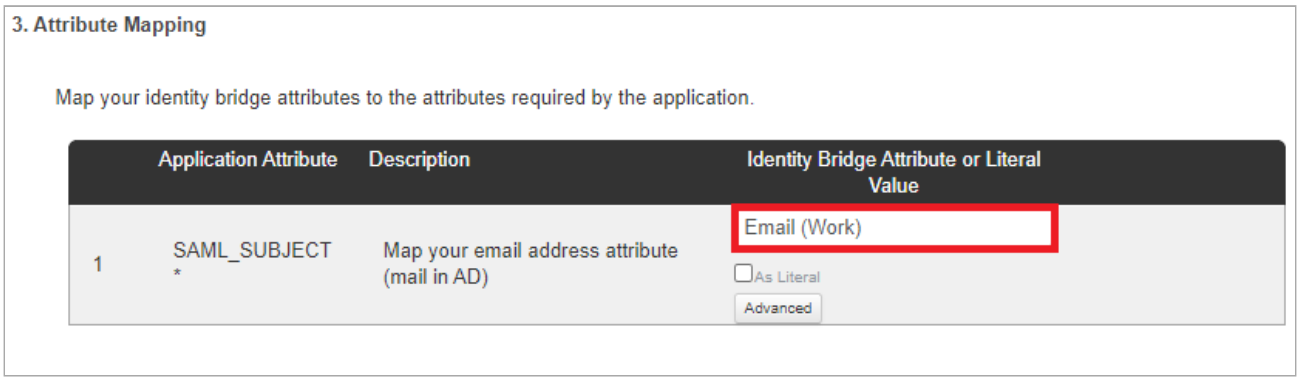
Add the HubSpot application to PingOne for Enterprise

1. Sign on to PingOne for Enterprise and go to **Applications → My Applications**.
2. On the **SAML** tab, click **Add Application**.

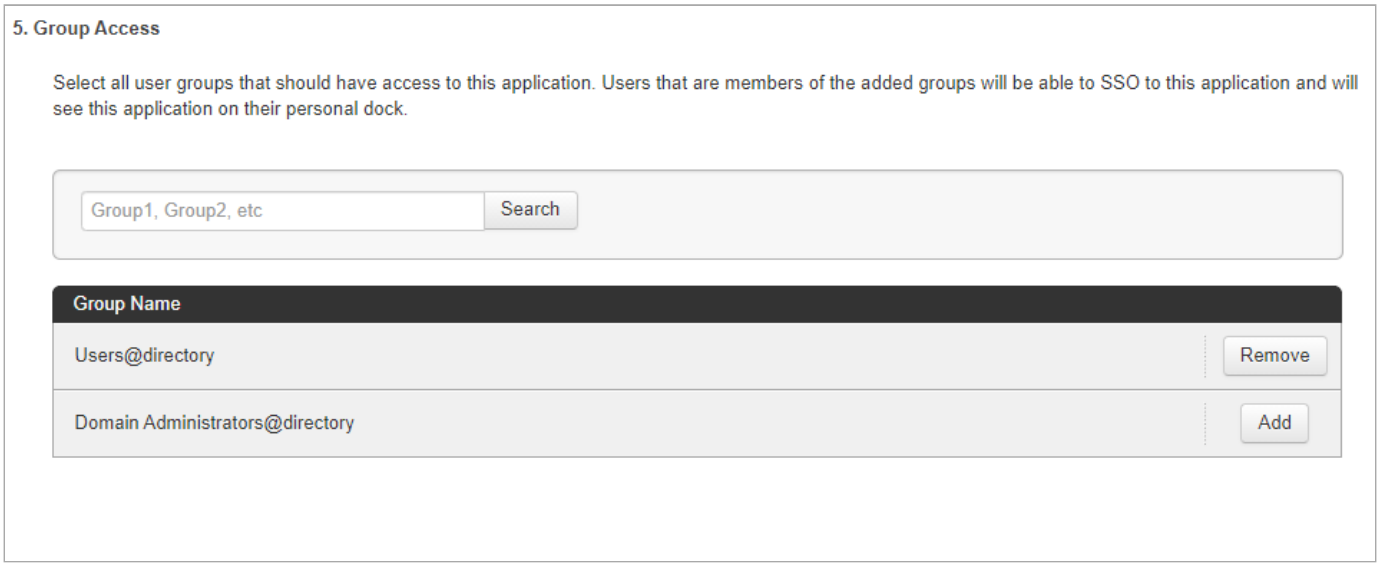


3. For the application name, enter `HubSpot`.
4. Enter a suitable description.
5. For the category, select **CRM**.
6. Click **Continue to Next Step**.
7. Set **Assertion Consumer Service (ACS)** to the HubSpot **Sign on URL, ACS, Recipient, or Redirect** value and **Entity ID** to the **HubSpot Audience URI** value.

8. Click **Continue to Next Step**.
9. HubSpot needs the email passed in.
    - If you use an email address to sign on using PingOne for Enterprise, click **Continue to Next Step**.
    - If you sign on with a username, enter your email attribute in the **SAML_SUBJECT** mapping, then click **Continue to Next Step**.



10. Click **Add** for all user groups that should have access to HubSpot.



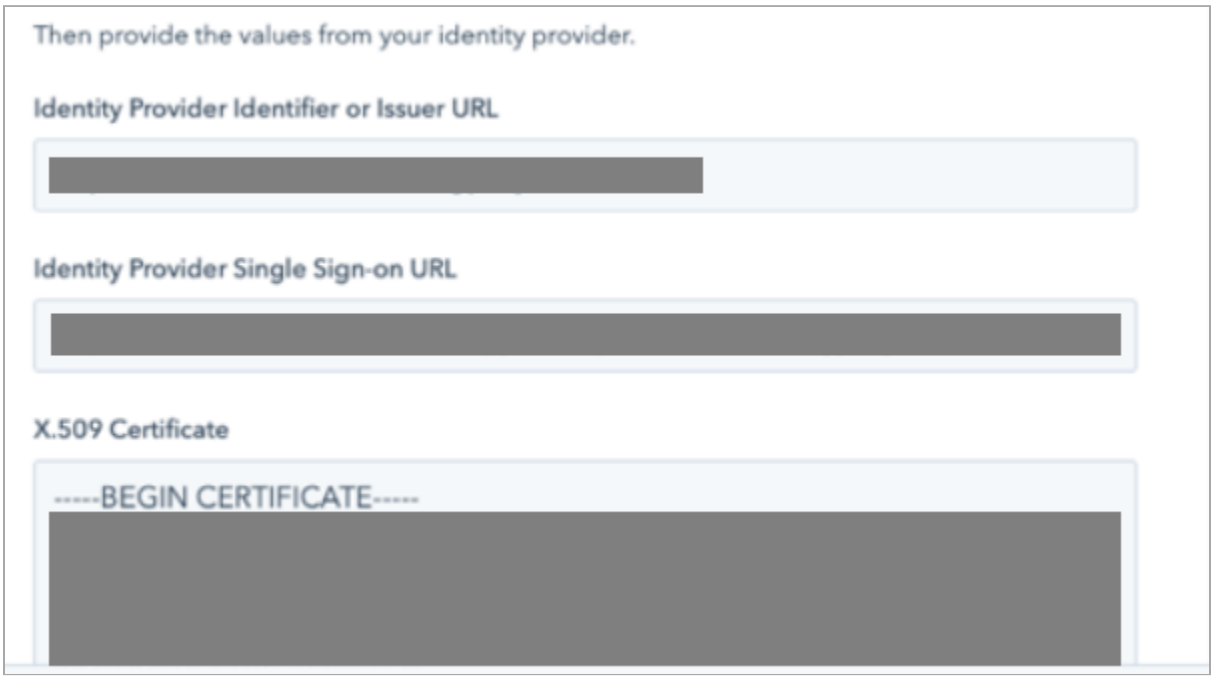
11. Click **Continue to Next Step**.
12. Copy and save the **Issuer** and **Initiate Single Sign-On (SSO) URL** values.

13. Download the PingOne for Enterprise signing certificate.

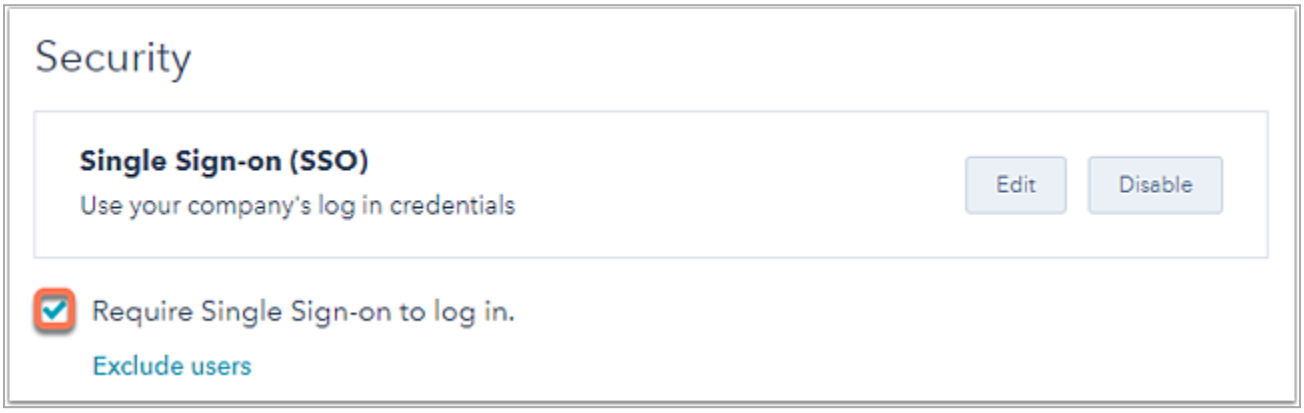
14. Click **Finish**.

Add the PingOne for Enterprise connection to HubSpot

1. Sign on to HubSpot, click the **Gear** icon (⚙), select **Account Details** from the **Settings** menu, and open the **Single Sign-on** settings.
2. In the **Identity Provider Identifier or Issuer URL** field, enter the PingOne for Enterprise **Issuer** value.
3. In the **Identity Provider Single Sign-on URL** field, enter the PingOne for Enterprise **Initiate Single Sign-On (SSO) URL** value.
4. Paste the PingOne for Enterprise signing certificate into the **X.509 Certificate** field.



5. Click **Verify**.
6. In the sidebar menu, click **Account Defaults**.
7. In the **Single Sign-on (SSO)** section, select the **Require Single Sign-on to log in** check box.



> **Note**
>
> The user setting this up is automatically excluded to ensure that their access is not lost in case of setup issues.

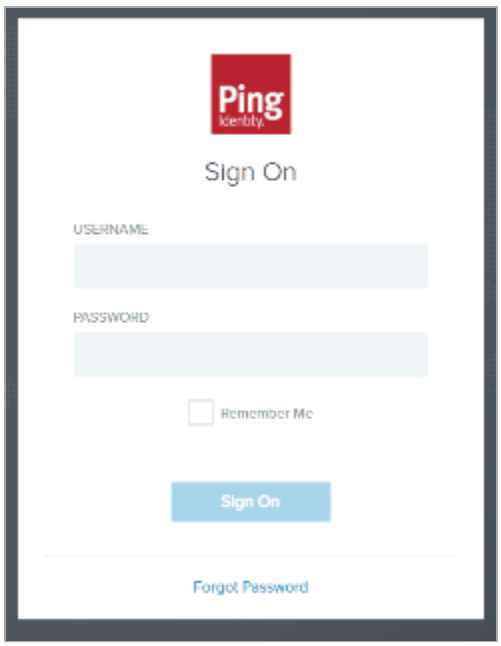
Test the PingOne for Enterprise IdP-initiated SSO integration

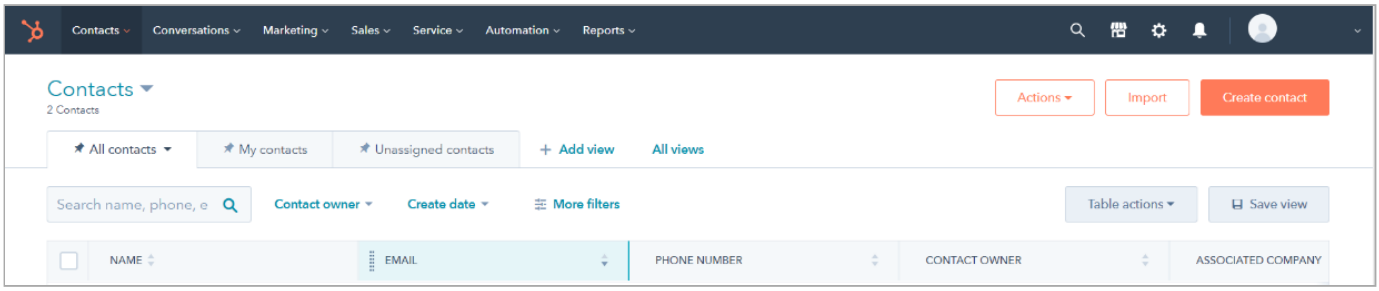
1. Go to your PingOne for Enterprise desktop as a user with HubSpot access.

   > **Note**
   >
   > To find the PingOne for Enterprise desktop URL in the Admin console, go to **Setup → Dock → PingOne Dock URL**.

2. Complete PingOne for Enterprise authentication.

   You're redirected to your HubSpot domain.



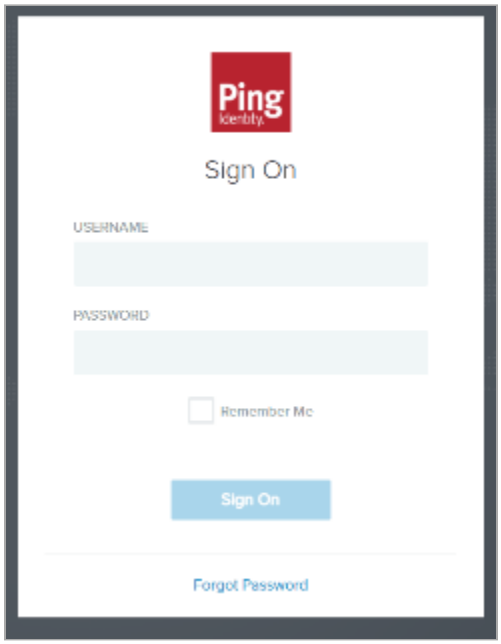


Test the PingOne for Enterprise SP-initiated SSO integration

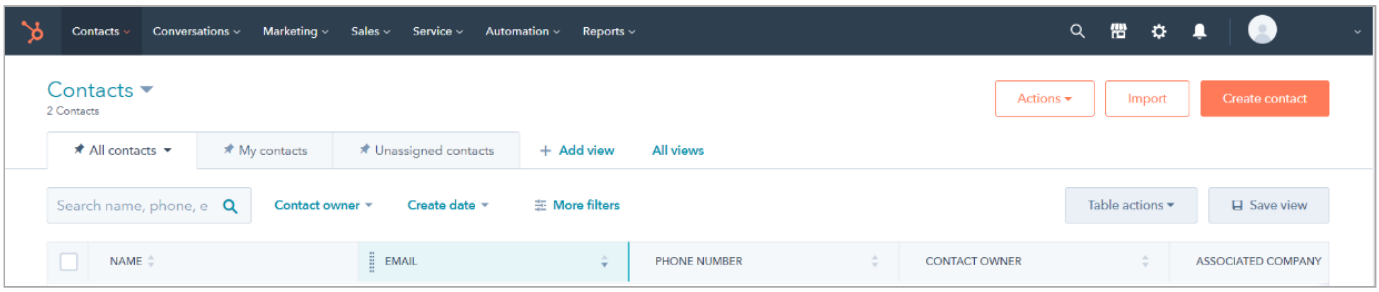
1. Go to https://app.hubspot.com/login/sso.

   You're redirected to PingOne for Enterprise.

2. Enter your PingOne for Enterprise username and password.



After successful authentication, you're redirected back to HubSpot.



Jamf

Configuring SAML SSO with Jamf Pro and PingFederate

Enable Jamf Pro sign-on from the PingFederate console (IdP-initiated sign-on) and direct Jamf Pro sign-on using PingFederate (SP-initiated sign-on).

Before you begin

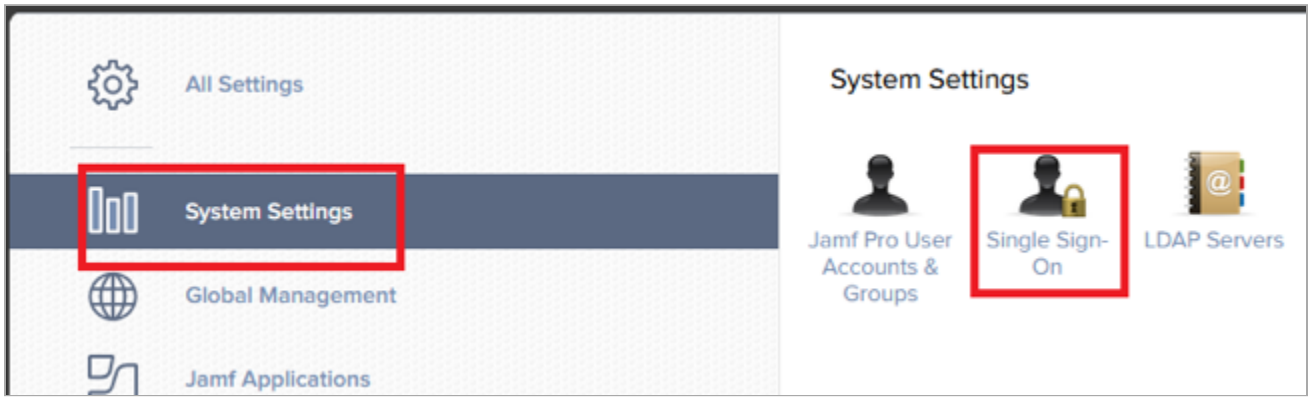
- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate Jamf Pro with at least one user to test access.
- You must have administrative access to PingFederate.

Create a PingFederate SP connection for Jamf Pro

1. Sign on to the PingFederate administrative console.
2. Create an SP connection for Jamf Pro in PingFederate:
    - Configure using **Browser SSO** profile **SAML 2.0**.
    - Set **Partner's Entity ID** to `https://your-instance.jamfcloud.com/saml/metadata`.
    - Enable the **IdP-Initiated SSO** and **SP Initiated SSO** SAML profiles.
        - In **Assertion Creation → Authentication Source Mapping → Attribute Contract Fulfillment**, map the **SAML_SUBJECT** to your `email` attribute.
        - In **Protocol Settings → Assertion Consumer Service URL**, set **Binding** to **POST** and set **Endpoint URL** to `https://your-instance.jamfcloud.com/saml/SSO`.
        - In **Protocol Settings → Allowable SAML Bindings**, enable **POST**.
        - In **Credentials → Digital Signature Settings**, select the **PingFederate Signing Certificate**.
3. Export the metadata for the newly-created Jamf Pro SP connection.
4. Export the signing certificate.

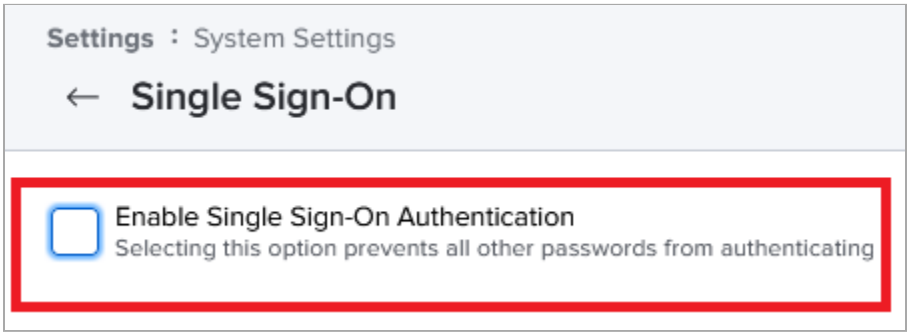
Add the PingFederate connection to Jamf Pro

1. Sign on to the Jamf Pro console as an administrator.
2. Click the **Gear** icon (⚙]).
3. Go to **System Settings → Single Sign-On**.



4. Click the **Edit** icon.

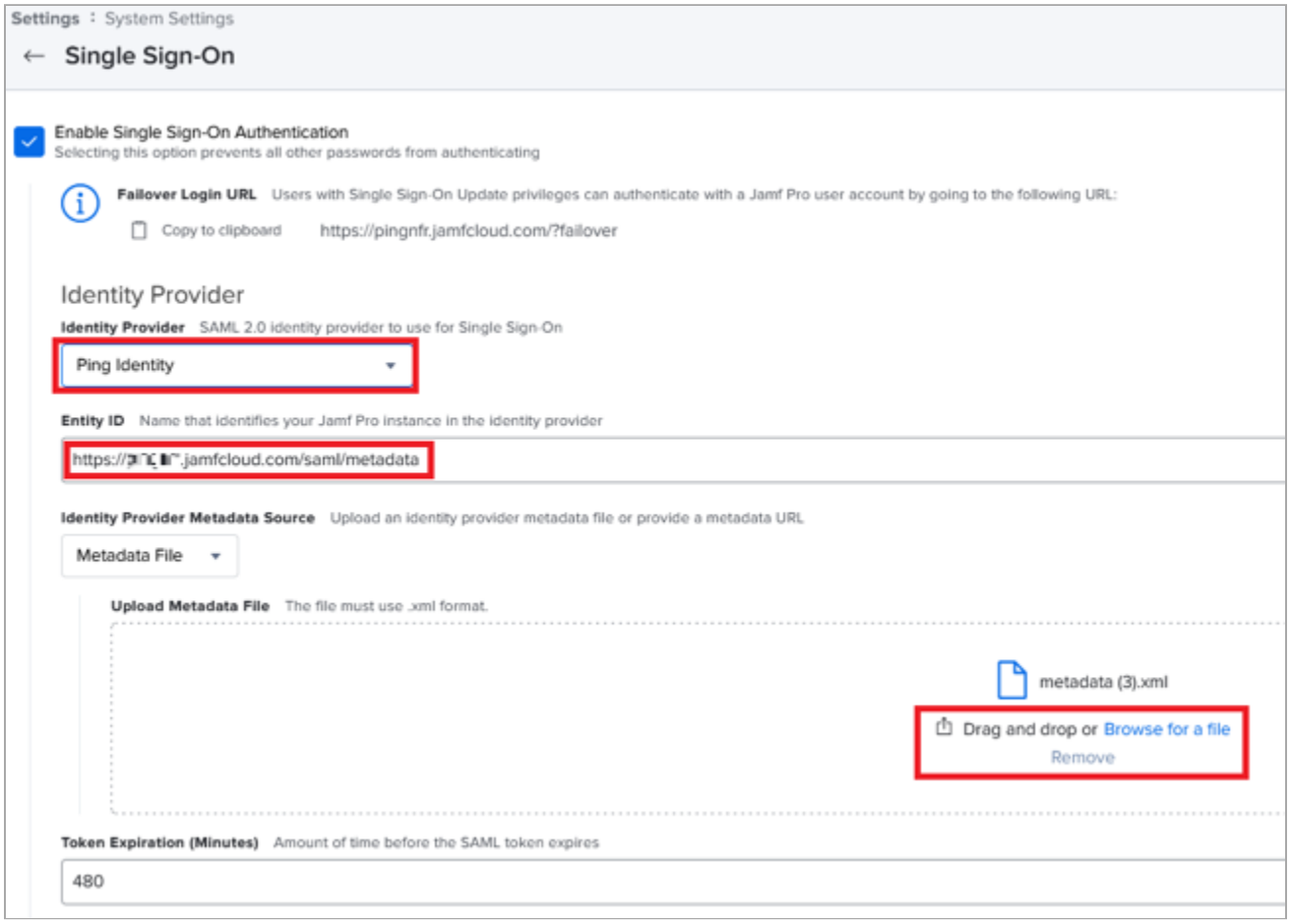
5. Select the **Enable Single Sign-On Authentication** check box.



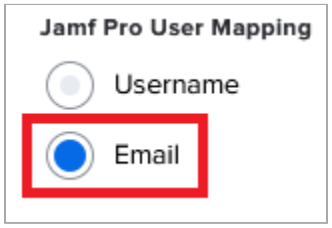
6. In the **Identity Provider** list, select **Ping Identity**.

7. Confirm that the **Entity ID** value matches the value you set previously in PingFederate.

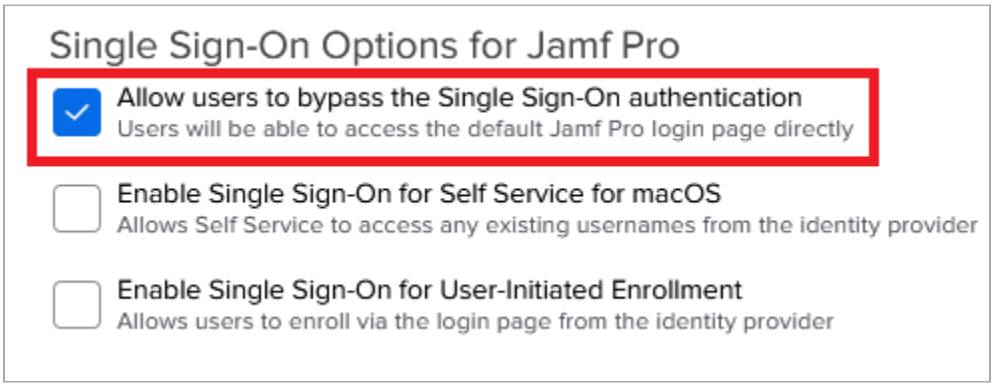
8. In the **Upload Metadata File** field, upload the PingFederate metadata file.



9. In the **Jamf Pro User Mapping** section, click **Email**.



10. In the **Single Sign-On Options for Jamf Pro** section, select the **Allow users to bypass the Single Sign-On authentication** check box.



11. Click **Save**.

Test the PingFederate IdP-initiated SSO integration

1. Go to the PingFederate SSO application endpoint for the Jamf Pro SP connection.
2. Complete the PingFederate authentication.

   You're redirected to your Jamf Pro domain.

Test the PingFederate SP-initiated SSO integration

1. Go to your Jamf Pro application.
2. After you are redirected to PingFederate, enter your PingFederate username and password.

   After successful authentication, you're redirected back to Jamf Pro.

Configuring SAML SSO with Jamf Pro and PingOne for Enterprise

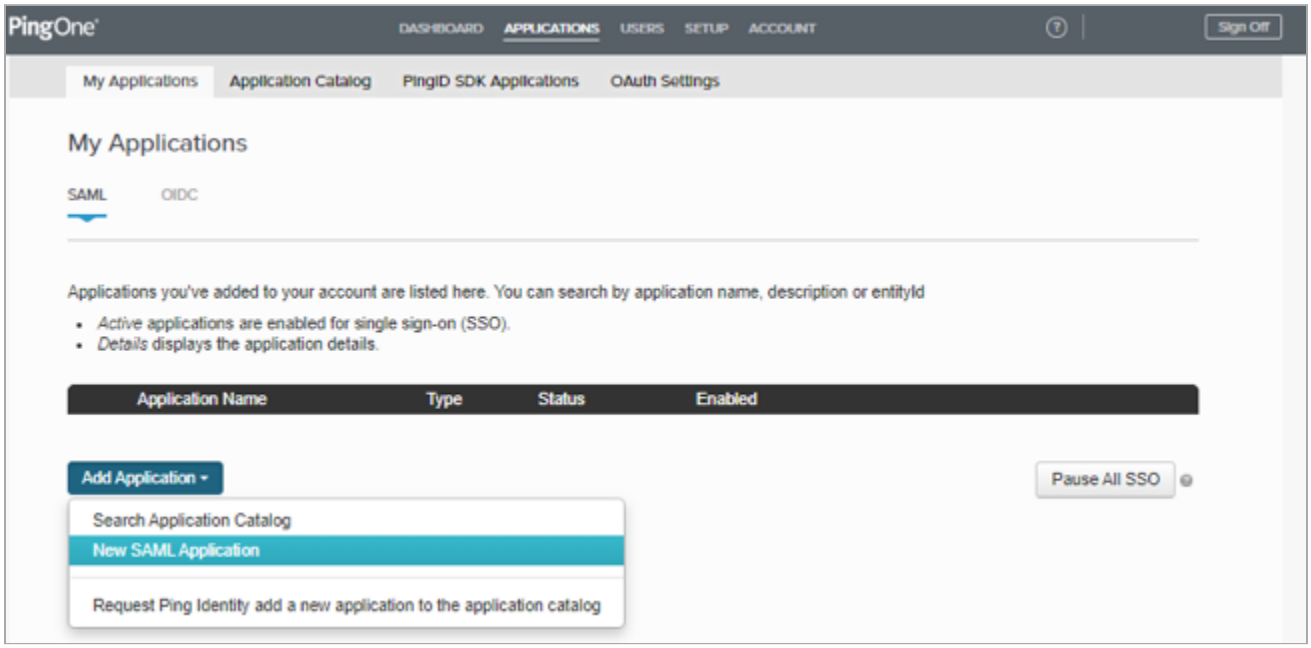
Enable Jamf Pro sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct JAMF Pro sign-on using PingOne for Enterprise (SP-initiated sign-on) with single logout (SLO).

Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate Jamf Pro with at least one user to test access.
- You must have administrative access to PingOne for Enterprise.

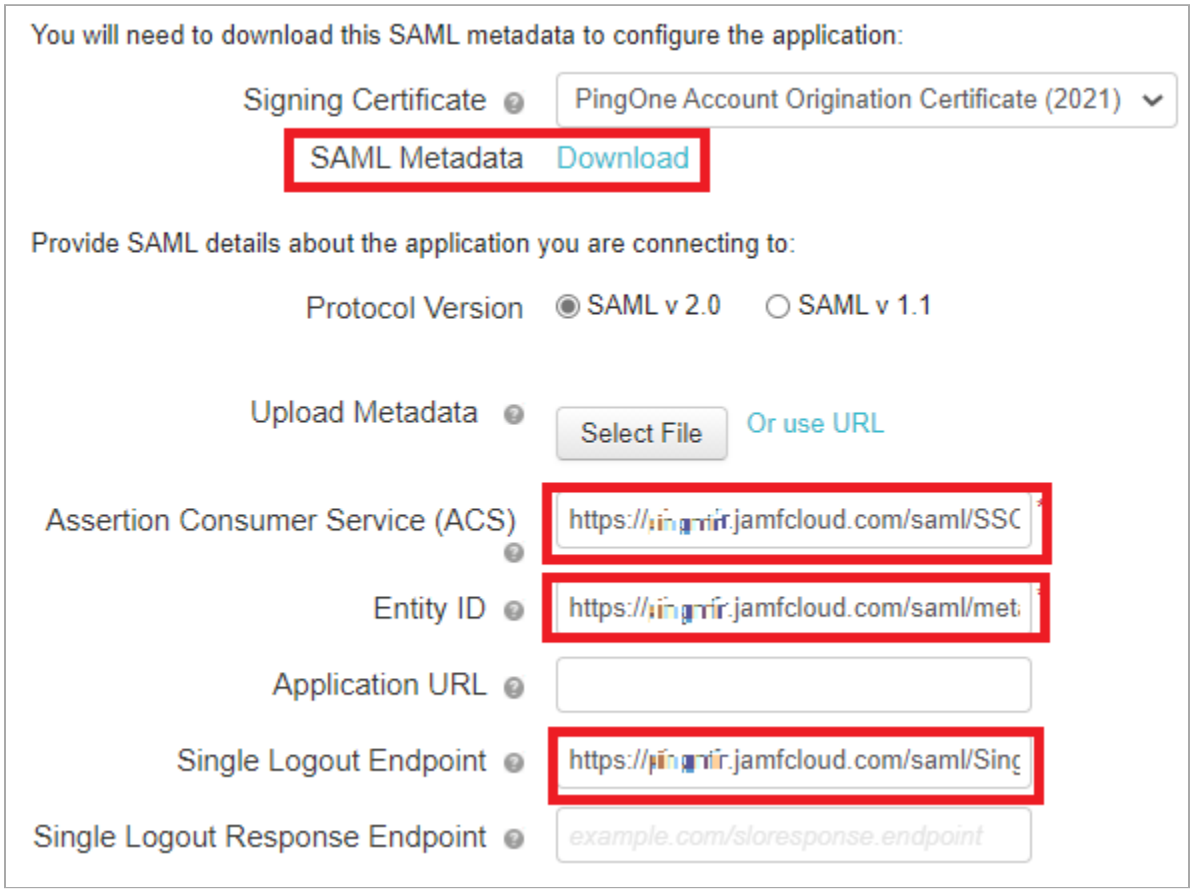
Add the Jamf Pro application to PingOne for Enterprise

1. Sign on to PingOne for Enterprise and go to **Applications → My Applications**.
2. On the **SAML** tab, click **Add Application**.

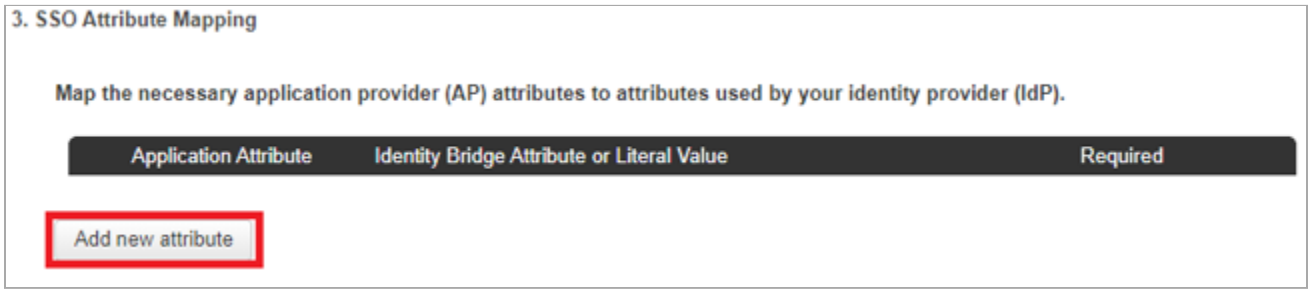


3. Enter `Jamf Pro` as the application name.
4. Enter a suitable description.
5. Choose a suitable category.
6. Click **Continue to Next Step**.
7. Enter the following values:

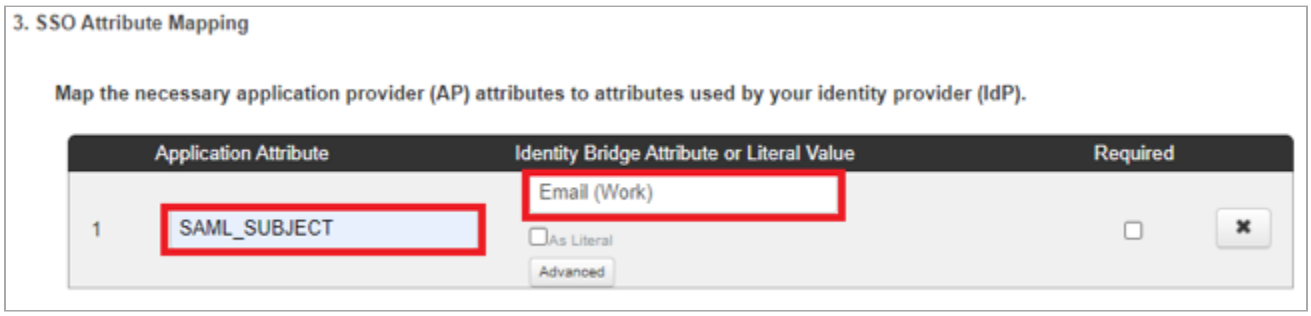
Field	Value
Assertion Consumer Service (ACS)	`https://your-instance.jamfcloud.com/saml/SSO`
Entity ID	`https://your-instance.jamfcloud.com/saml/metadata`
Single Logout (SLO) Endpoint	`https://your-instance.jamfcloud.com/saml/SingleLogout`
Single Logout Binding Type	`POST`



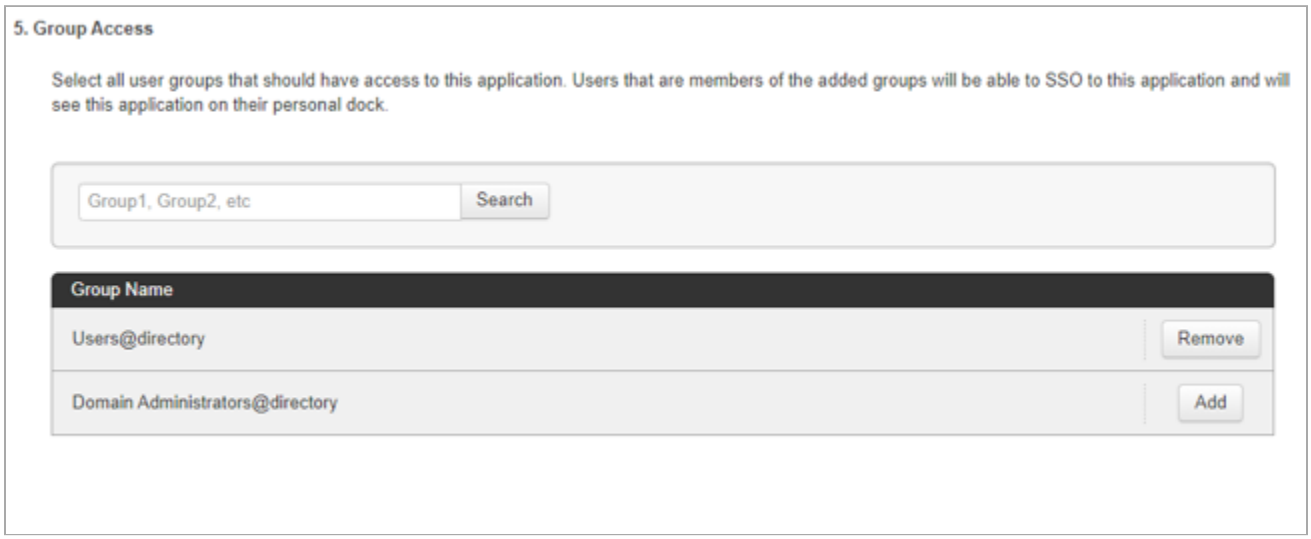
8. On the **SAML Metadata** line, click **Download**.
9. Click **Continue to Next Step**.
10. Click **Add new attribute**.



11. Add the **SAML_SUBJECT** attribute and map it to your email attribute.



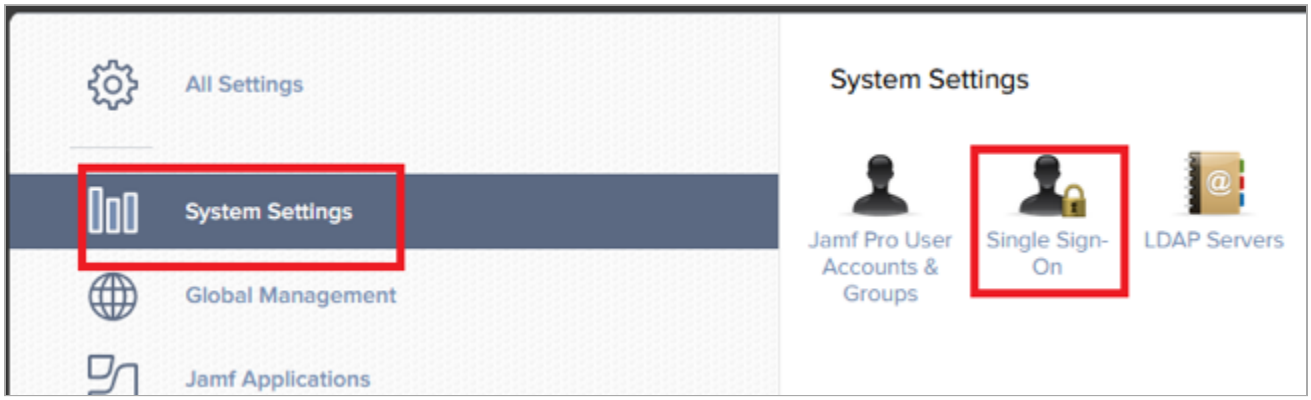
12. Click **Continue to Next Step**.
13. Click **Add** for each user groups that should have access to JAMF Pro.



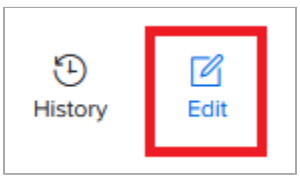
14. Click **Continue to Next Step**.
15. Click **Finish**.

Add the PingOne for Enterprise connection to JAMF Pro

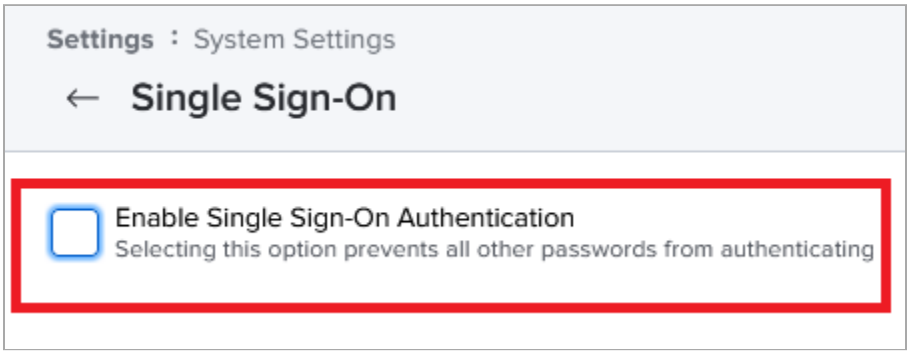
1. Sign on to the Jamf Pro console as an administrator.
2. Click the **Gear** icon (⚙]).
3. Go to **System Settings → Single Sign-On**.



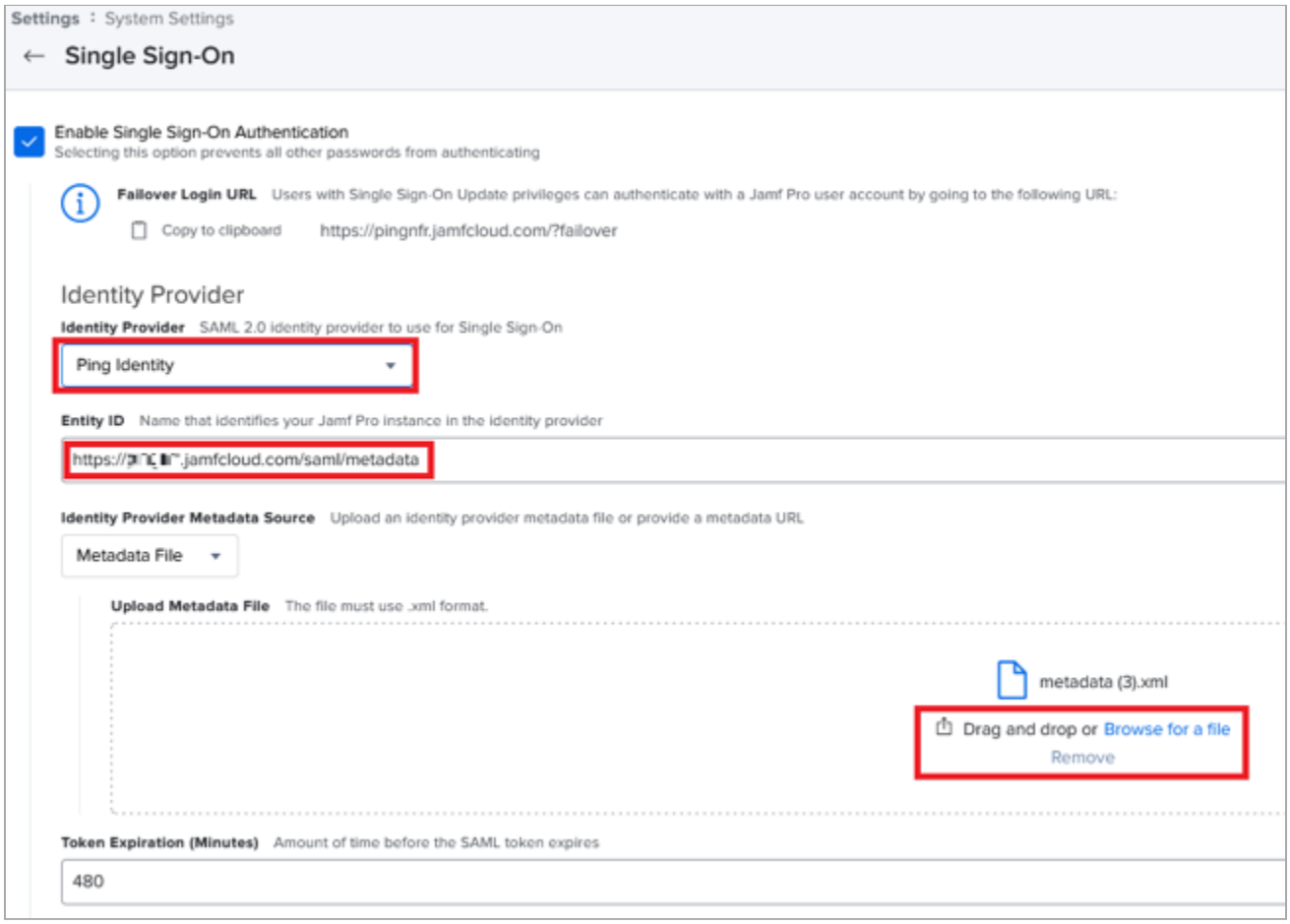
4. Click the **Edit** icon.



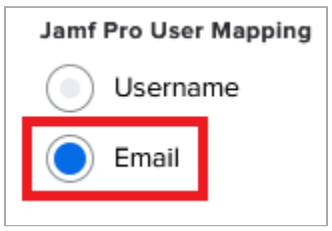
5. Select the **Enable Single Sign-On Authentication** check box.



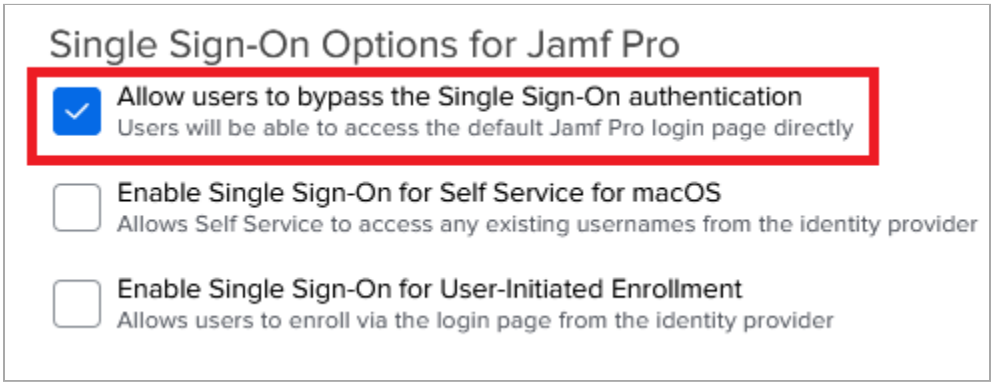
6. In the **Identity Provider** list, select **Ping Identity**.
7. Confirm that the **Entity ID** value matches the value you set previously in PingOne for Enterprise.
8. In the **Upload Metadata File** section, upload the PingOne for Enterprise metadata file.



9. In the **Jamf Pro User Mapping** section, click **Email**.



10. In the **Single Sign-On Options for Jamf Pro** section, select the **Allow users to bypass the Single Sign-On authentication** check box.



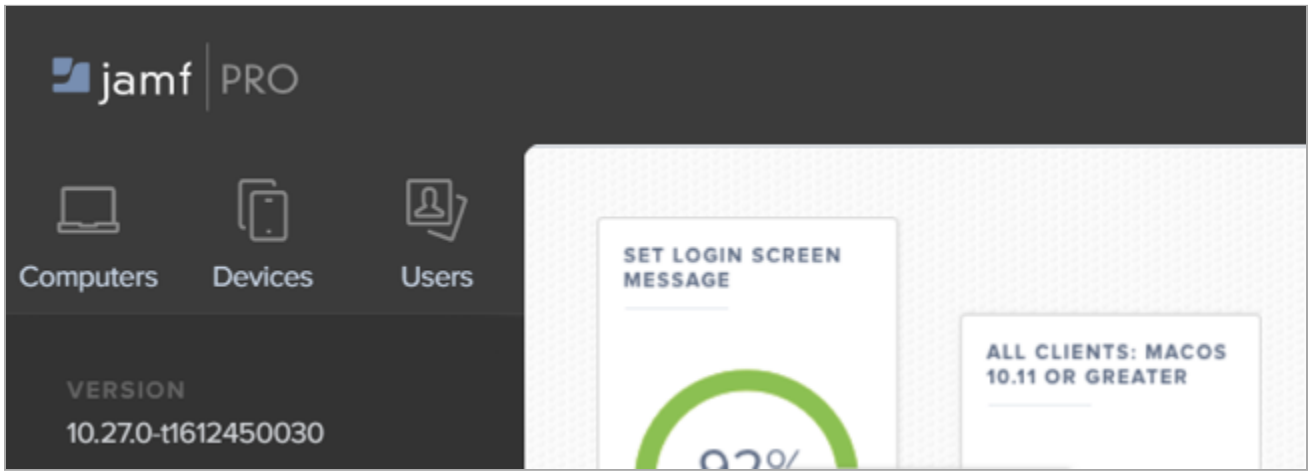
11. Click **Save**.

Test the PingOne for Enterprise identity provider (IdP)

1. Go to your Ping desktop as a user with Jamf Pro access.

> **Note**
>
> To find the Ping desktop URL, in the PingOne admin console, go to **Setup → Dock → PingOne Dock URL**.

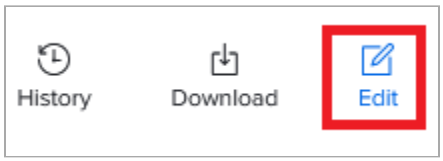
2. Complete the PingOne authentication.



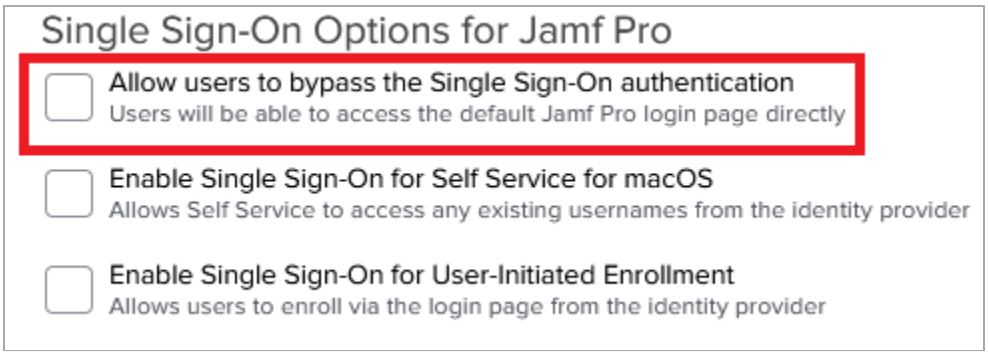
You're redirected to your Jamf Pro application.

Test the PingOne for Enterprise service provider (SP)

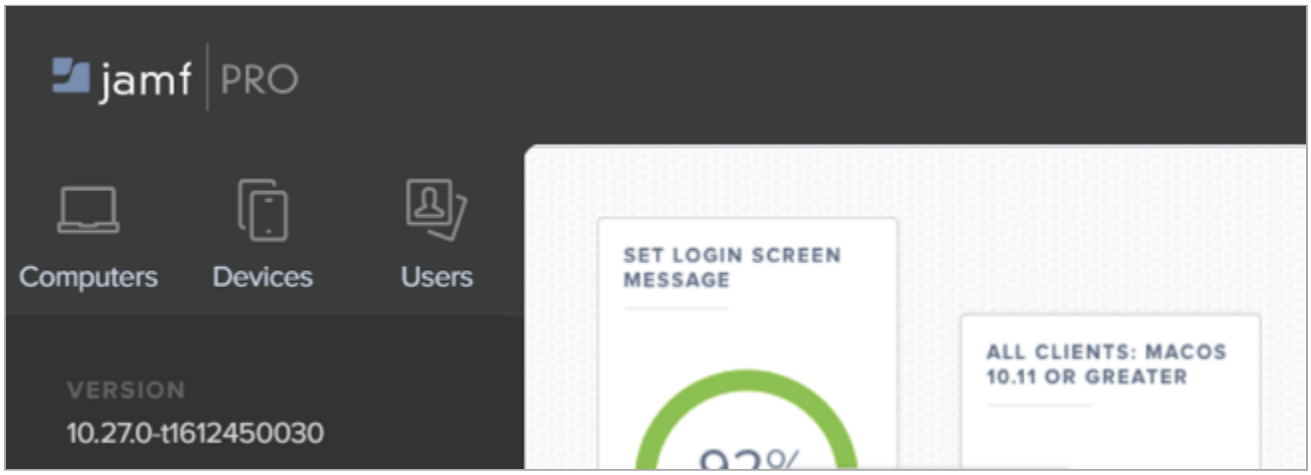
1. If you are using PingOne for Enterprise as the standard authentication method for Jamf Pro access, sign on to the Jamf Pro console as an administrator after you've completed PingOne for Enterprise IdP testing.
2. Go to **Settings → System Settings → Single Sign-On** and click **Edit**.



3. Clear the **Allow users to bypass the Single Sign-On authentication** check box.



4. Click **Save**.
5. Go to your Jamf Pro application.



   You're redirected to PingOne for Enterprise.

6. Enter your PingOne for Enterprise username and password.

   After successful authentication, you're redirected back to Jamf Pro.

Jira/Confluence

Configuring SAML SSO with Jira/Confluence and PingFederate

Learn how to configure SAML single sign-on with Jira/Confluence on premise and PingFederate.

About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
SAML_SUBJECT	Username	Required

Create a PingFederate SP Connection for Jira/Confluence

> **Note**
> The following configuration is untested and is provided as an example. Additional steps might be required.

1. Sign on to Atlassian application as an administrator and go to **Administration → System → SAML Authentication**.
2. Select **SAML Single Sign On**and note the **Audience URL (Entity ID)** and **Assertion Consumer Service URL** values.
3. Download the signing certificate.
4. Sign on to the PingFederate administrative console.
5. Using the details retrieved from the Atlassian application UI:
    1. Configure using **Browser SSO** profile **SAML 2.0**.
    2. Enable **IdP-Initiated SSO** and **SP Initiated SSO**.
    3. In **Assertion Creation: Attribute Contract**, set the **Subject Name Format** to `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`.
    4. In the **Assertion Creation: Attribute Contract Fulfilment**, map the attribute **SAML_SUBJECT** to the attribute **username**.
    5. In **Protocol Settings: Allowable SAML Bindings**, enable **Post** and **Redirect**.
6. Export the metadata for the newly-created SP connection.
7. Export the signing certificate public key.

Configure the PingFederate IdP connection for Jira/Confluence on premise

1. Sign on to Atlassian application as an administrator and go to **Administration → System → SAML Authentication**.
2. Select **SAML Single Sign-On**.
3. Configure the following.

Setting	Value
Single sign-on issuer	The issuer ID for your PingFederate instance. You can retrieve this from the metadata that you downloaded.
Identity provider single sign-on URL	The PingFederate **SingleSignOnService** URL. You can retrieve this from the metadata that you downloaded. For example, `https://hostname:port/idp/SSO.saml2`
X509 Certificate	Upload the PingFederate signing public certificate.
Login Mode	Choose whether SAML is primary or secondary authentication.

Configuration is complete.

Configuring SAML SSO with Jira/Confluence and PingOne for Enterprise

Learn how to configure SAML single sign-on (SSO) with Jira/Confluence on premise and PingOne for Enterprise.

About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
SAML_SUBJECT	Username	Required

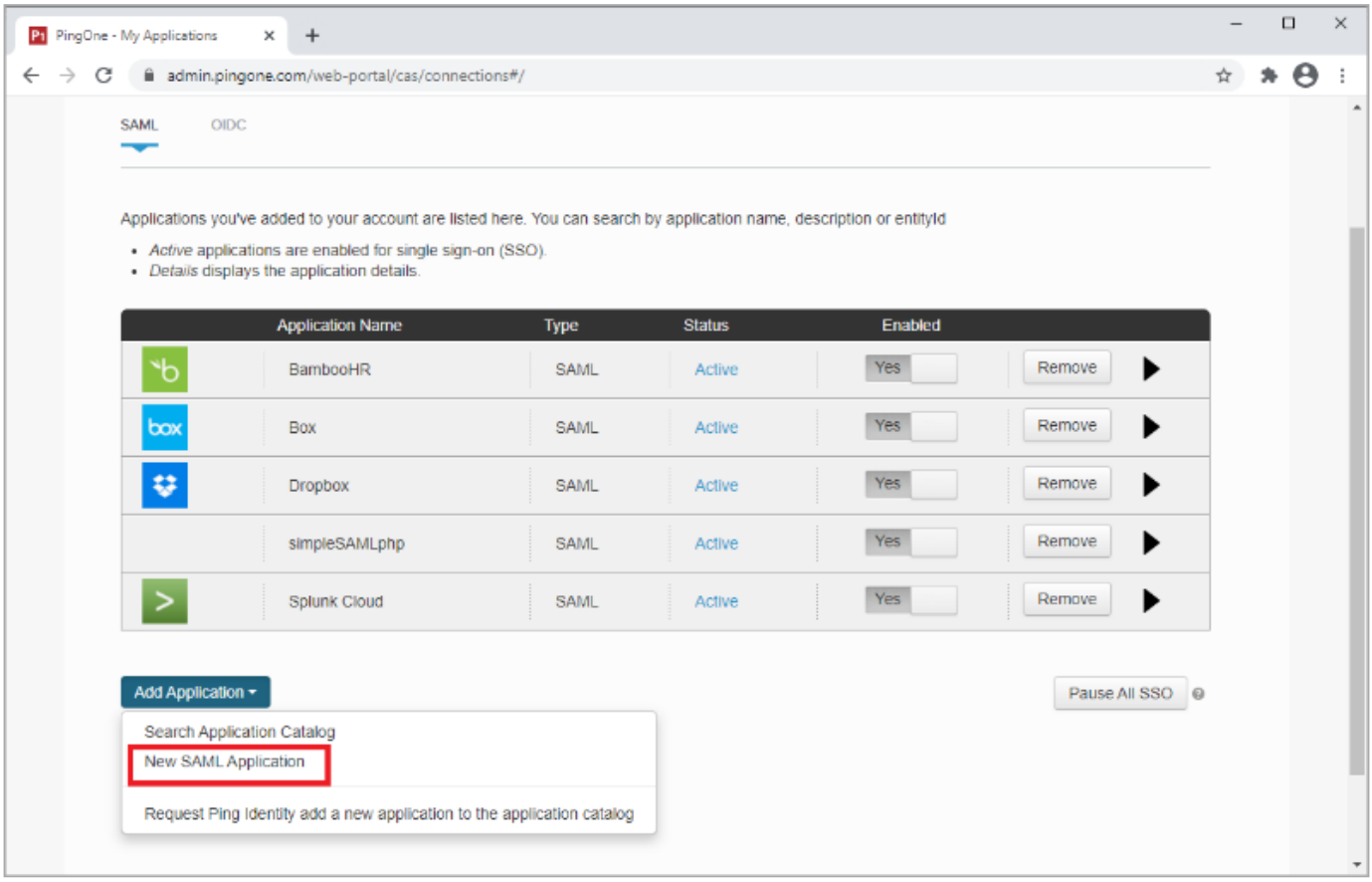
> **Note**
>
> A predefined application exists in the application catalog for use with Atlassian Cloud. It is recommended that this is used for Atlassian Cloud integrations.

Create a PingOne for Enterprise application for Jira/Confluence on premise

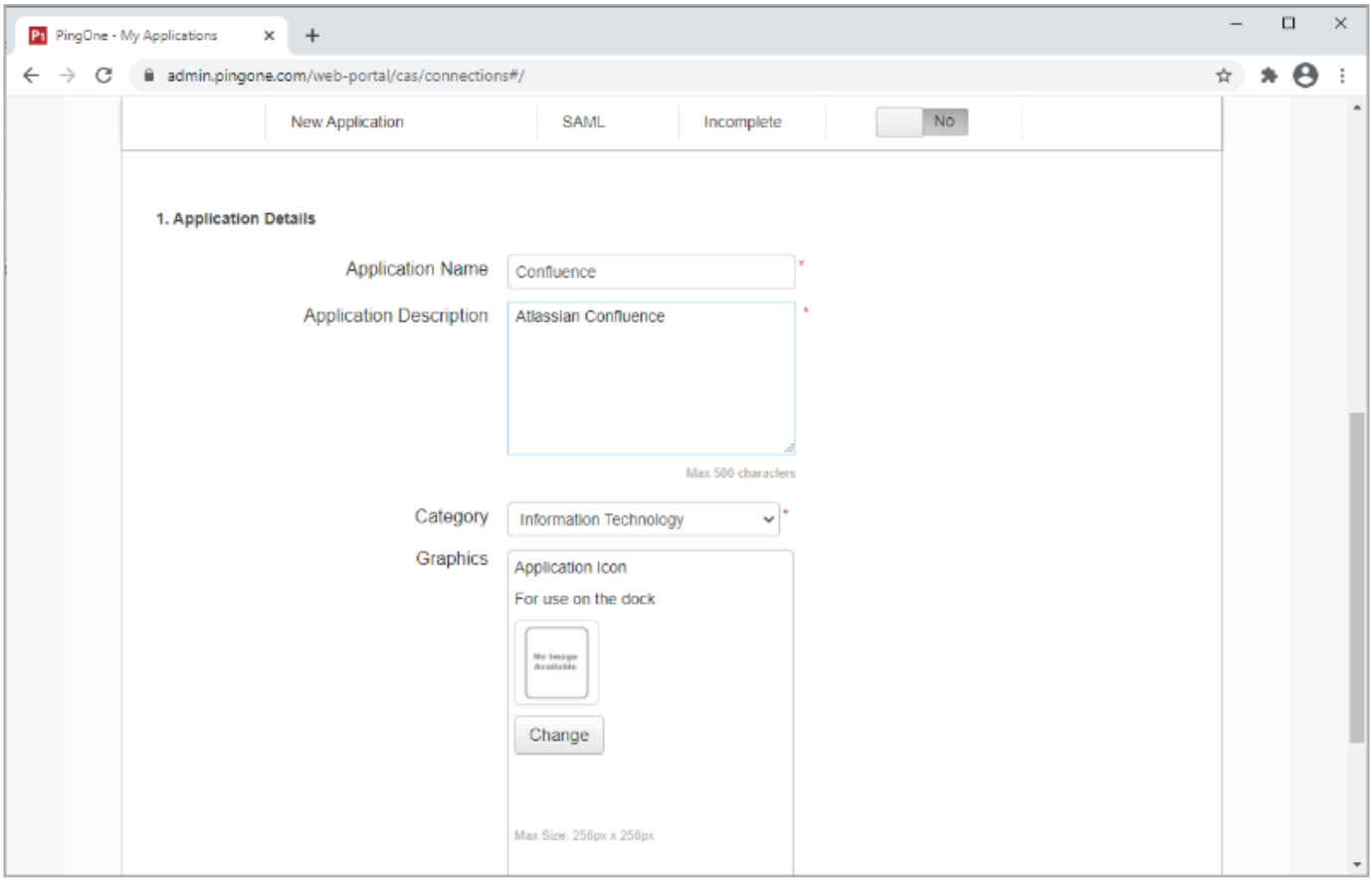
> **Note**
>
> The following configuration is untested and is provided as an example. Additional steps might be required.

1. Sign on to the Atlassian application as an administrator and go to **Administration → System → SAML Authentication**.

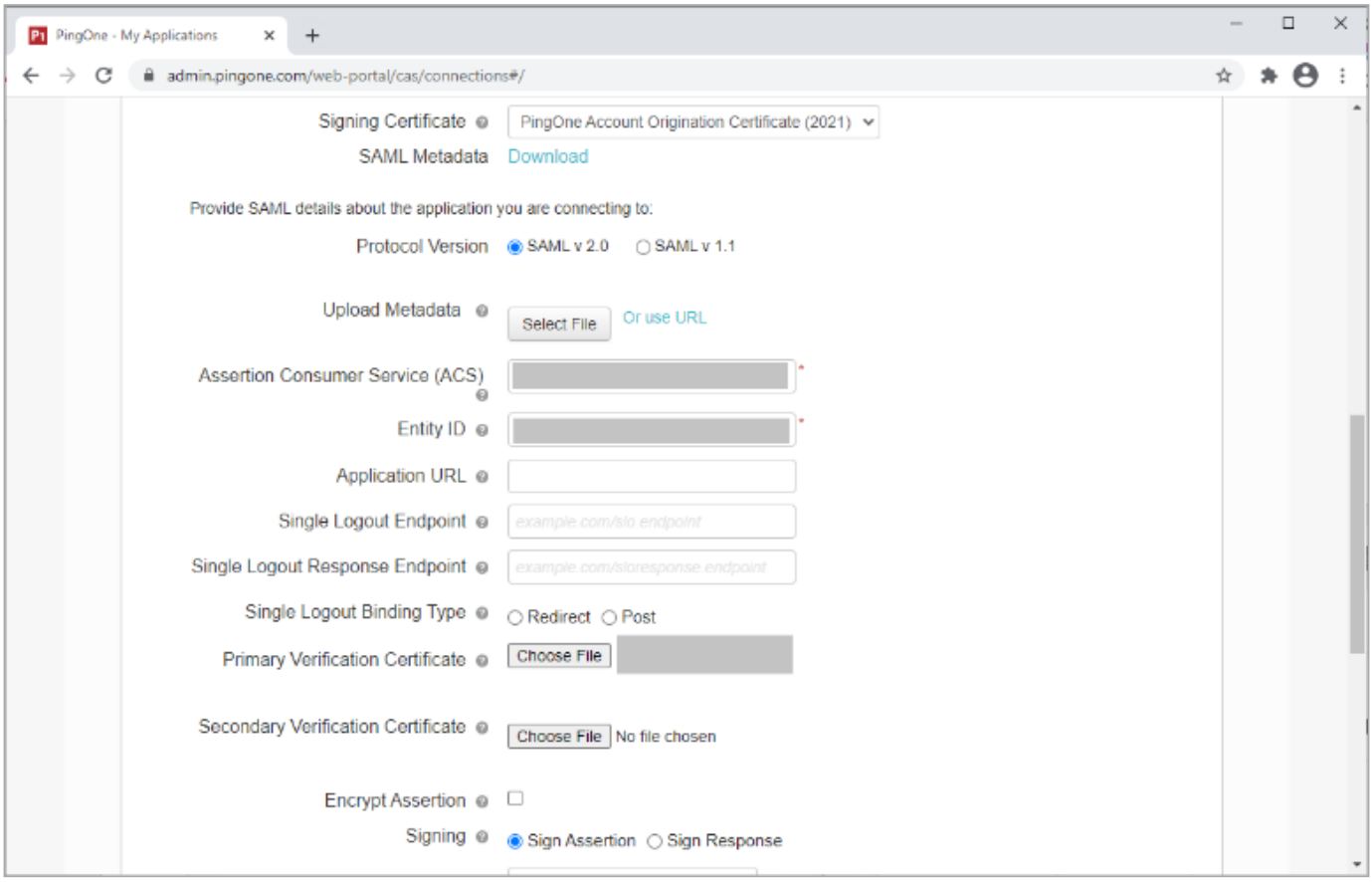
2. Select **SAML Single Sign On** and note the **Audience URL (Entity ID)** and **Assertion Consumer Service URL** values.
3. Download the signing certificate.
4. Sign on to PingOne for Enterprise and click **Applications**.
5. On the **SAML** tab, click **Add Application**.
6. Click **New SAML Application**.



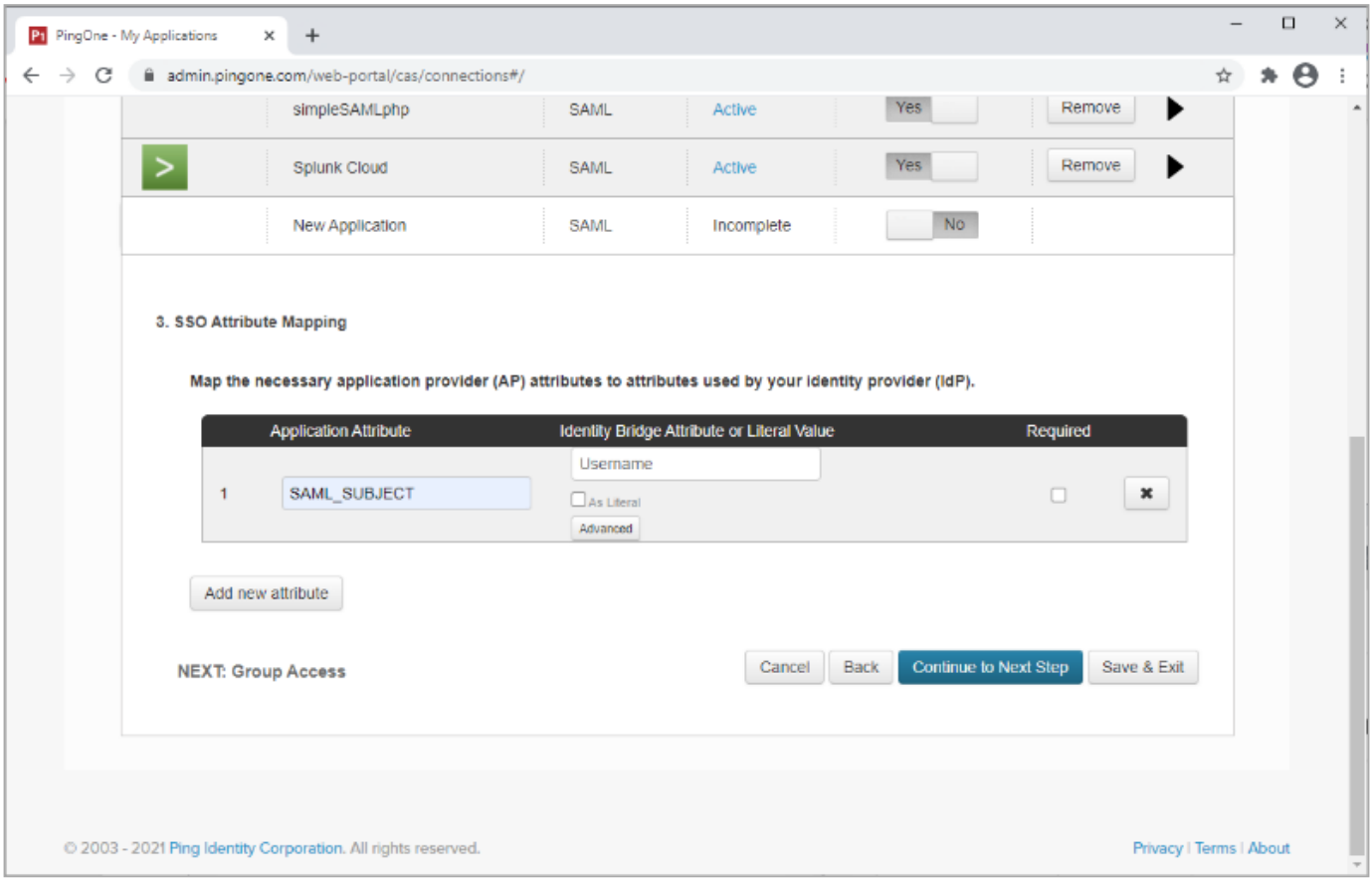
7. In the **Application Details** section, enter the following:
    - A suitable application name, such as Confluence.
    - A suitable description.
    - A suitable category, such as **Information Technology**.
    - (Optional) Upload an icon to be used in the PingOne for Enterprise dock.



8. Click **Continue to Next Step**.
9. Select **I have the SAML configuration**.
10. In the **Signing Certificate list**, select a suitable signing certificate.
11. For **Protocol Version**, click **SAML v.2.0**.
12. In the **Assertion Consumer Service (ACS)** field, enter the ACS value from the Atlassian single sign-on settings.
13. In the **Entity ID** field, enter the **Entity ID** value from the Atlassian single sign-on settings.
14. For **Primary Verification Certificate**, select the signing certificate that you downloaded.

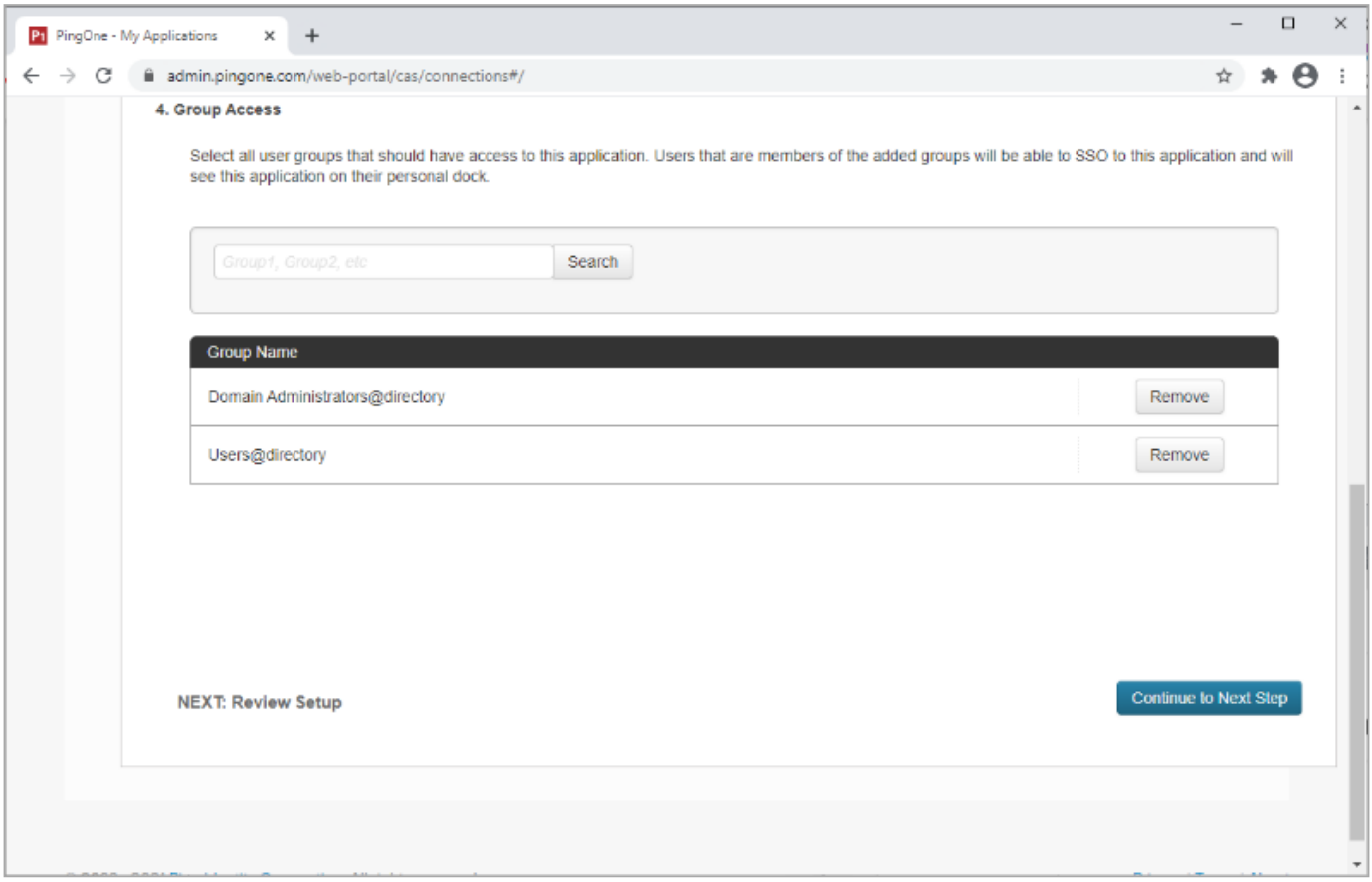


15. Click **Continue to Next Step**.
16. In the **SSO Attribute Mapping** section, add the following mapping for the **SAML_SUBJECT**:
    - For **Identity Bridge Attribute or Literal Value**, select the appropriate attribute. This should match the username for the user in the application.
    - Select the **Required** check box.



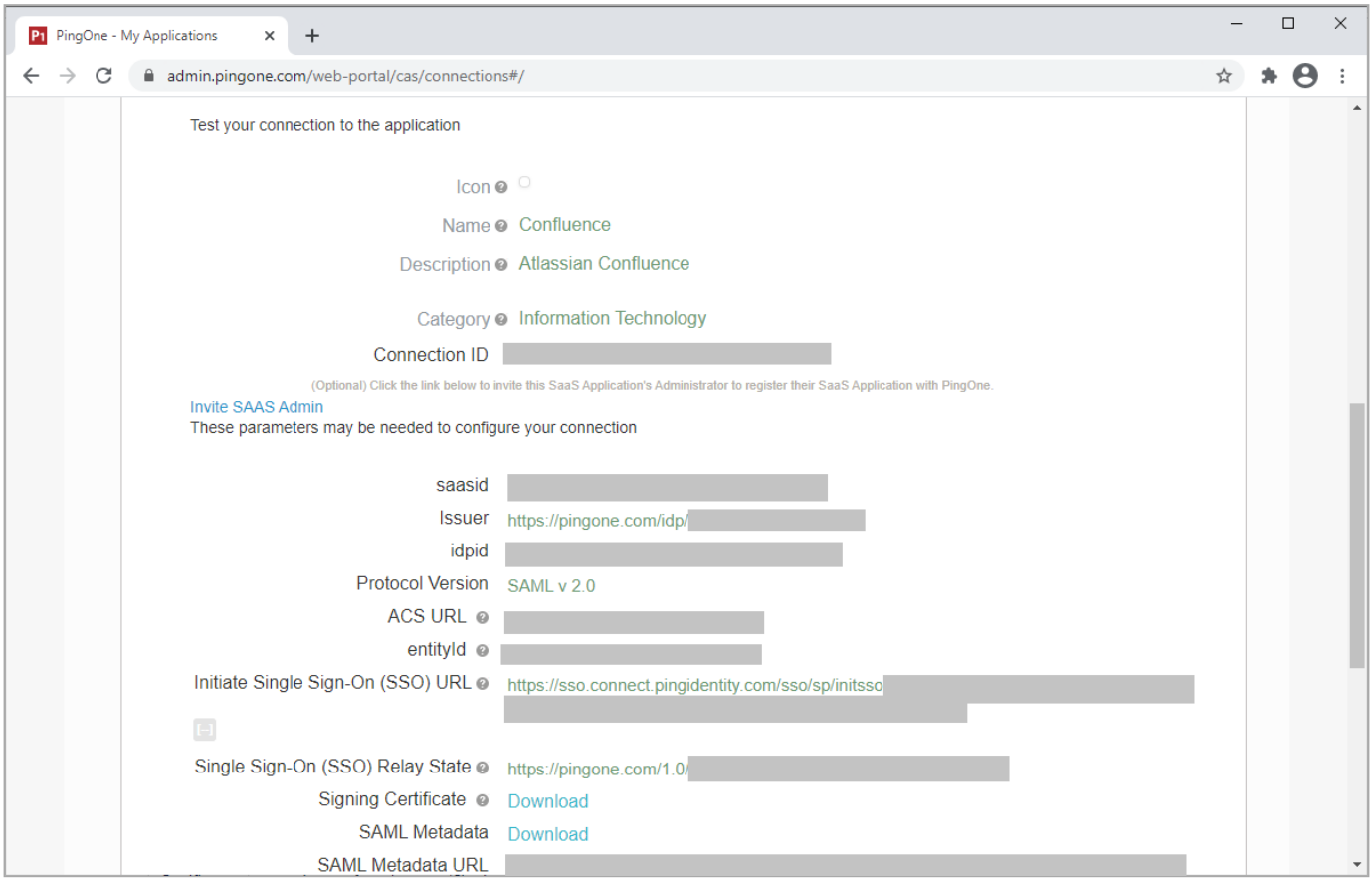
17. Click **Continue to Next Step**.

18. Add the user groups for the application.



19. Click **Continue to Next Step**.

20. Review the settings.



21. Copy the **Single Sign-On (SSO) URL** value to a temporary location.

    This is the IdP-initiated SSO URL that you can use for testing.

22. Note the **idpid** and **Issues** values.

23. On the **Signing Certificate** line, click **Download**.

    You'll use this for the application configuration.

24. On the **SAML Metadata** line, click **Download**.

    You'll use this for the application configuration.

25. Click **Finish**.

Configure the PingOne for Enterprise IdP Connection for Jira/Confluence on-premise

1. Sign on to the Atlassian application as an administrator.
2. Go to **Administration → System → SAML Authentication**.
3. Select **SAML Single Sign On**.
4. Configure the following.

Setting	Value
Single sign-on issuer	The issuer from PingOne for Enterprise application details noted earlier.
Identity provider single sign-on URL	Enter the **Single Sign-On Service URL** in the following form, using the idpid previously noted. `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=idpid` Alternatively, you can retrieve the URL from the metadata that you downloaded.
X509 Certificate	Upload the PingOne for Enterprise signing public certificate that you downloaded.
Login Mode	Choose whether SAML is your primary or secondary authentication.

Configuration is complete.

Jive

Configuring SAML SSO with Jive and PingFederate

Learn how to configure SAML SSO with Jive and PingFederate.

About this task

The following table details the references that are used within this guide that are environment specific. Replace these with the suitable value for your environment.

Reference	Description
jiveinstance	The host and port for the Jive instance.

> **Note**
> The following configuration is untested and is provided as an example. Additional steps might be required.

Create the PingFederate SP Connection for Jive

1. Sign on to the Jive Admin Console and enable single sign-on:
    1. Go to **People → Settings → Single Sign-On → SAML**.
    2. Check **Enabled**.
    3. Click **Save**.
    4. Restart Jive.

    > **Note**
    > Until SAML configuration is complete, you'll need to sign on by going directly to the admin console, `http://jiveinstance/admin` .
2. Download the Jive metadata from `http://jiveinstance/saml/metadata` .
3. Sign on to the PingFederate administrative console.
4. Using the metadata that you downloaded, create an SP connection in Ping Federate:
    1. Configure using **Browser SSO** profile **SAML 2.0**.

2. Enable the following **SAML Profiles**:
    - **IdP-Initiated SSO**
    - **SP-Initiated SSO**
3. In **Assertion Creation: Attribute Contract**, set the **Subject Name Format** to `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`.
4. In the **Assertion Creation: Attribute Contract Fulfilment**, map the attribute **SAML_SUBJECT** to the attribute `username`.
5. Add any additional attributes required into the attribute contract and contract fulfillment.
6. In **Protocol Settings: Allowable SAML Bindings**, enable **POST**, and **Redirect**.

5. Export the metadata for the newly-created SP connection.
6. Export the signing certificate public key.

Configure the PingFederate IdP connection for Jive

1. Sign on to the Jive Admin Console and go to **People → Settings → Single Sign-On → SAML**.
2. On the **IdP Metadata** tab, copy the contents of the metadata file into the metadata field.
3. Click **Save All SAML Settings**.
4. On the **User Attribute Mapping** tab, map the user attributes in the Jive profile to the attributes that you configured in PingFederate.
5. **Optional:** Select **Group Mapping Enabled** if you want to assign users to groups with a group attribute passed in the assertion.
6. Click **Save Settings**.

Configuring SAML SSO with Jive and PingOne for Enterprise

Learn how to configure SAML SSO with Jive and PingOne for Enterprise.

About this task

The following table details the references that are used within this guide that are environment specific. Replace these with the suitable value for your environment.

Reference	Description
jiveinstance	The host and port for the Jive instance.

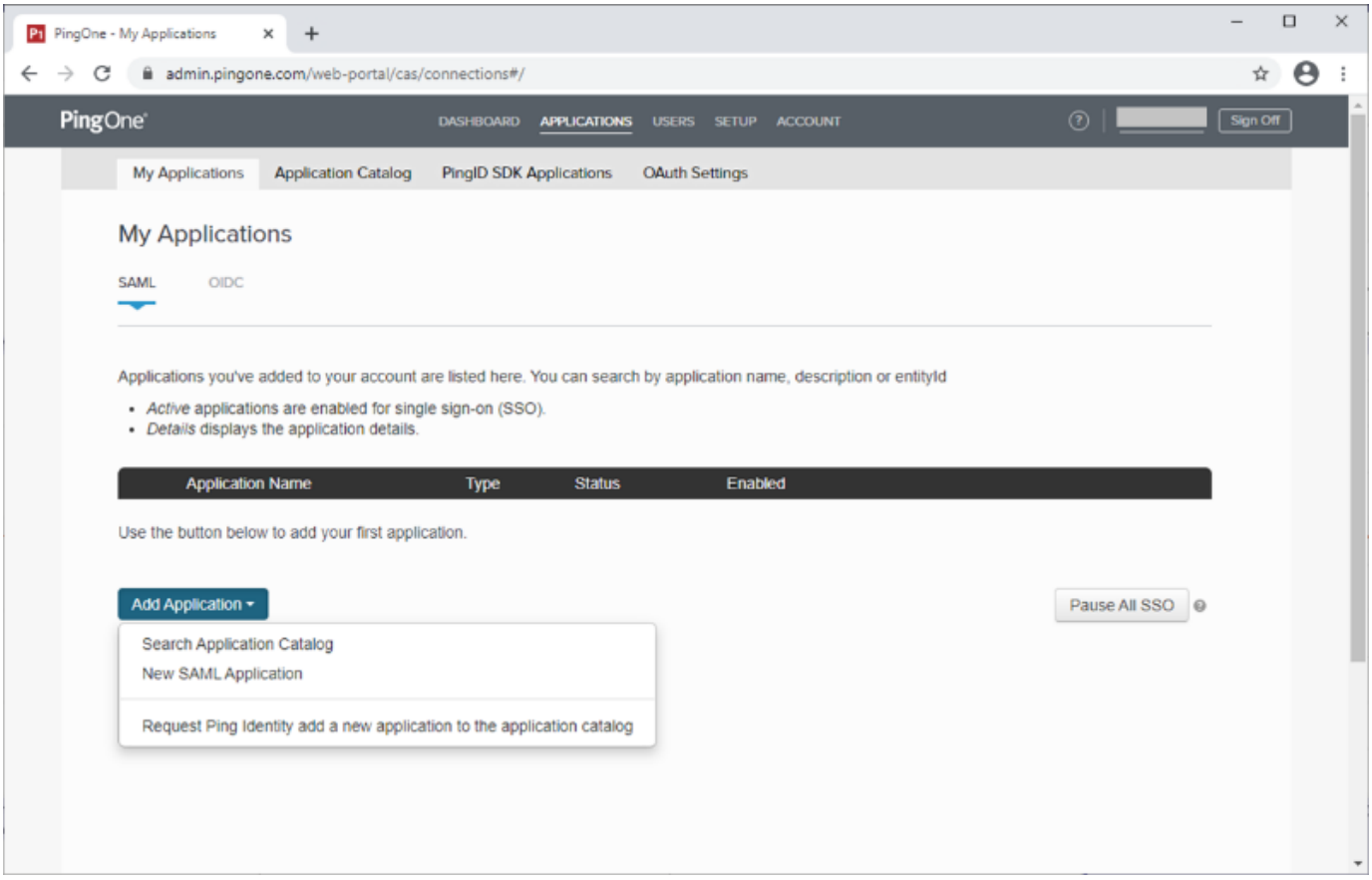
> **Note**
>
> The following configuration is untested and is provided as an example. Additional steps might be required.

Create a PingOne for Enterprise Application for Jive

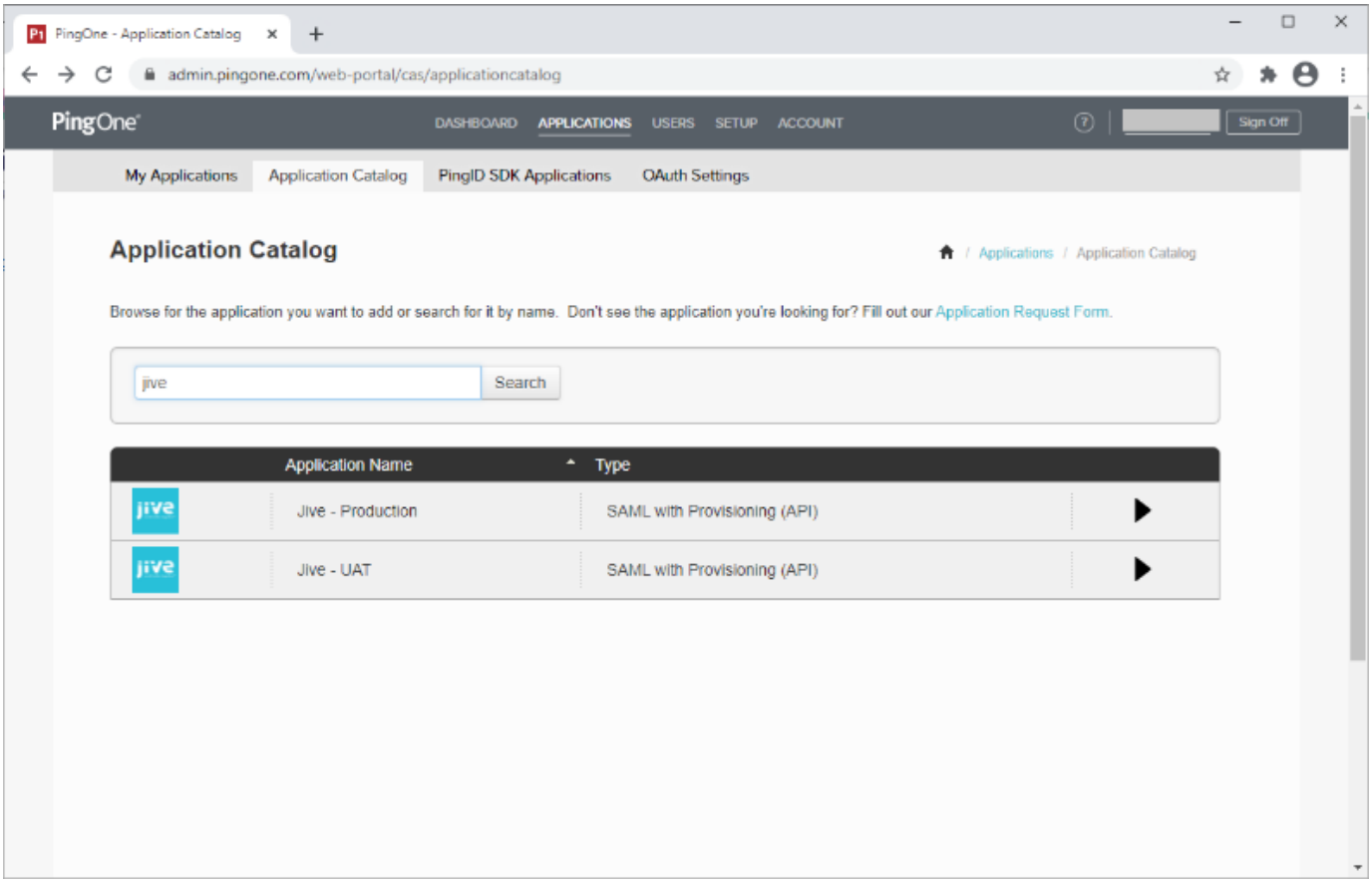
1. Sign on to the Jive Admin Console and enable single sign-on:
    1. Go to **People → Settings → Single Sign-On → SAML**.
    2. Check **Enabled**.
    3. Click **Save**.
    4. Restart Jive.

    > **Note**
    > Until SAML configuration is complete, you'll need to sign on by going directly to the admin console, `http://jiveinstance/admin` .

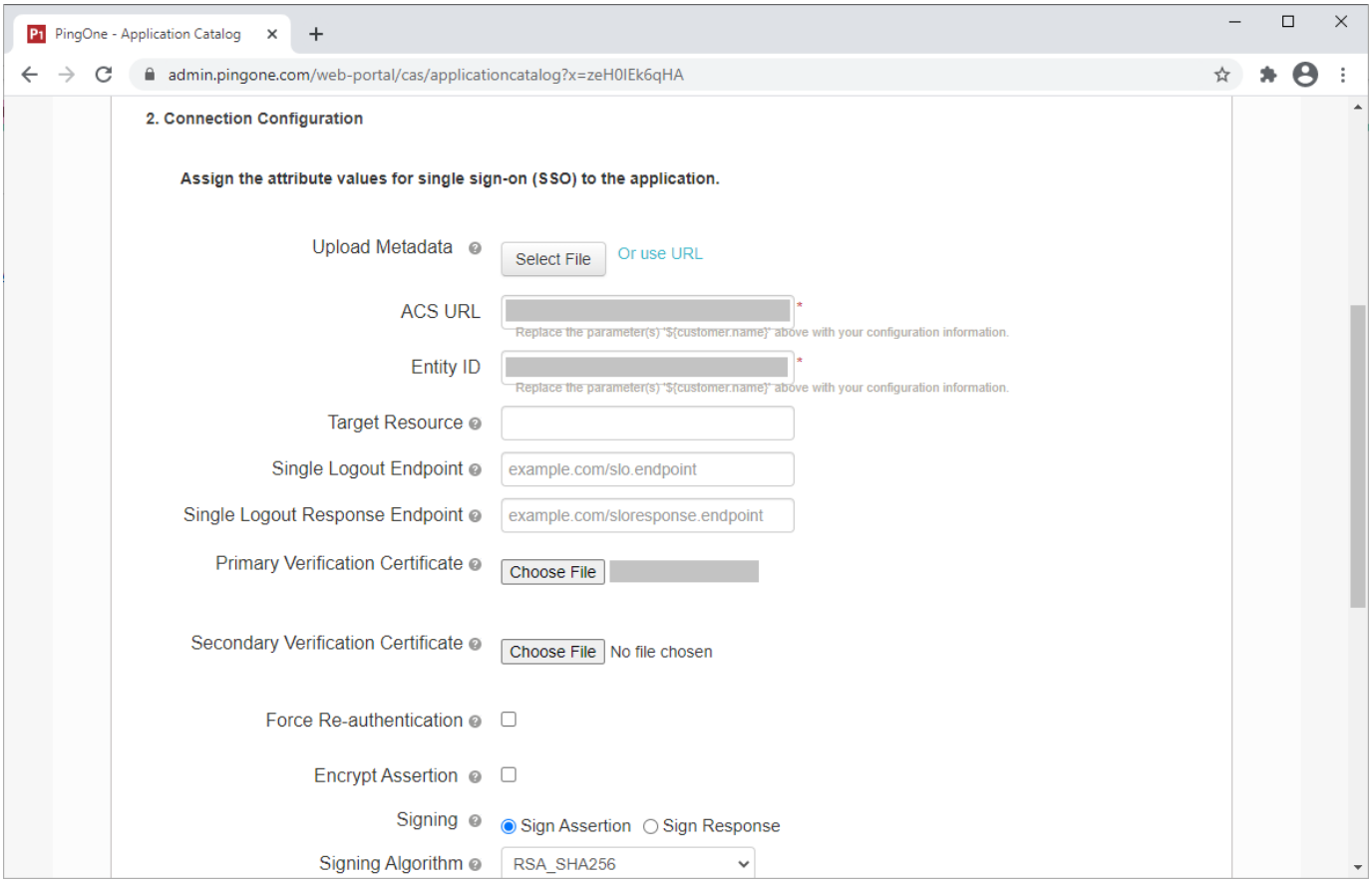
2. Download the Jive Metadata from `http://jiveinstance/saml/metadata` .
3. Sign on to PingOne for Enterprise and click **Applications**.
4. On the SAML tab, click **Add Application**.



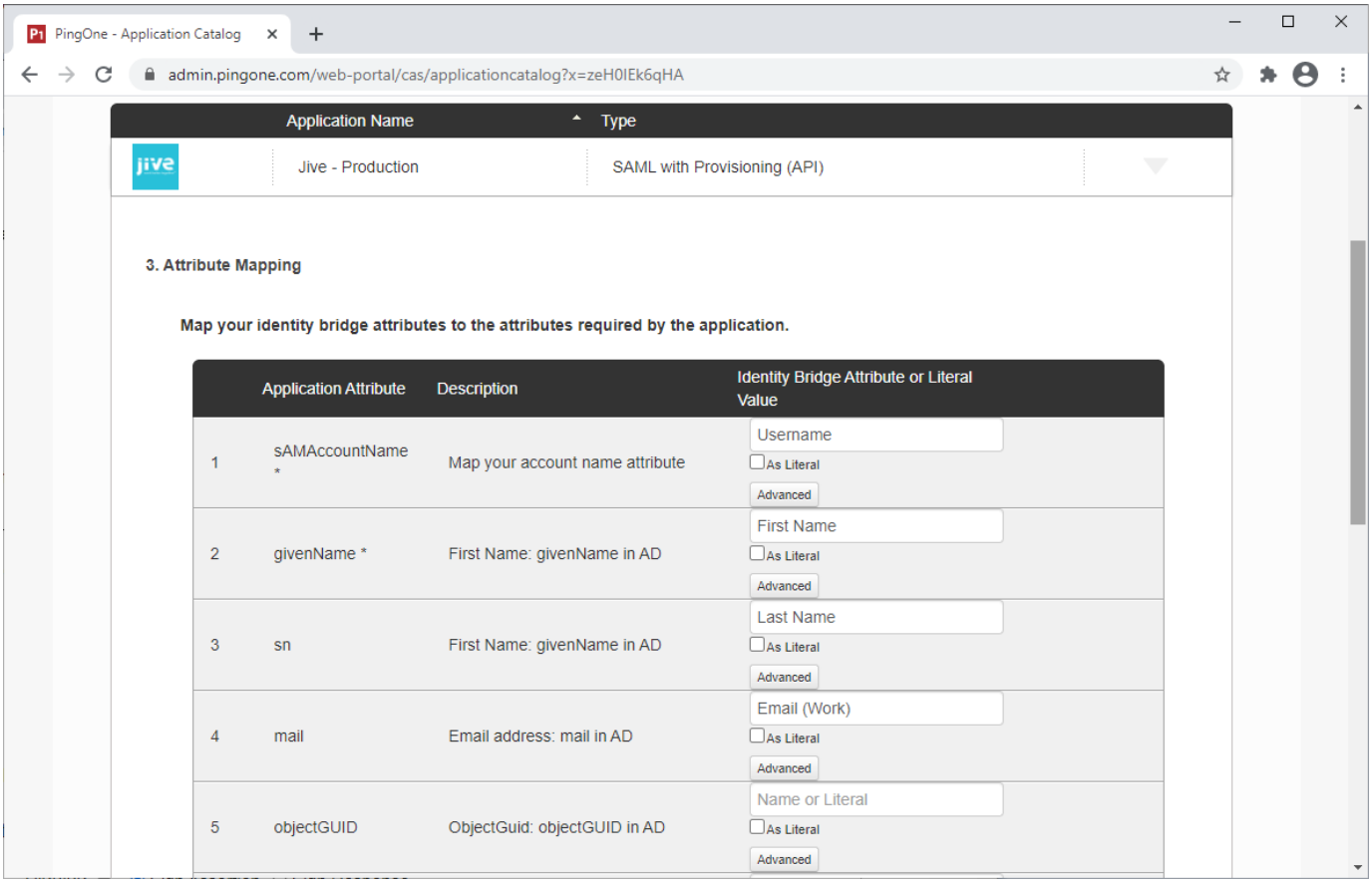
5. Click **Search Application Catalog** and search for `Jive` .
6. Click the **Jive - Production** row or click **Jive – UAT** for a non-production environment.



7. Click **Setup**.
8. Select the appropriate signing certificate from the list.
9. Review the steps, and note the **PingOne for Enterprise SaaS ID**, **IdP ID**, **Single Sign-on URL**, and **Issuer** values.
10. Click **Continue to Next Step**.
11. On the **Upload Metadata** row, click **Select File**, and upload the Jive metadata file that you previously downloaded.

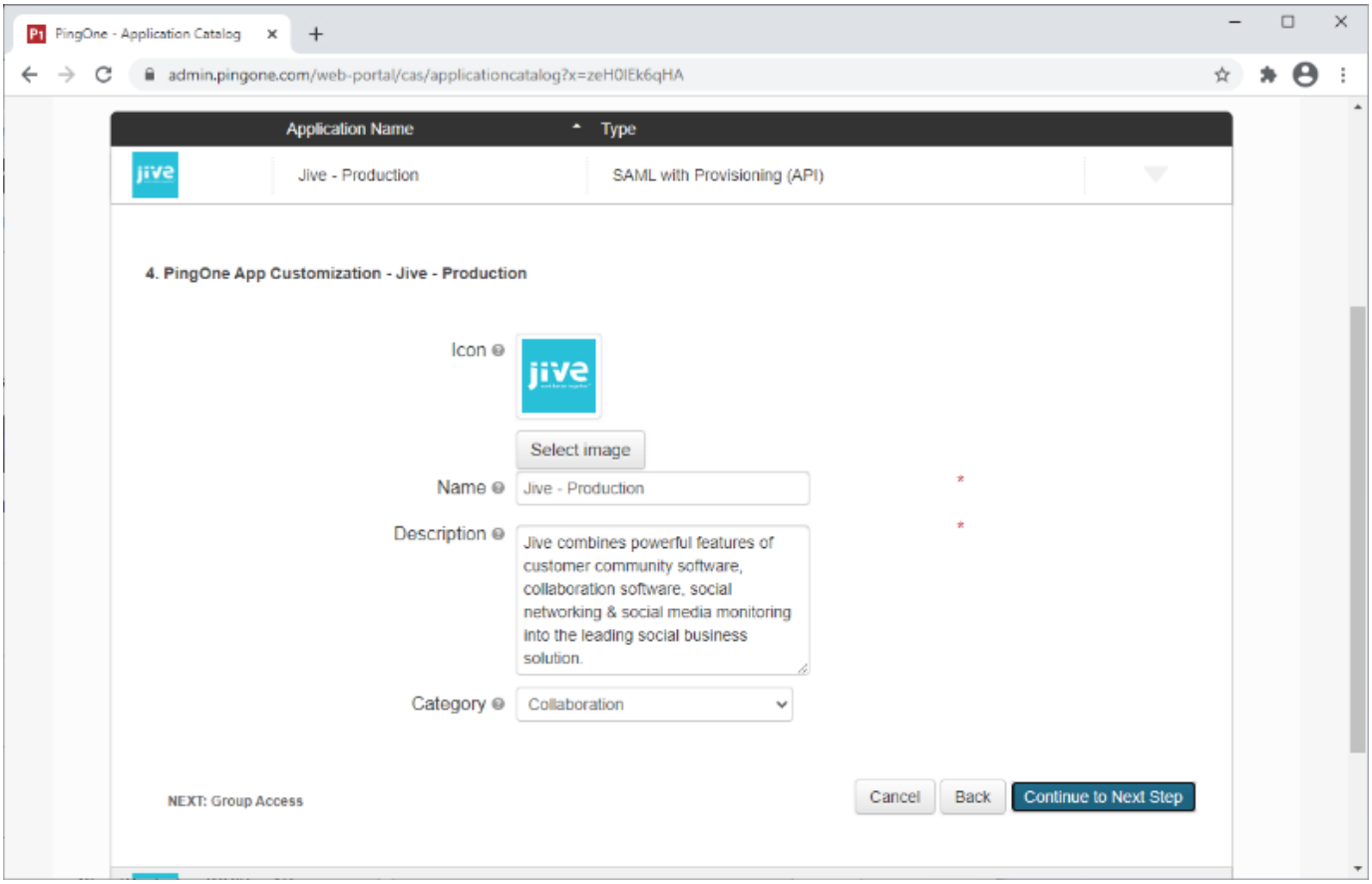


12. Click **Continue to Next Step**.
13. In the **Attribute Mapping** section, complete the attribute mappings as required.



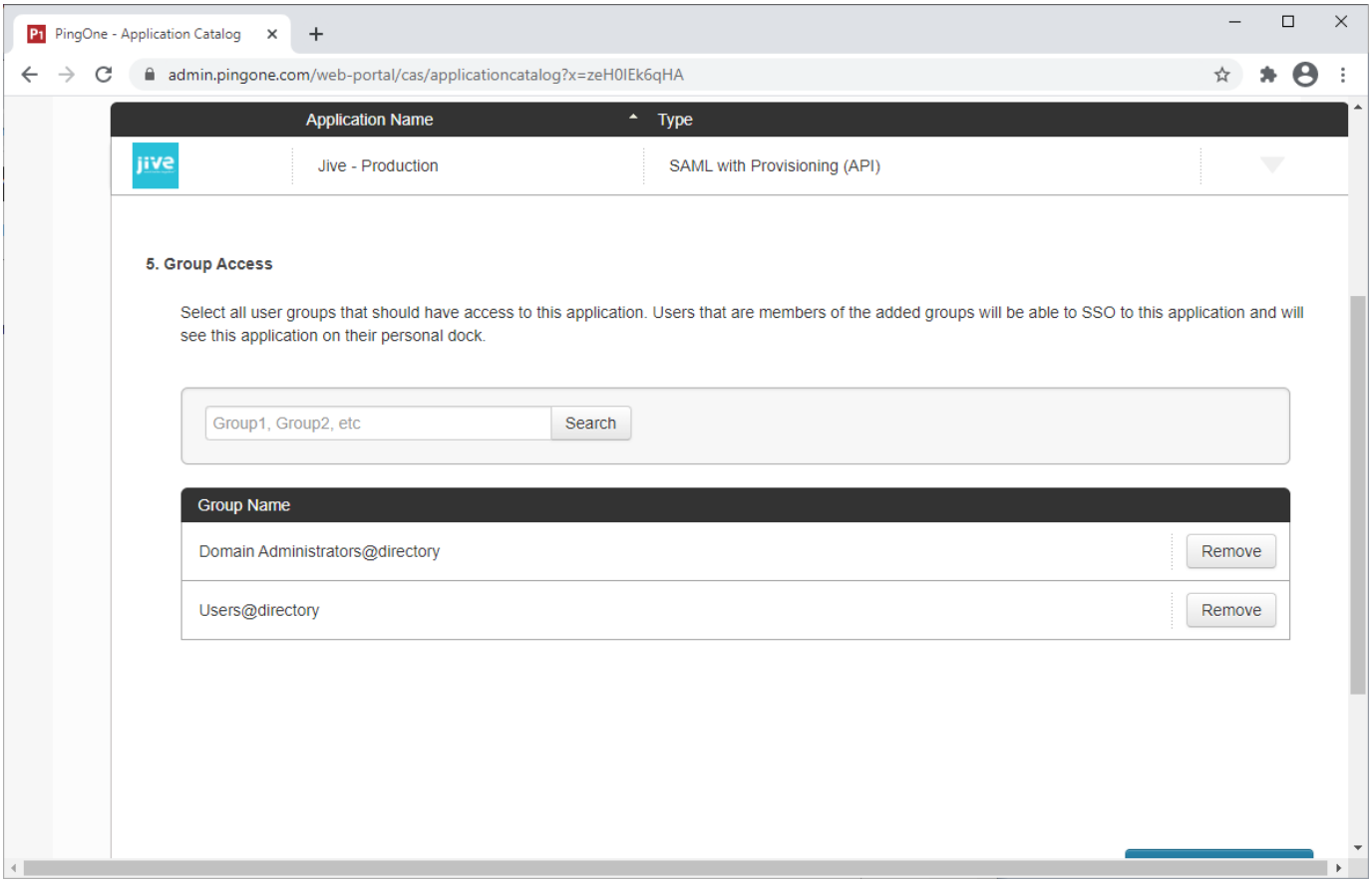
14. Click **Continue to Next Step**.

15. Update the **Name**, **Description**, and **Category** fields as required.



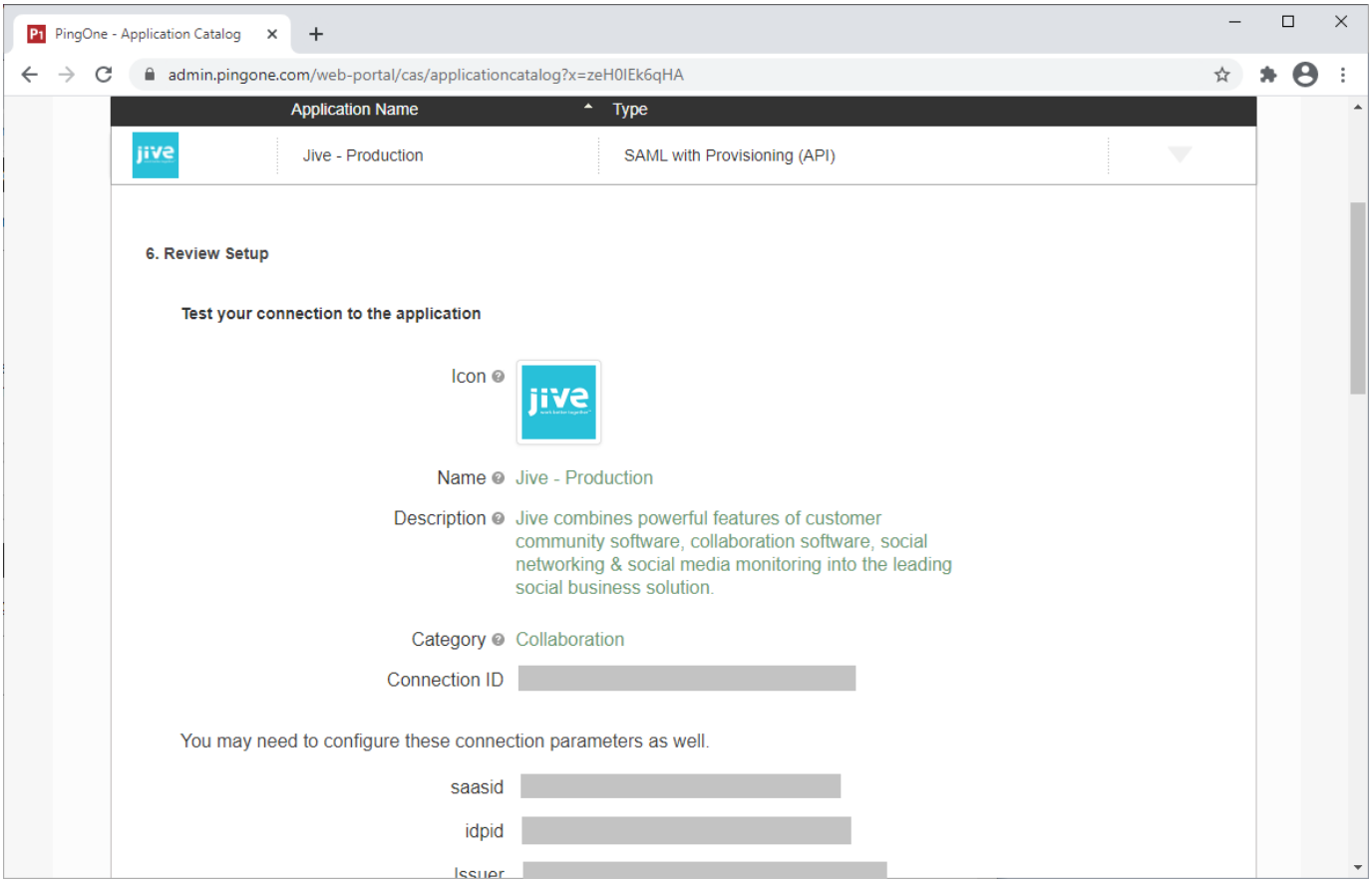
16. Click **Continue to Next Step**.

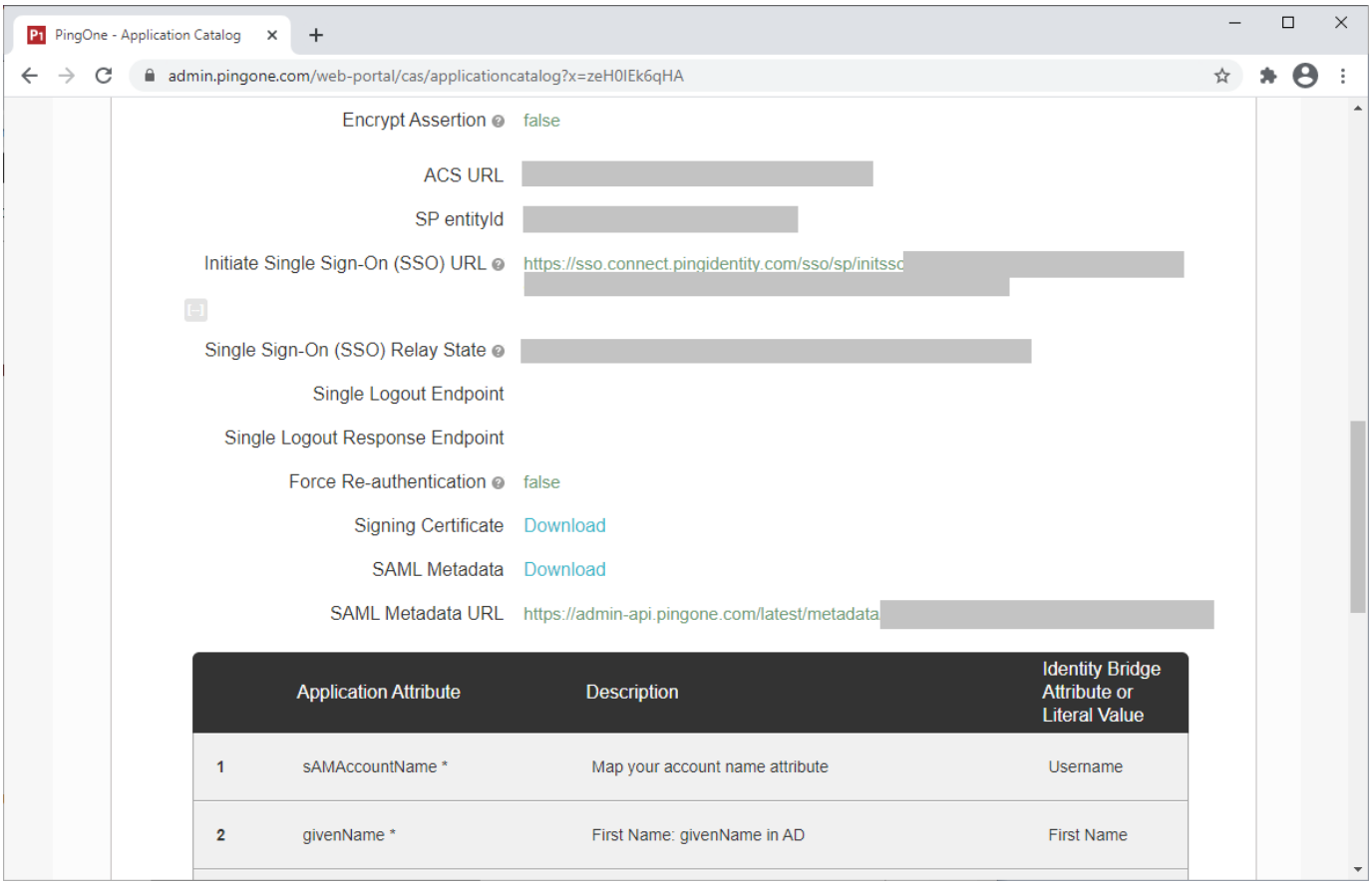
17. Add suitable user groups for the application.



18. Click **Continue to Next Step**.

19. Review the settings.





20. Copy the **Single Sign-On (SSO) URL** value to a temporary location.

    This is the IdP-initiated SSO URL that you can use for testing.

21. On the **Signing Certificate** row, click **Download**. You'll use this for the Jive configuration.
22. On the **SAML Metadata** row, click **Download**. You'll use this the Jive configuration.
23. Click **Finish**.

Configure the PingOne for Enterprise IdP connection for Jive

1. Sign on to the Jive Admin Console and go to **People → Settings → Single Sign-On → SAML**.
2. On the **IdP Metadata** tab, copy the contents of the metadata file into the metadata field.
3. Click **Save All SAML Settings**.
4. On the **User Attribute Mapping** tab, map the user attributes in the Jive profile to the attributes configured in PingOne for Enterprise.
5. **Optional:** Select **Group Mapping Enabled** if you want to assign users to groups using a group attribute passed in the assertion.
6. Click **Save Settings**.

Lookout Secure Access

Configuring SAML SSO with Lookout Secure Access

The Ping Identity and Lookout SAML integration supports service provider (SP) and identity provider (IdP) initiated single sign-on (SSO).

What it is

Lookout Cloud Security (Lookout SSE platform) is a data-centric cloud security solution that protects users from internet-based threats and protects data stored in cloud applications, private applications, and websites.

Lookout Cloud Security supports the following cloud security components:

Lookout Secure Internet Access

Protection for web or non-web internet-based traffic.

Lookout Secure Private Access

Protection for private application traffic.

Lookout Secure Cloud Access

Protection for cloud application traffic.

> **Note**
>
> Users must authenticate with your enterprise SSO provider during their initial access before accessing solutions such as Secure Internet Access and Secure Cloud Access.

The Lookout Cloud Security platform leverages the user or user group context to enforce access and activity policies on cloud apps, private apps, and websites.

What you'll need

- Have a PingOne account. Learn more in Starting a PingOne trial.
- Verify that you can sign on to the PingOne admin console. Learn more in Accessing the PingOne admin console.
- Have a Lookout SSE platform account. To enroll in a Lookout SSE platform account, contact Lookout.

What you'll do

To configure SAML SSO with Lookout Secure Access:

1. Gather the service provider (Lookout Secure Access) metadata.
2. Configure the service provider in PingOne.
3. Configure the identity provider (PingOne) in Lookout.
4. Enable SSO for the Lookout management console, endpoint client, and proxy authentication.
5. Configure IdP-initiated sign-on for Lookout management console.
6. Test SSO with Lookout Secure Access.

Step 1: Gather the SP metadata

To use PingOne as an IdP, you'll capture SAML values from the Lookout Management console:

1. In the Lookout Management console, go to **Administration → Enterprise Integration**.
2. Go to **Configuration → Single Sign-On**.
3. On the **SSO Groups** tab, go to the default group.
4. In the **SP Metadata** column, click the **Download** icon.

   The **SP Metadata** window opens.
5. Copy the **Assertion Consumer Service (ACS) URL** and **Entity ID** values.

Step 2: Configure the SP in PingOne

After you've captured the SAML values from Lookout Secure Access, you'll configure a SAML-based application in PingOne. This gives PingOne the information it needs to communicate with the Lookout Cloud Security Platform so that the platform can enforce policies based on user credentials.

1. In the PingOne admin console, go to **Applications → Application Catalog** and browse or search for `Lookout Secure Access`.
2. Click the **Lookout Secure Access** entry to open the details panel.
3. For **Quick Setup**, enter the following information:
   - **ACS URL**: Enter the **Assertion Consumer Service**value that you copied previously.
   - **Entity ID**: Enter the **Entity ID** value that you copied previously.
4. Click **Next**.
5. On the **Map Attributes** page, click **Next**.
6. On the **Select Groups** page, click **Save**without assigning groups.

   This allows users to have access to all applications by default.

> **Note**
>
> Assign groups to the application to restrict access to only those groups.

7. In **Application Instances**, select the **Lookout Secure Access Application** entry to open the **Connection Details** page.
8. On the **Connection Details** page, copy the **IDP Metadata URL** to use when configuring the SP.

Step 3: Configure the IdP in Lookout

Next, you'll link your PingOne instance to the Lookout Cloud Security Platform by configuring a new IdP instance. Lookout uses to retrieve user information from PingOne.

1. In the Lookout Management Console, go to **Administration → Enterprise Integration**.
2. Go to **Configuration → Single Sign-On**.
3. On the **SSO Providers** tab, click **New**.
4. Enter or select the following values:
   - **Name**: Enter a name that contains no more than 255 characters.
   - **Type**: Select **Identity Provider**.
   - **SSO Group**: Select **Default**.
   - **Metadata Link**: Enter the **IDP Metadata URL** value that you copied from the PingOne.
5. Click **Validate** and confirm that the Management Console populates the **Entity ID** field.
6. Click **Save**.

Step 4: Enable SSO for the Lookout management console, endpoint client, and proxy authentication

After you've configured the service provider, you'll enable SSO for the Lookout Cloud Security Platform.

1. In the Lookout Management Console, go to **Administration → System Settings → Enterprise Authentication**.
2. In the **Identity Provider** list, choose the IdP that you created.
3. To enable the **Management SSO**, click the toggle.
4. To enable the **Endpoint**, click the toggle.

> **Note**
>
> The **Native Proxy Authentication** toggle is enabled by default and cannot be disabled.

5. Click **Save**.

Step 5: Configure IdP-initiated sign-on for Lookout management console

Next, to set up IdP-initiated sign-on for the Lookout Management Console, you'll configure relay state on PingOne.

1. In the Lookout Management Console, go to **Administration → System Settings → Enterprise Authentication**.
2. In the **Enterprise Single Sign-on Settings** field, click **Copy** to copy the **Relay State** value.
3. In the PingOne admin console, go to **Applications → Applications**.
4. Click the **Lookout Secure Access** entry.
5. On the **Overview** tab, click **Enable Advanced Configuration**.

   The **Enable Advanced Configuration** window opens.
6. Click **Enable**.
7. On the **Configuration** tab, click on the **Pencil** icon to edit the **Connection Details**.
8. In the **Target Application URL** field, paste the **Relay State** value that you copied from the Lookout Management Console.
9. Click **Save**.

Step 6: Test SSO with Lookout Secure Access.

After you've configured IdP-initiated sign-on, you'll verify that SSO works.

1. In the PingOne admin console, go to **Applications → Applications**.
2. Click the **Lookout Secure Access** entry.
3. On the **Configuration** tab, copy the **Initiate Single Sign-On URL** value.
4. Paste the URL in a new browser window and hit enter.

   You are successfully redirected to the Lookout Management Console.

Marketo

Configuring SAML SSO with Marketo and PingFederate

Learn how to enable Marketo sign-on from PingFederate (IdP-initiated sign-on).

Before you begin

- Configure PingFederate to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- Populate Marketo with at least one user to test access.
- You must have administrative access to PingFederate.

Obtain your Munchkin Account ID

1. Sign on to the Marketo console as an administrator.
2. Select **Admin** in the toolbar.
3. Select **Intergration** in the left-hand pane.
4. **Copy** and **Save** your Munchkin Account ID.

Create an SP connection for Marketo in PingFederate

1. Sign on to PingFederate.
2. Configure using **Browser SSO** profile **SAML 2.0**.
3. Set **Partner's Entity ID** to `https://www.marketo.com/SAML/your-Munchkin-account-ID`.
4. Enable the **IDP-initiated SSO SAML Profile**.

> **Note**
>
> Marketo does not currently support SP-initiated SSO.

5. In **Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment**, map the **SAML_SUBJECT** to your email attribute.
6. In **Protocol Settings: Assertion Consumer Service URL**, set **Binding** to **POST** and set **Endpoint URL** to `https://login.marketo.com/saml/assertion/your-Munchkin-account-ID`.
7. In **Protocol Settings: Allowable SAML Bindings**, enable **POST**.
8. In **Credentials: Digital Signature Settings**, select the PingFederate Signing Certificate and download it.

Enable SAML SSO in Marketo

1. Sign on to the Marketo console as an administrator.
2. Select **Admin** in the toolbar.
3. Select **Other Stuff** in the left navigation pane.
4. Select **Single Sign-On**.

> **Note**
>
> If you don't see **Single Sign-On**, contact support@marketo.com to enable SAML for your account.

5. Next to **SAML Settings**, select **Edit**.
6. For the **Issuer ID**, enter the value you entered for the **IdP Entity ID** in PingFederate.
7. For the **Entity ID**, enter the value you entered for the **IdP Entity ID** in PingFederate.
8. For the **User ID** Location, click the **In Name identifier** element of **Subject**.
9. Click **Browse** next to **Identity Provider Certificate** and upload your public certificate.
10. Click **Save**.

Test the PingFederate IdP-initiated SSO Integration

1. Go to the PingFederate SSO Application Endpoint for the Marketo SP connection.
2. Authenticate with PingFederate.

   You're redirected to your Marketo domain.

Configuring SAML SSO with Marketo and PingOne

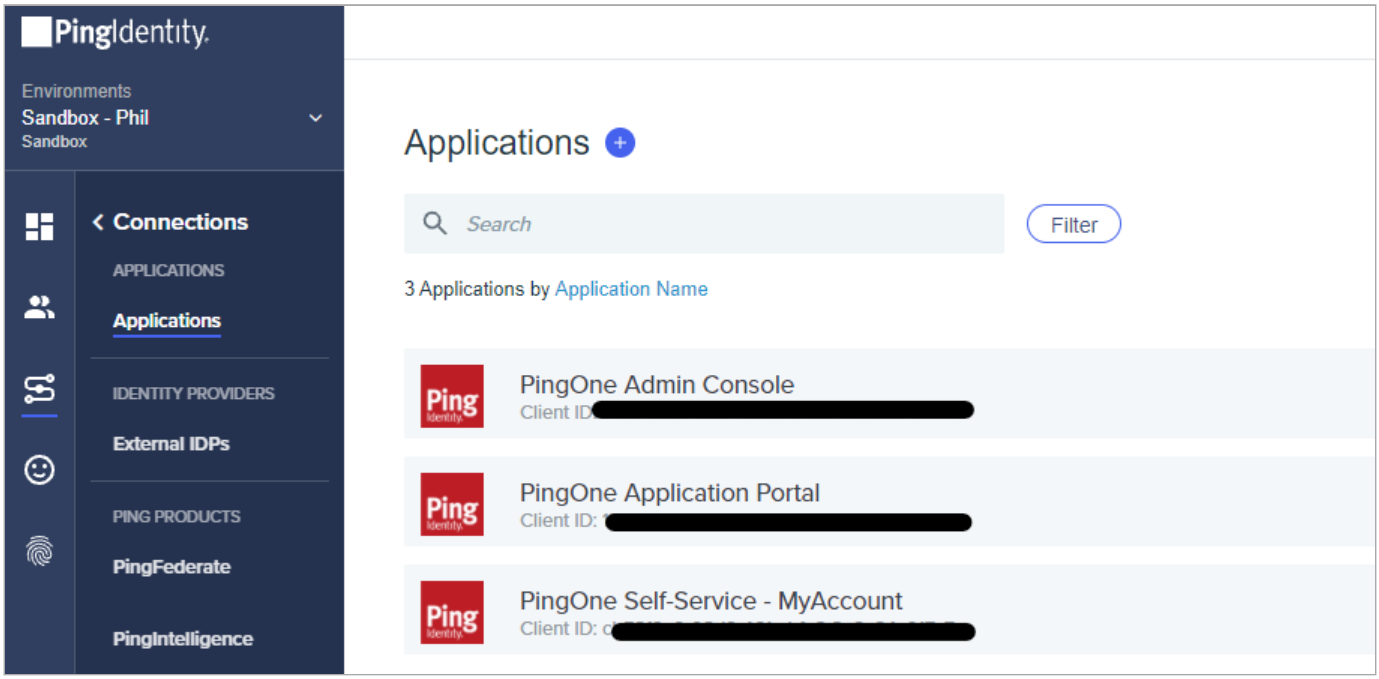
Learn how to enable Marketo sign-on from PingOne (IdP-initiated sign-on).

Before you begin

- Link PingOne to an identity repository containing the users requiring application access.
- Populate Marketo with at least one user to test access.
- Gather your Munchkin Account ID.
- You must have administrative access to PingOne and an admin account on Marketo.

Add the Marketo Application to PingOne

1. In PingOne, go to **Connections → Applications** and click the + icon.



2. When you're prompted to select an application type, select **WEB APP** and then click **Configure** next to **SAML** for the chosen connection type.
3. Enter `Marketo` as the application name.
4. Enter a suitable description.
5. **Optional:** Upload an icon.
6. Click **Next**.
7. For **Provide App Metadata**, select **Enter Manually**.
8. For **ACS URLS**, enter `https://login.marketo.com/saml/assertion/your-Munchkin-account-ID`.
9. For **EntityID** enter `https://login.marketo.com/saml/your-Munchkin-account-ID`.
10. Choose the **Signing Key** to use and then click **Download Signing Certificate** to download as X509 PEM (.crt).
11. Leave **SLO Endpoint** and **SLO Response Endpoint** blank.
12. In the **Subject NameID Format** list, select **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.
13. Enter a suitable value for **Assertion Validity Duration (in seconds)**. A value of 300 seconds is typical.
14. Click **Save and Continue**.
15. Marketo expects an email address to identify a user in the SSO security assertion:
    - If you use an email address to sign on through PingOne, click **Save and Close**.
    - If you sign on with a username, in the **PingOne User Attribute** list, select **Email Address** to map that to the **SAML_SUBJECT**, then click **Save and Close**.
16. Click the toggle to enable the application.

17. On the Configuration tab of the newly-created Marketo application, copy and save the **IDP Metadata URL** value.

    You'll need this when configuring SAML on Marketo.

Enable SAML SSO with Marketo

1. Sign on to the Marketo console as an administrator.
2. Select **Admin** in the toolbar.
3. Select **Other Stuff** in the left navigation pane.
4. Select **Single Sign-On**.

> **Note**
>
> If you don't see **Single Sign-On**, contact support@marketo.com to enable SAML for your account.

5. Select **Edit** next to **SAML Settings**.
6. For the **Issuer ID**, enter the value you entered for the **IdP Entity ID** in PingOne.
7. For the **Entity ID**, enter the value you entered for the **IdP Entity ID** in PingOne.
8. For the **User ID** Location, click the **In Name identifier** element of **Subject**.
9. Click **Browse** next to **Identity Provider Certificate** and upload your public certificate.
10. Click **Save**.

Test the PingOne IdP integration

1. Go to the PingOne Application Portal and sign on with a user account.

> **Note**
>
> In the Admin console, go to **Dashboard → Environment Properties** to find the **PingOne Application Portal URL**.

2. Click the Marketo icon.

   You're redirected to the Marketo website and signed on with SSO.

Microsoft 365

Configuring SAML SSO with Microsoft 365 and PingFederate

Learn how to enable Microsoft 365 sign-on from a PingFederate URL (IdP-initiated sign-on) and direct Microsoft 365 sign-on using PingFederate (SP-initiated sign-on).

Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Make sure Microsoft 365 has a valid, non-default domain and is populated with at least one AD synced user in that domain to test access.
- You must have administrative access to PingFederate and Microsoft 365.
- You must have access to run the Microsoft Azure Active Directory Module for Windows PowerShell.

Create a PingFederate SP connection for Microsoft 365

1. Download the Microsoft 365 SAML metadata from https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml.
2. Sign on to the PingFederate administrative console.
3. Create an SP connection for Microsoft 365 in Ping Federate:
    1. Configure using **Browser SSO** profile **SAML 2.0**.
    2. Import the metadata from the downloaded Microsoft 365 metadata file.
    3. Enable the following **SAML Profiles**:
        - **IdP-Initiated SSO**
        - **SP-Initiated SSO**
        - **SP Initiated SLO**
    4. In **Assertion Creation: Attribute Contract**, extend the contract to add the attributes **guid** and **SAML_NAME_FORMAT**.
    5. In **Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment** map the following:
        - **SAML_SUBJECT** to **guid** (**guid** should map to your attribute holding the Microsoft 365 user objectID and be in Base64 binary format)
        - **SAML_NAME_FORMAT** to **urn:oasis:names:tc:SAML:2.0:nameid-format:persistent**.

6. In **Protocol Settings: Allowable SAML Bindings**, enable **POST** and **REDIRECT**.
7. In **Protocol Settings: Signature Policy**, select **Always Sign Assertion**.
8. In **Credentials: Digital Signature Settings**, select the PingFederate signing certificate.

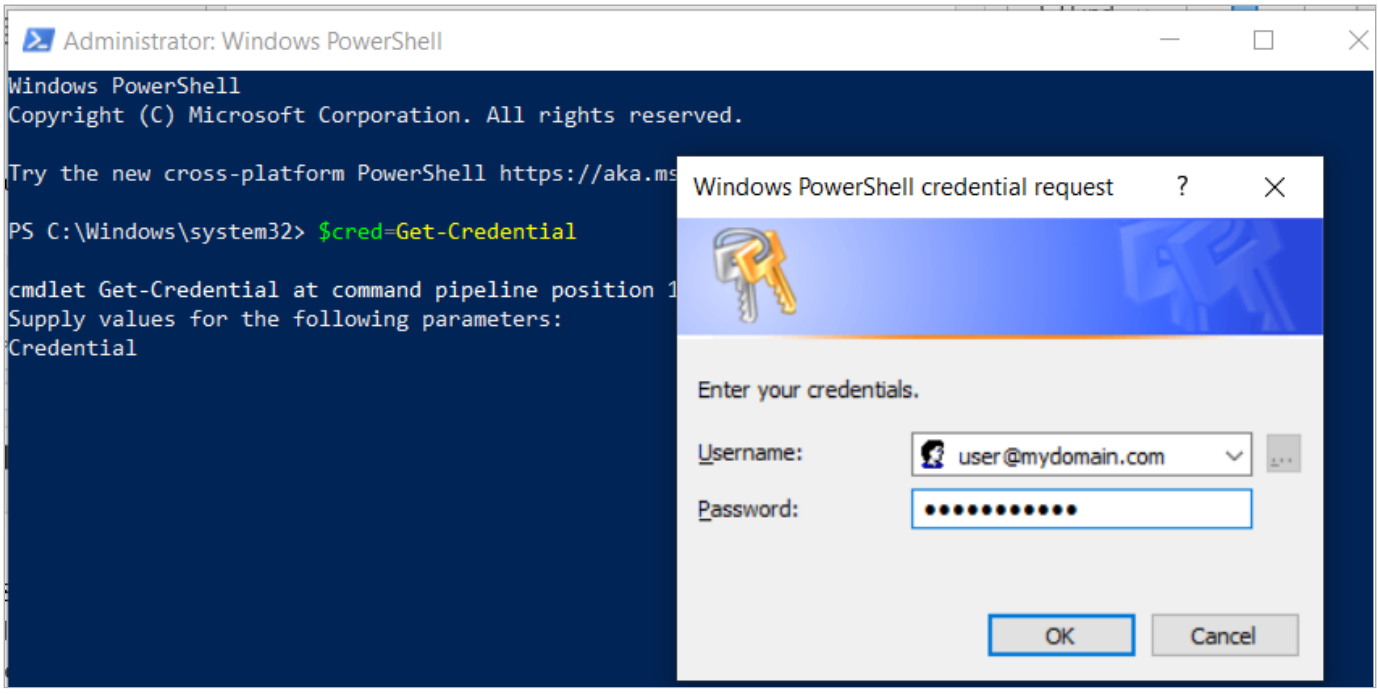
4. Save the configuration.
5. Export the signing certificate.
6. Export and then open the metadata file and copy the values for the following:
   - entityID
   - Location entry for SSO (`https://your-value/idp/SSO.saml2`)
   - Location entry for SLO (`https://your-value/idp/SLO.saml2`)

Add the PingFederate connection to Microsoft 365

1. Open an elevated Windows PowerShell Command Prompt window on any internet-connected computer and type:

```
$cred = Get-Credential
```

2. Enter the username and password of your Microsoft 365 administrator account in the pop-up.



3. Connect with MsolService.

```
Connect-MsolService -Credential $cred
```

4. List your domains.

```
Get-MsolDomain
```

5. Select the domain for which you would like to enable SSO.

```
$dom = "your-O365-domain"
```

6. Set the `uri` parameter to the PingFederate **entityID** value.

```
$uri ="your-entityID"
```

7. Set the `url` parameter to the PingFederate **Location for SSO** value.

```
$url="your-Passive-Log-On-Uri"
```

8. Set the `logouturl` parameter to the PingFederate **Location for SLO** value.

```
$logouturl="your-Log-Off-Uri"
```

9. Open the downloaded signing certificate in Notepad, copy the encoded contents, and paste them into the command below to set the certificate parameter.

```
$cert="your-certificate-contents"
```

10. Run the following command to setup SAML SSO for your domain.

```
Set-MsolDomainAuthentication `
-DomainName $dom `
-FederationBrandName $dom `
-Authentication Federated `
-PassiveLogOnUri $url `
-SigningCertificate $cert `
-IssuerUri $uri `
-LogOffUri $logouturl `
-PreferredAuthenticationProtocol SAMLP
```

11. Run the following command to see the completed SSO settings.

```
Get-MSolDomainFederationSettings -DomainName "your-O365-domain" | Format-List *
```

Test the PingFederate IdP-initiated SSO integration

1. Go to the PingFederate SSO application endpoint for the Microsoft 365 SP connection.
2. Complete PingFederate authentication.

   You're redirected to your Microsoft 365 domain.

Test the PingFederate SP-initiated SSO integration

1. Go to https://portal.office.com.
2. Enter your email address.
3. After you're redirected to PingFederate, enter your PingFederate username and password.

   You're redirected back to Microsoft 365.

Configuring SAML SSO with Microsoft 365 and PingOne for Enterprise

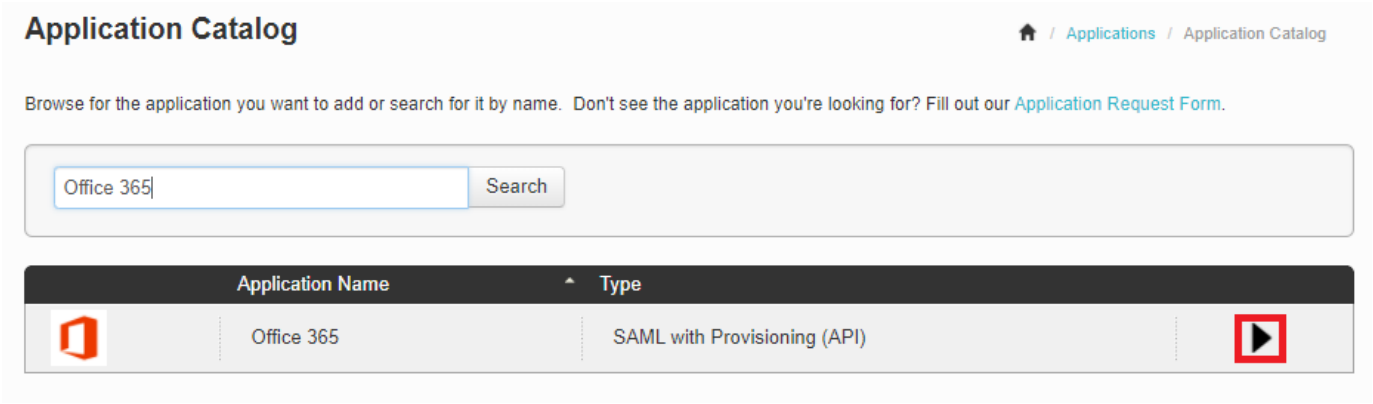
Learn how to enable Microsoft 365 sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct Microsoft 365 sign-on using PingOne for Enterprise (SP-initiated sign-on).

Before you begin

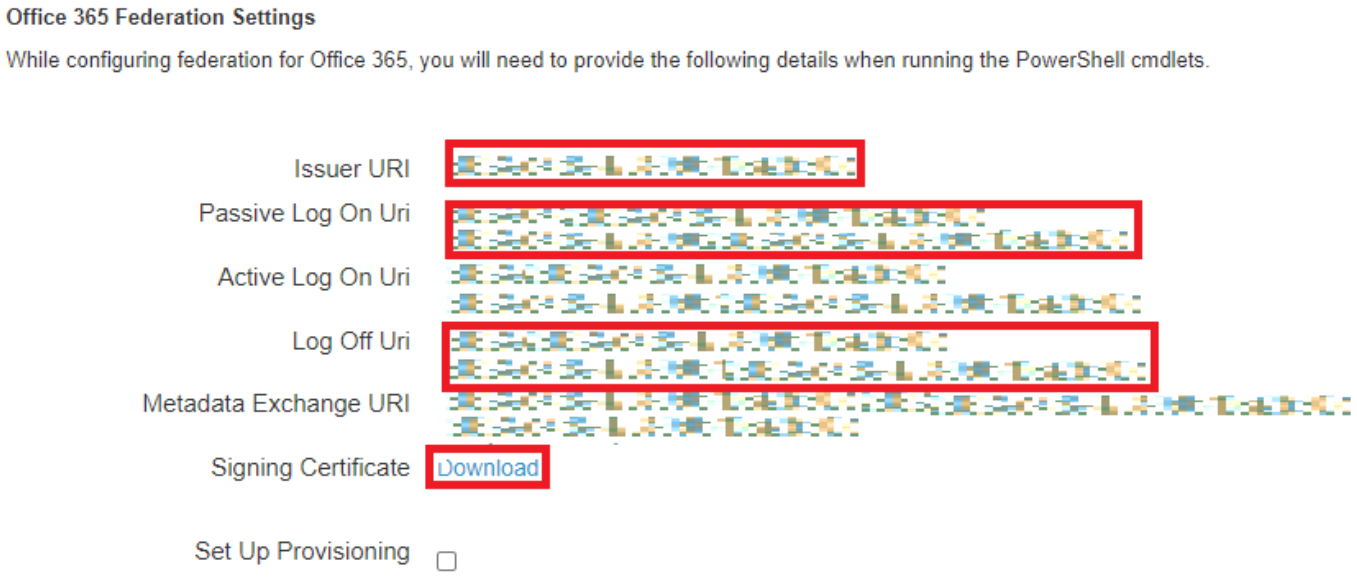
- Link PingOne for Enterprise to an identity repository containing the users requiring application access. Learn more in Connecting to an identity repository in the PingOne for Enterprise documentation.
- Make sure Microsoft 365 has a valid, non-default domain and is populated with at least one AD synced user in that domain to test access.
- You must have administrative access to PingOne for Enterprise and Microsoft 365.
- You must have access to run the Microsoft Azure Active Directory Module for Windows PowerShell.

Obtain the PingOne for Enterprise values for the Microsoft 365 application

1. Sign on to PingOne for Enterprise and go to **Applications → Application Catalog**.
2. Search for `Microsoft 365`.
3. Expand the Microsoft 365 entry and click the **Setup** icon.



4. Click **Continue to Next Step**.
5. Copy the **Issuer URI**, **Passive Log On Uri**, and **Log Off Uri** values.
6. Download the signing certificate.

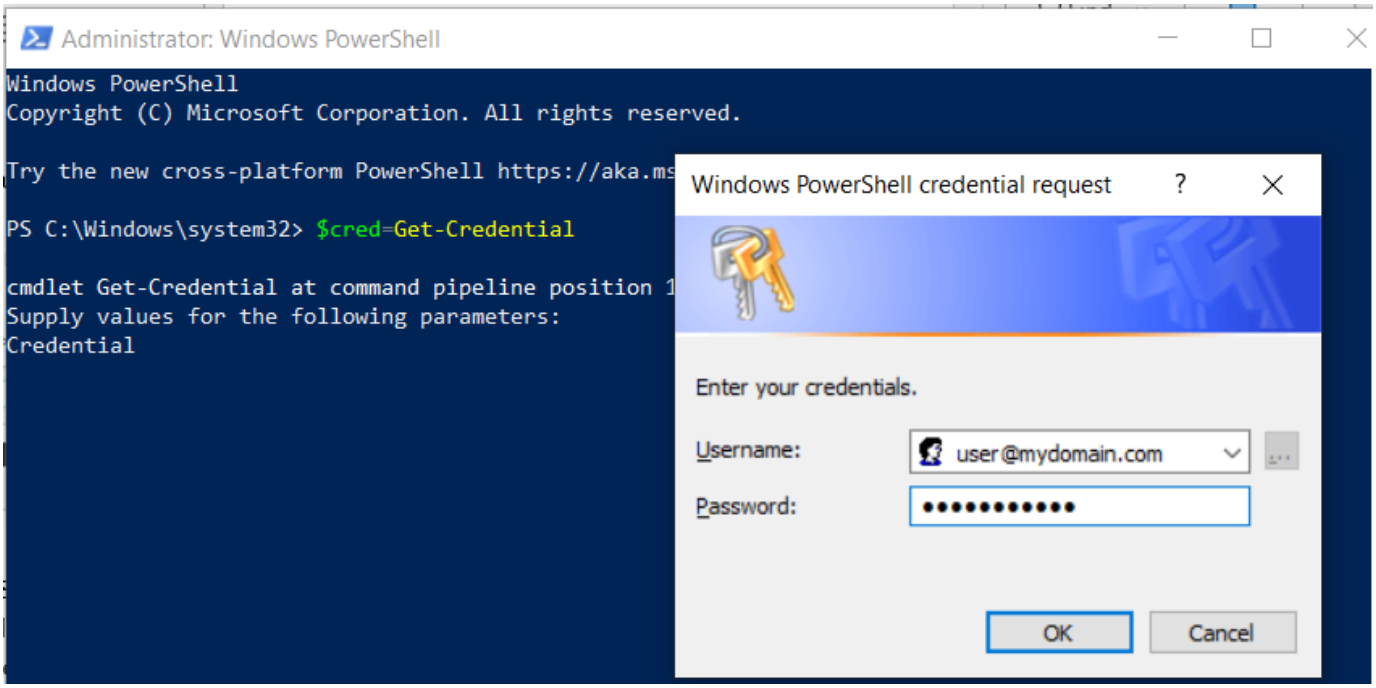


Add the PingOne for Enterprise IdP Connection to Microsoft 365

1. Open an elevated Windows PowerShell Command Prompt window on any internet-connected computer and type:

```
$cred = Get-Credential
```

2. Enter the username and password of your Microsoft 365 administrator account in the pop-up.



3. Connect with `MsolService`.

```
Connect-MsolService -Credential $cred
```

4. List your domains.

```
Get-MsolDomain
```

5. Enter the domain for which you would like to enable SSO.

```
$dom = "your-O365-domain"
```

6. Set the `uri` parameter to the PingOne for Enterprise **Issuer URI** value.

```
$uri ="your-Issuer-URI"
```

7. Set the `url` parameter to the PingOne for Enterprise **Passive Log On Uri** value.

```
$url="your-Passive-Log-On-Uri"
```

8. Set the `logouturl` parameter to the PingOne for Enterprise **Log Off Uri** value.

```
$logouturl="your-Log-Off-Uri"
```

9. Open the downloaded signing certificate in Notepad, copy the encoded contents, and paste them into the command below to set the certificate parameter.

```
$cert=your-certificate-contents
```

10. Run the following command to set up SAML SSO for your domain.

```
Set-MsolDomainAuthentication `
-DomainName $dom `
-FederationBrandName $dom `
-Authentication Federated `
-PassiveLogOnUri $url `
-SigningCertificate $cert `
-IssuerUri $uri `
-LogOffUri $logouturl `
-PreferredAuthenticationProtocol SAMLP
```

11. Run the following command to see the completed SSO settings.

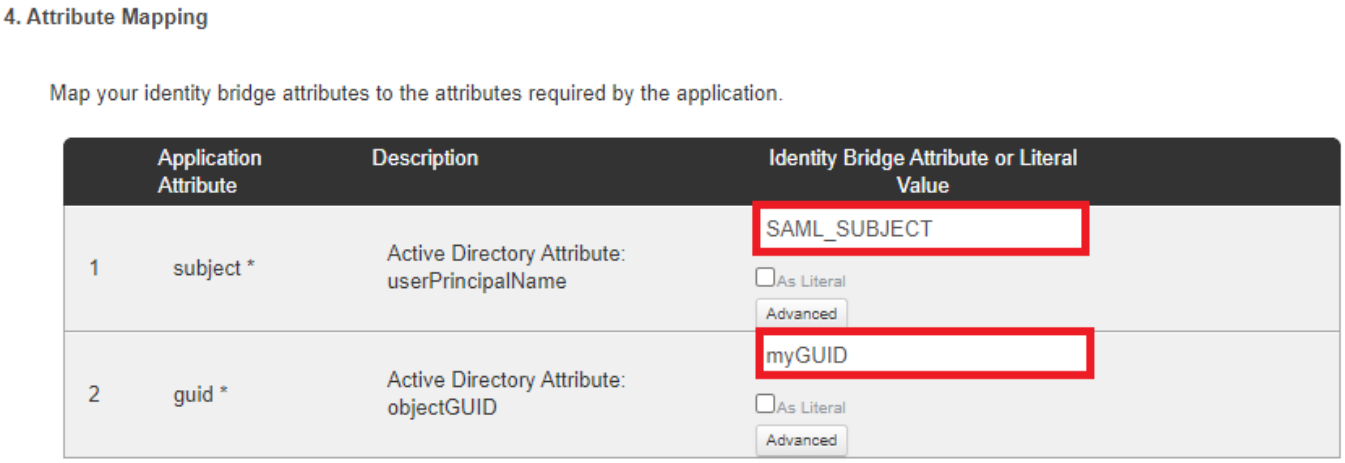
```
Get-MSolDomainFederationSettings -DomainName "your-O365-domain" | Format-List *
```

Complete the Microsoft 365 setup in PingOne for Enterprise

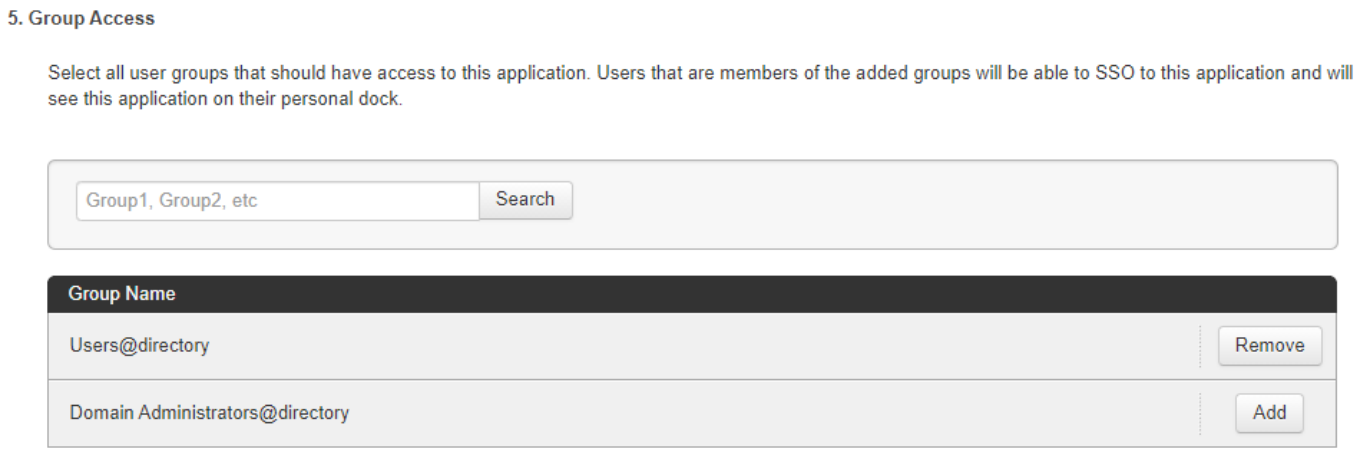
1. Continue editing the Microsoft 365 entry in PingOne for Enterprise.

> **Note**
>
> If the session has timed out, complete the initial steps to the point of clicking **Setup**.

2. Click **Continue to Next Step** until you reach the **Attribute mapping** page.
3. Map **subject** to **SAML_SUBJECT**.
4. Map **guid** to your attribute containing the Microsoft 365 user objectGUID.



5. Click **Continue to Next Step** twice.
6. Click **Add** for all user groups that should have access to Microsoft 365.



7. Click **Continue to Next Step**.
8. Click **Finish**.

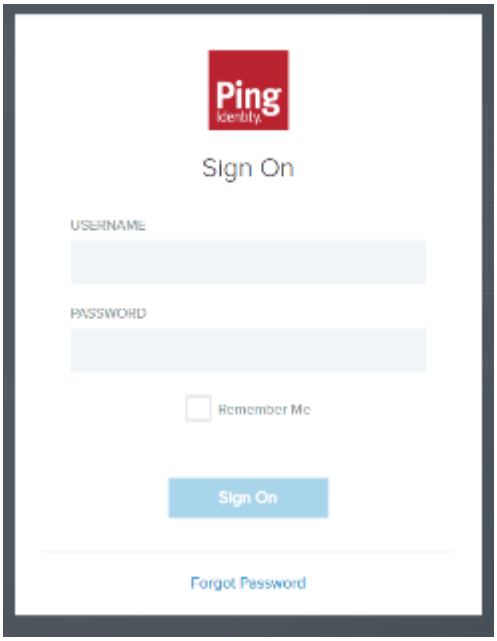
Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with Microsoft 365 access.

> **Note**
>
> To find the Ping desktop URL in the Admin console, go to **Setup → Dock → PingOne Dock URL**.

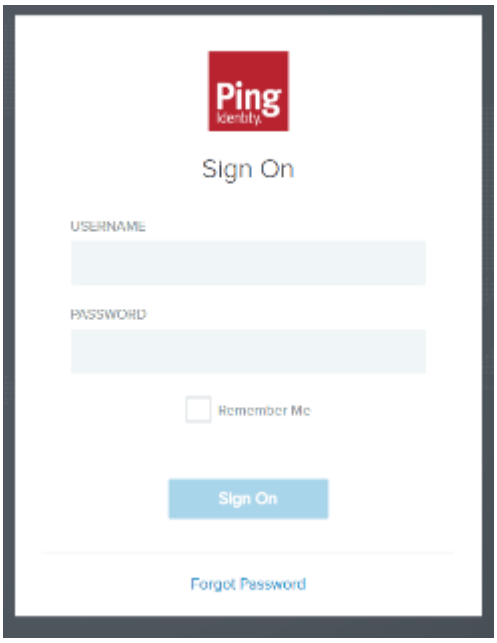
2. Complete PingOne for Enterprise authentication.

   You're redirected to your Microsoft 365 domain.



Test the PingOne for Enterprise SP-initiated SSO integration

1. Go to https://portal.office.com.
2. Enter your email address.
3. After you're redirected to PingOne for Enterprise, enter your PingOne for Enterprise username and password.



You're redirected back to Microsoft 365.

Mimecast

Configuring SAML SSO with Mimecast and PingFederate

Learn how to enable Mimecast sign-on from PingFederate (IdP-initiated sign-on) and direct Mimecast sign-on using PingFederate (SP-initiated sign-on).

Before you begin

- Configure PingFederate to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- Populate Mimecast with at least one user to test access.
- You must have administrative access to PingFederate.

Create the Mimecast metadata

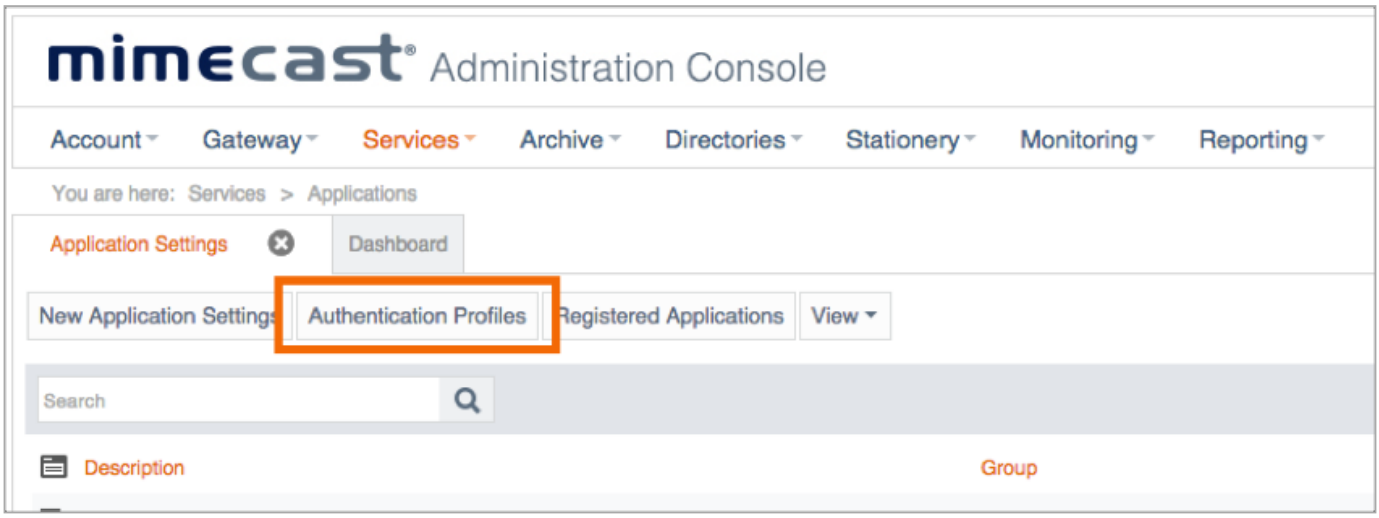
1. In PingFederate, create a service provider (SP) connection for Mimecast:
    1. Configure using **Browser SSO** profile **SAML 2.0**.
    2. Set **Partner's Entity ID** to `your-Mimecast-account-hosting-location-api.mimecast.com.accountcode`.
    3. Enable the following SAML profiles:
        - **IdP-Initiated SSO**
        - **SP-Initiated SSO**
    4. In **Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfilment**, map the **SAML_SUBJECT** to your email attribute.
    5. In **Protocol Settings: Assertion Consumer Service URL**, set **Binding** to **POST** and set **Endpoint URL** to `https://your-Mimecast-account-hosting-location-api.mimecast.com/sign on/saml`.
    6. In **Protocol Settings: Allowable SAML Bindings**, enable **POST**.
    7. In **Credentials: Digital Signature Settings**, select the **PingFederate Signing Certificate**.

    > **Note**
    >
    > Note the metadata URL for the newly-created Mimecast SP connection.

Add the PingFederate connection to Mimecast

1. Sign on to the Mimecast console as an administrator.

2. Select **Administration** on the lefthand pane.
3. Click the **Services** tab.
4. Select **Application Settings**.
5. Select **Authentication Profiles**.



6. Click **New Authentication Profile**.
7. Select the **Enforce SAML Authentication for Administration Console** option.

   The page expands to reveal the **SAML Settings**.
8. Under **Provider**, select **Other**.
9. Enter the **Metadata URL** for the Mimecast SP Connector in PingFederate.

Test the PingFederate IdP-initiated SSO integration

1. Go to the PingFederate SSO Application Endpoint for the Mimecast SP connection.
2. Authenticate with PingFederate.

   You're redirected to your Mimecast domain.

Test the PingFederate SP-initiated SSO integration

1. Sign on to Mimecast.
2. After you're redirected to PingFederate, enter your PingFederate username and password.

   After successful authentication, you're redirected back to Mimecast.

Configuring SAML SSO with Mimecast and PingOne

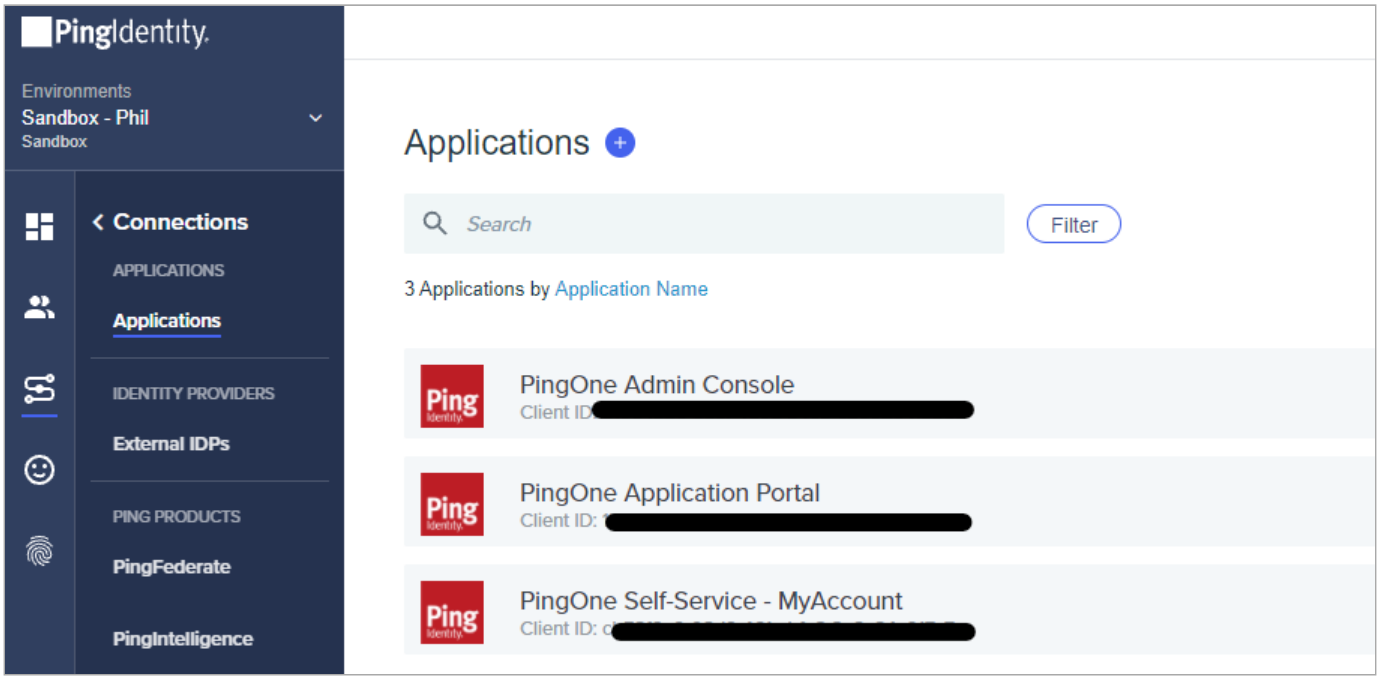
Learn how to enable Mimecast sign-on from the PingOne console (IdP-initiated sign-on) and direct Mimecast sign-on using PingOne (SP-initiated sign-on).

Before you begin

- Link PingOne to an identity repository containing the users requiring application access.
- Populate Mimecast with at least one user to test access.
- You must have administrative access to PingOne and a Super Admin account for an Enterprise Organization on Mimecast.

Add the Mimecast application to PingOne

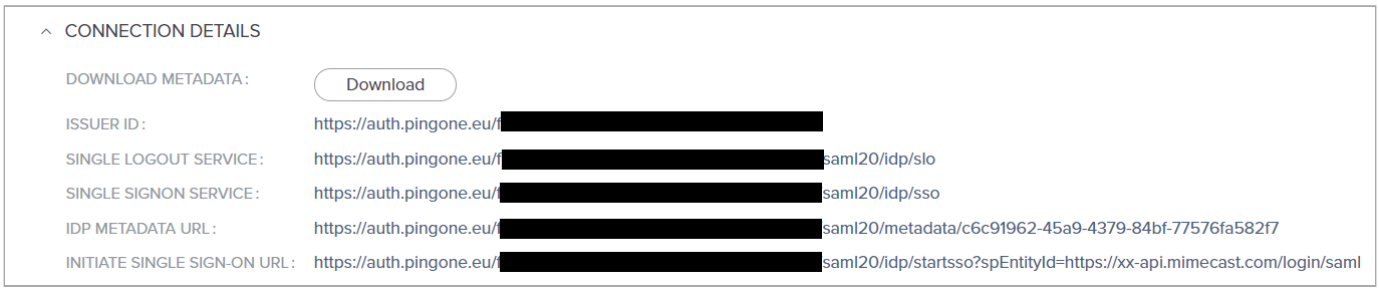
1. In PingOne, go to **Connections → Applications** and click the + icon.



2. When you're prompted to select an application type, select **WEB APP** and then click **Configure** next to **SAML** for the chosen connection type.
3. Enter `Mimecast` as the application name.
4. Enter a suitable description.
5. **Optional:** Upload an icon.
6. Click **Next**.
7. For **Provide App Metadata**, select **Enter Manually**.
8. In the **ACS URL** field, enter `https://account-hosting-location-api.mimecast.com/login/saml`.
9. Select the **Signing Key** to use and then click **Download Signing Certificate** to download as X509 PEM (.crt).

10. For **Entity ID**, enter `https://account-hosting-location-api.mimecast.com.accountcode`.
11. Leave **SLO Endpoint** and **SLO Response Endpoint** blank.
12. In the **Subject NameID Format** list, select **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.
13. Enter a suitable value for **Assertion Validity Duration (in seconds)**. A value of 300 seconds is typical.
14. Click **Save and Continue**.
15. Mimecast expects an email address to identify a user in the SSO security assertion:
    - If you use an email address to sign on through PingOne, click **Save and Close**.
    - If you sign on with a username, in the **PingOne User Attribute** list, select **Email Address** to map that to the **SAML_SUBJECT**, then click **Save and Close**.
16. Click the toggle to enable the application.
17. On the **Configuration** tab of the newly-created Mimecast application, copy and save the **IDP Metadata URL** value.

    You'll need this metadata when configuring SAML on Mimecast.



Add PingOne as identity provider (IdP) in Mimecast

1. Sign on to Mimecast with an Admin account for your Enterprise Organization.
2. Go to **Administration → Services → Applications**.
3. Select **Authentication Profiles**.
4. Select **New Authentication Profile**.
5. Enter a **Description** for the new profiled.
6. Select **Enforce SAML Authentication for Administration Console**.
7. For **Provider**, select **Other**.
8. In the **Metadata URL** field, enter the URL value that you copied previously.
9. Go to **Administration → Services → Applications**.
10. Click **Lookup** to find the authentication profile that you created.
11. Click **Save and Exit**.

Test the PingOne IdP integration

1. Go to the PingOne Application Portal and sign on with a user account.

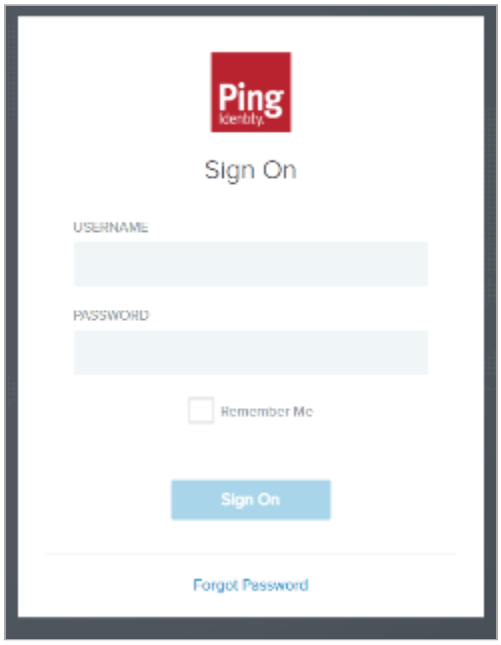
   > **Note**
   >
   > In the Admin console, go to **Dashboard → Environment Properties** to find the **PingOne Application Portal URL**.

2. Click the Mimecast icon.

   You're redirected to the Mimecast website and logged in with SSO.

Test the PingOne SP integration

1. Go to login.mimecast.com, and choose the option to sign on with SSO. Enter your email address only.
2. In the PingOne sign-on prompt, enter your PingOne username and password.



   You're redirected back to Mimecast and signed on.

Namely

Configuring SAML SSO with Namely and PingFederate

Learn how to enable Namely sign-on from the PingFederate console (IdP-initiated sign-on) and direct Namely sign-on using PingFederate (SP-initiated sign-on).

Before you begin

- PingFederate should be configured to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- Populate Namely with at least one user to test access.
- You must have administrative access to PingFederate.

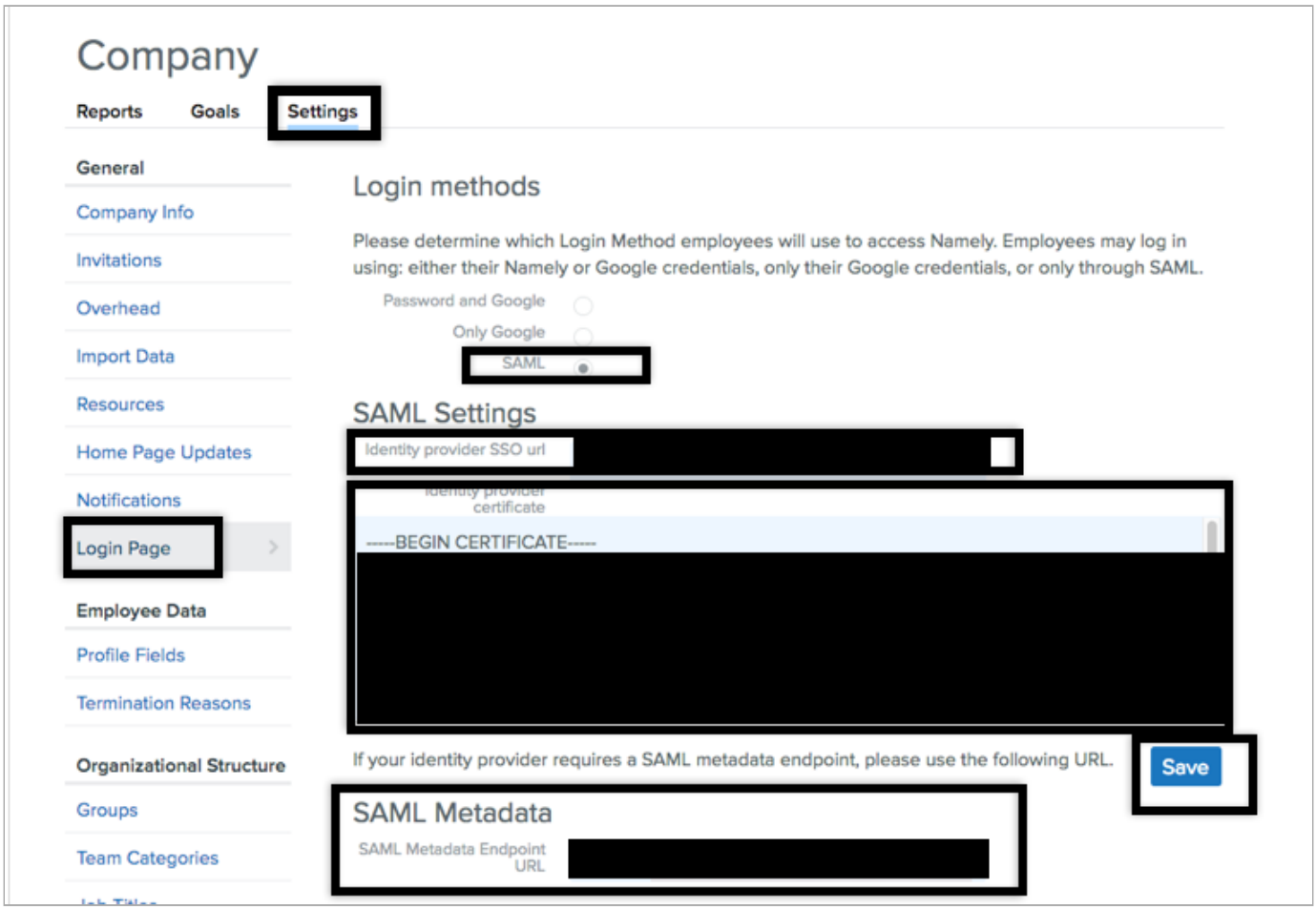
Create the Namely metadata

1. In PingFederate, create a service provider (SP) connection for Namely:
    1. Configure using **Browser SSO** profile **SAML 2.0**.
    2. Set **Partner's Entity ID** to `https://your-subdomain.namely.com/saml/metadata`.
    3. Enable the following SAML profiles:
        - **IdP-Initiated SSO**
        - **SP-Initiated SSO**
    4. In **Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfilment,** map the **SAML_SUBJECT** to your email attribute.
    5. In **Protocol Settings: Assertion Consumer Service URL**, set **Binding** to **POST** and set **Endpoint URL** to `https://your-subdomain.namely.com/saml/consume`.
    6. In **Protocol Settings: Allowable SAML Bindings**, enable **POST**.
    7. In **Credentials: Digital Signature Settings**, select the **PingFederate Signing Certificate**.
    8. Note the metadata URL for the newly-created Namely SP connection.

Add the PingFederate connection to Namely

1. Sign on to the Namely console as an administrator.
2. Select **Company** on the top navigation bar.

3. Click the **Settings** tab.
4. In the left navigation pane, click **Login Page**.
5. In the **Login Methods** section, click **SAML**.
6. Enter the **Identity Provider SSO URL** from PingFederate.
7. Copy and paste the IdP Provider Certificate value into the **Identity provider certificate**.
8. Enter the **SAML Metadata URL** from PingFederate.



9. Click **Save**.

Test the PingFederate IdP-initiated SSO integration

1. Go to the PingFederate SSO Application Endpoint for the Namely SP connection.
2. Authenticate with PingFederate.

   You're redirected to your Namely domain.

Test the PingFederate SP-initiated SSO integration

1. Go to `https://your-subdomain.namely.com/users/login`.

2. After you're redirected to PingFederate, enter your PingFederate username and password.

   You're redirected back to Namely.

Configuring SAML SSO with Namely and PingOne

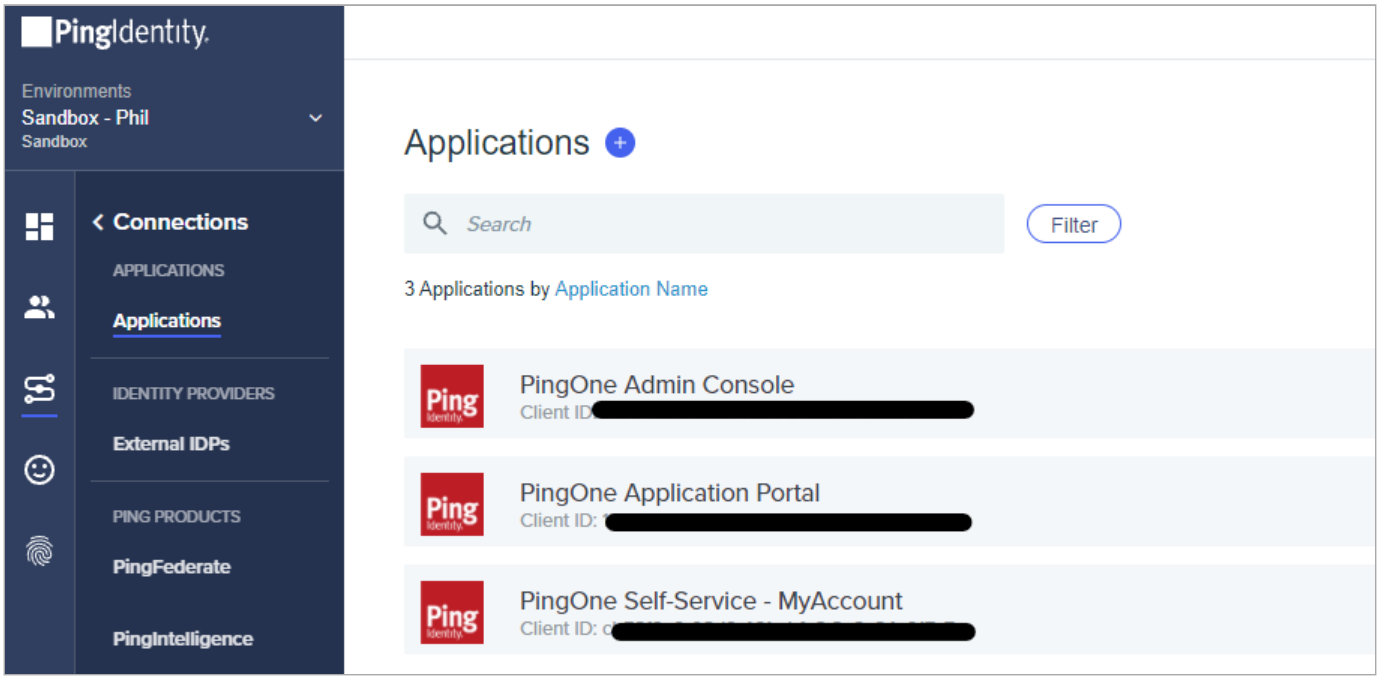
Learn how to enable Namely sign-on from the PingOne console (IdP-initiated sign-on) and direct Namely sign-on using PingOne (SP-initiated sign-on).

Before you begin

- Link PingOne to an identity repository containing the users requiring application access.
- Populate Namely with at least one user to test access.
- You must have administrative access to PingOne and an Admin account on Namely.

Add the Namely application to PingOne

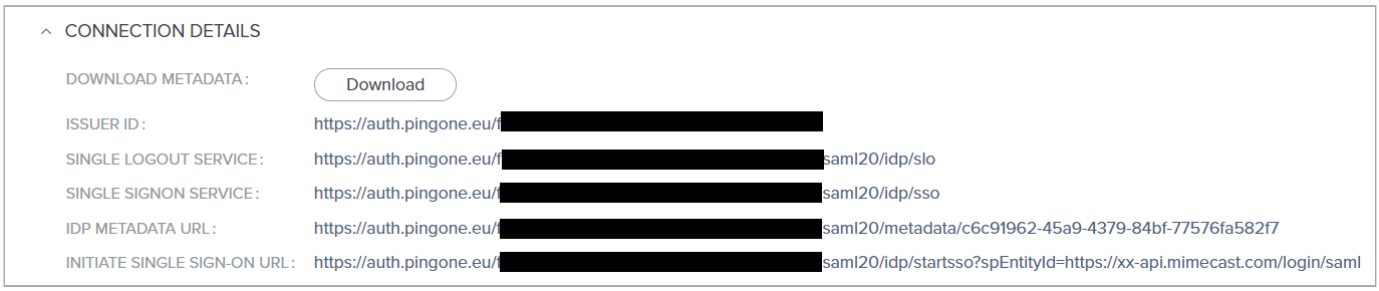
1. In PingOne, go to **Connections → Applications** and click the + icon.



2. When you're prompted to select an application type, select **WEB APP** and then click **Configure** next to **SAML** for the chosen connection type.
3. Enter `Namely` as the application name.
4. Enter a suitable description.
5. **Optional:** Upload an icon.
6. Click **Next**.

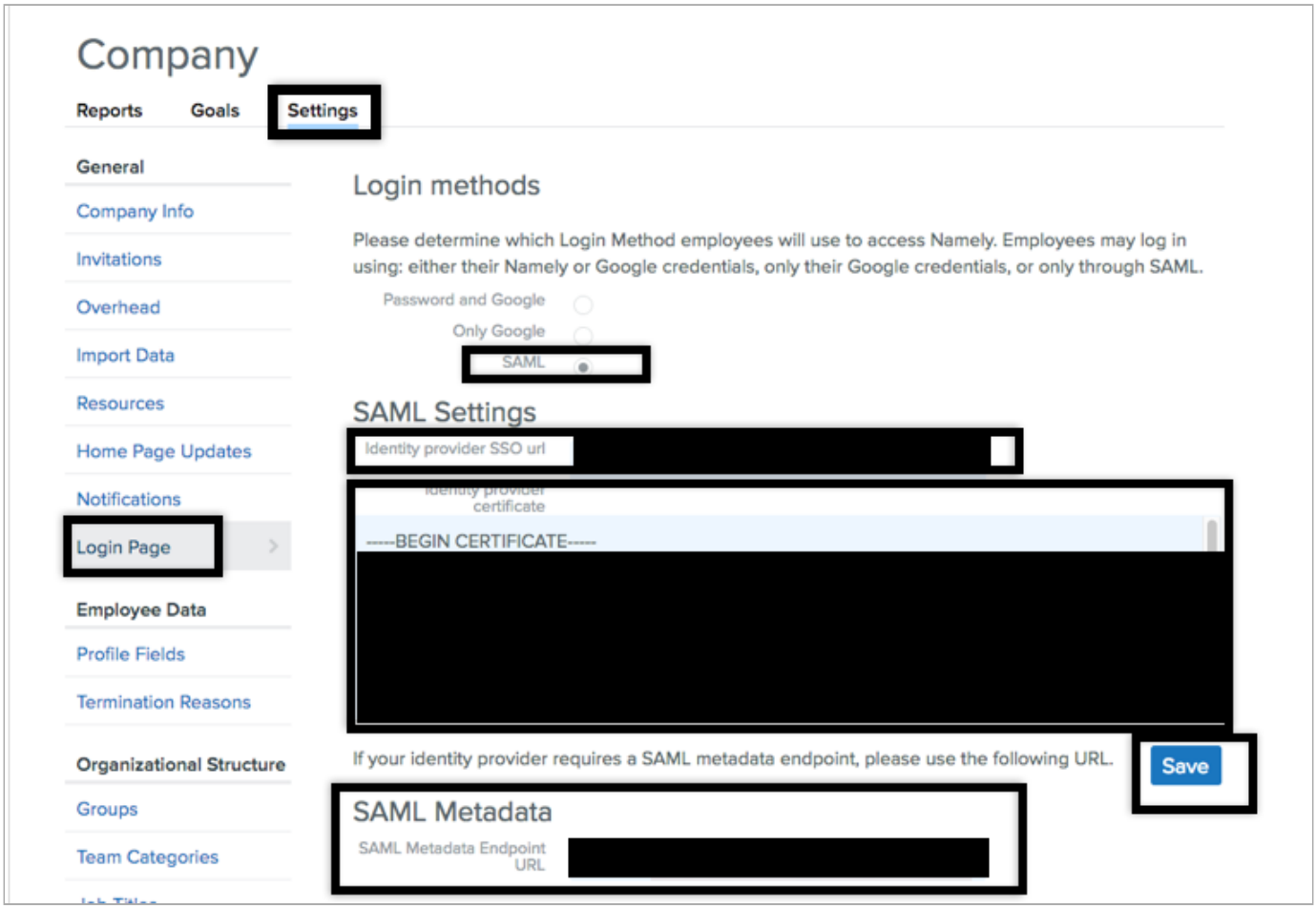
7. For **Provide App Metadata**, select **Enter Manually**.
8. In the **ACS URLS** field, enter `https://your-subdomain.namely.com/saml/consume`.
9. In the **Entity ID** field, enter `https://your-subdomain.namely.com/saml/consume`.
10. Select the **Signing Key** to use and then click **Download Signing Certificate** to download as X509 PEM (.crt).
11. Leave **SLO Endpoint** and **SLO Response Endpoint** blank.
12. In the **Subject NameID Format** list, select **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.
13. Enter a suitable value for **Assertion Validity Duration (in seconds)**. A value of 300 seconds is typical.
14. Click **Save and Continue**.
15. Namely expects an email address to identify a user in the SSO security assertion:
    - If you use an email address to sign on through PingOne, click **Save and Close**.
    - If you sign on with a username, in the **PingOne User Attribute** list, select **Email Address** to map that to the **SAML_SUBJECT**, then click **Save and Close**.
16. Click the toggle to enable the application.
17. On the **Configuration** tab of the newly-created Namely application, copy and save the **IDP Metadata URL** value.

    You'll need this when configuring SAML on Namely.



Enable SAML SSO in Namely

1. Sign on to the Namely console as an administrator.
2. Select **Company** on the top navigation bar.
3. Click the **Settings** tab.
4. In the left navigation pane, click **Login Page**.
5. In the **Login Methods** section, click **SAML**.
6. In the **Identity Provider SSO URL** field, enter the **Initiate Single Sign-On URL** value from PingOne.
7. Copy and paste the **IdP Provider Certificate** value into the **Identity provider certificate** field.
8. In the **SAML Metadata** field, enter the **IdP Metadata URL** value from PingOne.



9. Click **Save**.

Test the PingOne IdP integration

1. Go to the PingOne Application Portal and sign on with a user account.

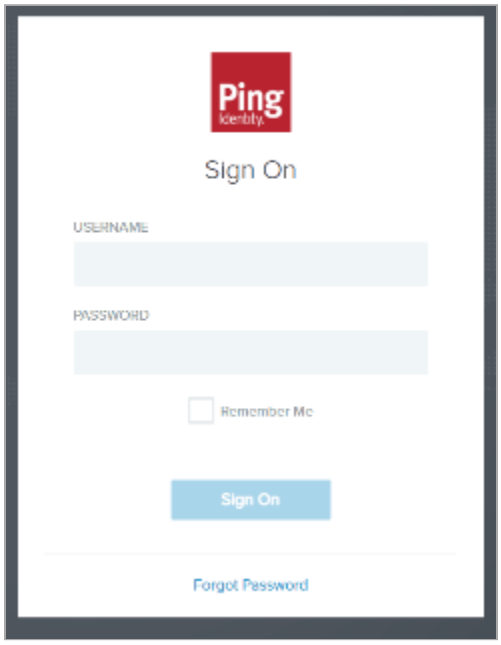
> **Note**
>
> In the Admin console, go to **Dashboard → Environment Properties** to find the **PingOne Application Portal URL**.

2. Click the Namely icon.

   You're redirected to the Namely website and logged in with SSO.

Test the PingOne SP integration

1. Go to `https://your-subdomain.namely.com/users/login` and enter your email address only.
2. In the PingOne sign-on prompt, enter your PingOne username and password.



You’re redirected back to Namely and signed on.

Osano

Configuring SAML SSO with Osano and PingOne

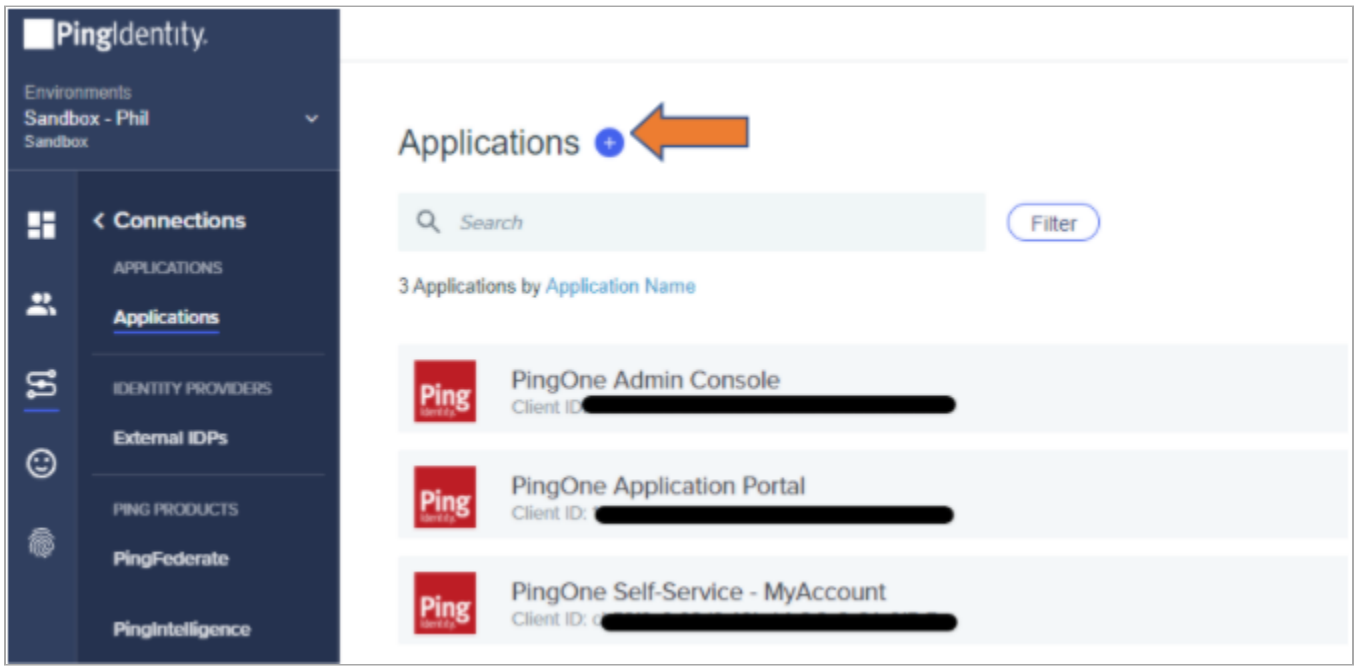
Learn how to enable Osano sign-on from the PingOne console (IdP-initiated sign-on) and direct Osano sign-on using PingOne (SP-initiated sign-on).

Before you begin

- Link PingOne to an identity repository containing the users requiring application access.
- Populate Osano with at least one user to test access.
- You must have administrative access to PingOne and an Admin account for an Enterprise Organization on Osano.

Add the Osano application to PingOne

1. In PingOne, in the left menu, click **Connections**, then **Applications**.
2. To add a new application, click the + icon next to the **Applications** heading.



3. Select **Web App** when prompted to select an application type and click **Configure** next to **SAML** for the chosen connection type.
4. Enter `Osano` as the application name.
5. Enter a suitable description.

6. Upload an icon if desired.
7. Click **Next**.
8. For **Provide App Metadata**, select **Manually Enter**.
9. For ACS URL, enter the value: `https://auth.osano.com/saml2/idpresponse`.
10. Select the **Signing Key** to use and click **Download Signing Certificate** to download as X509 PEM (`.crt`).
11. For **Entity ID**, enter the value: `urn:amazon:cognito:sp:us-east-1_7GtagkRKw`.

> **Note**
>
> Leave **SLO Endpoint** and **SLO Response Endpoint** blank. Osano does not support single logout (SLO).

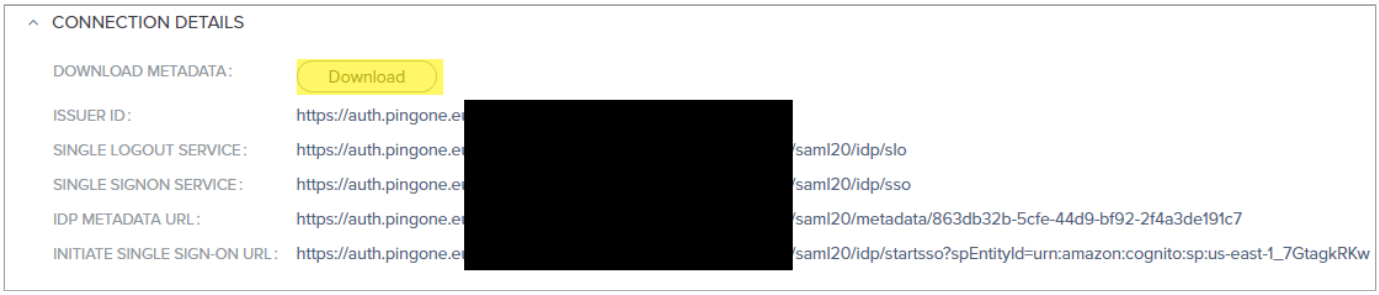
12. In the **Subject** NameID Format list, select **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.
13. Set a suitable value for **Assertion Validity Duration (in seconds)**. A value of 300 seconds is typical.
14. Click **Save and Continue**.
15. Change the **saml_subject** attribute to **Email Address**.

> **Note**
>
> Osano expects an email address to identify a user in the SSO security assertion.

16. Select **Add Attribute** and **Ping One Attribute** and enter `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress` as the **Application Attribute**.

    Map this to the PingOne **User Attribute** for **Email Address**.
17. Select **Add Attribute** and **Ping One Attribute** and enter `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name` as the **Application Attribute**.

    Map this to the **PingOne User Attribute** for **Name**.
18. Click **Save and Close**.
19. Enable user access to this new application by moving the toggle to the right.
20. On the **Configuration** tab of the newly created Osano application, download the metadata.



Add PingOne as the identity provider (IdP) to Osano

1. Open a Support request with your Osano Support Representative and supply the Metadata File exported in the previous procedure. This file should contain the following:
    - **Identity Provider Issuer**
    - **Identity Provider Single Sign-On URL**
    - X.509 Certificate

    Osano configures these settings for your account, and the connection is established.

Test the PingOne IdP integration

1. Go to the PingOne SSO Application Endpoint for the Osano SP connection.
2. Complete the PingOne authentication.

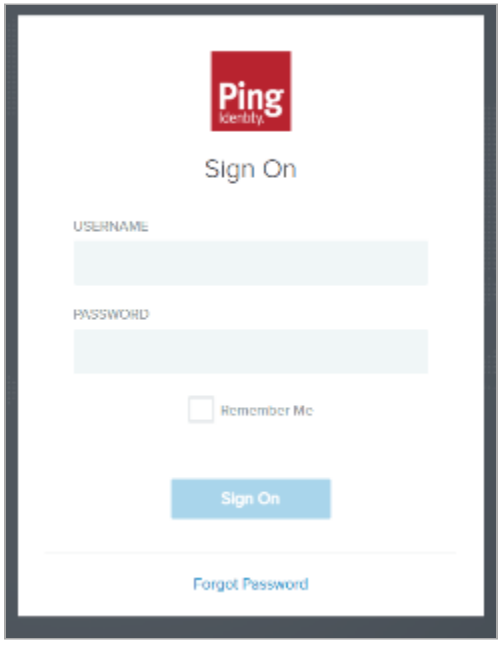
    You're redirected to your Osano domain.

Test the PingOne SP connection

1. Go to https://my.osano.com, select the option to sign on with SSO, and enter your email address only.

    You're redirected and presented with a PingOne sign on prompt.

2. Enter your PingOne username and password.



After successful authentication, you're redirected back to Osano and signed on.

RingCentral

Configuring SAML SSO with RingCentral and PingFederate

Learn how to enable RingCentral sign-on for the PingFederate console (IdP-initiated sign-on) and direct RingCentral sign-on using PingFederate (SP-initiated sign-on).

Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users that need application access.
- Populate RingCentral with at least one user for testing access.
- You must have administrative access to PingFederate and RingCentral.

Export the PingFederate metadata

1. In the PingFederate administrative console, go to **System → Protocol Metadata → Metadata Export**.
2. Select **I am the identity provider** then click **Next**.
3. On the **Metadata Mode** tab, select **Select information to include in metadata manually**. Click **Next**.
4. On the **Protocol** tab, click **Next**.
5. On the **Attribute Contract** tab, click **Next**.
6. On the **Signing Key** tab, select a signing certificate. Click **Next**.
7. **Optional:** On the **Metadata Signing** tab, select a certificate to sign the metadata XML file. Click **Next**.
8. On the **XML Encryption Certificate** tab, click **Next**.
9. On the **Export & Summary** tab, click **Export**.
10. Save the `metadata.xml` file.
11. Click **Done**.

Configure RingCentral for SSO

1. In the RingCentral administrative console, go to **More → Security and Compliance → Single Sign-on**.
2. Select **Set up SSO by yourself**.
3. Upload the PingFederate metadata that you downloaded previously.
4. Select the email attributes to map.

5. In the **Certificate Management** section, upload the certificate and set it as the primary.
6. Download the RingCentral SP metadata file.
7. Toggle **Enable SSO** and click **Save**.

Create a PingFederate SP connection for RingCentral

1. In the PingFederate administrative console, go to **Applications → SP Connections → Create Connection**.
2. Configure using **Browser SSO** profile **SAML 2.0**.
3. Import the RingCentral metadata file that you downloaded previously.
4. Enable the following SAML profiles:
    - **IdP-Initiated SSO**
    - **SP-Initiated SSO**
5. In **Assertion Creation: Attribute Contract**, next to **SAML_SUBJECT**, map the **Subject Name Format** to **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.
6. In **Assertion Creation: Authentication Policy Mapping: Attribute Contract Fulfillment**, map **SAML_SUBJECT** to your email attribute.
7. In **Protocol Settings: Allowable SAML Bindings**, enable **POST** and **REDIRECT**.
8. In **Credentials: Digital Signature Settings**, in the **Signing Certificate** list, select your signing certificate.
9. Note the **SSO Application Endpoint** for your newly-created SP connection.

Test the PingFederate IdP-initiated SSO integration

1. Go to the PingFederate **SSO Application Endpoint** for the RingCentral SP connection.
2. Authenticate with PingFederate.

   You're redirected to RingCentral.

Test the PingFederate SP-initiated SSO integration

1. Go to https://service.ringcentral.com/login/startupSSOLogin.html.
2. Enter your email address and click **Submit**.
3. After you're redirected to PingFederate, enter your PingFederate username and password. s+ You're redirected to RingCentral.

Salesforce

Configuring SAML SSO with Salesforce and PingFederate

Enable Salesforce sign-on from a PingFederate URL (IdP-initiated sign-on) plus single logout (SLO).

Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate Salesforce with at least one user to test access.
- You must have administrative access to PingFederate and Salesforce.

Create a PingFederate SP connection for Salesforce

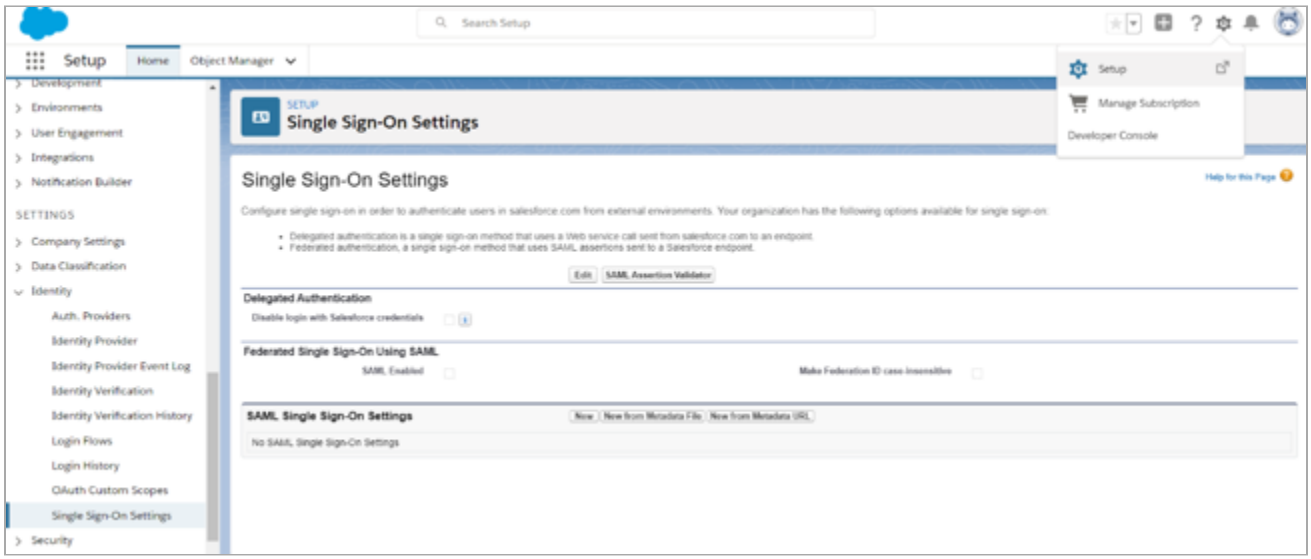
1. Sign on to the PingFederate administrative console.
2. Create an SP connection for Salesforce in PingFederate:
    1. Configure using **Browser SSO** profile **SAML 2.0**.
    2. Set **Partner's Entity ID** to **Entity ID**.
        - Enable the following SAML Profiles:
        - **IDP-Initiated SSO**
        - **SP Initiated SSO**
        - **IDP-Initiated SLO**
        - **SP Initiated SLO**
    3. In **Assertion Creation → Authentication Source Mapping → Attribute Contract Fulfillment**, map the **SAML_SUBJECT** to the attribute containing the Salesforce username.
    4. In **Protocol Settings → Assertion Consumer Service URL**, set **Binding** to **POST** and set **Endpoint URL** to **ACS URL**.
    5. In **Protocol Settings → SLO Service URLs**, set **Binding** to **POST** and set **Endpoint URL** to **SLO URL**.
    6. In **Protocol Settings → Allowable SAML Bindings**, enable **POST**.
    7. In **Credentials → Digital Signature Settings**, select the **PingFederate Signing Certificate**.
    8. In **Credentials → Signature Verification**, set **Trust Model** to **Unanchored**.
    9. In **Credentials → Signature Verification → Signature Verification Certificate**, select the **PingFederate Signing Certificate**.

> **Note**
>
> This certificate is a placeholder and will be replaced with a Salesforce certificate.

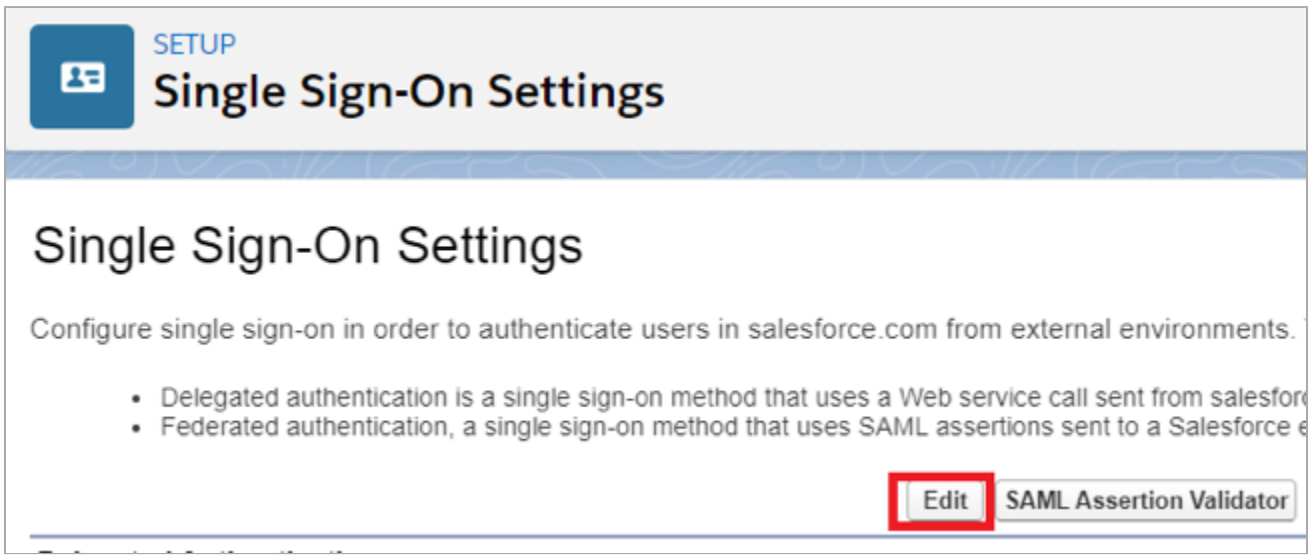
3. Export the metadata for the newly created Salesforce SP connection.
4. Export the signing certificate.

Add the PingFederate IDP Connection to Salesforce

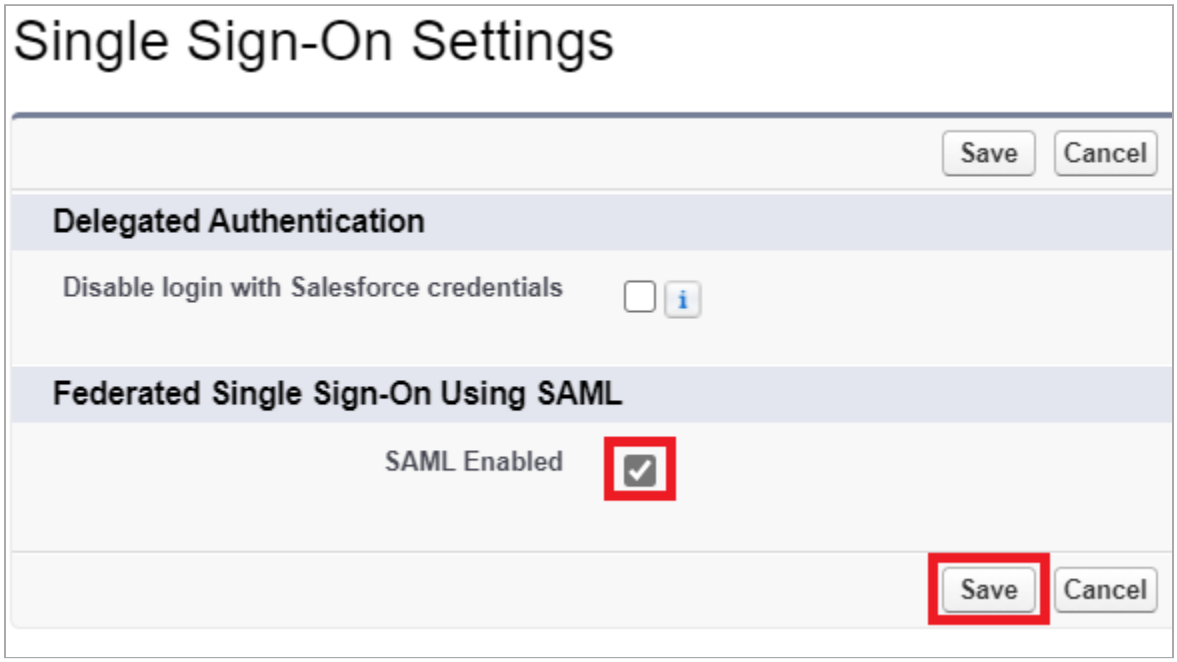
1. Sign on to your Salesforce domain as an administrator.
2. Click the **Gear** icon, then go to **Setup → Identity → Single Sign-On Settings**.



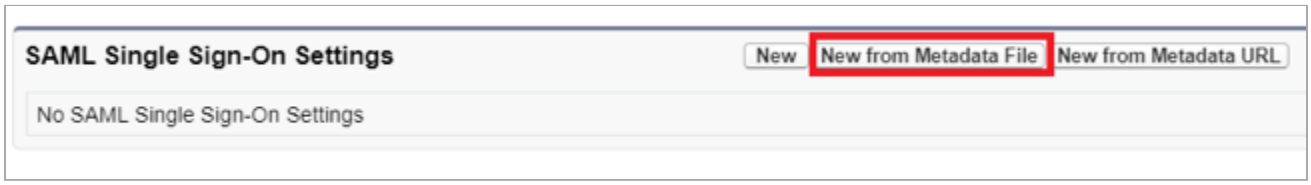
3. On the **Single Sign-On Settings** page, click **Edit**.



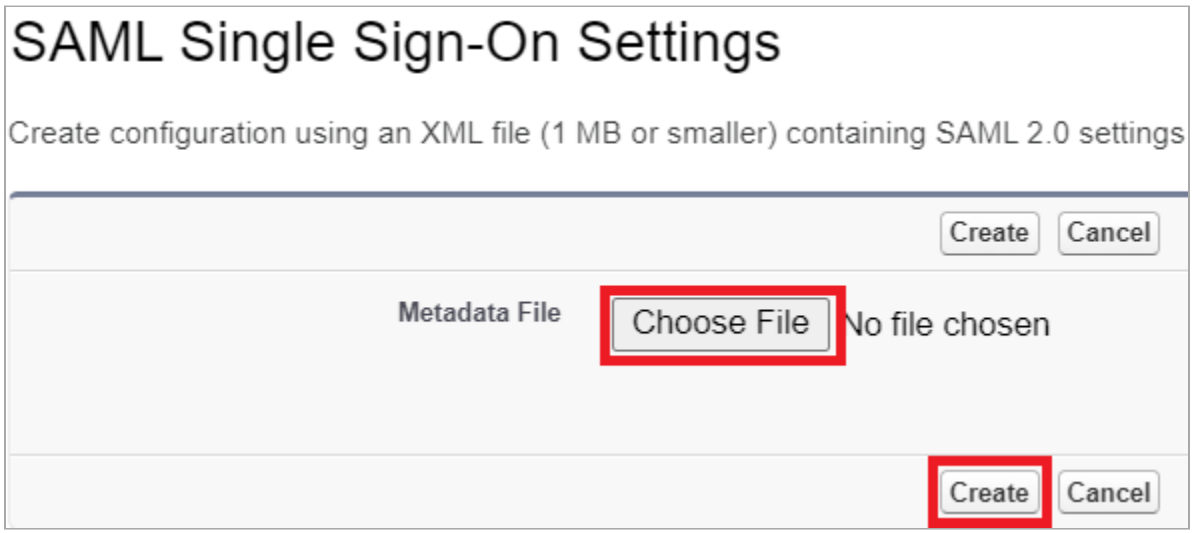
4. Select the **SAML Enabled** check box to enable the use of SAML single sign-on. Click **Save**.



5. Click **New From Metadata File**.



6. Click **Choose File**, select the metadata that you downloaded from PingFederate, and click **Create**.

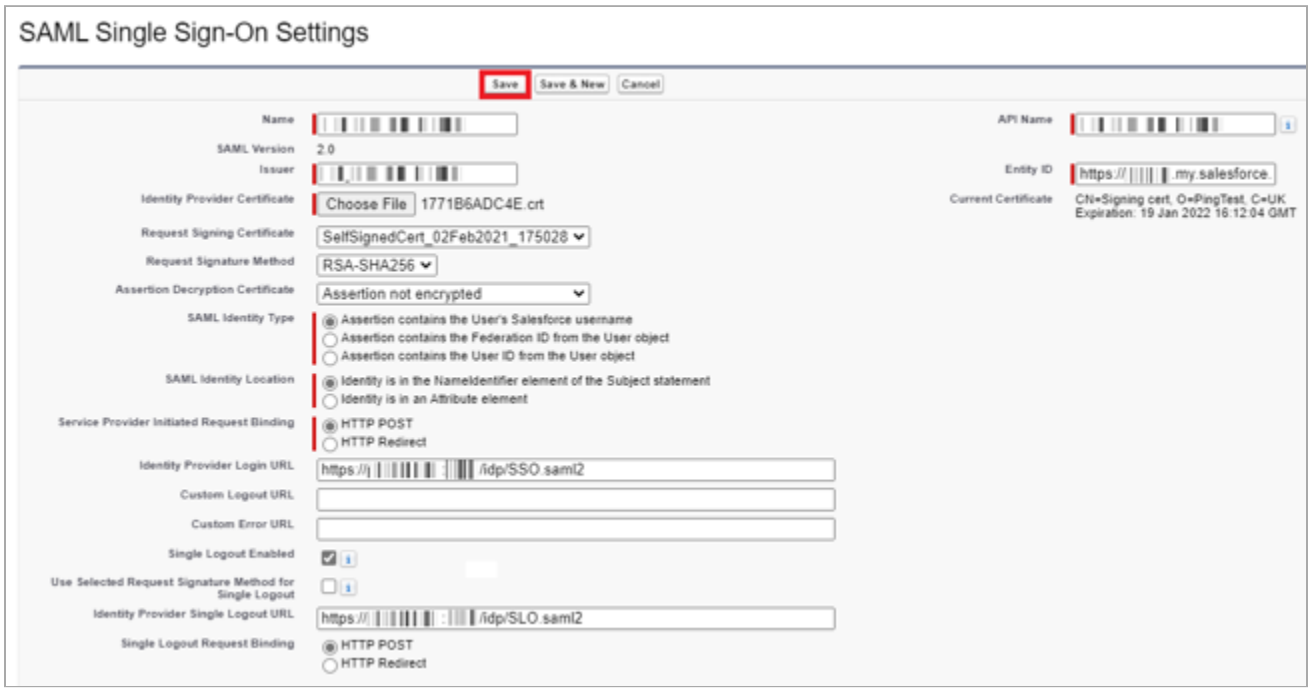


The summary screen opens.

7. In the **Identity Provider Certificate** section, click **Choose file** and select the signing certificate that you downloaded from PingFederate.

8. Clear the **Single Logout Enabled** check box if you don't require single logout.

The summary page opens.



9. Click **Save**.
10. On the summary page for the configuration that you saved in the previous step, click **Edit**.

11. Click the link on the **Request Signing Certificate** line.

12. Click **Download Certificate**.

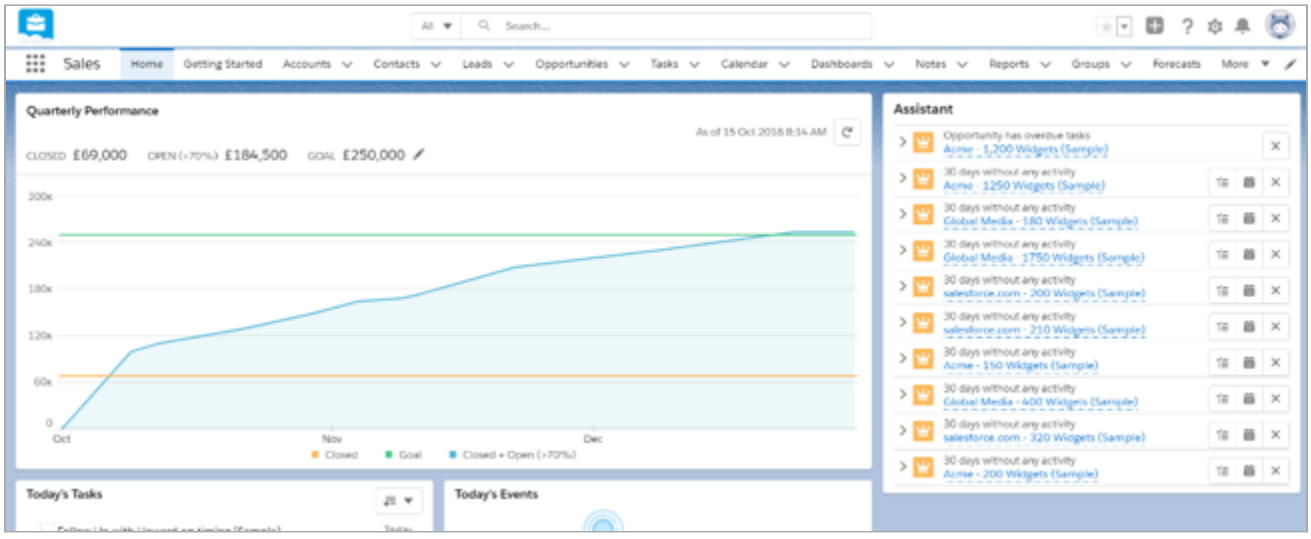
Import the Salesforce certificate into PingFederate

1. Sign on to the PingFederate administrative console.
2. Open the Salesforce SP connection and click **Signature Verification Certificate**.
3. Delete the placeholder certificate and upload the certificate that you downloaded from Salesforce.
4. Save the configuration.

Test the PingFederate IdP-initiated SSO integration

1. Go to the PingFederate SSO application endpoint for the Salesforce SP connection.
2. Complete PingFederate authentication.

   You're redirected to your Salesforce domain.



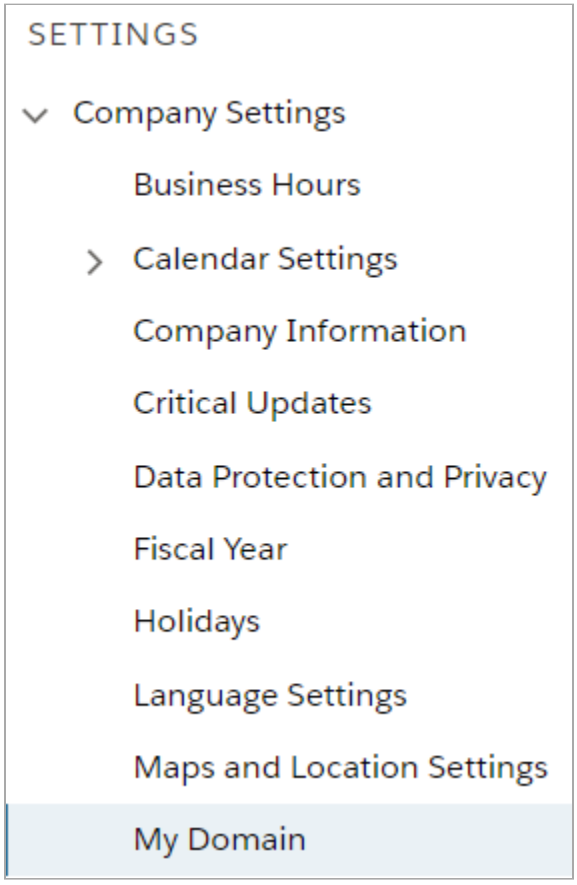
Configure direct Salesforce sign-on using PingFederate (SP-initiated sign-on) plus single logout (SLO)

Before you begin

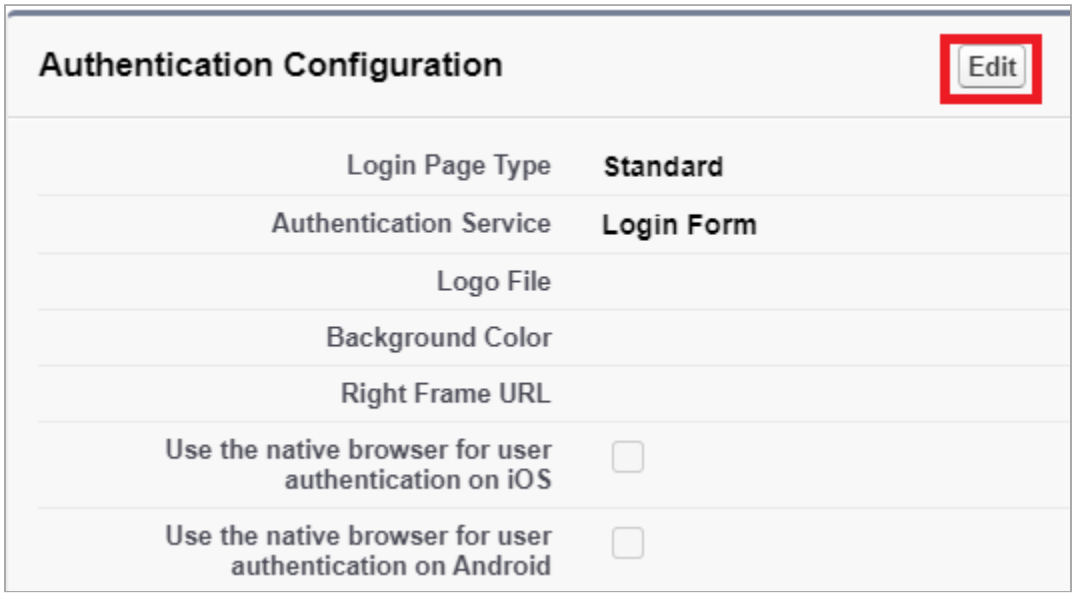
- You must first enable IdP-initiated sign-on.

Enable PingFederate authentication in Salesforce

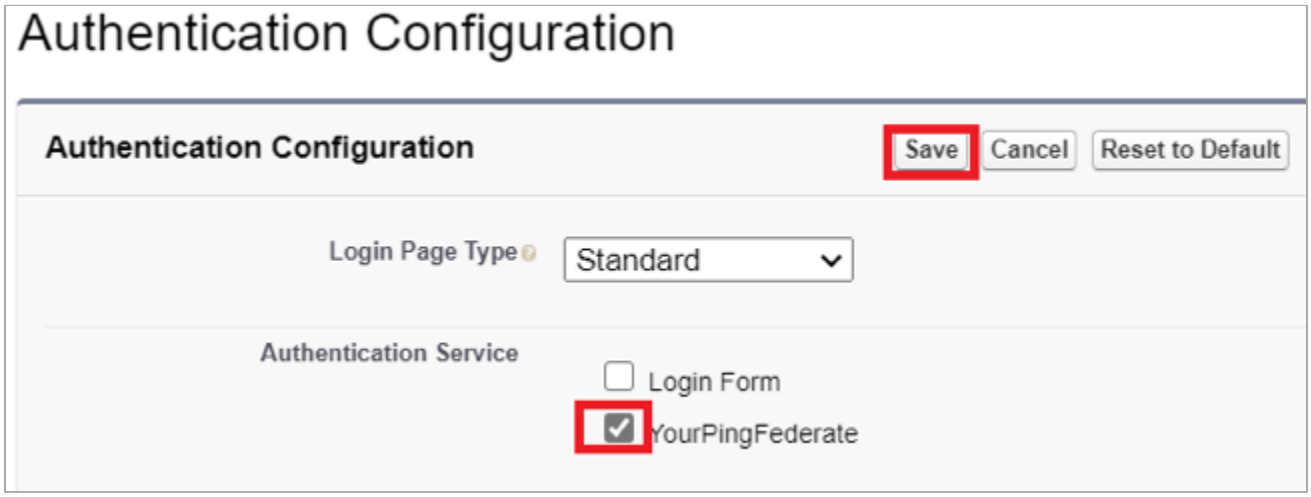
1. Sign on to your Salesforce domain as an administrator.
2. Click the **Gear** icon, then go to **Setup → Company Settings → My Domain**.



3. Make a note of your domain name, such as `https://your-company.my.salesforce.com`.
4. In the **Authentication Configuration** section, click **Edit**.



5. In the **Authentication Service** list, select **YourPingFederate**. Click **Save**.



> **Note**
>
> The "YourPingFederate" entry was created as a result of the IdP-initiated login tasks above.

Configuration is complete.

Salesforce will now redirect to PingFederate for authentication of all new sessions.

You should also select the **Login Form** check box during the testing phase in case of authentication issues. Testers will be offered the option of the standard Salesforce login form or PingFederate authentication. After you've successfully tested authentication against PingFederate, you can clear the **Login Form** check box so that authentication automatically defaults to PingFederate.

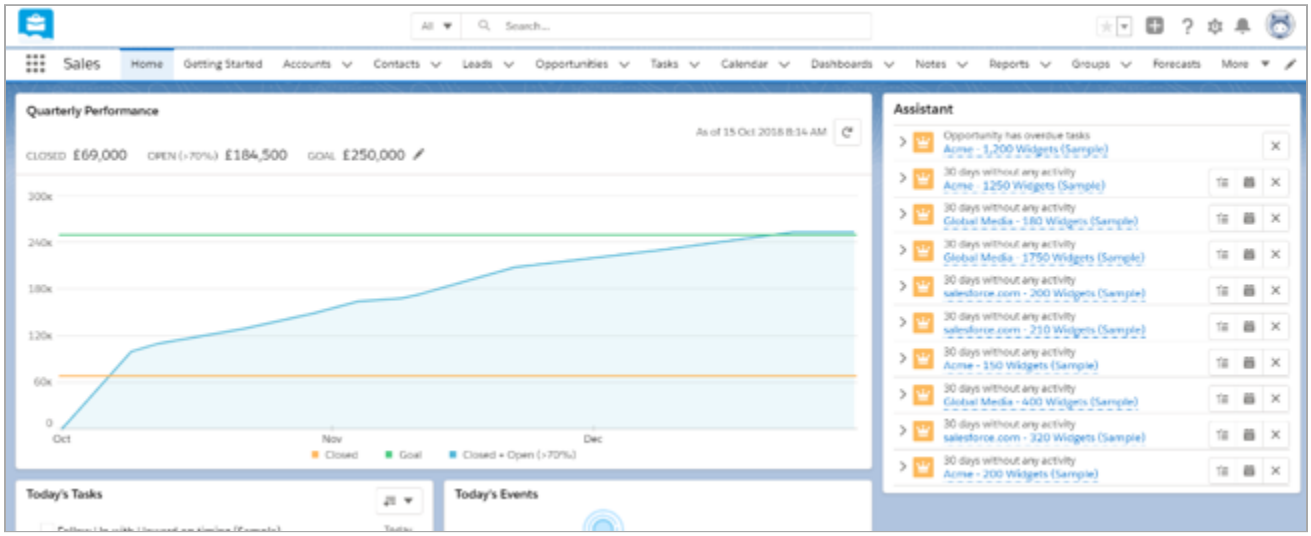
Test the PingFederate SP-initiated SSO integration

1. Go to your Salesforce domain.

> **Note**
>
> If the **Login Form** check box is still selected, the Salesforce sign on screen still displays, and you're offered a choice of Salesforce sign on or PingFederate sign on, select **PingFederate**.
> If you've cleared the **Login Form** check box, you're not offered a choice.

2. When you are redirected to PingFederate, enter your PingFederate username and password.

   After successful authentication, you're redirected back to Salesforce.



Configuring SAML SSO with Salesforce and PingOne for Enterprise

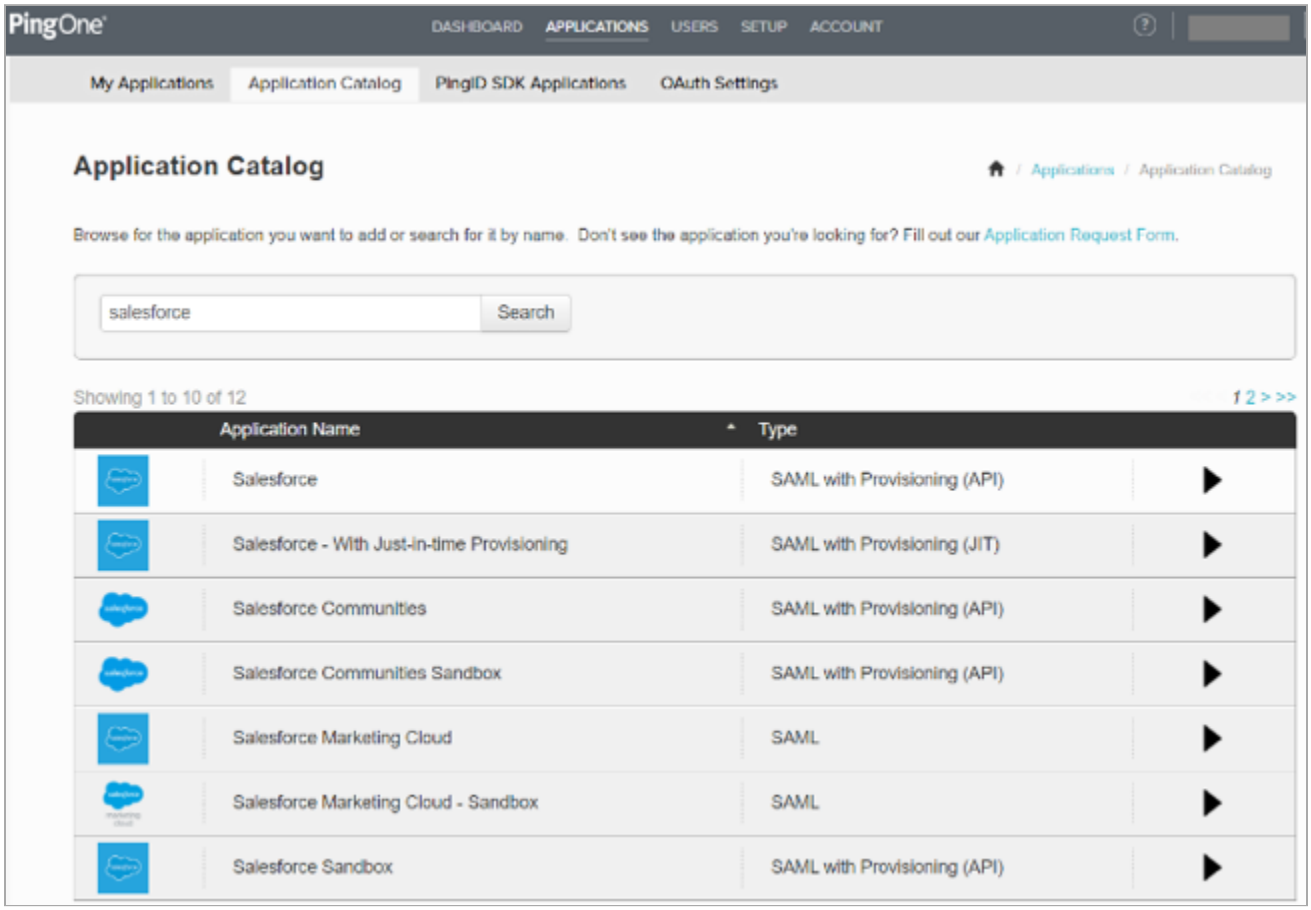
Enable Salesforce sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) plus single logout (SLO).

Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate Salesforce with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and Salesforce.

Extract the PingOne for Enterprise metadata for Salesforce

1. Sign on to PingOne for Enterprise and go to **Applications → Application Catalog**.
2. Search for `Salesforce`.

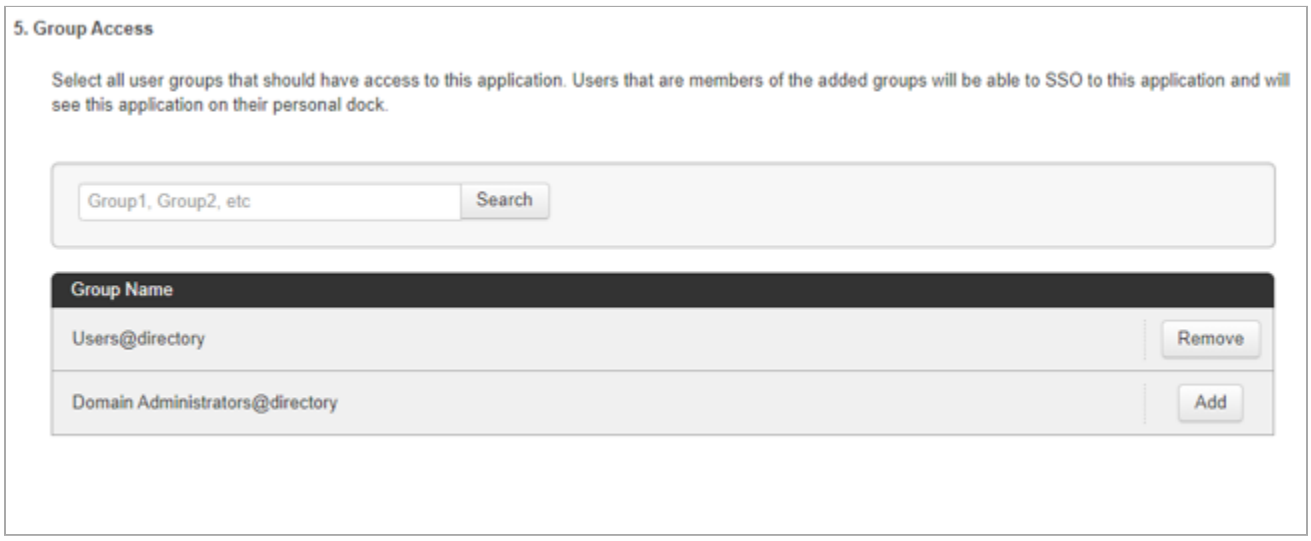


3. Expand the Salesforce entry and click the **Setup** icon.

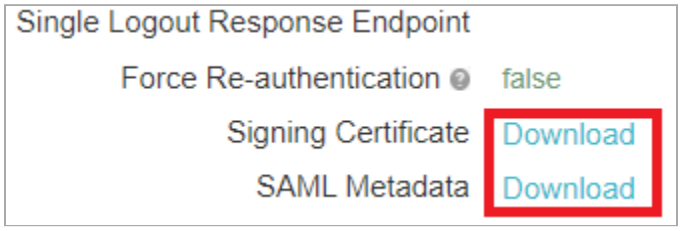
4. Click **Continue to Next Step** until you're on the **Group Access** page.

> **Note**
>
> You'll configure the application settings later through metadata.

5. Click **Add** for each user group that should have access to Salesforce.

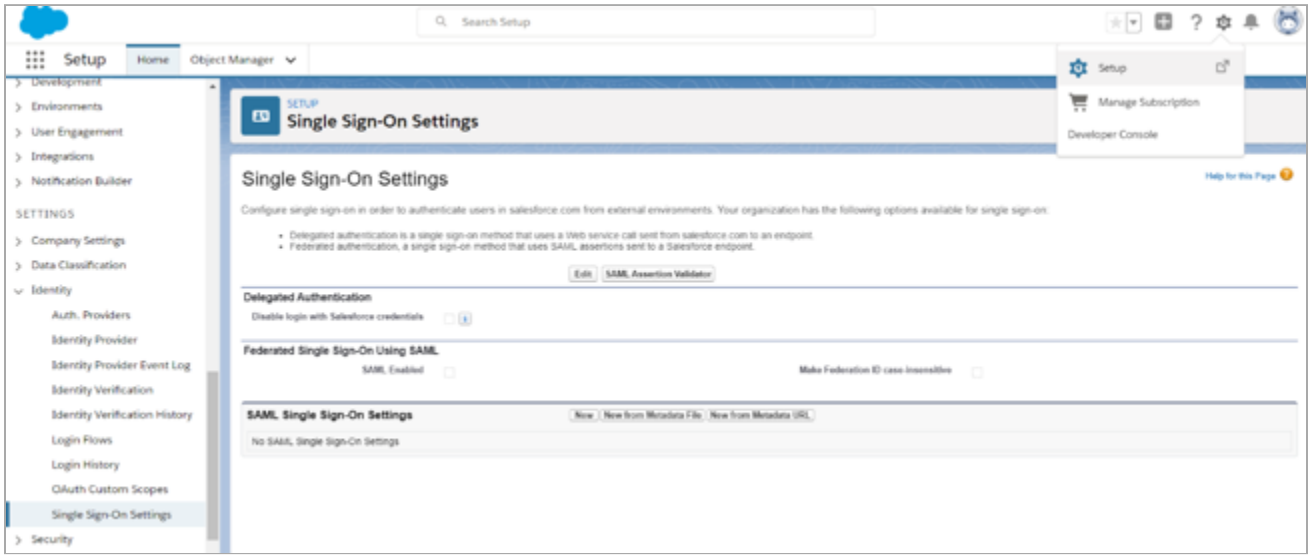


6. Click **Continue to Next Step**.
7. Download the PingOne for Enterprise signing certificate and SAML metadata.
8. Click **Finish**.

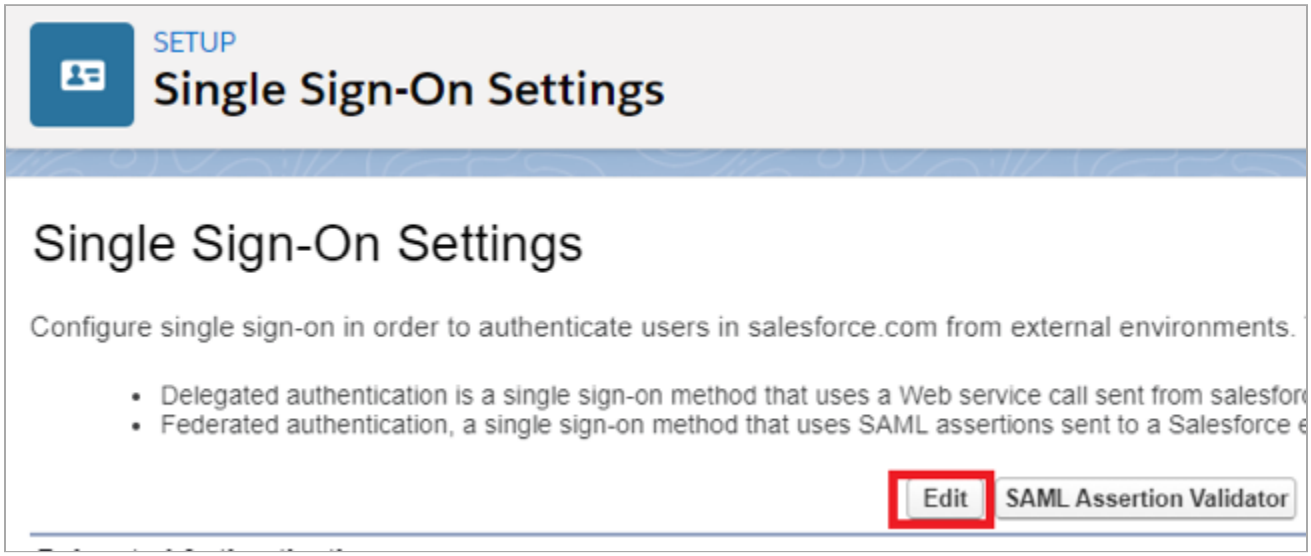


Add the PingOne for Enterprise IdP Connection to Salesforce

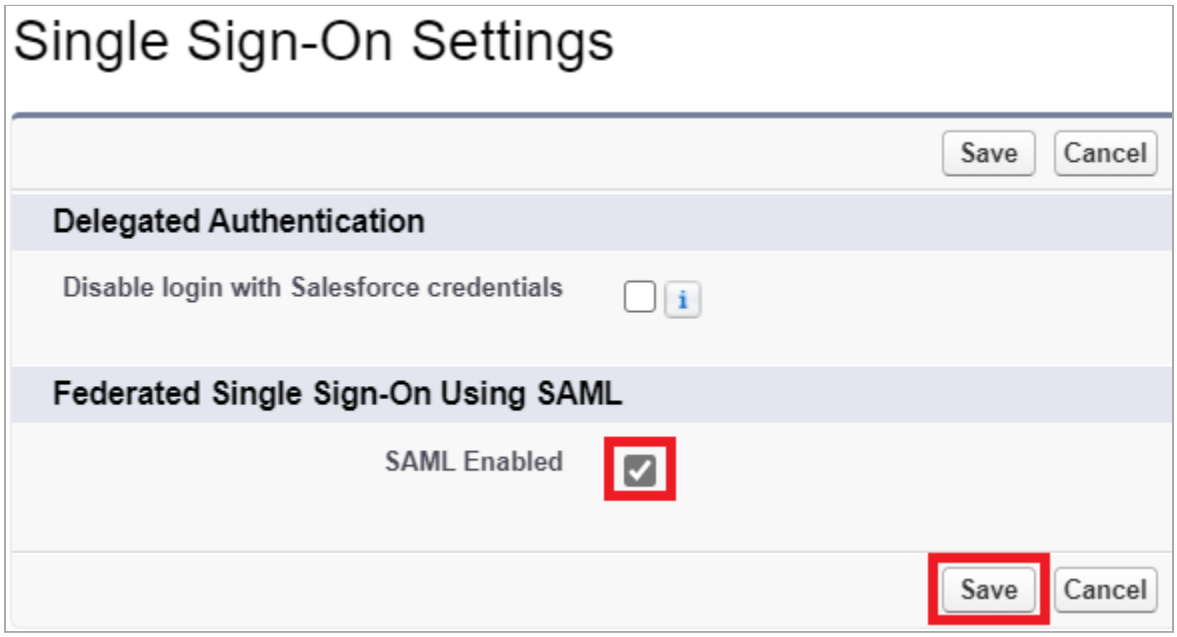
1. Sign on to your Salesforce domain as an administrator.
2. Click the **Gear** icon (⚙), then go to **Setup → Identity → Single Sign-On Settings**.



3. On the **Single Sign-On Settings** page, click **Edit**.

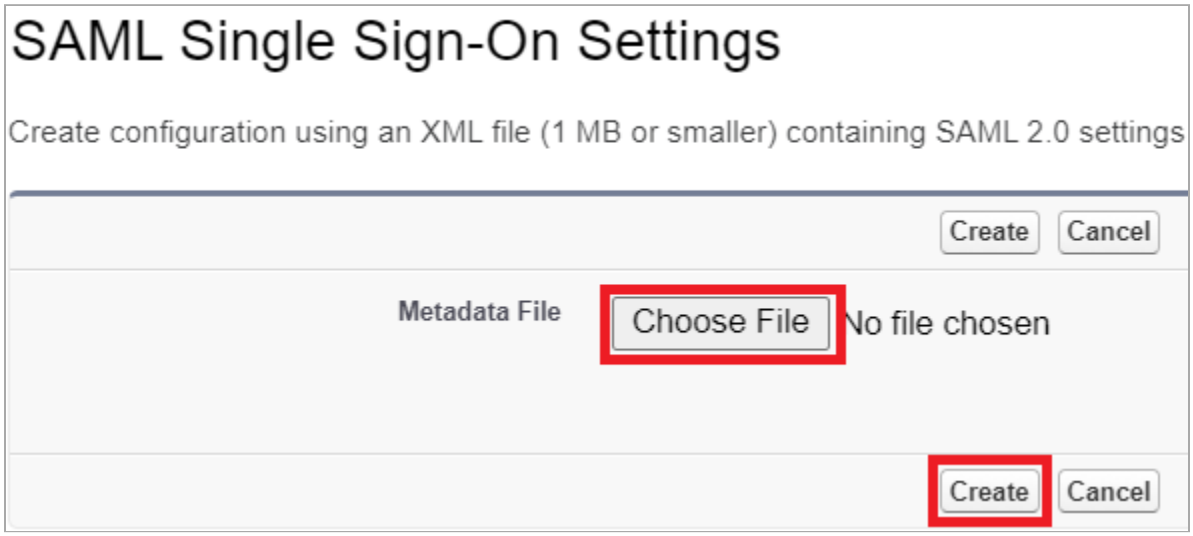


4. Select the **SAML Enabled** check box to enable the use of SAML SSO. Click **Save**.



5. Click **New From Metadata File**.

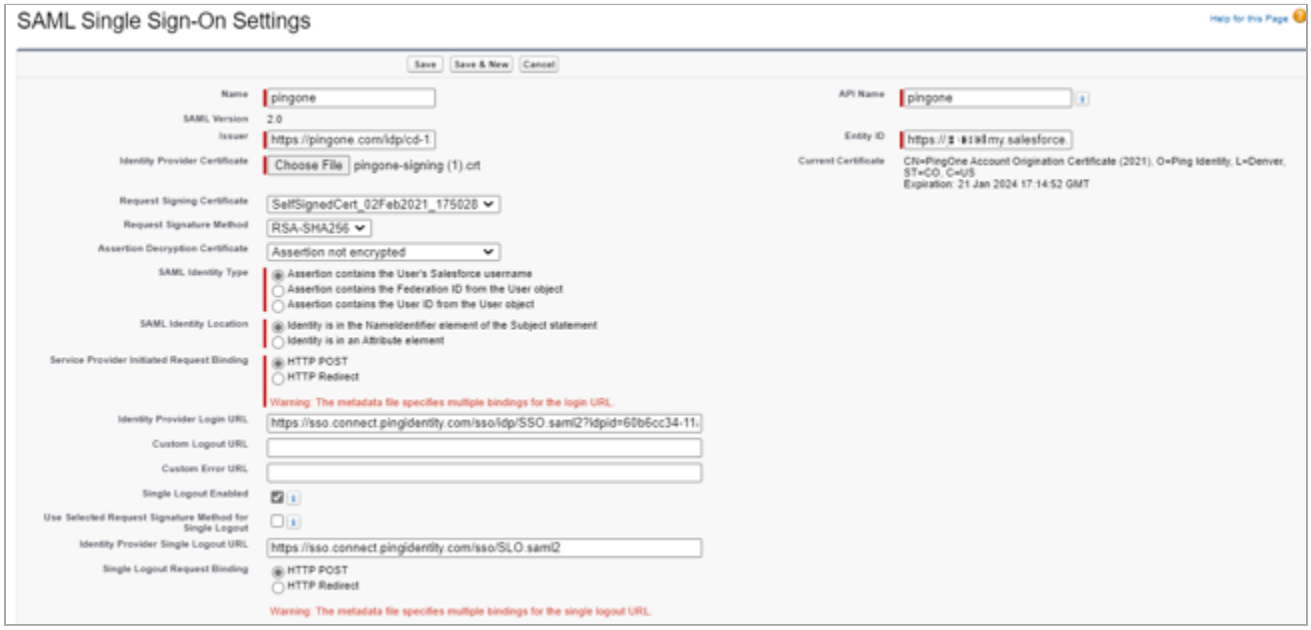
6. Click **Choose File**, select the SAML metadata file that you downloaded from PingOne for Enterprise, and click **Create**.



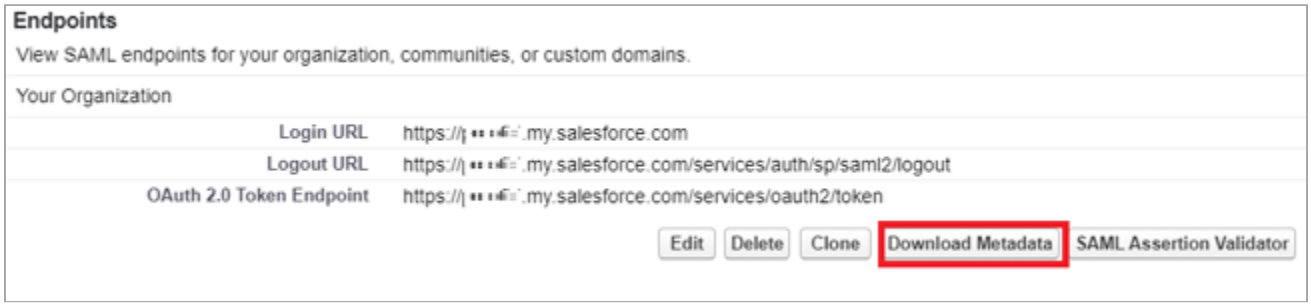
The summary screen opens.

7. On the **Identity Provider Certificate** line, click **Choose File** and select the signing certificate that you downloaded from PingOne for Enterprise.
8. Set **Service Provider Initiated Request Binding** to **HTTP POST**.
9. Set **Single Logout Request Binding** to **HTTP POST**.
10. Clear the **Single Logout Enabled** check box if you don't require single logout.

    The summary screen will resemble the following:

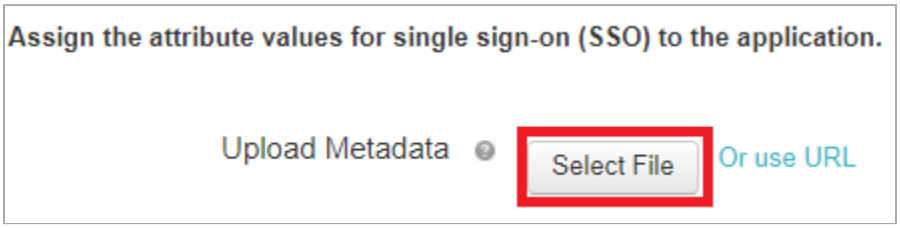


11. Ignore the metadata file warnings and click **Save**.
12. Click **Download Metadata** to save the Salesforce metadata.

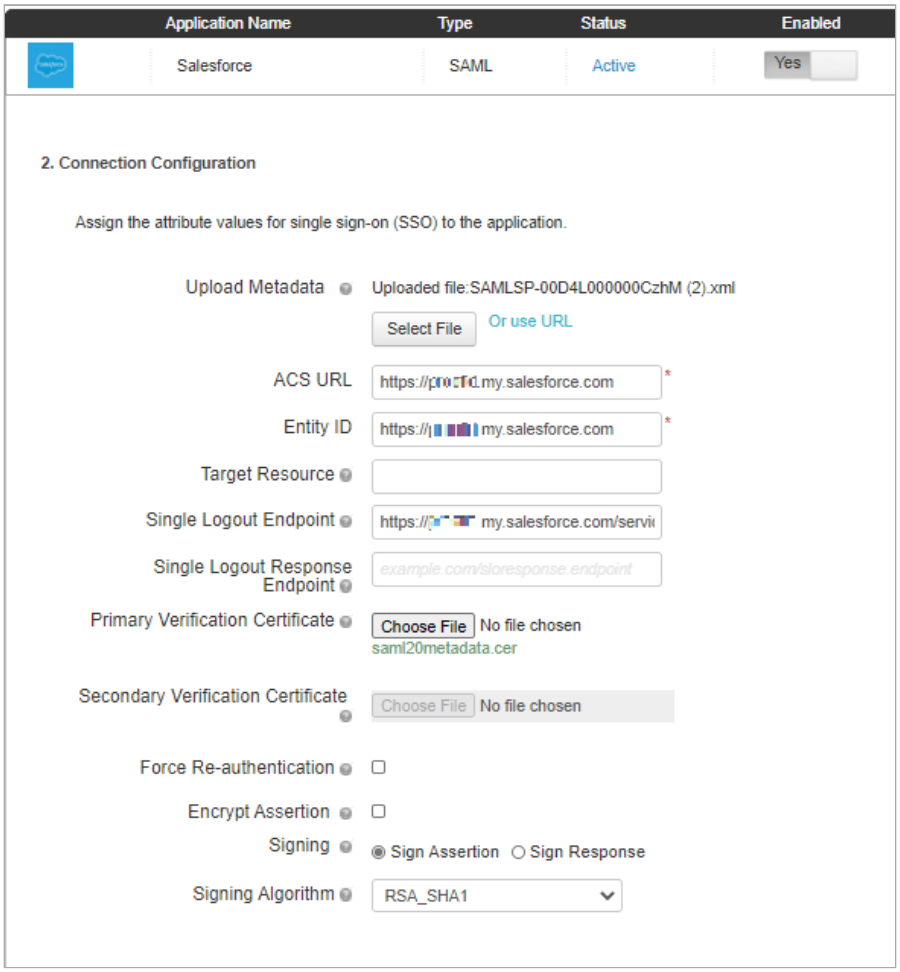


Import the Salesforce metadata into PingOne.

1. Sign on to PingOne for Enterprise and go to **Applications → My Applications**.
2. Expand the Salesforce entry and click **Edit**.
3. Click **Continue to Next Step**.
4. Click **Select File** and select the metadata file that you downloaded from Salesforce.



The **ACS URL**, **Entity ID**, **Single Logout Endpoint**, and **Primary Verification Certificate** fields should now be populated.



5. Click **Continue to Next Step** on the remaining pages then click **Finish**.

> **Note**
>
> This step assumes that your usernames in Salesforce match the ones in PingOne for Enterprise. If this is not the case, then you must map the expected Salesforce username value on the third page.

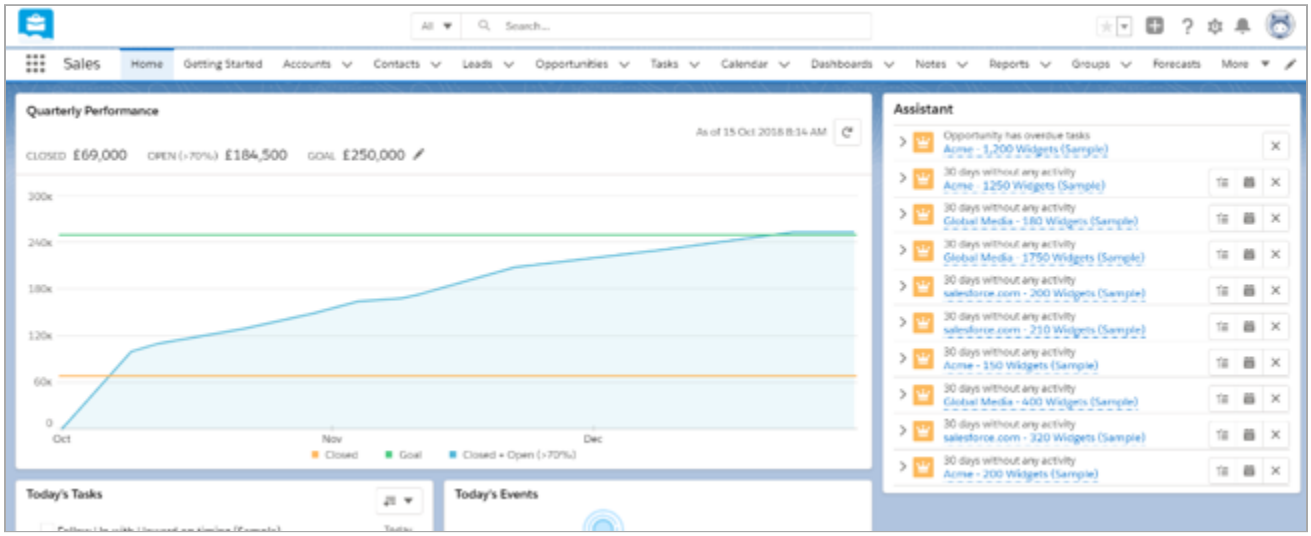
Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with Salesforce access.

> **Note**
>
> To find the Ping desktop URL in the Admin console, go to **Setup → Dock → PingOne Dock URL**.

2. Complete PingOne for Enterprise authentication.

   You're redirected to your Salesforce domain.



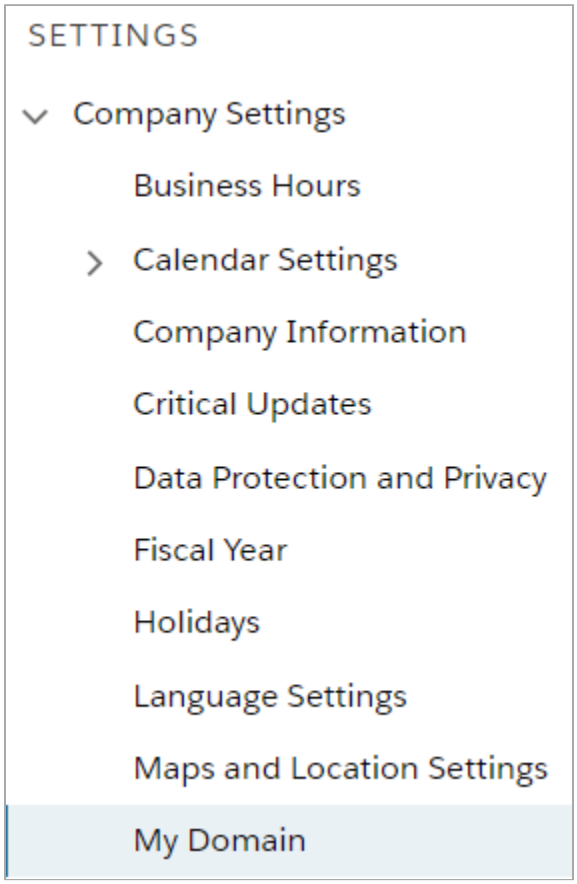
Configure direct Salesforce sign on using PingOne (SP-initiated login) plus SLO

Before you begin

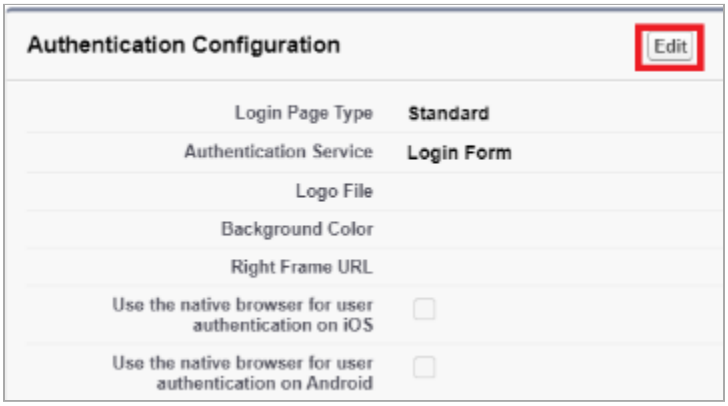
- You must first enable identity provider (IdP)-initiated sign-on.

Enable PingOne authentication in Salesforce

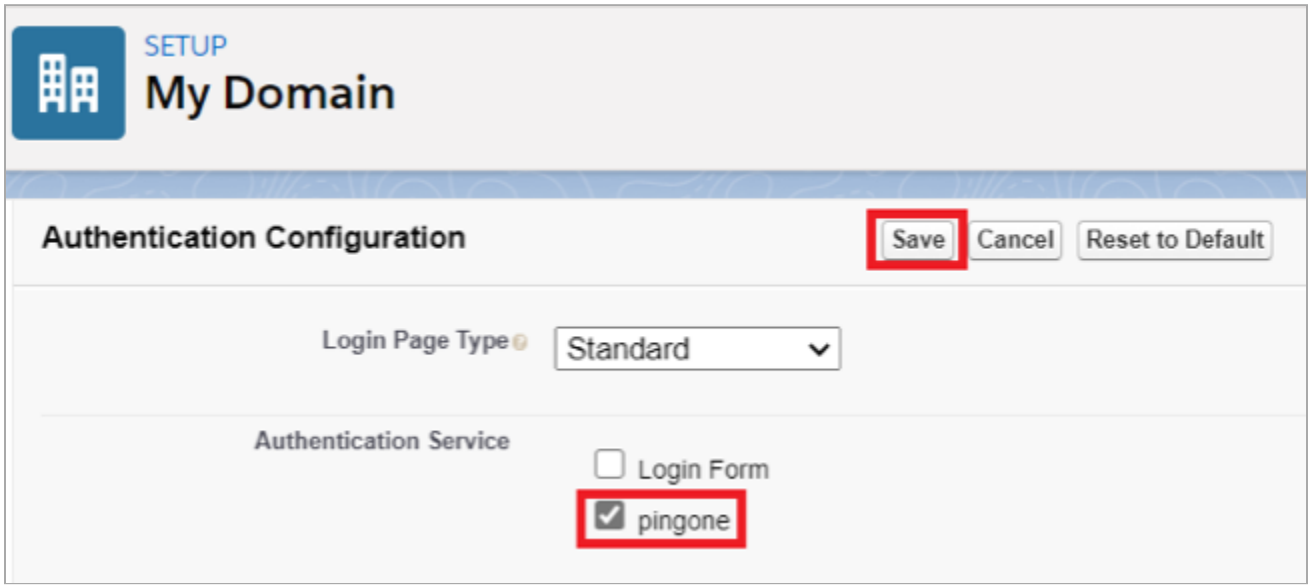
1. Sign on to your Salesforce domain as an administrator.
2. Click the **Gear** icon, then go to **Setup → Company Settings → My Domain**.



3. Make a note of your domain name, for example, `https://your-company.my.salesforce.com`
4. In the **Authentication Configuration** section, click **Edit**.



5. In the **Authentication Service** list, select **PingOne**. Click **Save**.



> **Note**
>
> This entry was created as a result of the IdP-initiated sign-on task.

Configuration is complete.

> **Note**
>
> Salesforce will now redirect to PingOne for authentication of all new sessions. You should also select the **Login Form** check box during the testing phase in case of authentication issues.
> Testers will be offered the option of the standard Salesforce login form or PingOne authentication.
> After you've successfully tested authentication, you can clear the **Login Form** check box so that authentication automatically defaults to PingOne.

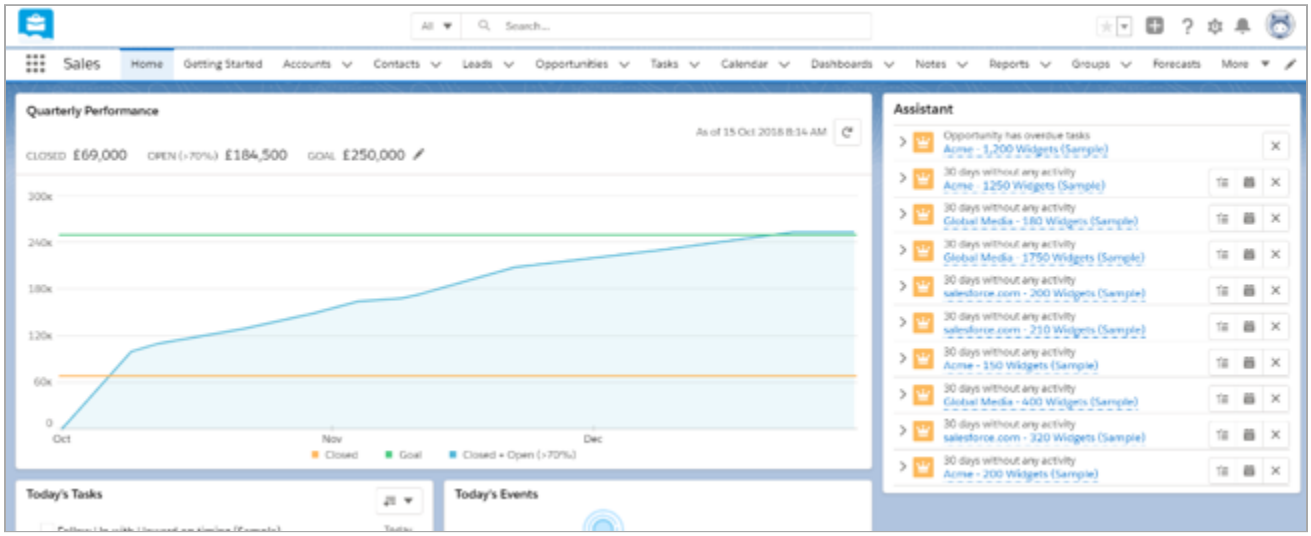
Test the PingOne SP-initiated SSO integration

1. Go to your Salesforce domain.

   > **Note**
   >
   > If the **Login Form** check box is still selected, the Salesforce sign-on screen still displays, and you're offered a choice of Salesforce sign on or PingOne sign, select PingOne.
   > If you've cleared the **Login Form** check box, you're not offered a choice.

2. When you are redirected to PingOne, enter your PingOne username and password.

   After successful authentication, you're redirected back to Salesforce.



SAP Netweaver

Configuring SAML SSO with SAP Netweaver and PingFederate

Learn how to configure SAML SSO with SAP Netweaver and PingFederate.

Before you begin

Refer to the vendor documentation and complete the following:

1. Ensure that HTTPS is enabled for your SAP system.
2. Activate Secure Session Management.
3. Enable SAML 2.0 support:
    1. Create a local provider.
    2. Export metadata for local provider.

About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
SAML_SUBJECT	Username	Required

Create a PingFederate SP connection for SAP Netweaver

> **Note**
> The following configuration is untested and is provided as an example. Additional steps might be required.

1. Sign on to the PingFederate administrative console.
2. Using the details retrieved from SAP Netweaver:
    1. Configure using **Browser SSO** profile **SAML 2.0**.
    2. Enable the following **SAML Profiles**:
        - **IdP-Initiated SSO**
        - **SP-Initiated SSO**

3. In **Assertion Creation: Attribute Contract**, set the **Subject Name Format** to **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified**.
4. In **Assertion Creation: Attribute Contract Fulfilment**, map the attribute **SAML_SUBJECT** to the attribute **username**.

   This should match the username for the user in SAP Netweaver.
5. In **Protocol Settings: Allowable SAML Bindings**, enable **Post** and **Redirect**.

3. Export the metadata for the newly-created SP connection.
4. Export the signing certificate public key.

Configure the PingFederate IdP connection for SAP Netweaver

1. Sign on to SAP Netweaver as an administrator.
2. Go to **Trusted Partners** and select **Identity Providers**.
3. Click **Add**.
4. Click **Upload Metadata File**, select the file that you downloaded from PingFederate, and click **Next**.
5. On the **Provider Name** page, verify the data populated. Click **Next**.
6. On the **Signature and Encryption** page, verify the data populated. Click **Next**.
7. On the **Single Sign-On Endpoints** page, verify the data populated. Click **Next**.
8. On the **Single Logout Endpoints** screen, verify the data populated. Click **Next**.
9. Select **Binding** as **HTTP POST**. Click **Finish**.
10. Enable the provider.
11. Configuration is completed.

After testing, you can enable SP-initiated SSO for SAP Netweaver by editing the configuration in `sap/opu/odata/iwfnd/catalogservice`.

Configuring SAML SSO with SAP Netweaver and PingOne for Enterprise

Learn how to configure SAML SSO with SAP Netweaver and PingOne for Enterprise.

Before you begin

Refer to the vendor documentation and complete the following:

1. Ensure that HTTPS is enabled for your SAP system.
2. Activate Secure Session Management.
3. Enable SAML 2.0 support:
   1. Create a local provider.

2. Export metadata for local provider.

About this task

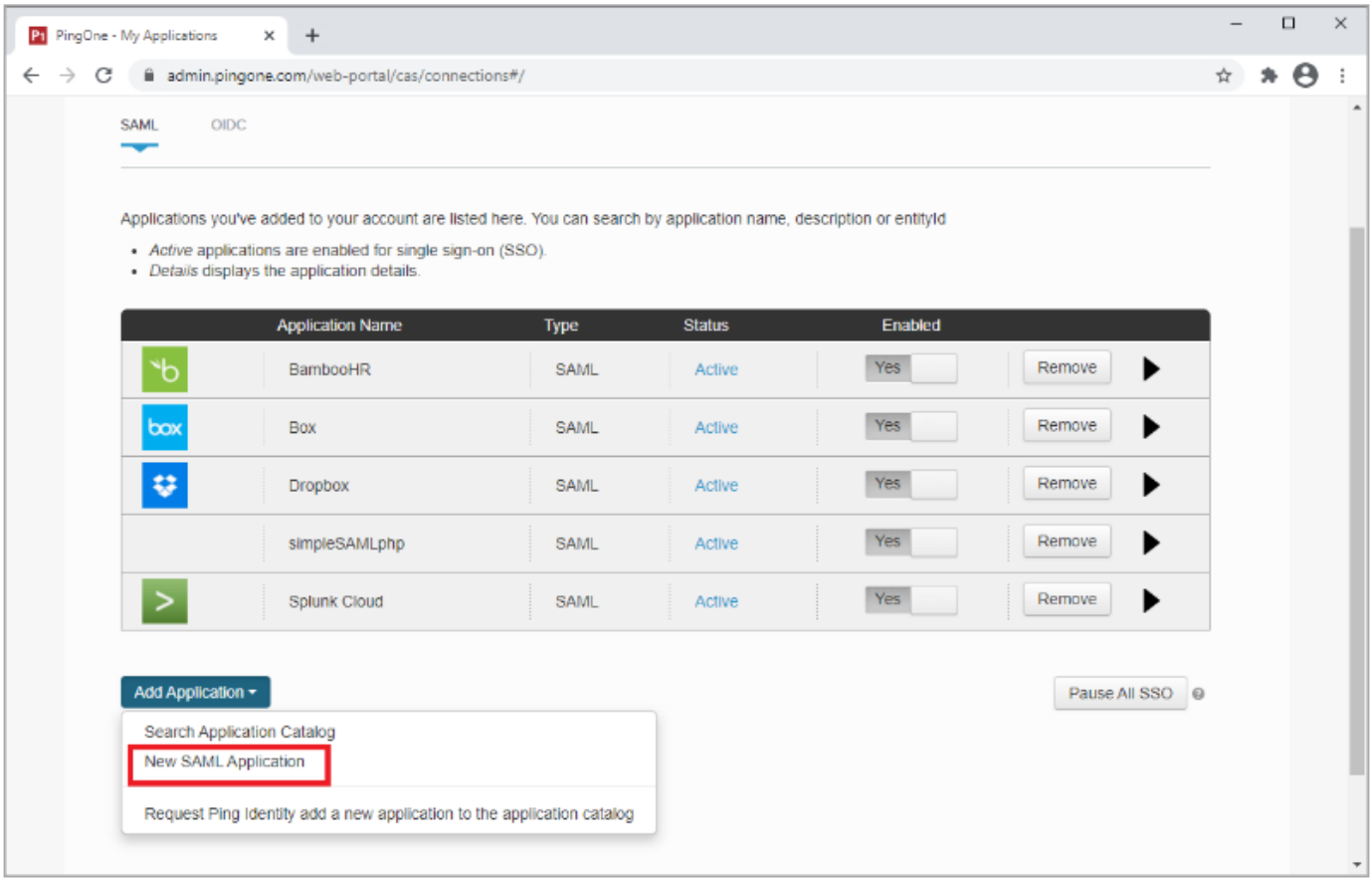
The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
SAML_SUBJECT	Username	Required

Create a PingOne for Enterprise application for SAP Netweaver

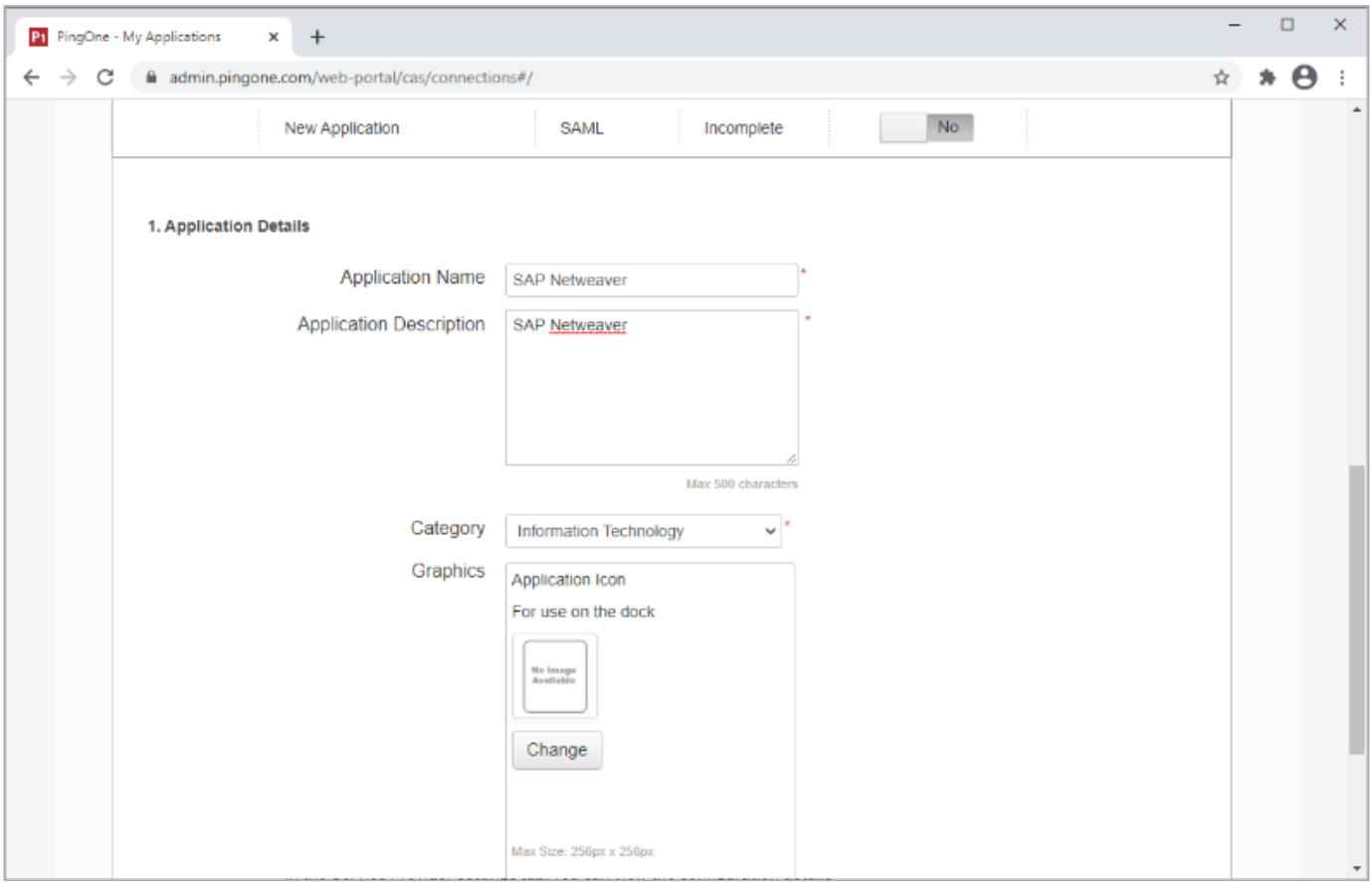
> **Note**
>
> The following configuration is untested and is provided as an example. Additional steps might be required.

1. Sign on to PingOne for Enterprise and click **Applications**.
2. On the **SAML** tab, click **Add Application**.

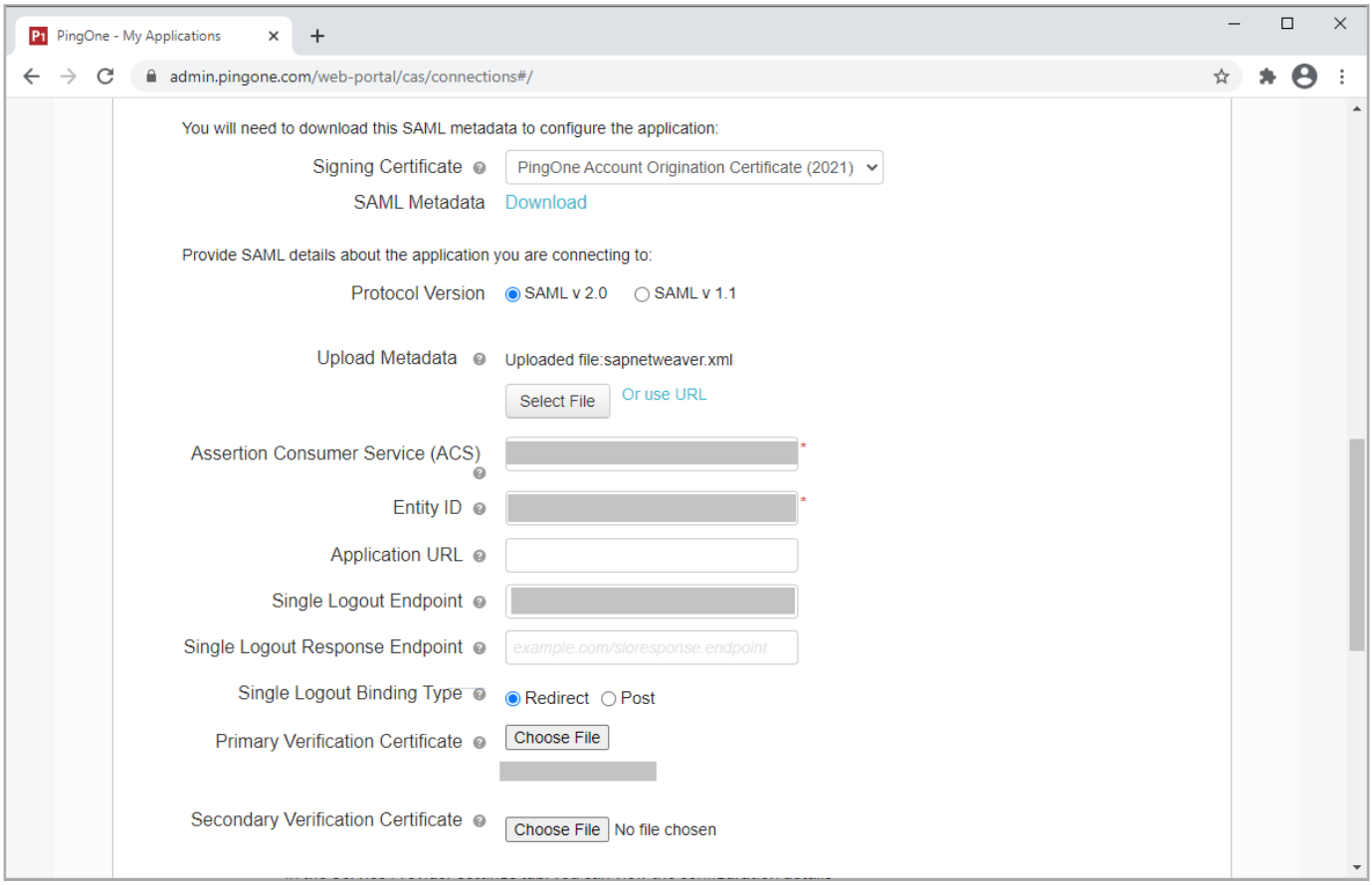


3. Enter the following:
   - A suitable **Application Name**, such as `SAP Netweaver`.
   - A suitable **Application Description**.

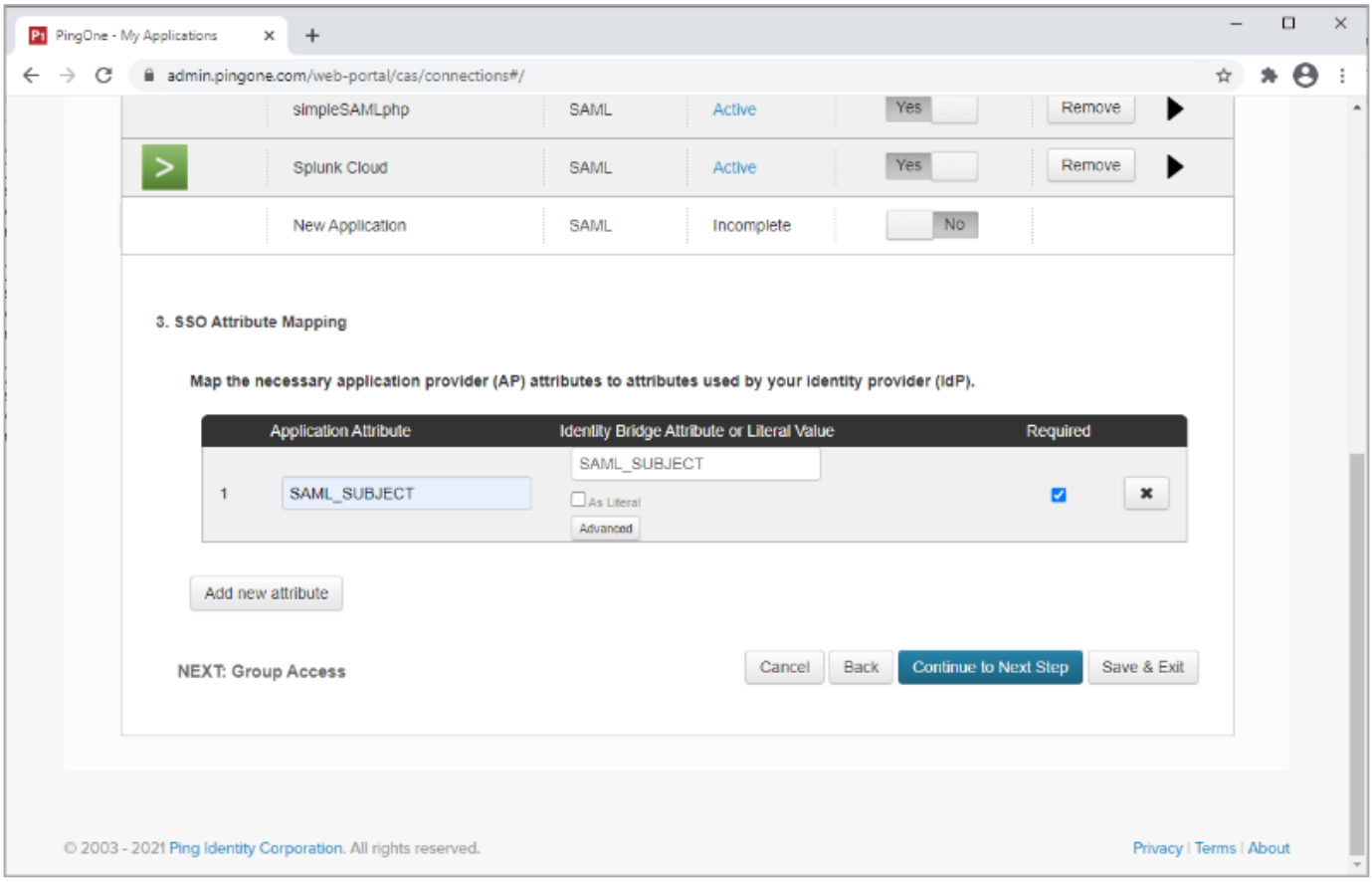
- A suitable **Category**, such as `Information Technology`.
- (Optional) Upload an icon to be used in the PingOne for Enterprise dock.



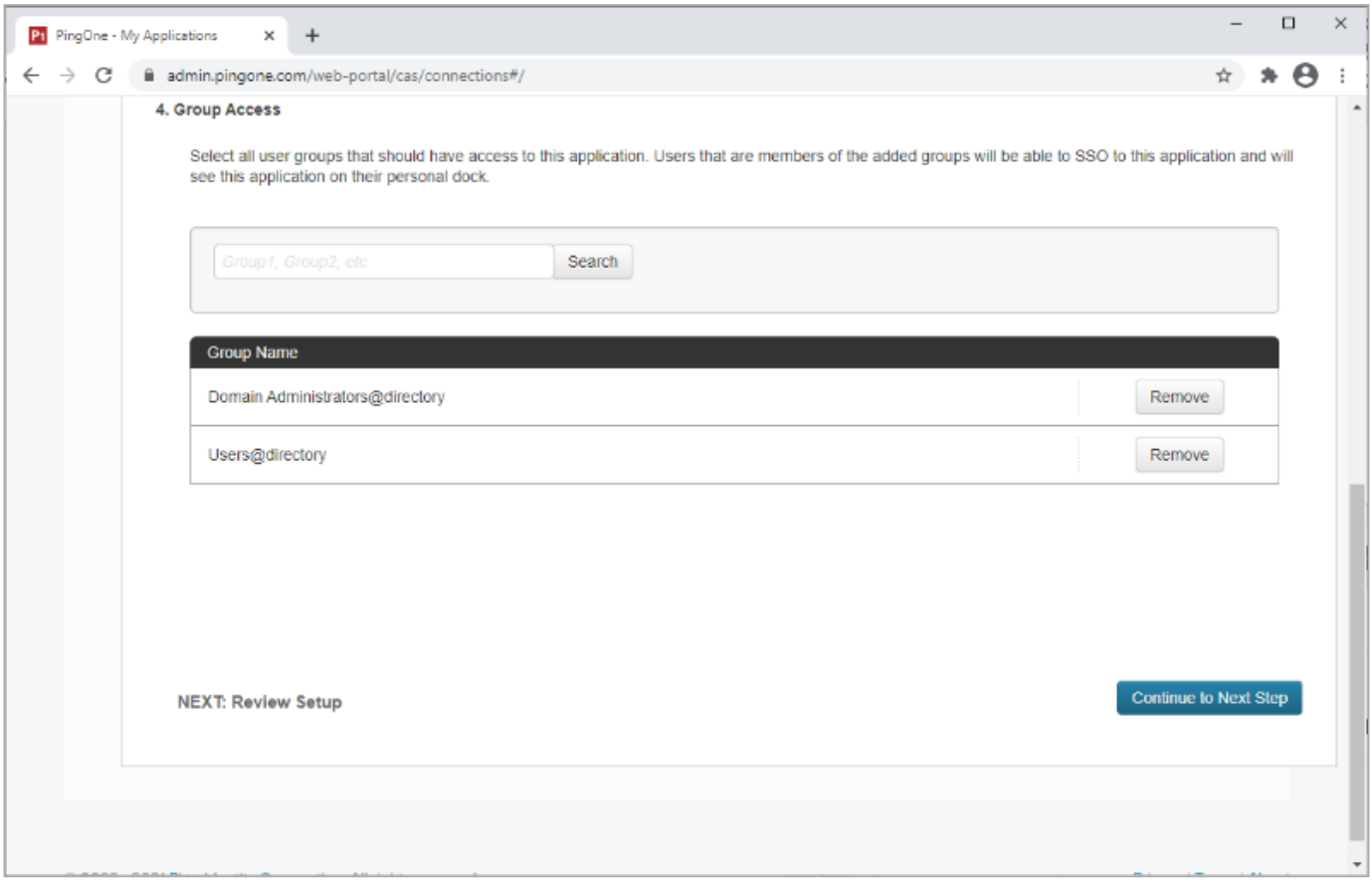
4. Click **Continue to Next Step**.
5. Select **I have the SAML configuration**.
6. In the **Signing Certificate list**, select a suitable signing certificate.
7. For **Protocol Version**, click **SAML v.2.0**.



8. Upload the metadata from your SAP Netweaver local provider configuration.
9. Click **Continue to Next Step**.
10. In the **SSO Attribute Mapping** section, add the following mapping for the **SAML_SUBJECT**:
    - For **Identity Bridge Attribute or Literal Value**, select the appropriate attribute. This should match the username for the user in SAP Netweaver.
    - Select the **Required** check box.

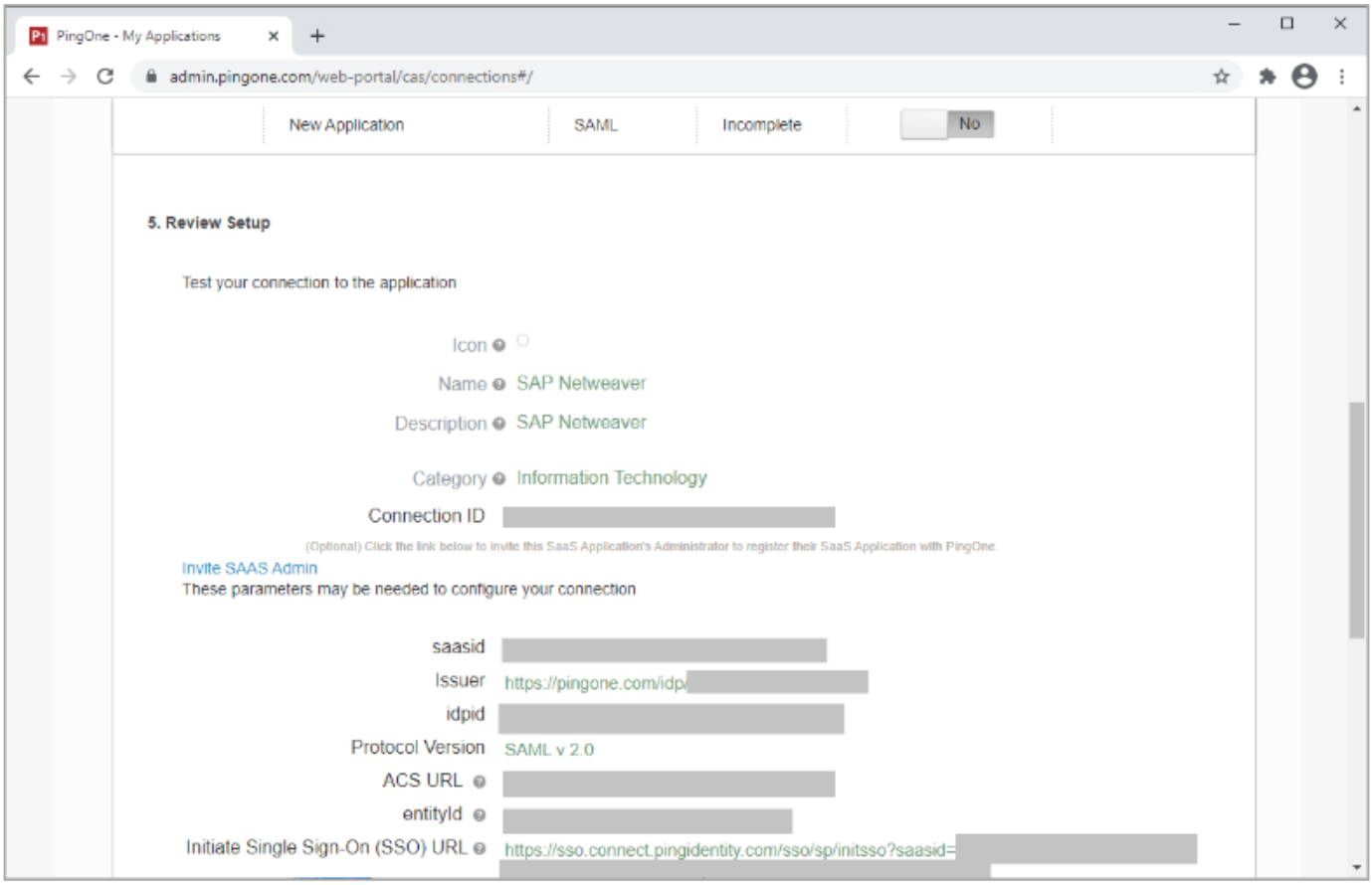


11. Click **Continue to Next Step**.
12. Add the user groups for the application.



13. Click **Continue to Next Step**.

14. Review the settings.



15. Copy the **Single Sign-On (SSO) URL** value to a temporary location.

    This is the IdP-initiated SSO URL that you can use for testing.

16. Note the **idpid** and **Issuer** values.
17. On the **Signing Certificate** line, click **Download**.

    You'll use this for the application configuration.

18. On the **SAML Metadata** line, click **Download**.

    You'll use this for the application configuration.

19. Click **Finish**.

Configure the PingOne for Enterprise IdP connection for SAP Netweaver

1. Sign on to SAP Netweaver as an administrator.
2. Go to **Trusted Partners** and select **Identity Providers**.
3. Click **Add**.
4. Click **Upload Metdata File**, select the file that you downloaded from PingOne for Enterprise, and click **Next**.
5. On the **Provider Name** page, verify the data populated. Click **Next**.

6. On the **Signature and Encryption** page, verify the data populated. Click **Next**.
7. On the **Single Sign-On Enpoints** page, verify the data populated. Click **Next**.
8. On the **Single Logout Endpoints** page, verify the data populated. Click **Next**.
9. Select **Binding** as **HTTP POST**. Click **Finish**.
10. Enable the provider.

After testing, you can enable SP-initiated SSO for SAP Netweaver by editing the configuration in `sap/opu/odata/iwfnd/catalogservice`.

ServiceNow

Configuring SAML SSO with ServiceNow and PingOne for Enterprise

Learn how to configure SAML SSO with ServiceNow and PingOne for Enterprise

About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

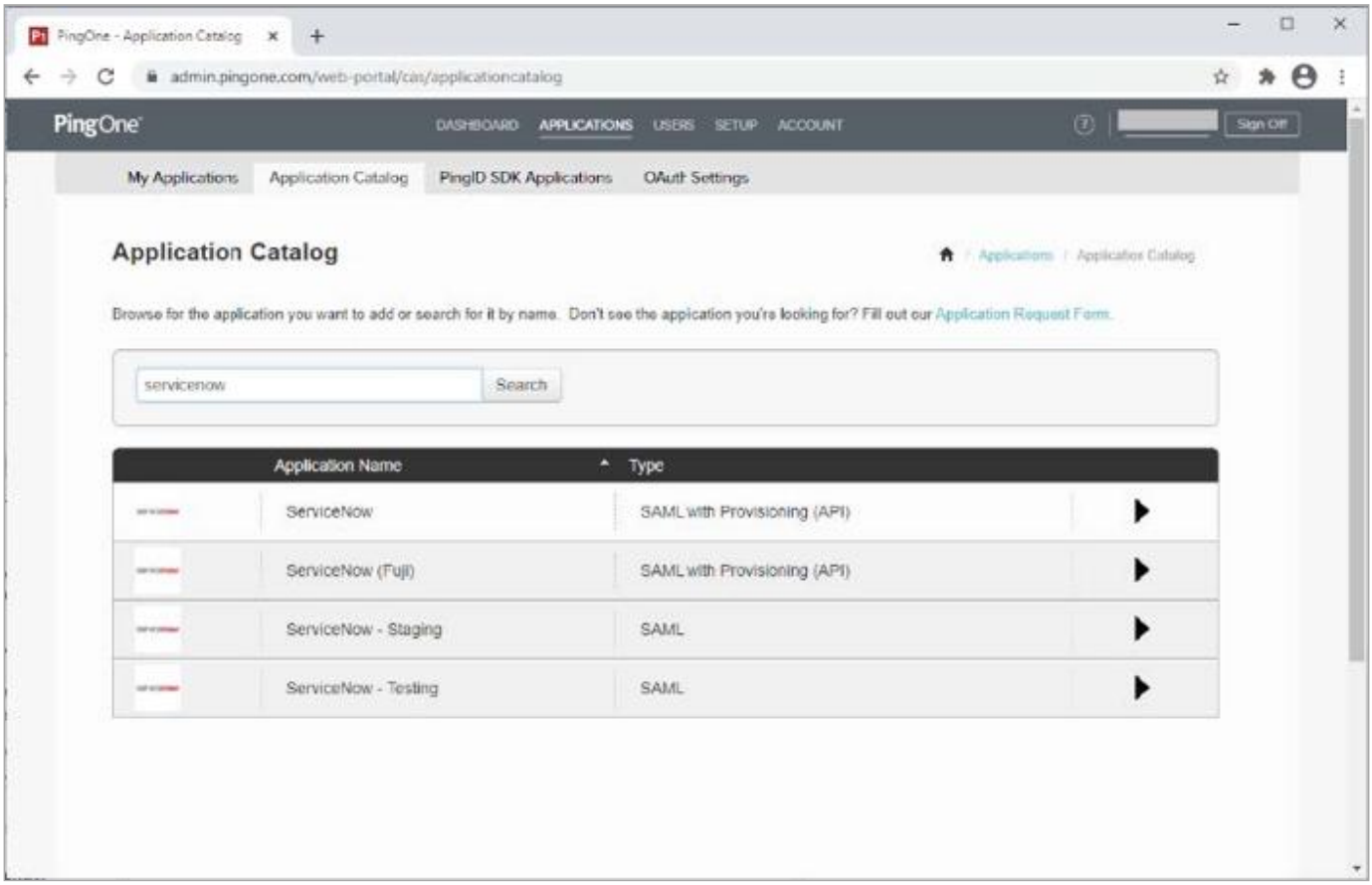
Attribute Name	Description	Required / Optional
NameID	NameID and format is configurable in ServiceNow. This guide uses email.	Required

The following table details the references that are used within this guide that are environment specific. Replace these with the suitable value for your environment.

Reference	Description
`tenant`	The instance name for your ServiceNow tenant you want to integrate with PingOne for Enterprise.

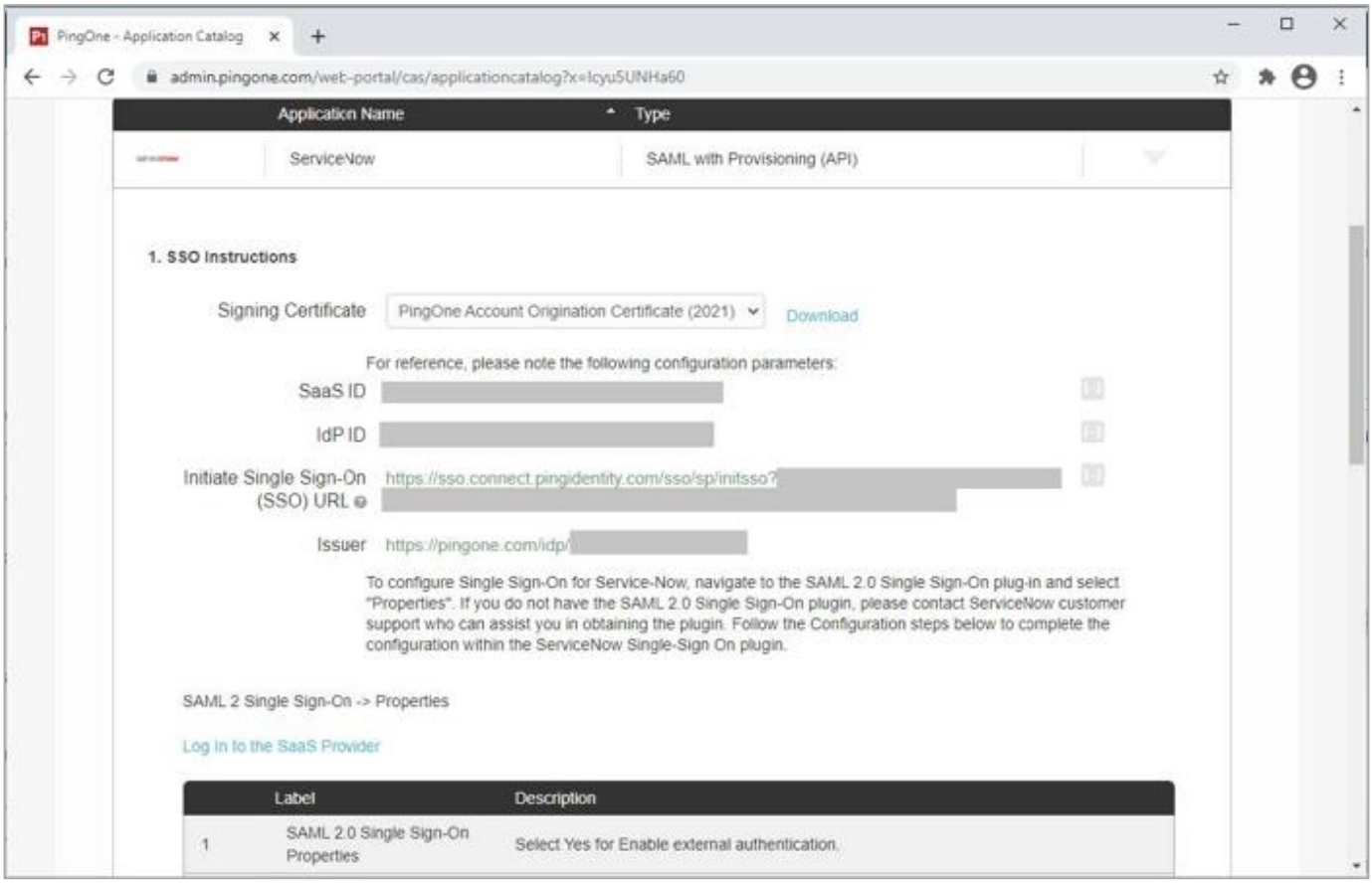
Create a PingOne for Enterprise application for ServiceNow

1. Sign on to PingOne for Enterprise and go to **Applications → Application Catalog**.
2. Search for `ServiceNow` and then click the **ServiceNow** row.

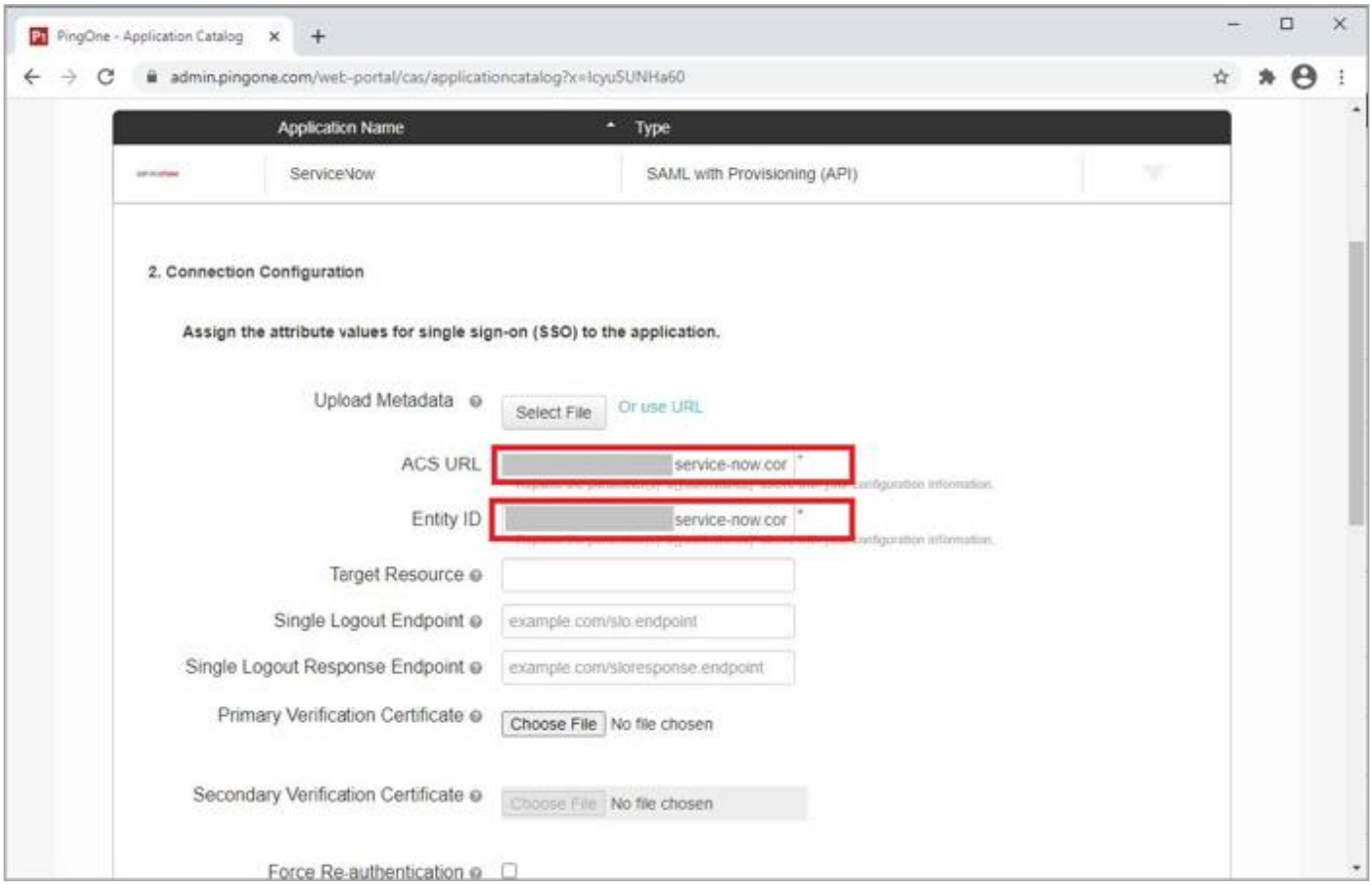


3. Click **Setup**.

4. Review the steps and make a note of the **PingOne SaaS ID**, **IdP ID**, **Single Sign-on URL**, and **Issuer** values.

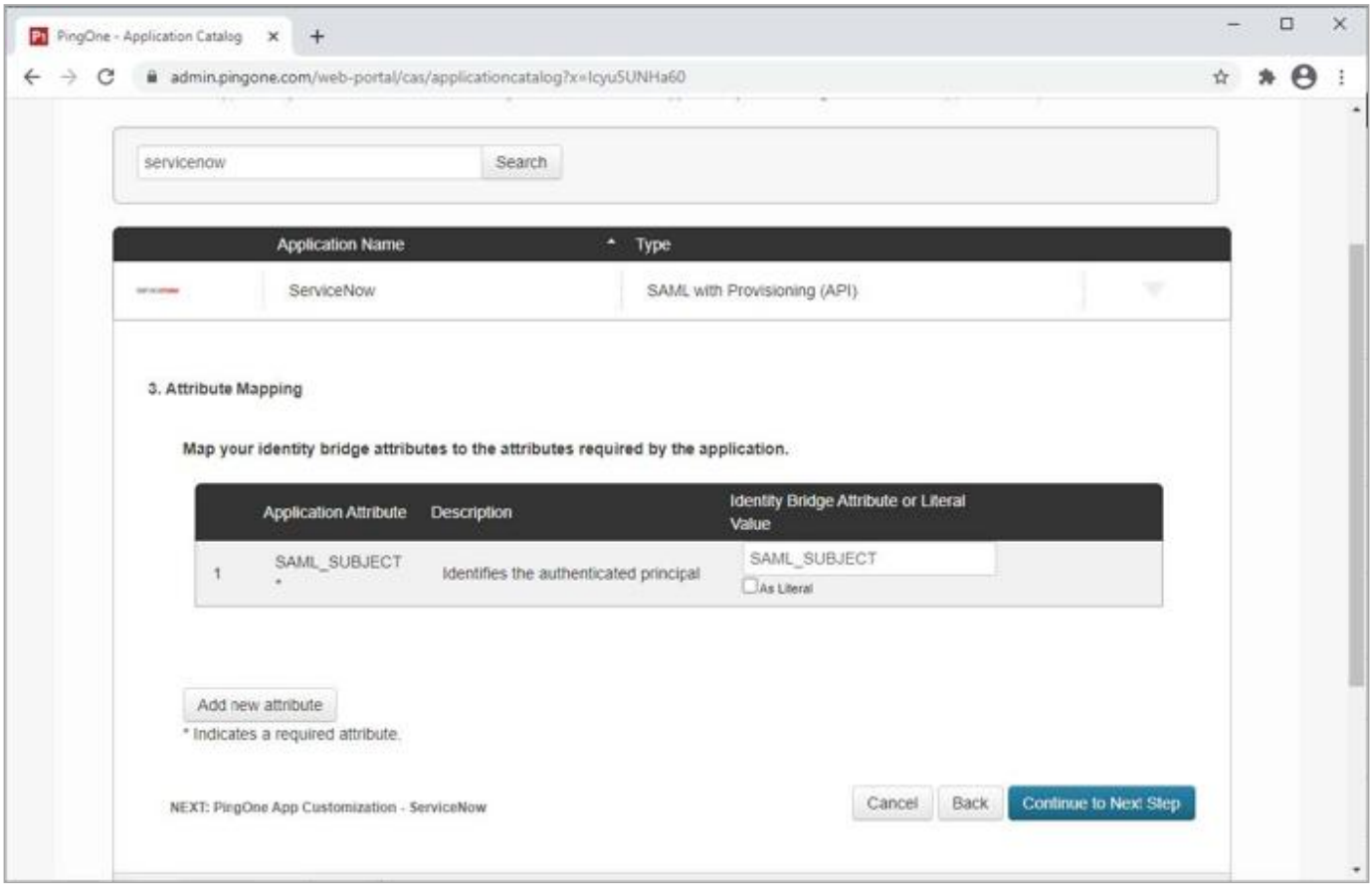


5. Click **Continue to Next Step**.
6. Verify the following:
    - **ACS URL** is set to `https://tenant.service-now.com/navpage.do`.
    - **Entity ID** is set to `https://tenant.service-now.com`.



7. Click **Continue to Next Step**.

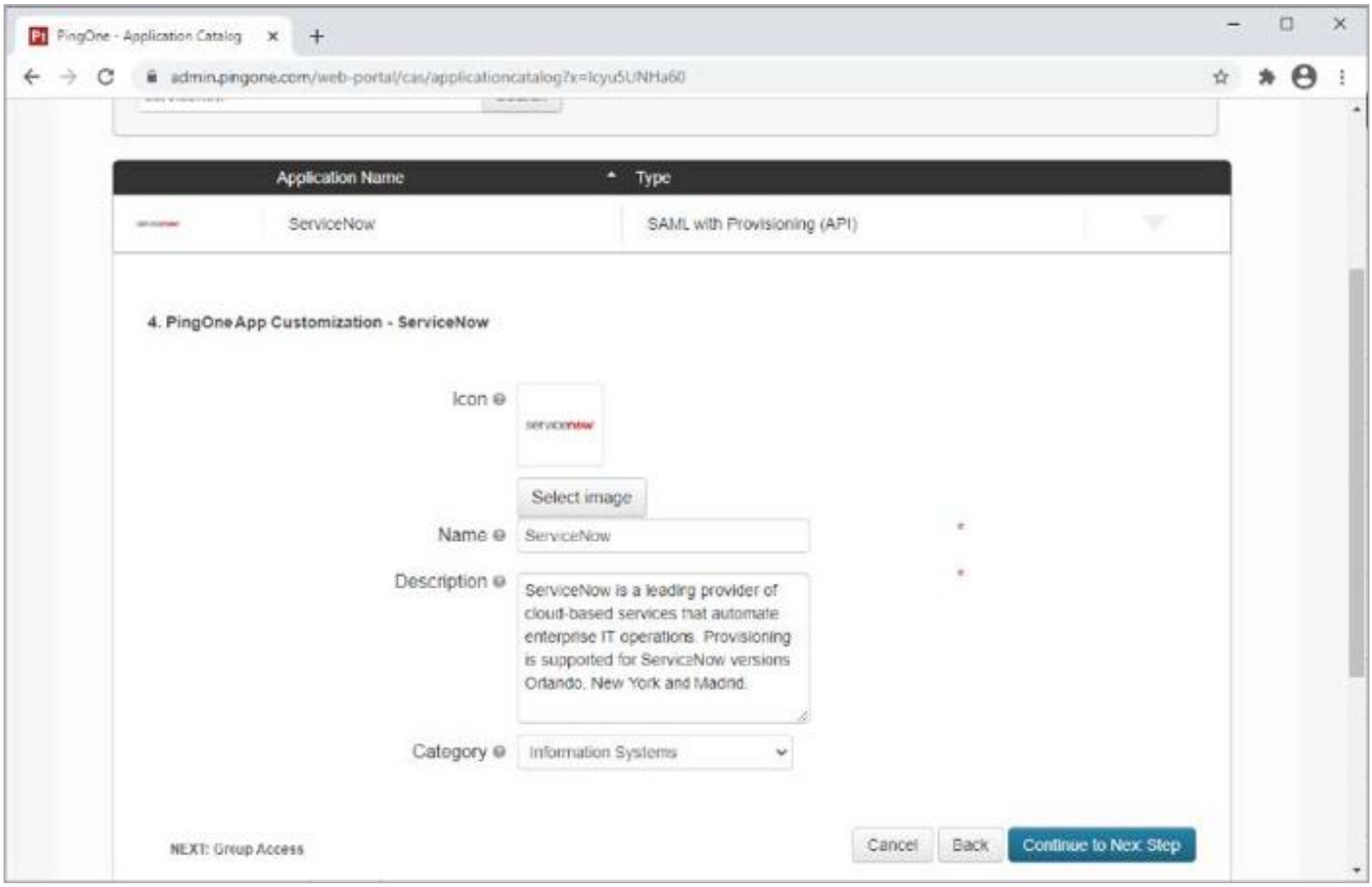
8. In the **Attribute Mapping** section, in the **Identity Bridge Attribute or Literal Value** column of the **SAML_Subject** row, select a suitable attribute, such as **SAML_SUBJECT**.



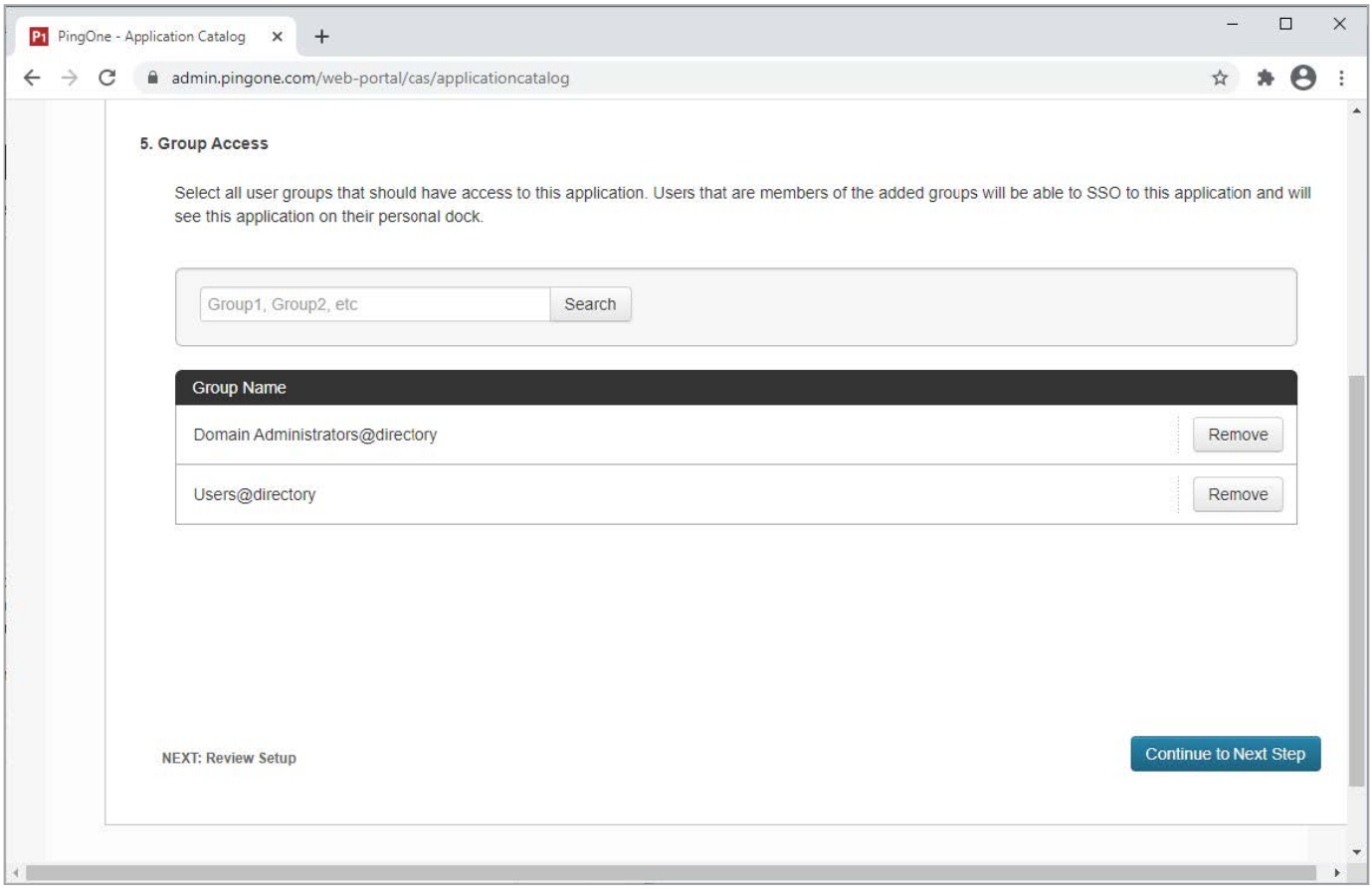
NameID is configurable in ServiceNow.

> **Note**
>
> This guide assumes email is used and that **SAML_SUBJECT** contains the email address for the user in PingOne for Enterprise.

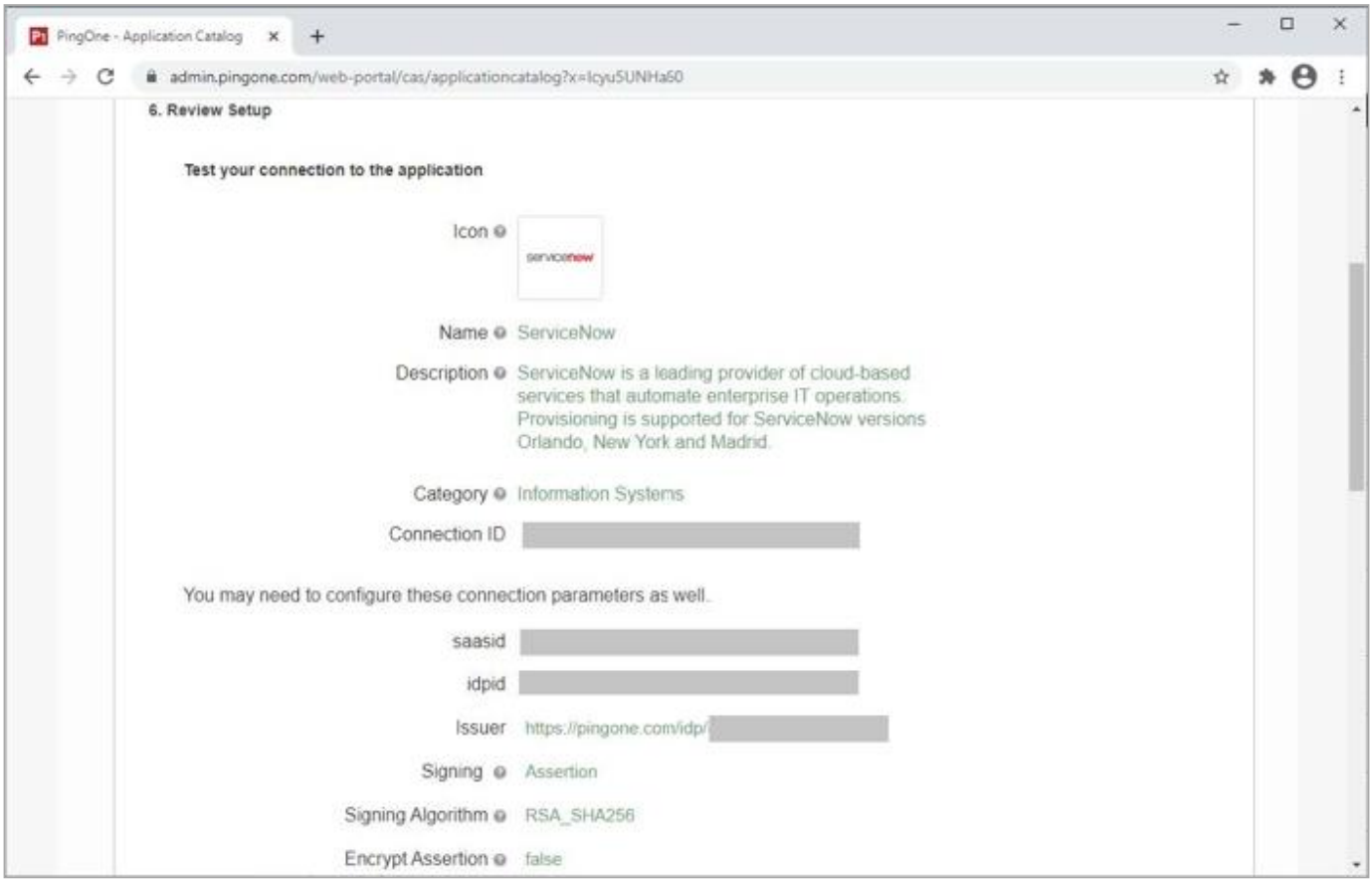
9. Click **Continue to Next Step**.
10. Update the **Name**, **Description**, and **Category** fields as required.

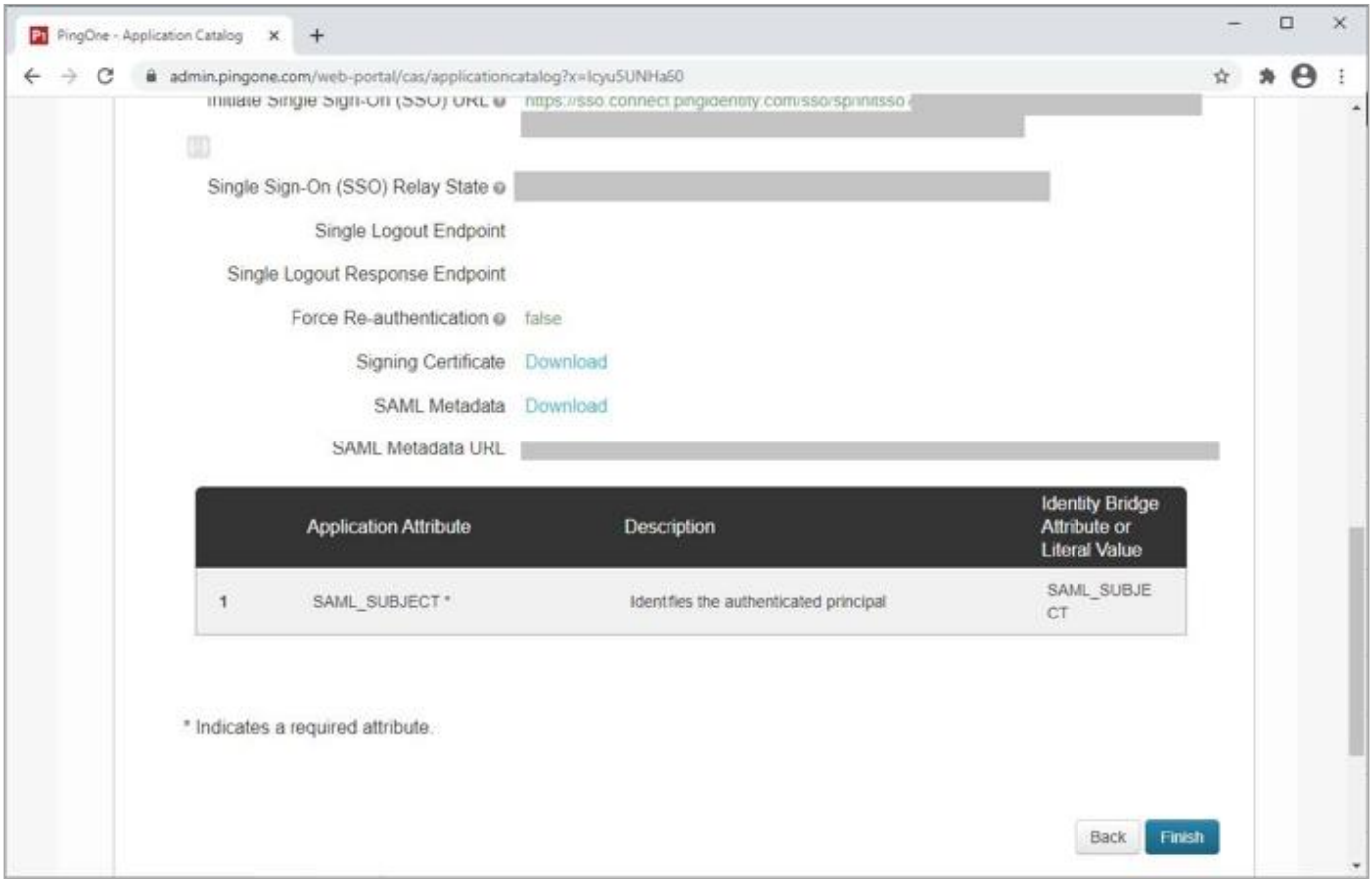


11. Click **Continue to Next Step**.
12. Add suitable user groups for the application.



13. Click **Continue to Next Step**.
14. Review the settings.





15. Copy the **Single Sign-On (SSO) URL** value to a temporary location.

    This is the IdP-initiated SSO URL that you can use for testing.

    > **Note**
    >
    > Make a note of the following values. You'll use them later in the ServiceNow configuration:
    > - PingOne for Enterprise **Issuer**
    > - PingOne for Enterprise **idpid**

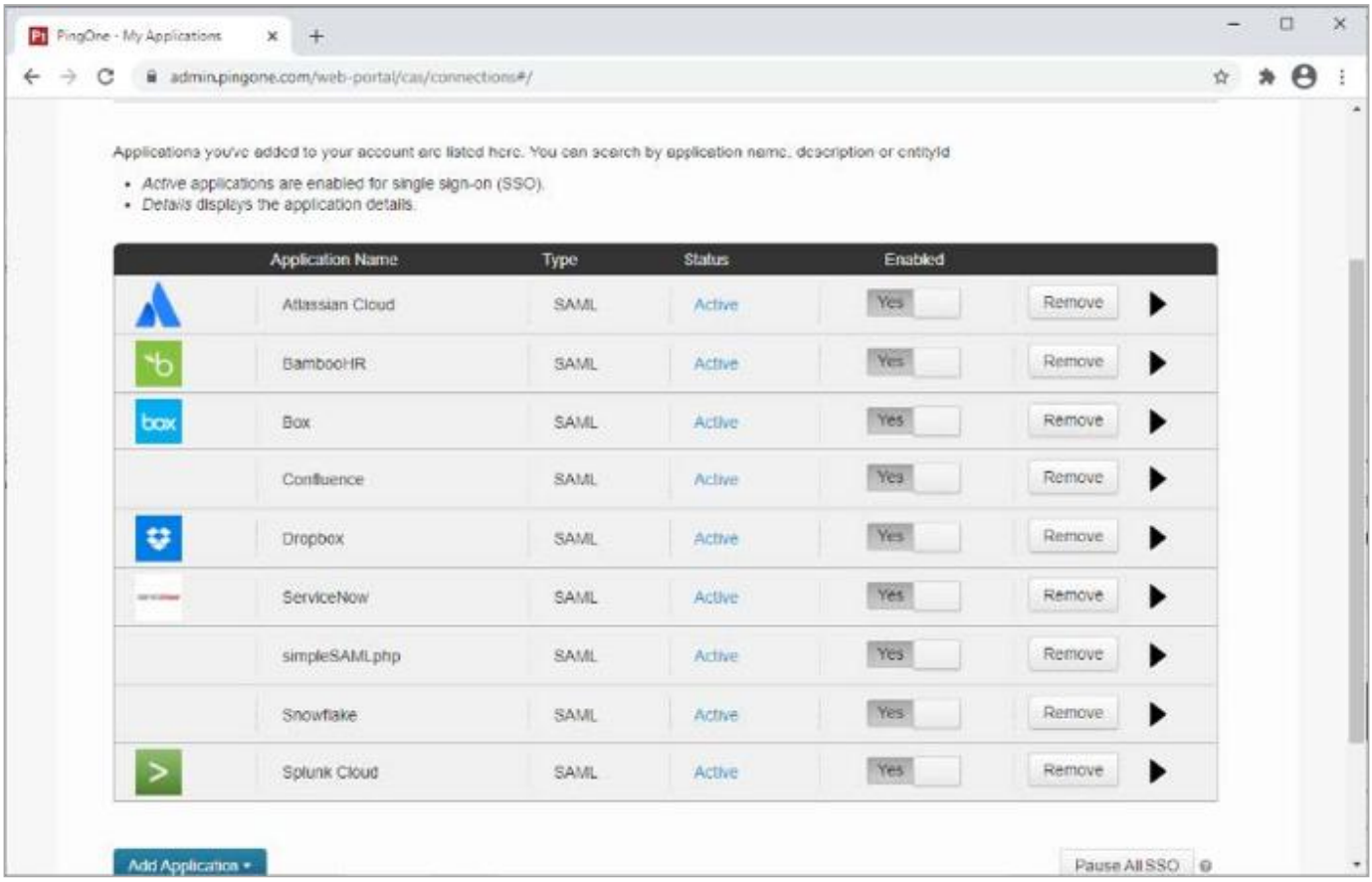
16. On the **SAML Metadata** line, click **Download**.

    You will use this later for the ServiceNow configuration.

17. On the **Signing Certificate** line, click **Download**.

    You will use this later for the ServiceNow configuration.

18. Click **Finish**.



Configure the PingOne for Enterprise IdP connection for ServiceNow

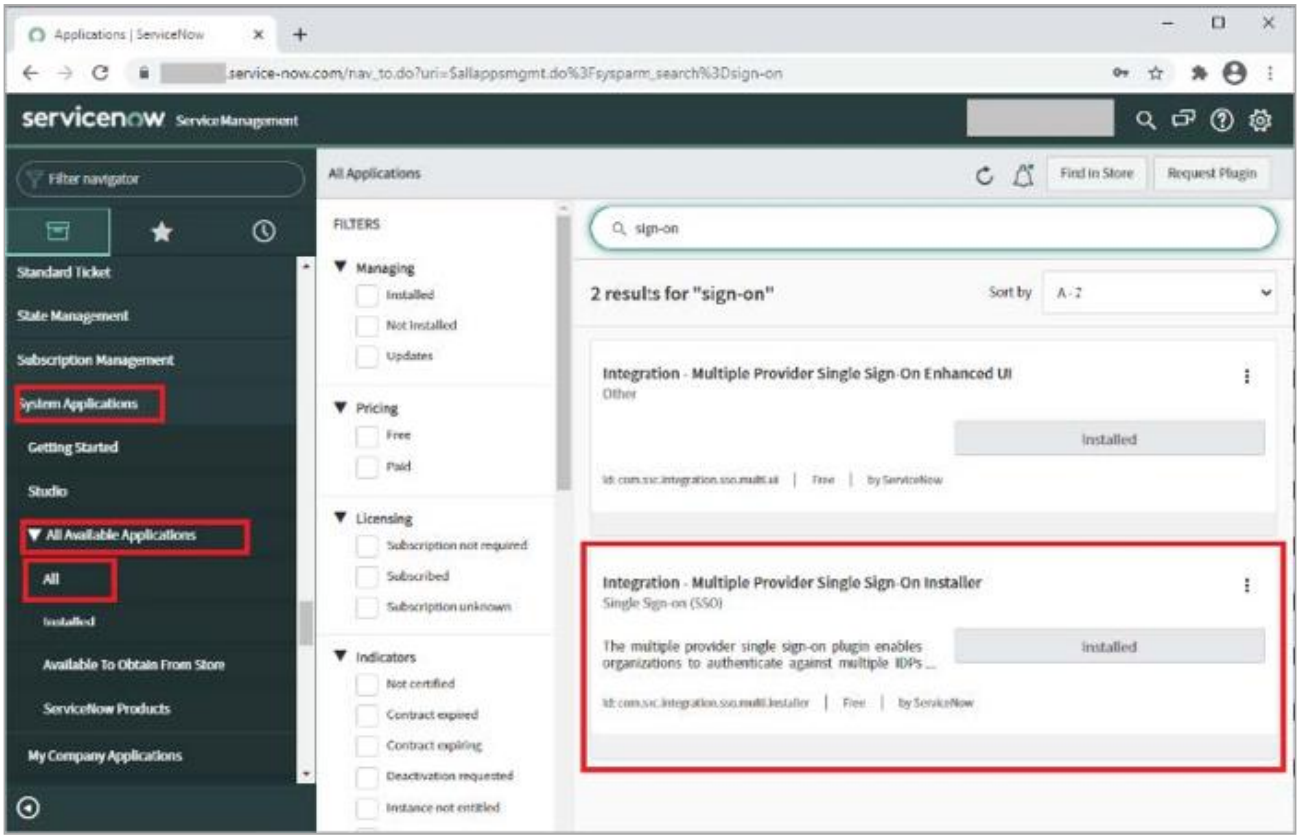
1. Sign on to ServiceNow as an administrator.
2. Activate SAML 2.0:
    1. Go to **System Applications**.

2. Click **All Available Applications**.

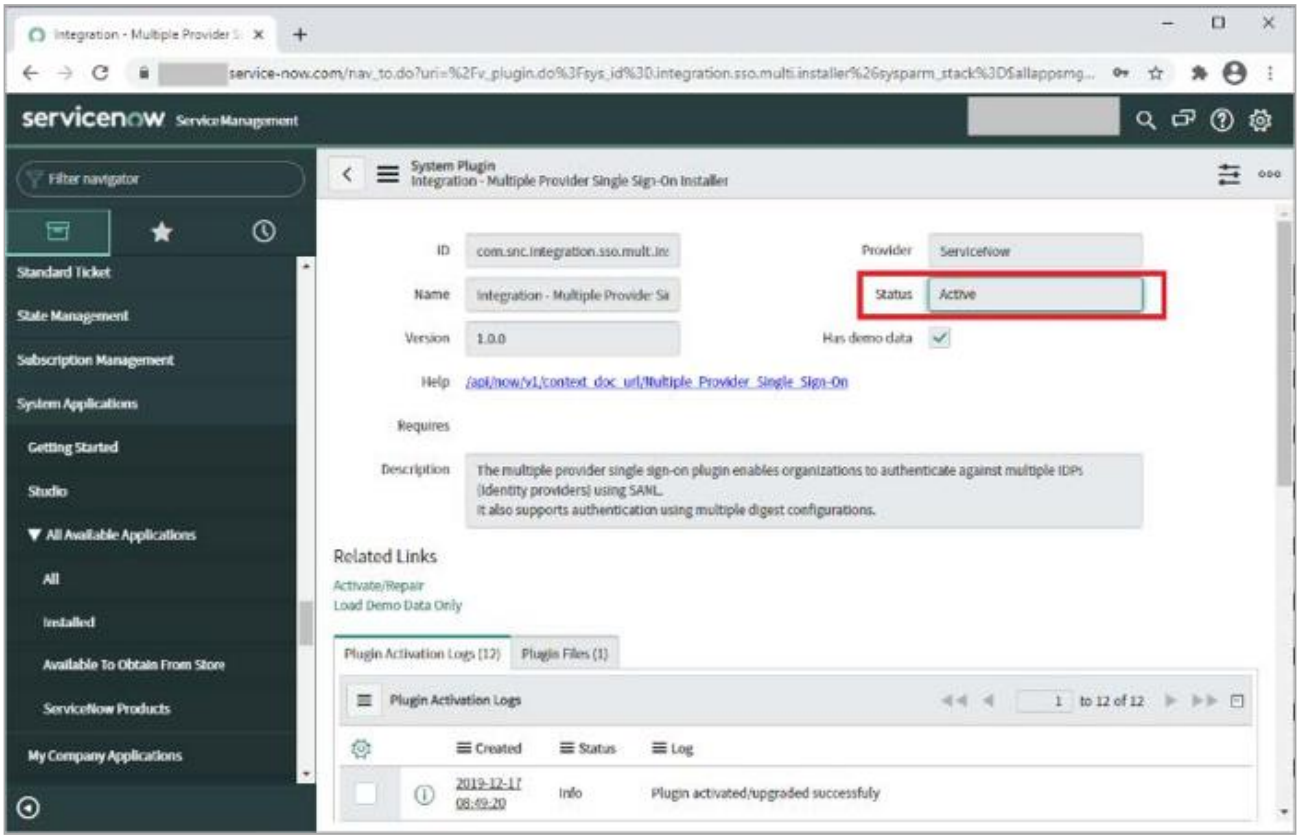
3. Click **All**.

4. Locate the **Integration - Multiple Provider Single Sign-On Installer** plugin.

> **Note**
>
> If you can't find the plugin, you can request it from ServiceNow customer support.

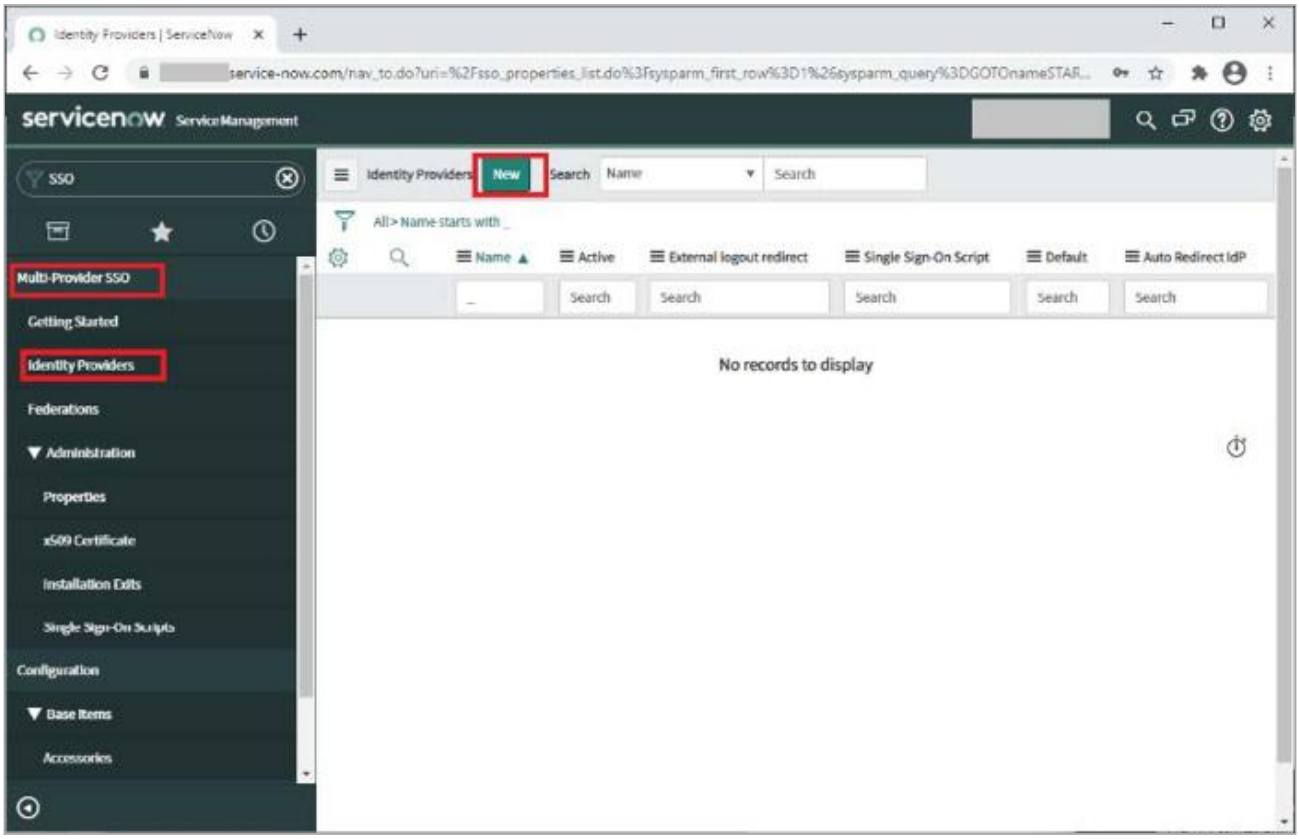


5. Check if the plugin is installed. If the plugin is not installed, click **Install**.

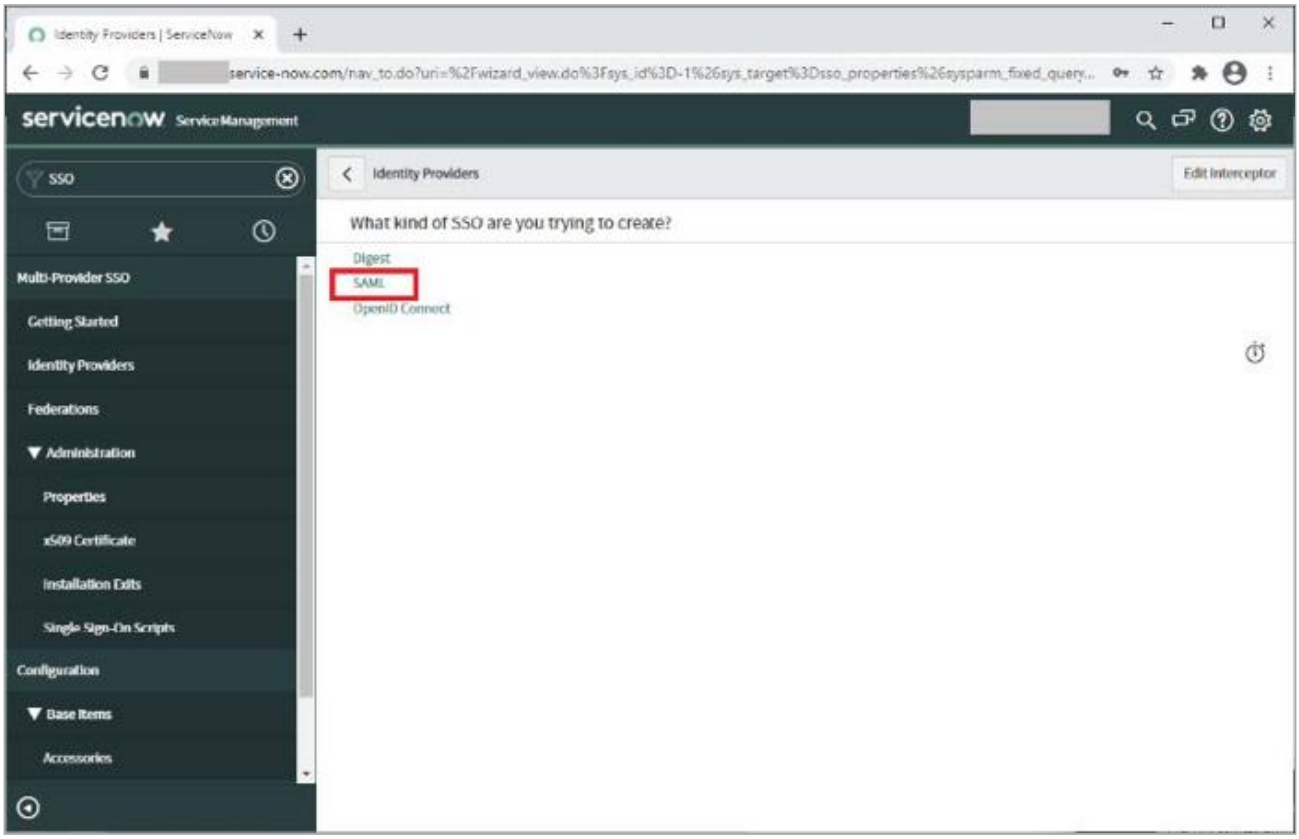


3. Configure a new identity provider:

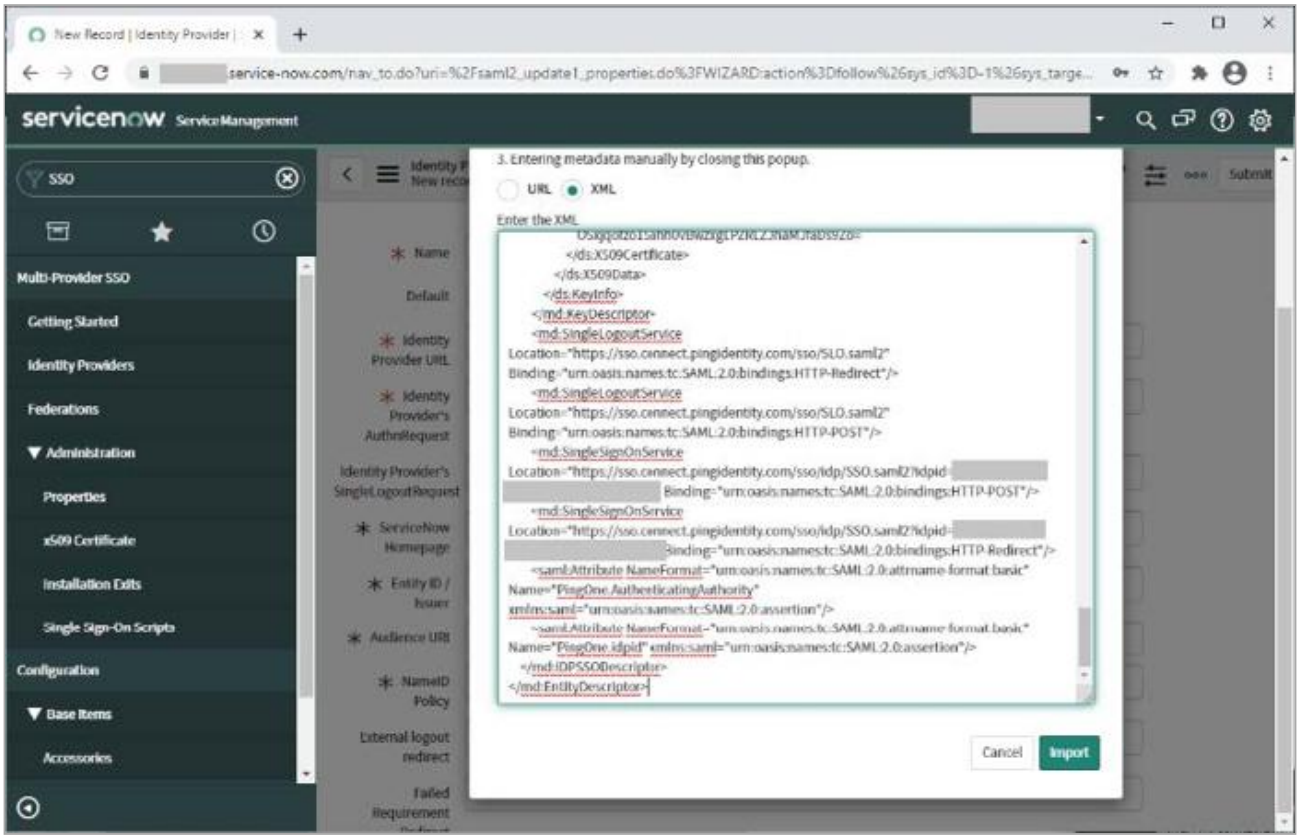
    1. In the left navigation pane, select **Multi-Provider SSO**.



2. Click **Identity Providers**.
3. Click **New**.
4. Click **SAML**.



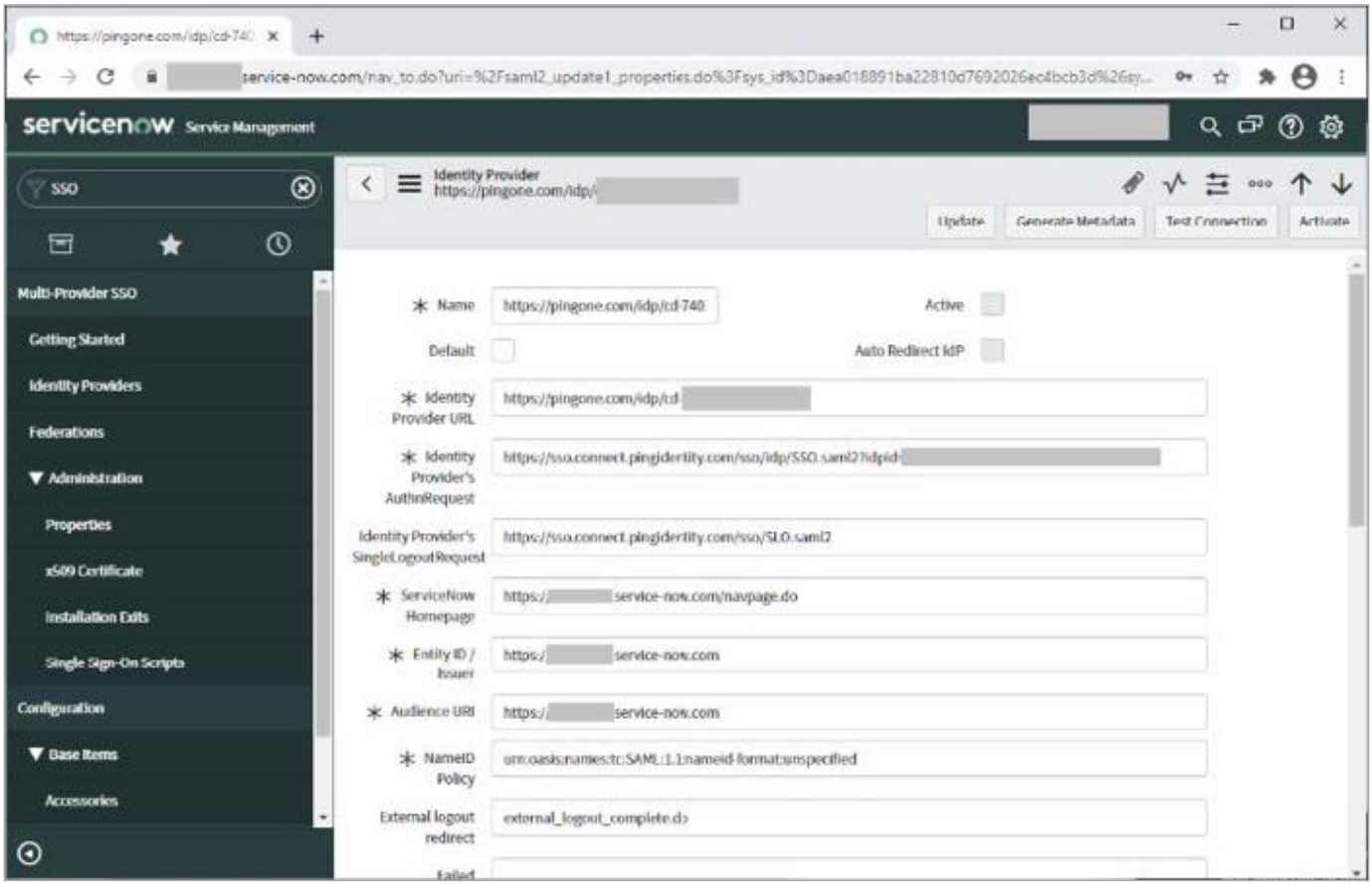
5. Click **XML**.
6. Paste the contents of the PingOne for Enterprise metadata file that you previously downloaded into the **Enter the XML** field.



7. Update the **NameID Policy** to `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`.
8. Click **Update**.
9. Click **Test**.

   A browser window opens to validate the configuration. It prompts you to authenticate at the IdP and then sign out of the session. If successful, you can then activate the connection.
10. Click **Activate**.

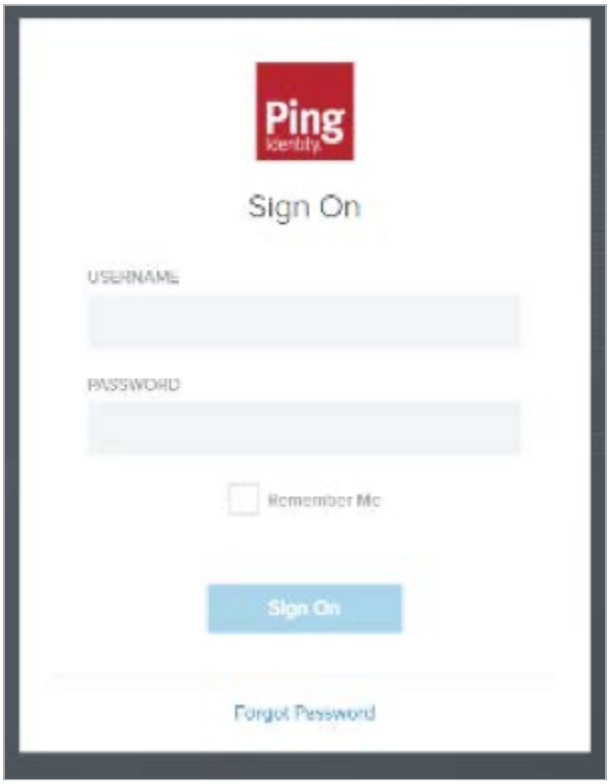
If you receive an error stating that you must test the connection, something failed in the test. Validate the settings, and use the **Script Debugger → Debug** log to re-run the test to determine the cause of the failure.

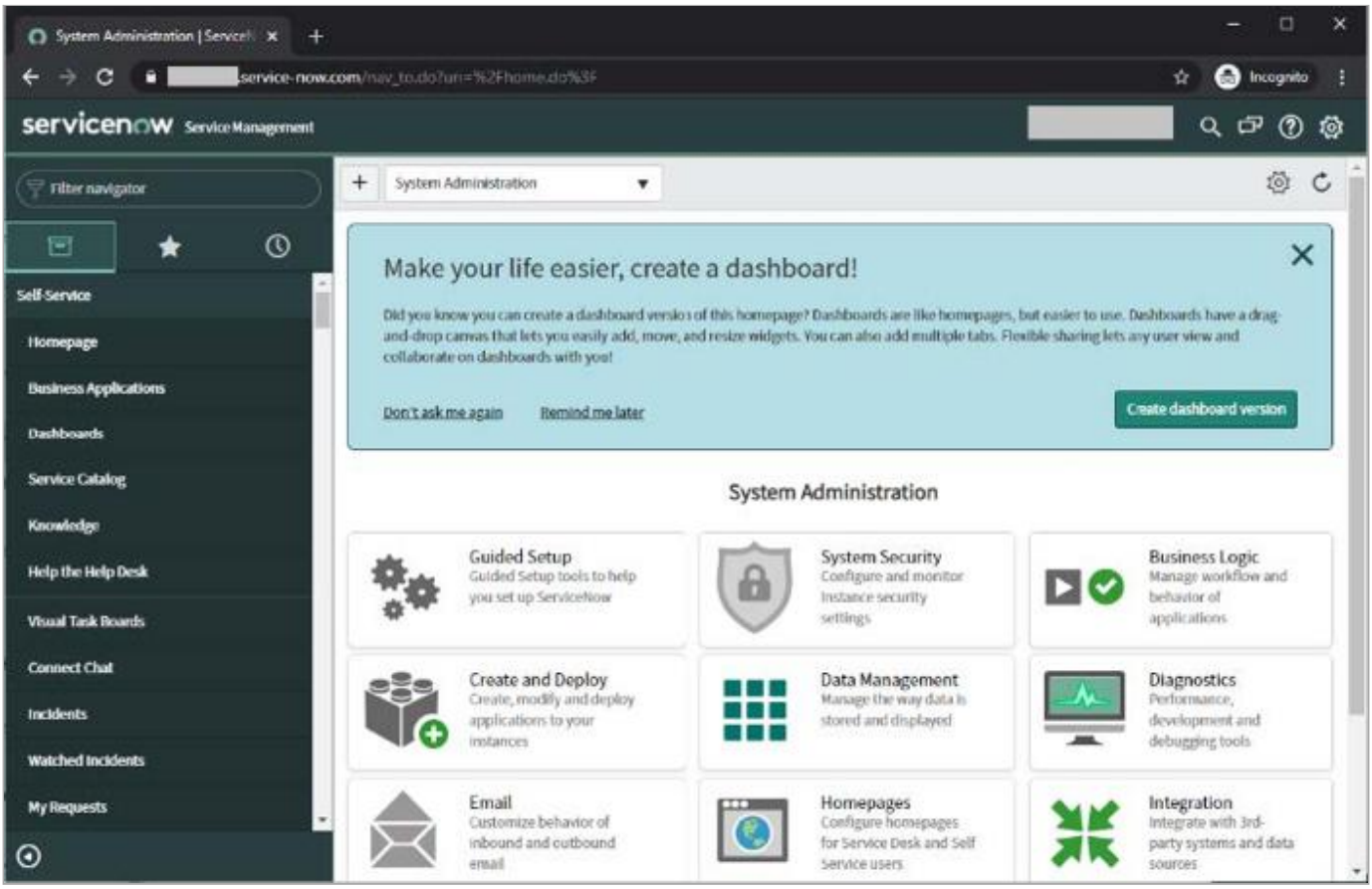


Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to the **Single Sign-On (SSO) URL** from the PingOne for Enterprise application configuration to perform IdP-initiated SSO.

   For example, `https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=saasid&idpid=idpid`

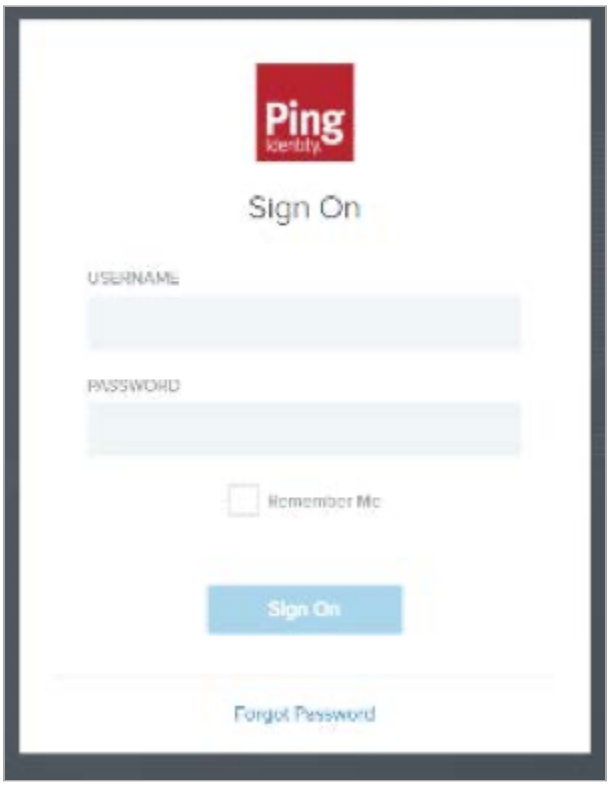


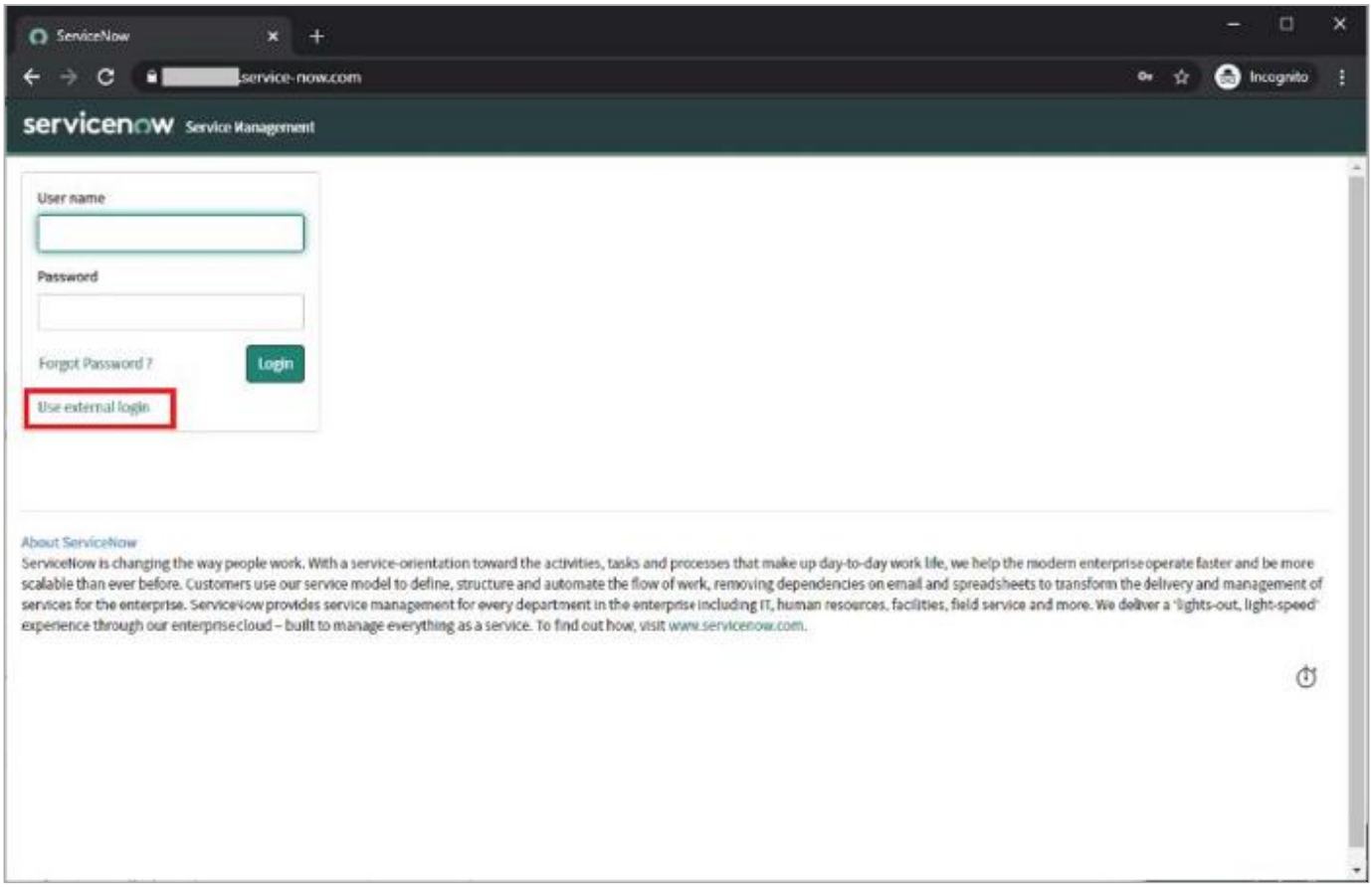


Test the PingOne for Enterprise SP-initiated SSO integration

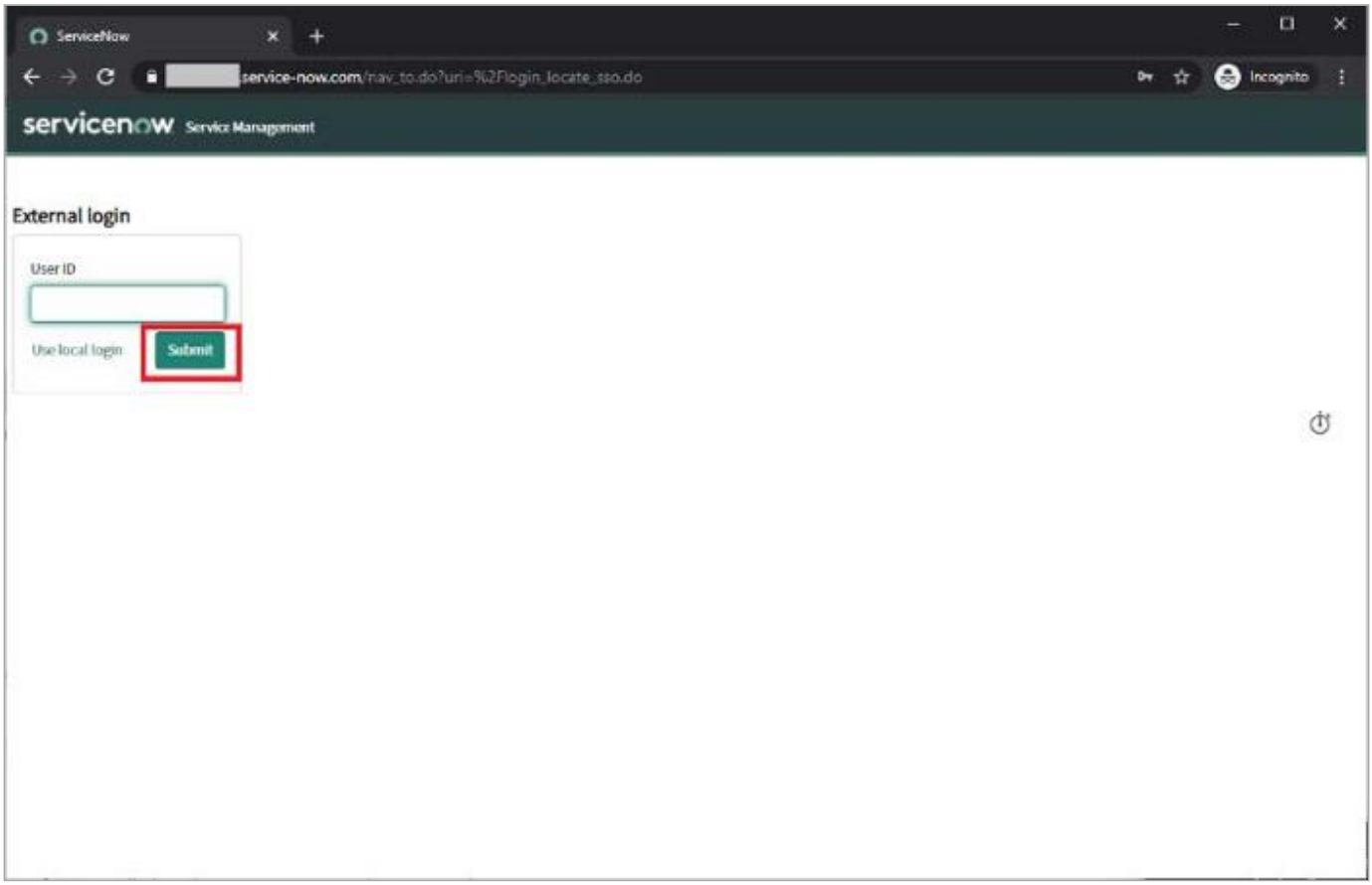
1. Go to your ServiceNow URL.

   For example, `https://your-environment.service-now.com`





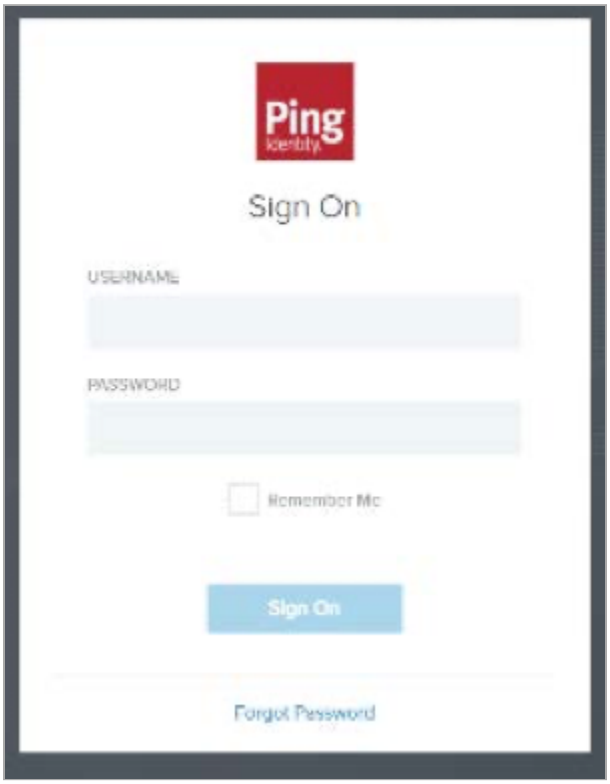
2. Click **Use external login**.

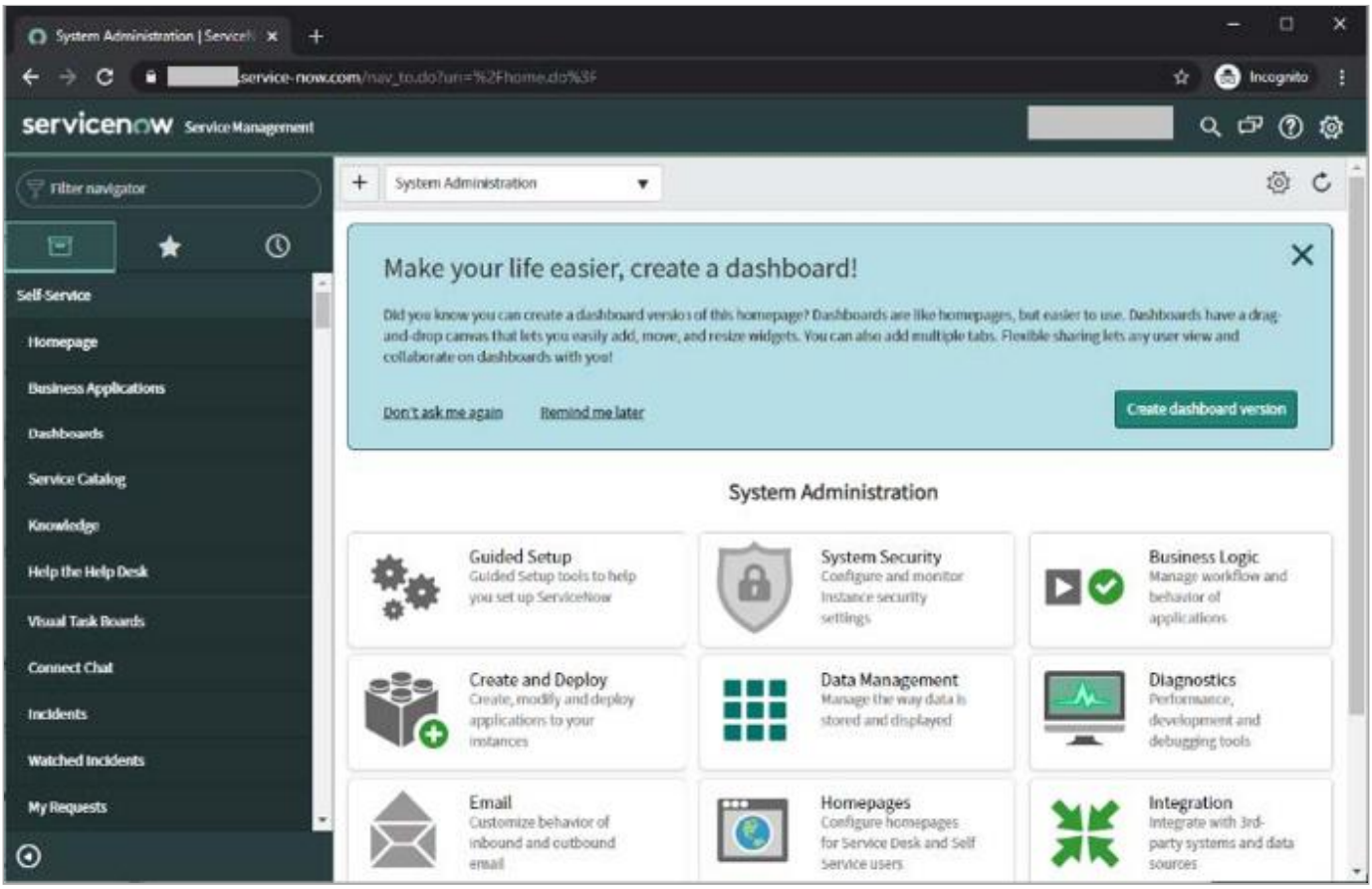


3. Click **Submit**.
4. Click **Continue**.

   You're redirected to PingOne for Enterprise for authentication.

5. After you're redirected to PingOne for Enterprise, enter your PingOne username and password.





Slack

Configuring SAML SSO with Slack and PingFederate

Enable Slack sign-on from a PingFederate URL (IdP-initiated sign-on) and direct Slack sign-on using PingFederate (SP-initiated sign-on) with JIT provisioning.

Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users that require application access.
- You must have administrative access to PingFederate and Slack.

Create a PingFederate SP connection for Slack

1. Sign on to the PingFederate administration console.
2. Create a service provider (SP) connection for Slack in PingFederate:
    1. Configure using **Browser SSO** profile **SAML 2.0**.
    2. Set **Partner's Entity ID** to `https://slack.com`.
    3. Enable the following **SAML Profiles**:
        - **IdP-Initiated SSO**
        - **SP-Initiated SSO**
    4. In **Assertion Creation** > **Attribute Contract**, extend the contract with the following attributes:
        - `SAML_NAME_FORMAT`
        - `User.Email`
        - `User.Username`
        - `first_name`
        - `last_name`

       Use the following attribute name format:

       `urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified`
    5. In **Assertion Creation → Authentication Source Mapping → Attribute Contract Fulfillment**:
        1. Map **SAML_SUBJECT**, **User.Email**, **User.Username**, **first_name**, and **last_name**.
        2. Map **SAML_NAME_FORMAT** to a text value of `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`.

6. In **Protocol Settings → Assertion Consumer Service URL**, set the following properties:
    - Set **Binding** to **POST**.
    - Set **Endpoint URL** to `https://your-slack-domain.slack.com/sso/saml`.
7. In **Protocol Settings → Allowable SAML Bindings**, enable **POST** and **REDIRECT**.
8. In **Protocol Settings → Signature Policy**, select **Always Sign Assertion**.
9. In **Credentials → Digital Signature Settings**, select the **PingFederate Signing Certificate**.

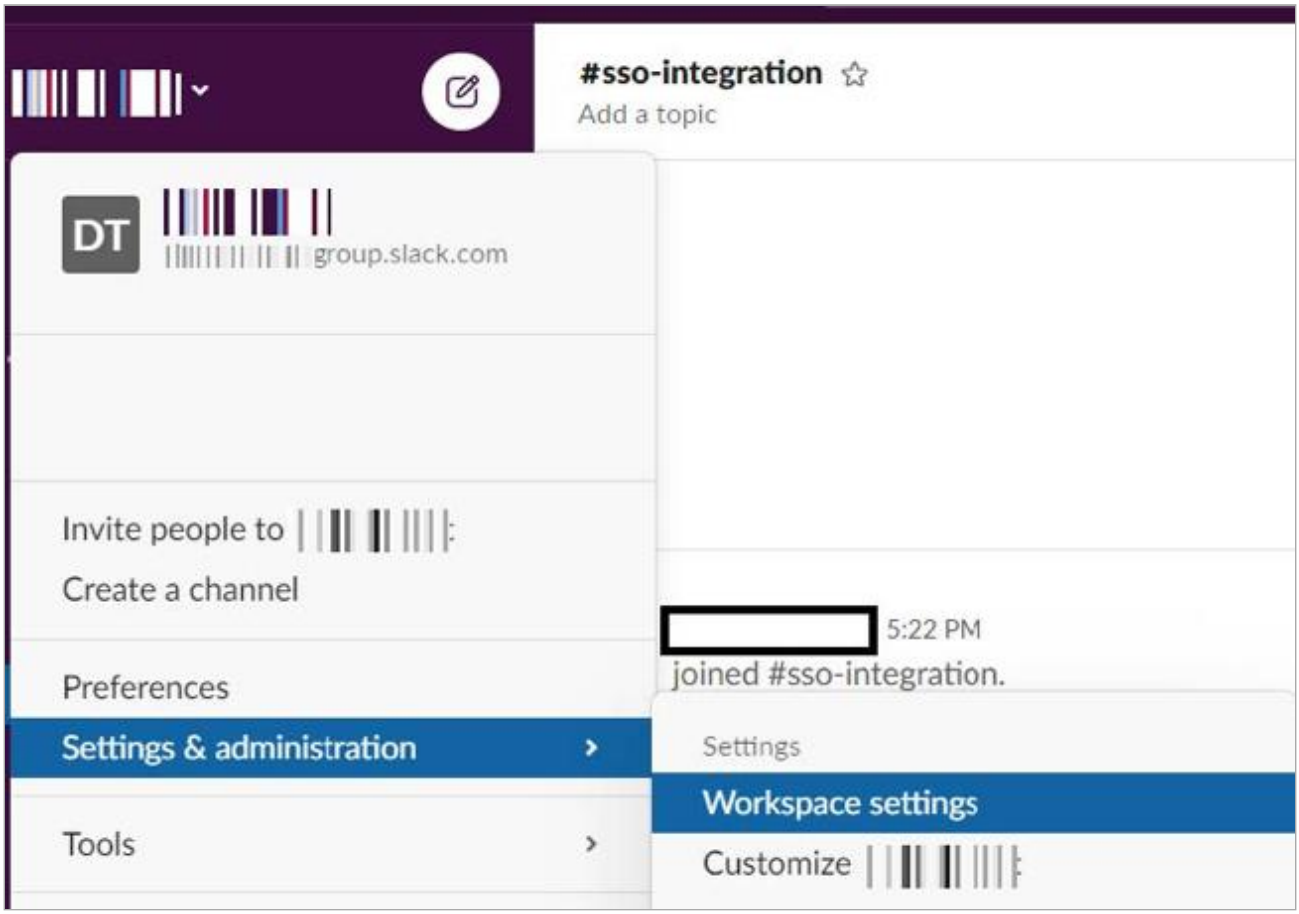
3. Save the configuration.
4. Export the signing certificate.
5. Export the metadata file, open it in a text editor, and copy:
    - The entityID
    - The Location entry, `https://your-value/idp/SSO.saml2`

Add the PingFederate connection to Slack

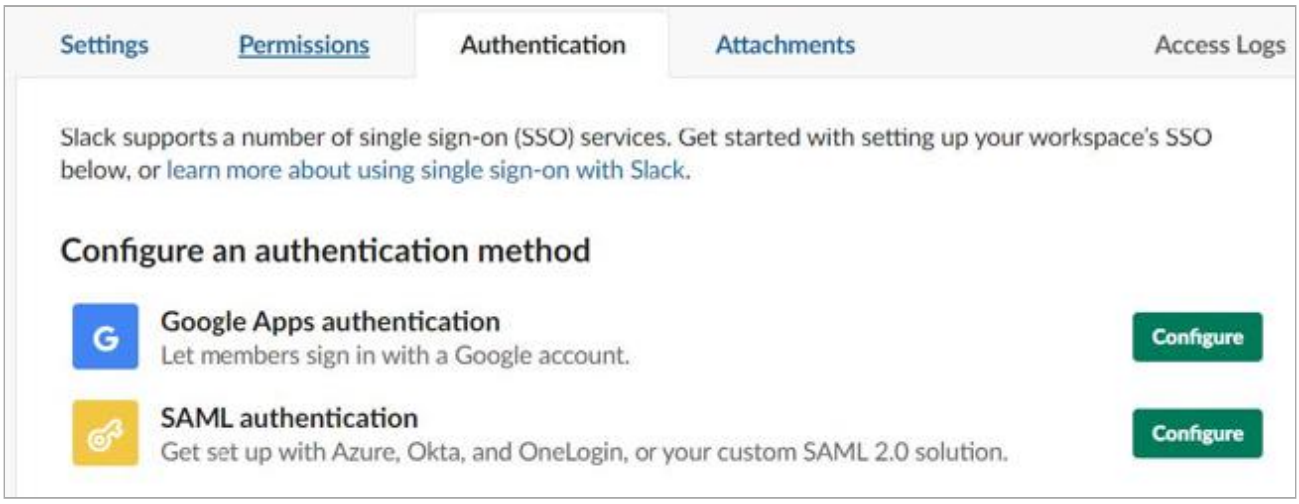
Choose from:

For Slack Standard or Plus, do the following

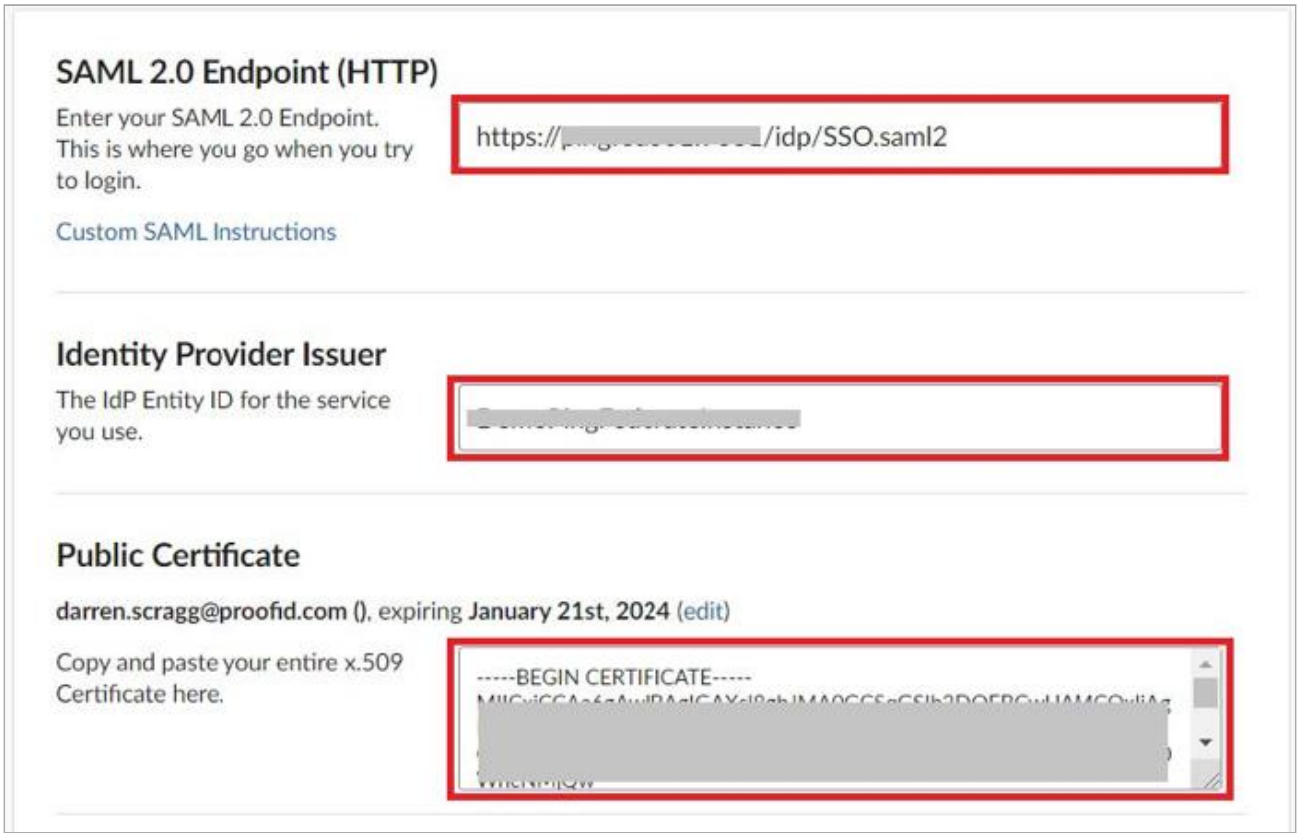
1. Sign on to your Slack Workspace as an administrator.
2. Go to **Settings & Administration → Workspace Settings**.



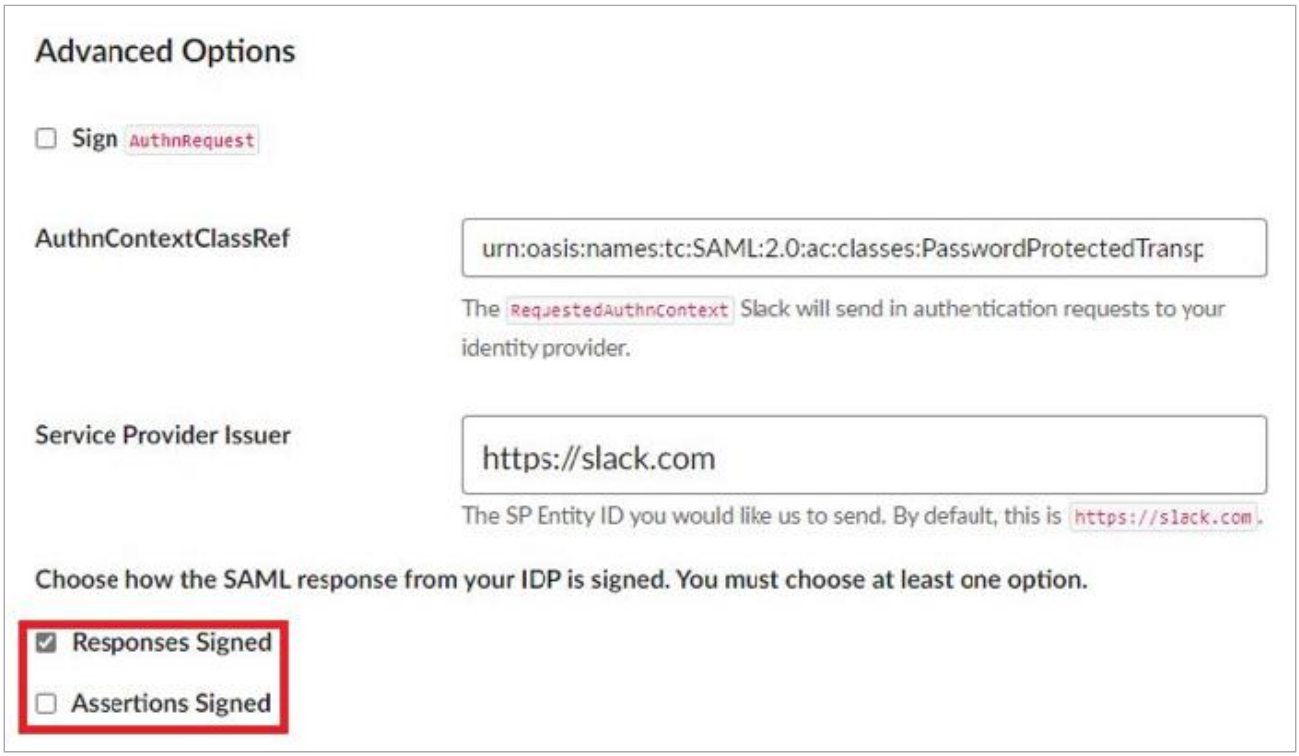
3. Click the **Authentication** tab.
4. In the **Configure an authentication method** section, on the **SAML authentication** line, click **Configure**.



5. If prompted, enter your password to continue.
6. In the **SAML 2.0 Endpoint (HTTP)** field, enter the PingFederate **Location** value.
7. In the **Identity Provider Issuer** field, enter the PingFederate **entityID** value.
8. In the **Public Certificate** field, paste in the contents of the PingFederate signing certificate.

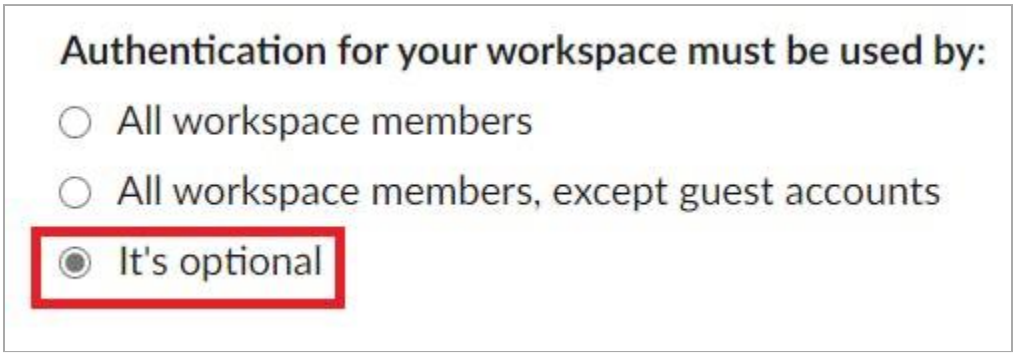


9. Expand the **Advanced Options** section, and clear the **Assertions Signed** check box.

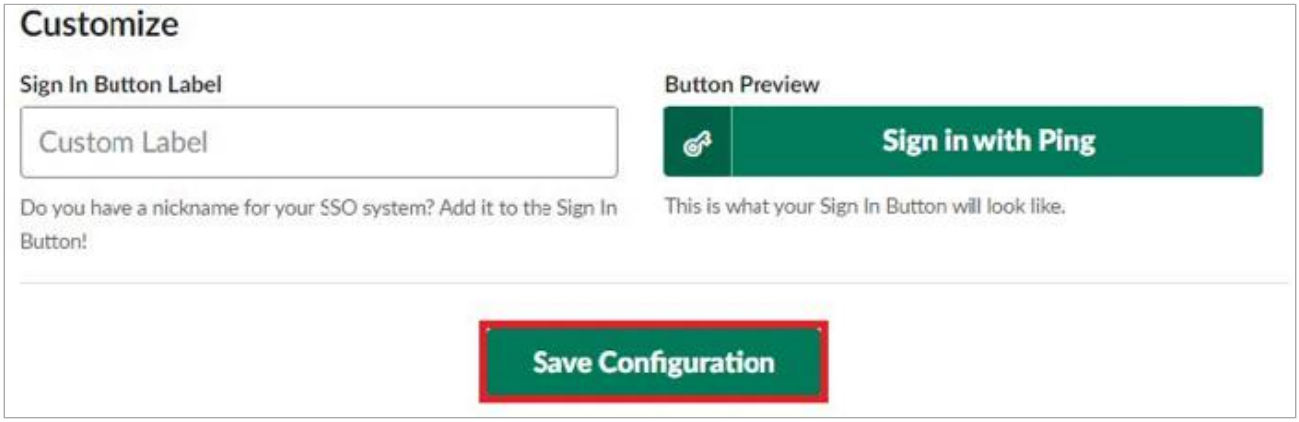


10. In the **Settings** section, select the **It's optional** radio button for the authentication setting.

> **Note**
>
> You can change the authentication setting to your desired value after you have completed testing.



11. Click **Save Configuration**.

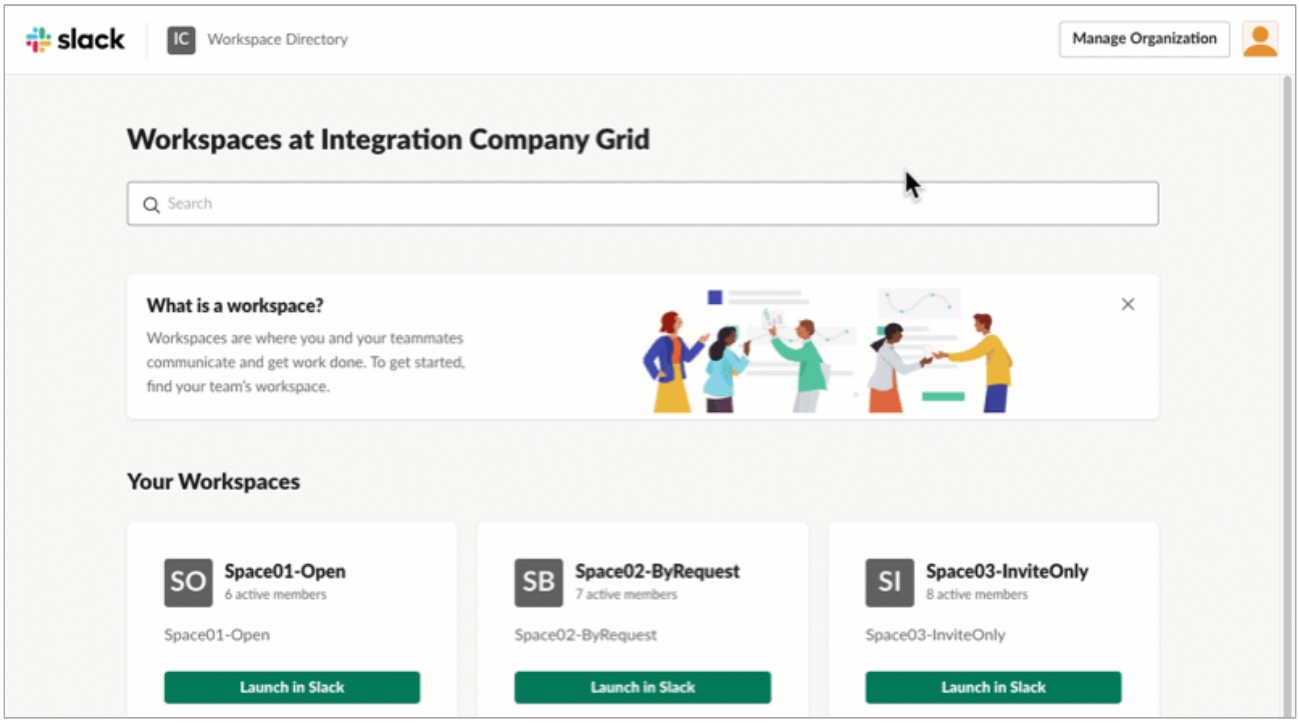


12. When you're redirected to PingFederate, authenticate with PingFederate.

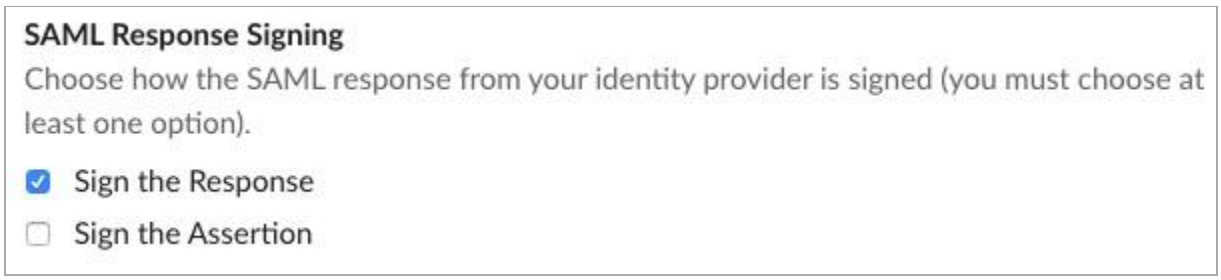
    Your selection is confirmed against PingFederate and saved if successful.

For Slack Enterprise Grid, do the following

1. Sign on to your Slack Organization (not Workspace) as an administrator.
2. Go to **Manage Organization → Security → SSO Settings → Configure SSO**.



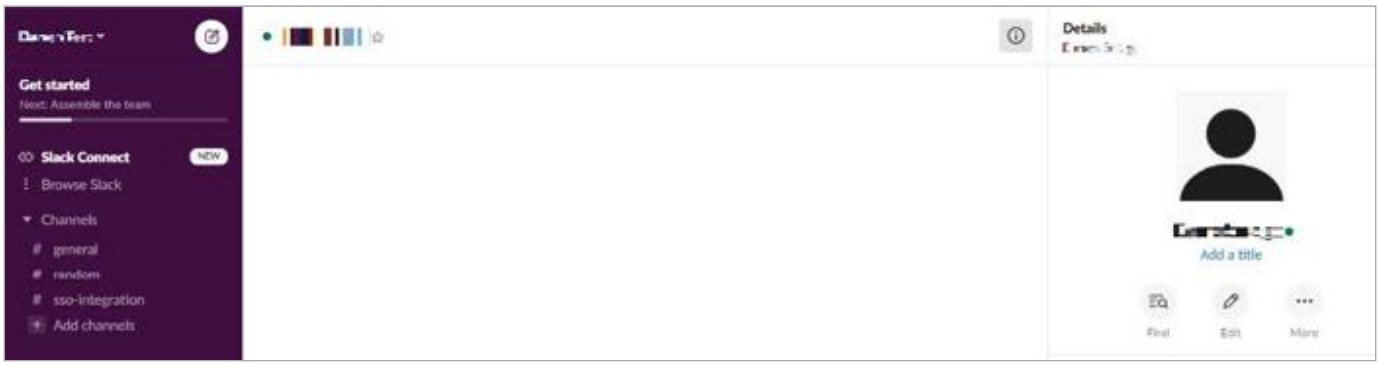
3. In the **SAML 2.0 Endpoint (HTTP)** field, enter the PingFederate **Location** value from the metadata file.
4. In the **Service Provider Issuer URL**, use the default value of **https://slack.com**.
5. In the **Public (X.509) Certificate** field, enter the contents of your PingFederate signing certificate.
6. Enable authentication request signing.
    1. Select the **Sign the AuthnRequest** check box.
    2. Copy the certificate text.
    3. Create a new `.crt` file on your computer and paste the certificate text.
    4. In PingFederate, import the `.crt` file as a trusted certificate authority. For help, see Manage Trusted Certificate Authorities in the PingFederate documentation.
7. Clear the **Sign the Assertion** check box.



8. Click **Test Configuration**.
9. Sign out of Slack and then sign back on using SSO.

Test the PingFederate IdP-initiated SSO integration

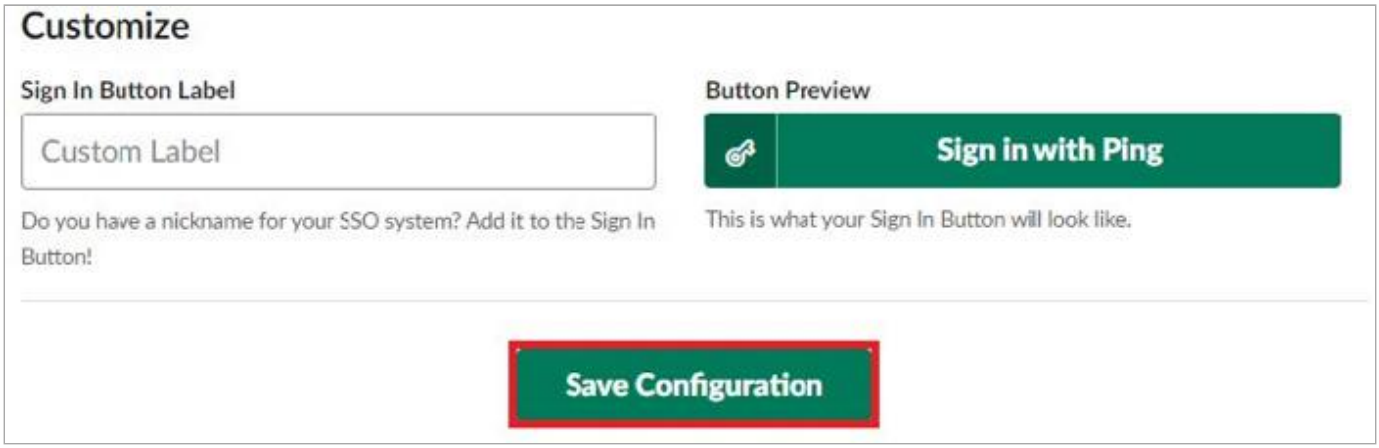
1. Go to the PingFederate SSO application endpoint for the Slack SP connection.
2. Complete the PingFederate authentication.



You're redirected to your Slack domain.

Test the PingFederate SP-initiated SSO integration

1. Go to your Slack domain, `https://your-domain.slack.com`.
2. Click **Sign in with Ping**.



3. After you're redirected, enter your PingFederate username and password.

   After successful authentication, you're redirected back to Slack.

> **Note**
>
> If the user doesn't exist in Slack, you are prompted to accept the Slack terms.

Configuring SAML SSO with Slack and PingOne for Enterprise

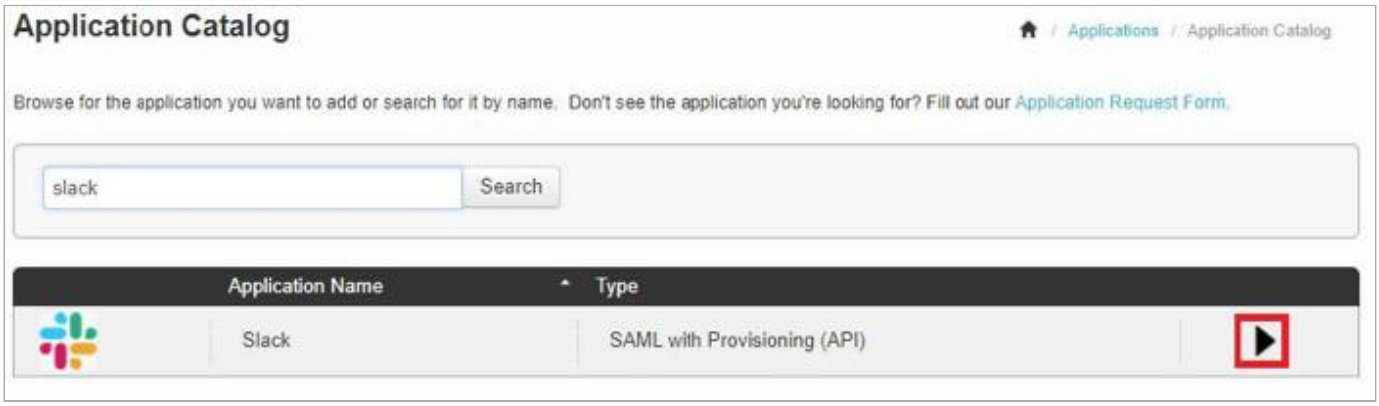
Enable Slack sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct Slack sign-on using PingOne for Enterprise (SP-initiated sign-on) with JIT provisioning.

Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- You must have administrative access to PingOne for Enterprise and Slack.

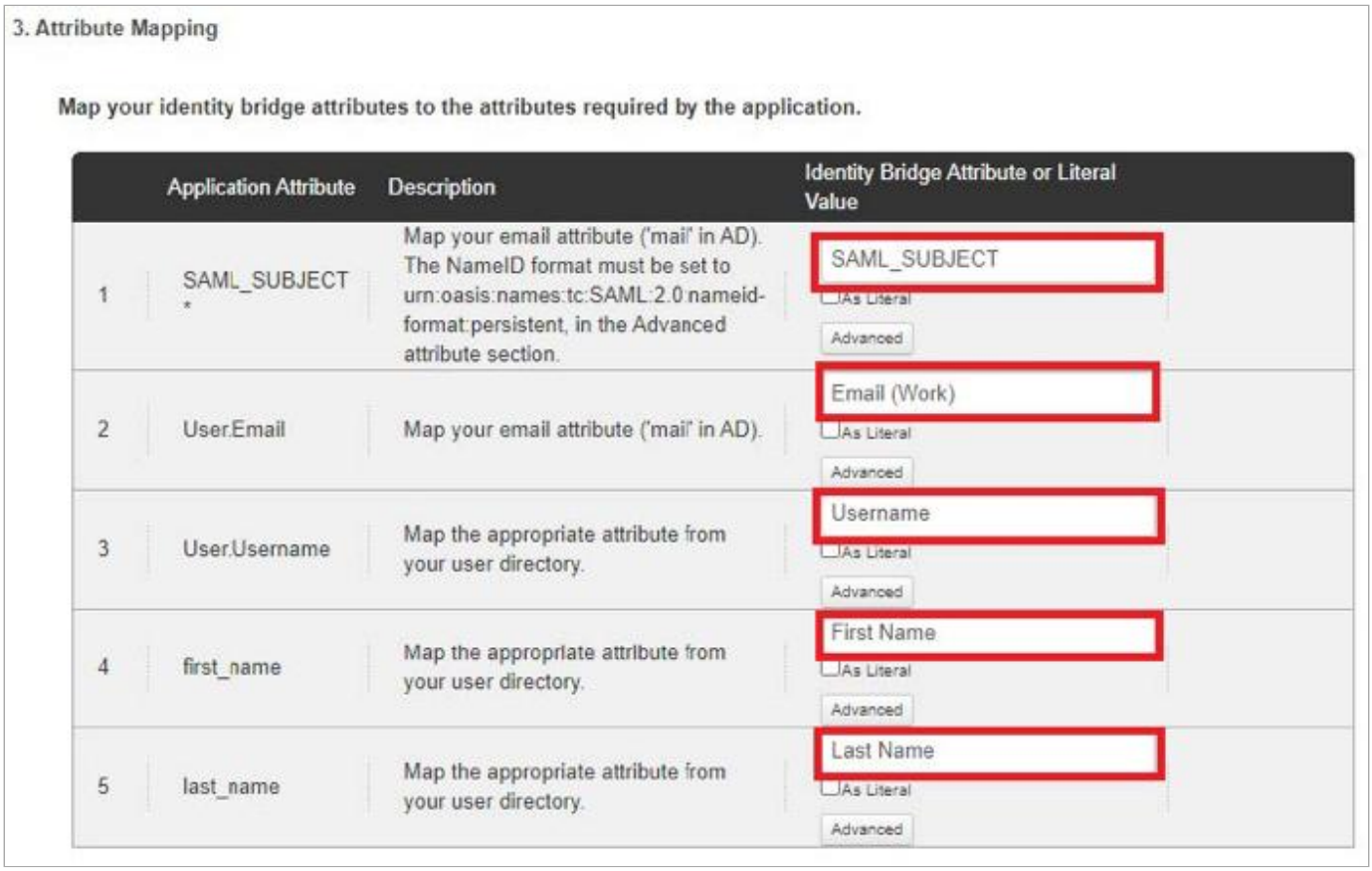
Set up the Slack application in PingOne for Enterprise

1. Sign on to PingOne for Enterprise and go to **Applications → Application Catalog**.
2. Search for `Slack`.



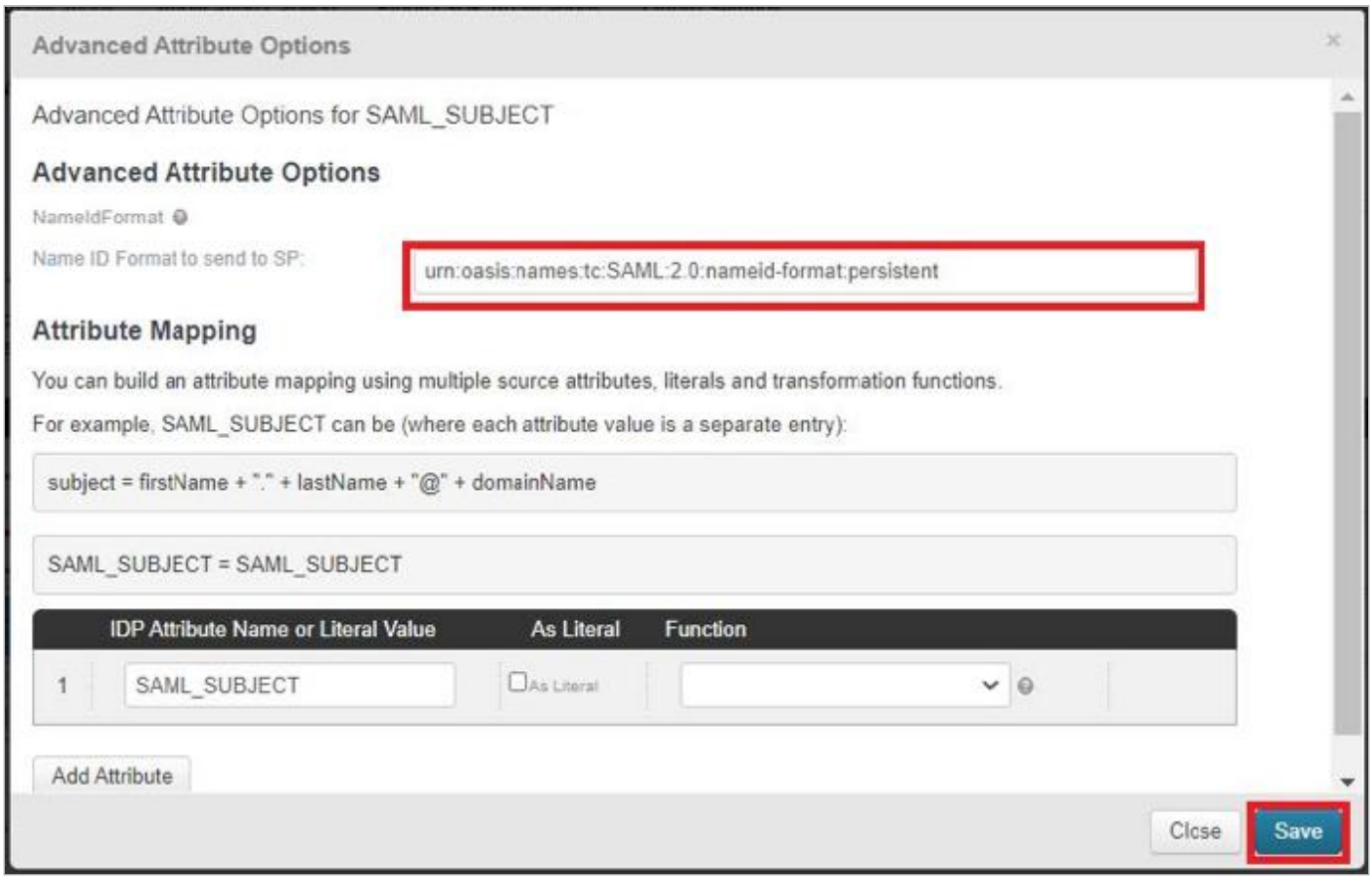
3. Expand the Slack entry and click the **Setup** icon.
4. Copy the **Issuer** and **IdP ID** values.
5. Download the signing certificate.

6. Click **Continue to Next Step**.
7. Set **ACS URL** to `https://your-slack-domain.slack.com/sso/saml`.
8. Click **Continue to Next Step**.
9. In the **Attribute Mapping** section, map the attributes to the corresponding attributes in your userstore.



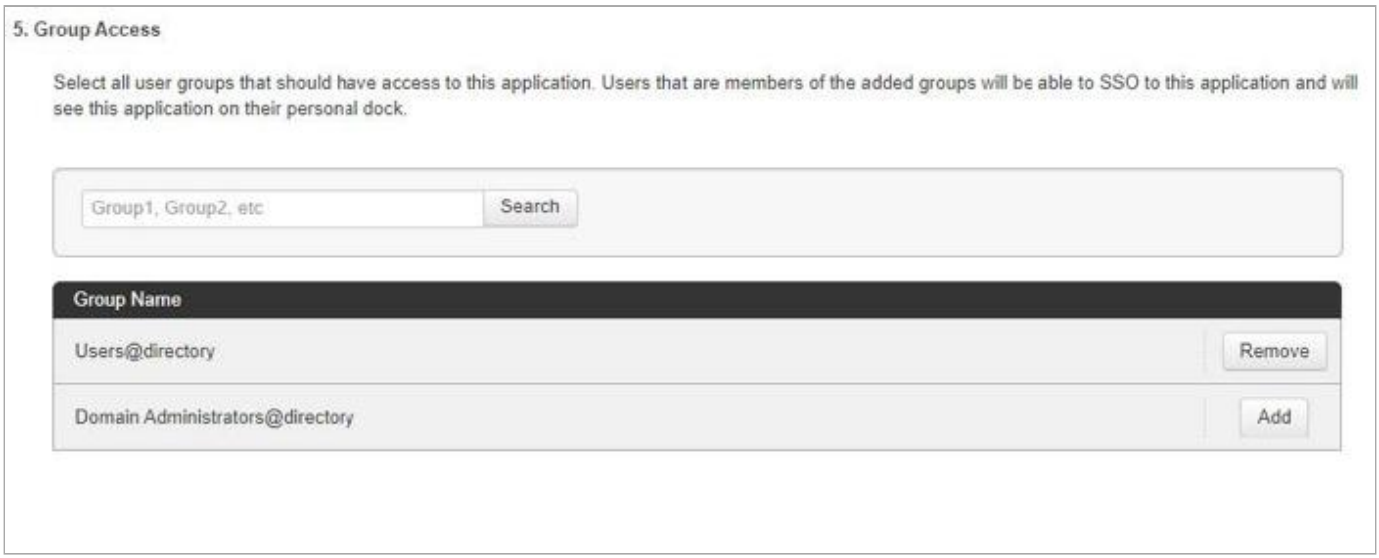
10. In the **SAML_SUBJECT** row, click **Advanced**.
11. In the **NameID Format to send to SP field**, enter `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`.

12. Click **Save**.



13. Click **Continue to Next Step**.

14. Click **Add** for each user group that should have access to Slack.

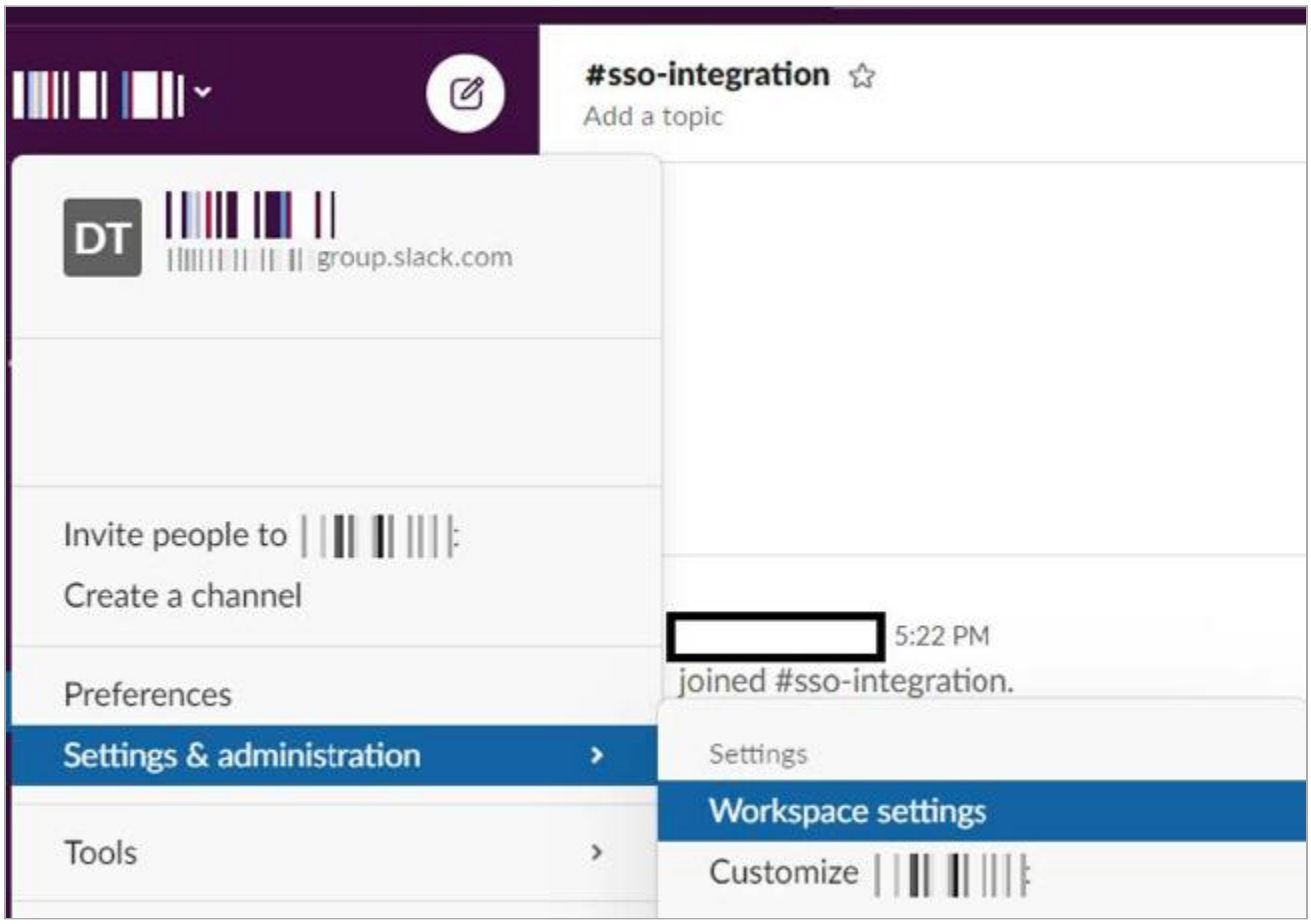


15. Click **Continue to Next Step**.

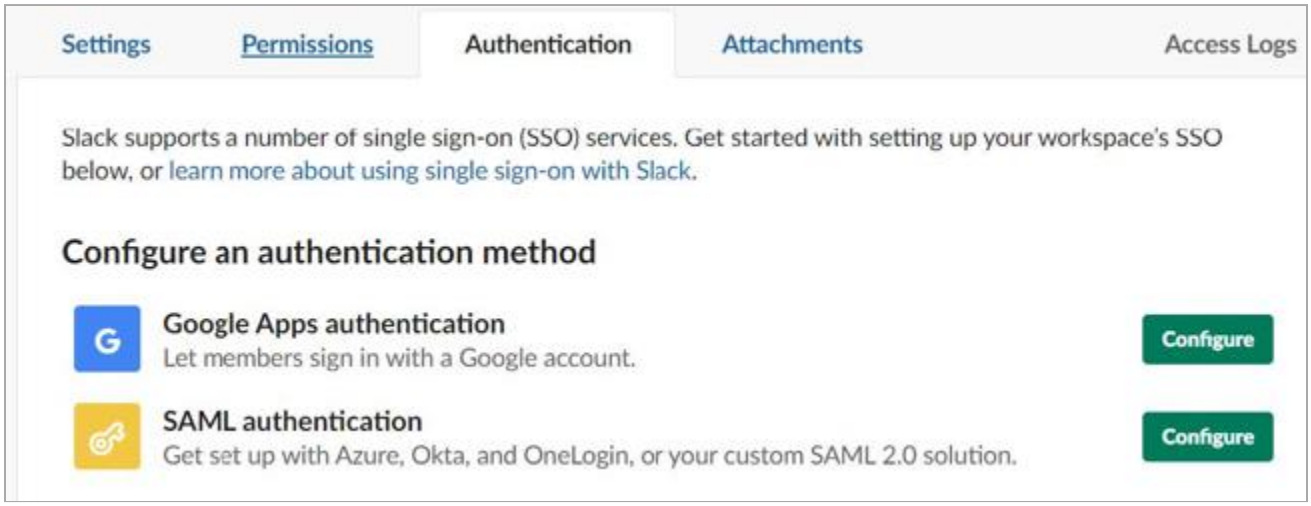
16. Click **Finish**.

Add the PingOne for Enterprise IdP connection to Slack

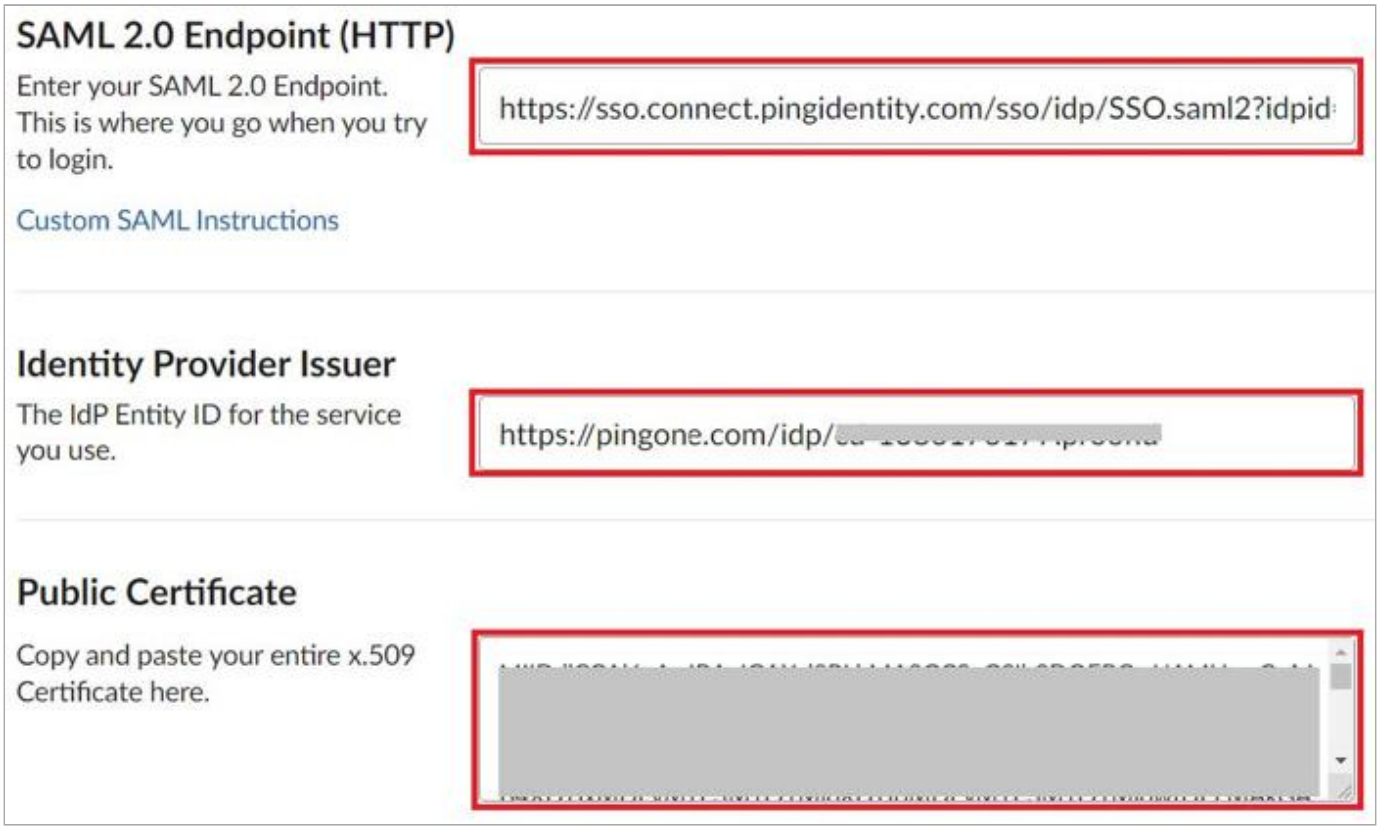
1. Sign on to your Slack Admin account as an administrator.
2. Go to **Settings & Administration → Workspace Settings**.



3. Click the **Authentication** tab.
4. In the **Configure an authentication method** section, on the **SAML authentication** line, click **Configure**.



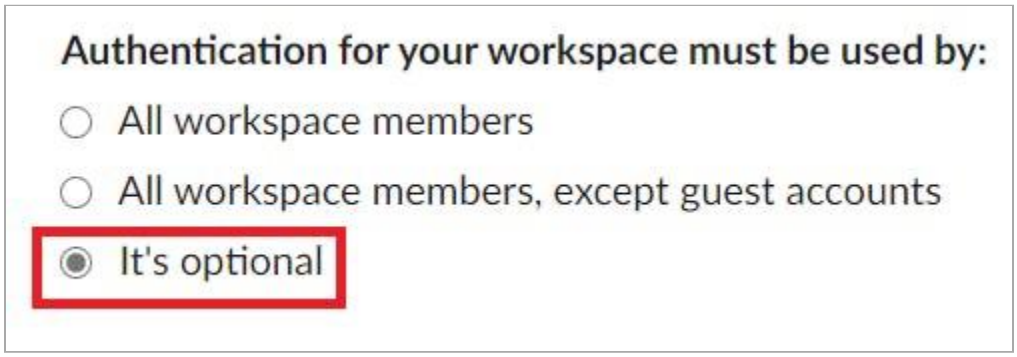
5. If prompted, enter your password to continue.
6. In the **SAML 2.0 Endpoint (HTTP)** field, enter `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=PingOne-IdP-ID-value`.
7. In the **Identity Provider Issuer** field, enter `PingOne-Issuer-value`.
8. In the **Public Certificate** field, paste in the contents of the PingOne for Enterprise signing certificate.



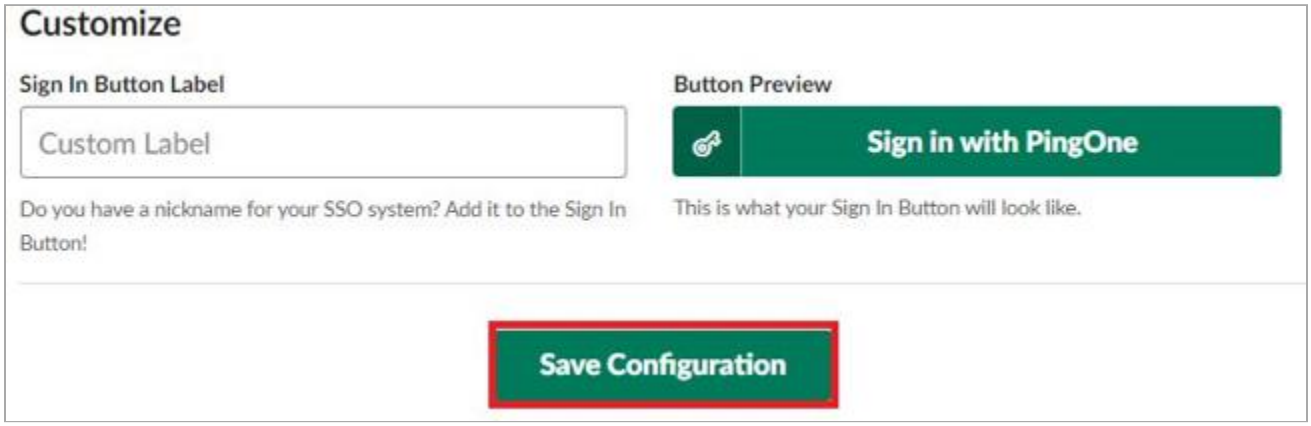
9. Expand the **Advanced Options** section and clear the **Responses Signed** check box.

10. In the **Settings** section, select the **It's optional** check box for the authentication setting.

> **Note**
>
> You can change the authentication setting to your desired value after testing has been completed.



11. Click **Save Configuration**.



Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with Slack access.

   > **Note**
   >
   > To find the Ping desktop URL in the Admin console, go to **Setup → Dock → PingOne Dock URL**.

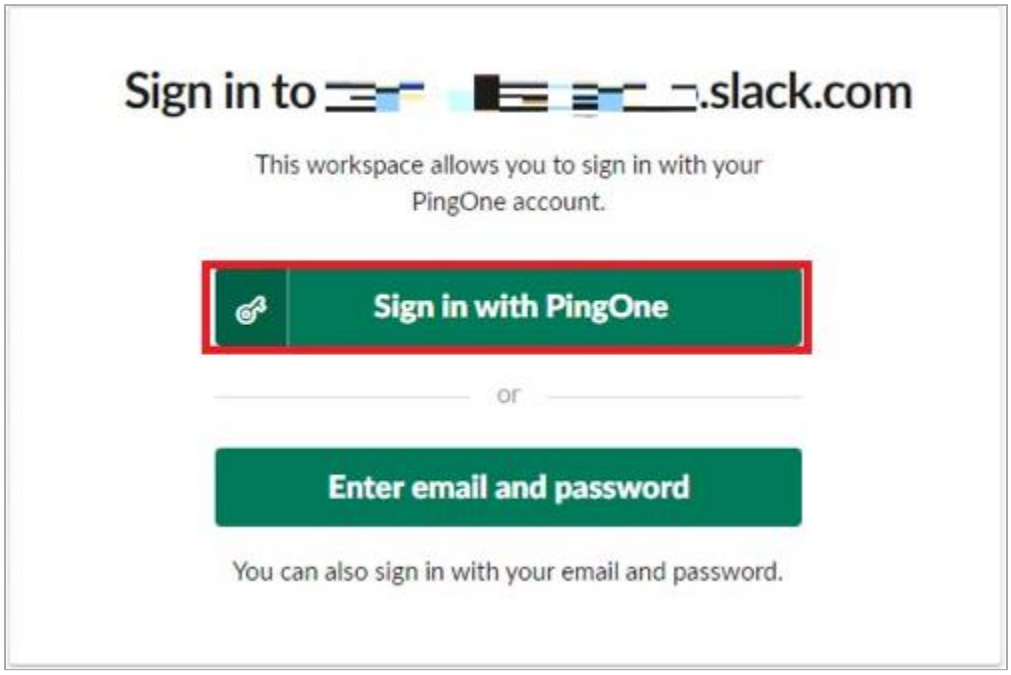
2. Complete the PingOne for Enterprise authentication.

   You're redirected to your Slack domain.

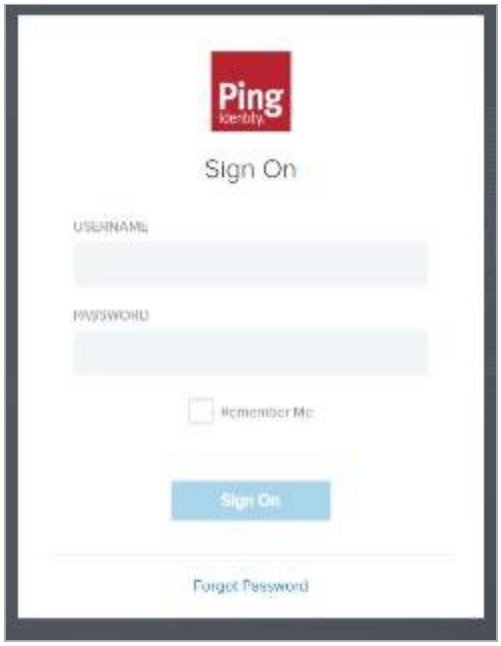
   > **Note**
   >
   > If the user doesn't exist in Slack, you are prompted to accept the Slack terms.

Test the PingOne for Enterprise SP-initiated SSO integration

1. Go to your Slack domain, `https://your-domain.slack.com`.
2. Click **Sign in with PingOne**.



3. After you're redirected to PingOne for Enterprise, enter your PingOne for Enterprise username and password.



After successful authentication, you're redirected back to Slack.

> **Note**
>
> If the user doesn't exist in Slack, you are prompted to accept the Slack terms.

Next steps

After successful testing, you can change the Slack **It's optional** authentication setting as necessary.

Splunk

Configuring SAML SSO with Splunk Cloud and PingFederate

Learn how to configure SAML SSO with Splunk Cloud and PingFederate.

About this task

> **Note**
>
> An error in configuration could cause users and administrators to be unable to sign on to Splunk Cloud. The following **Direct Login** link can be used for local authentication: `https://tenant.splunkcloud.com/en-US/account/login?loginType=splunk` .

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
`SAML_SUBJECT`		Required
`Role`	User role as per SAML Groups. Attribute name is configurable in SAML configuration for application.	Required
`Email`	User Email address. Attribute name is configurable in SAML configuration for application.	Optional
`RealName`	User display name. Attribute name is configurable in SAML configuration for application.	Optional

The following table details the references that are used within this guide that are environment-specific. Replace these with the suitable value for your environment.

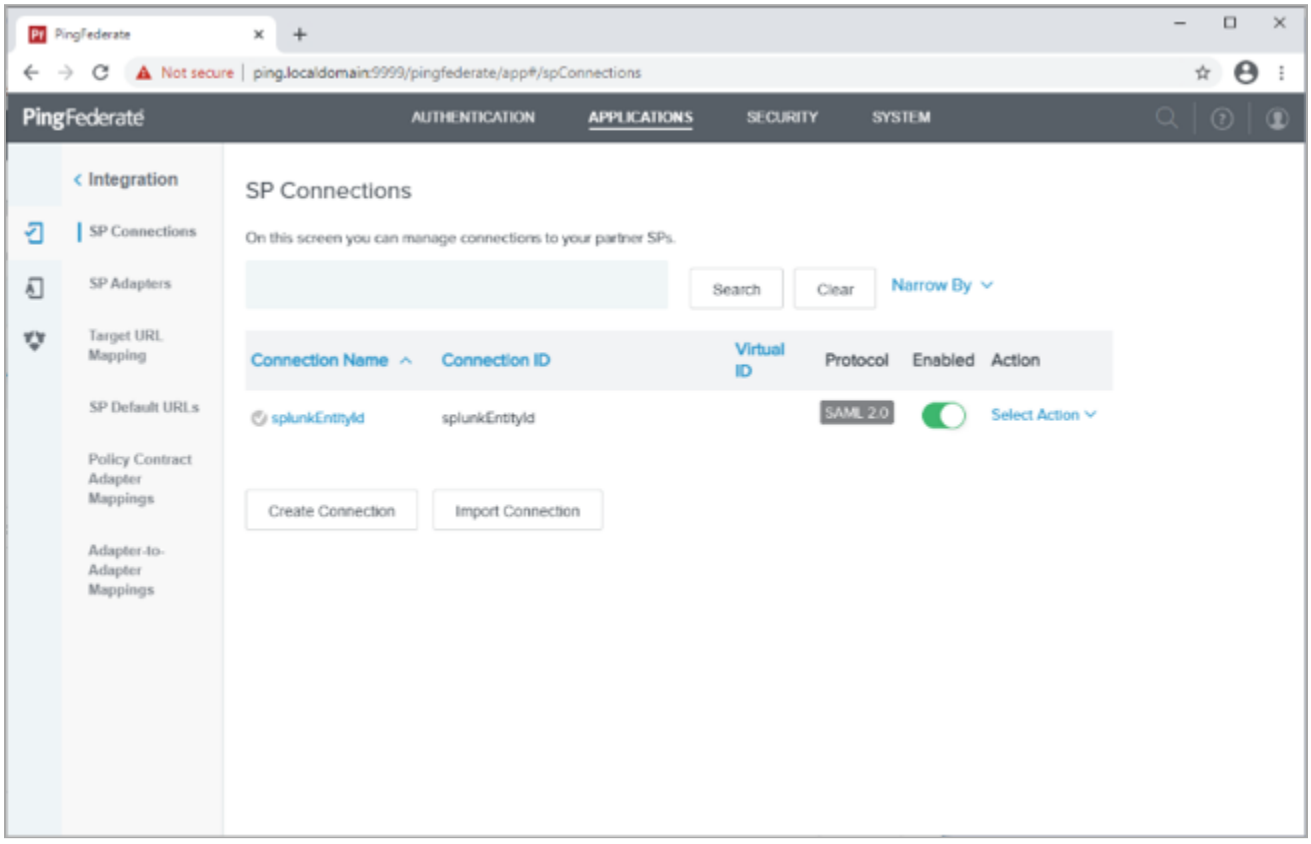
Reference	Description
`tenant`	The instance name for the Splunk Cloud tenant.

> **Note**
>
> The following configuration is untested, and is provided as an example. Additional steps might be required.

Create a PingFederate SP connection for Splunk Cloud

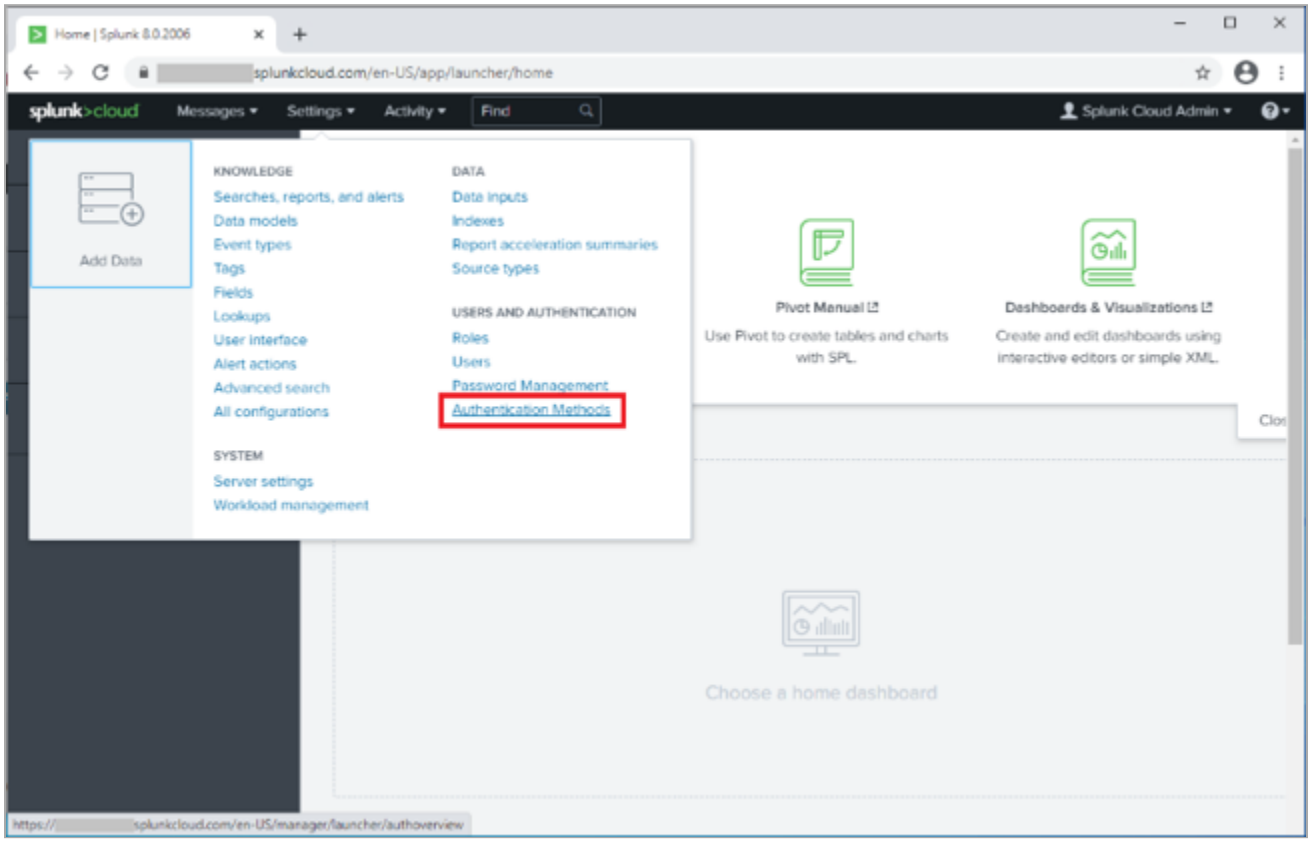
1. Download the Splunk Cloud metadata from `https://tenant.splunkcloud.com/en-US/saml/spmetadata` .

2. Sign on to the PingFederate administrative console.
3. Using the metadata that you downloaded, create an SP connection in PingFederate:
    1. Configure using **Browser SSO profile SAML 2.0**.
    2. Enable the following **SAML Profiles**:
        - **IdP-Initiated SSO**
        - **SP-Initiated SSO**
        - **IdP-Initiated SLO**
        - **SP-Initiated SLO**
    3. In **Assertion Creation: Attribute Contract**, set the **Subject Name Format** to **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.
    4. Extend the contract:
        - **Attribute**: `Role`
        - **Format**: `urn:oasis:names:tc:SAML:2.0:attrname-format-basic`
    5. In the **Assertion Creation: Attribute Contract Fulfilment**, map attribute **SAML_SUBJECT** to the attribute **mail** and map attribute **Role** to the LDAP attribute containing the Splunk role.
    6. In **Protocol Settings: Allowable SAML Bindings**, enable **Redirect** and **POST**.
4. Export the metadata for the newly-created SP connection.
5. Export the signing certificate public key.

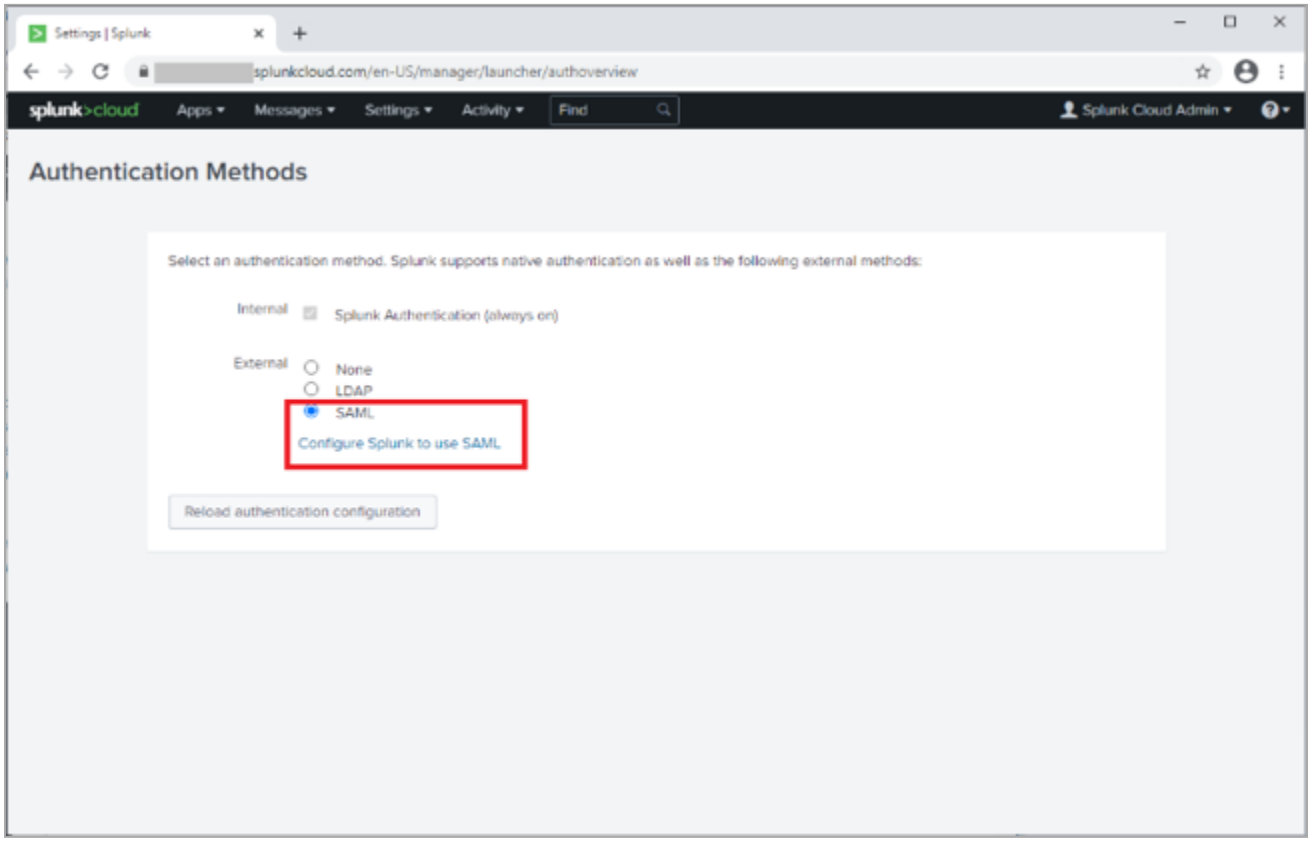


Configure the PingFederate IdP-connection for Splunk Cloud

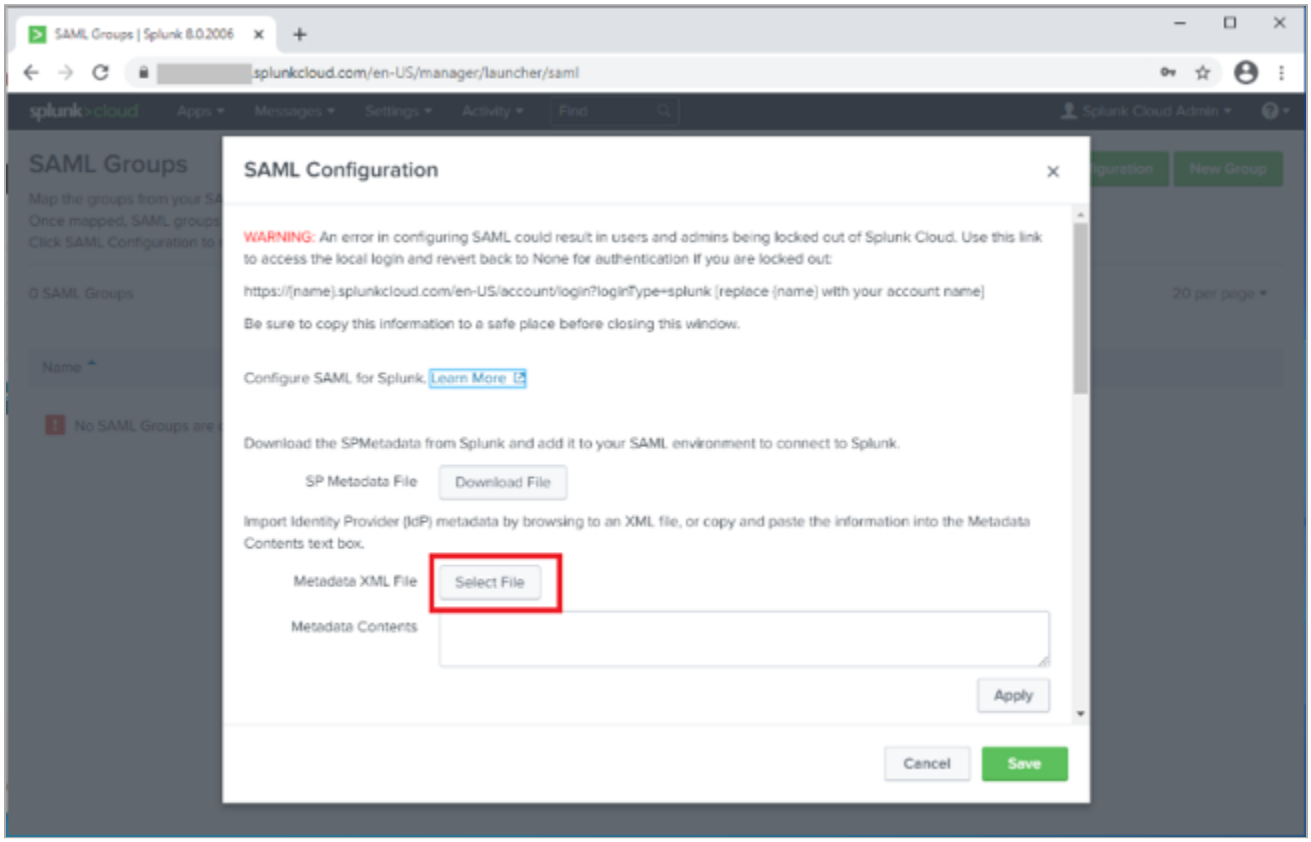
1. Sign on to Splunk Cloud as an administrator.
2. In the top navigation bar, click **Settings**.
3. Click **Authentication Methods**.



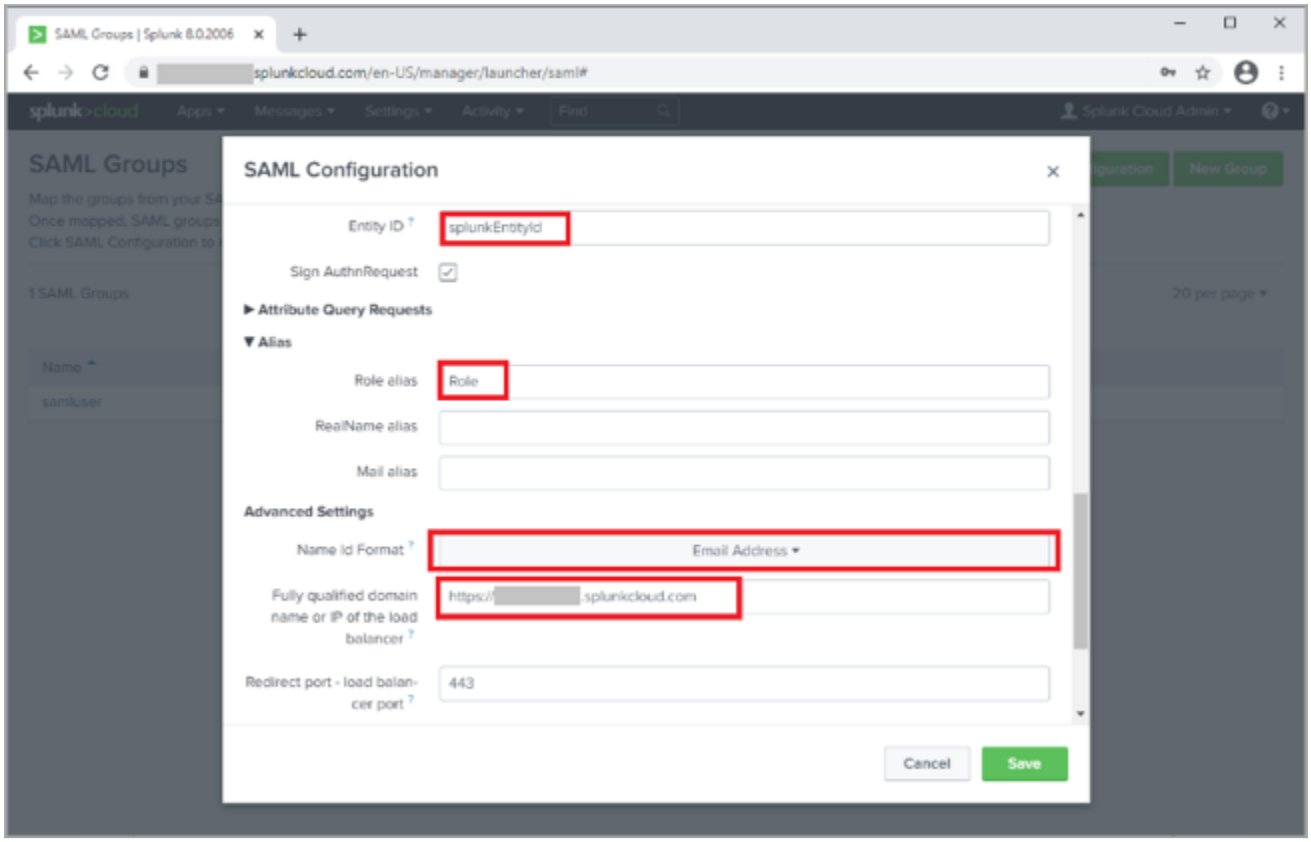
4. Click **SAML**, and then click **Configure Splunk to use SAML**.



5. On the **SAML Configuration** window, note the warning and save the **Direct Login** URL so that you can use it in the event of integration errors.
6. In the **Metadata XML File** field, click **Select File**, and select the PingFederate metadata file that you exported.



7. Review the configuration loaded from the metadata.
8. Set the **Entity ID** to the one that you configured in PingFederate when creating the SP configuration, such as `splunkEntityId`.
9. Set the **Role** alias to the value that you configured in PingFederate for the attribute contract, such as `Role`.
10. Set the **Name ID Format** to **Email Address**.



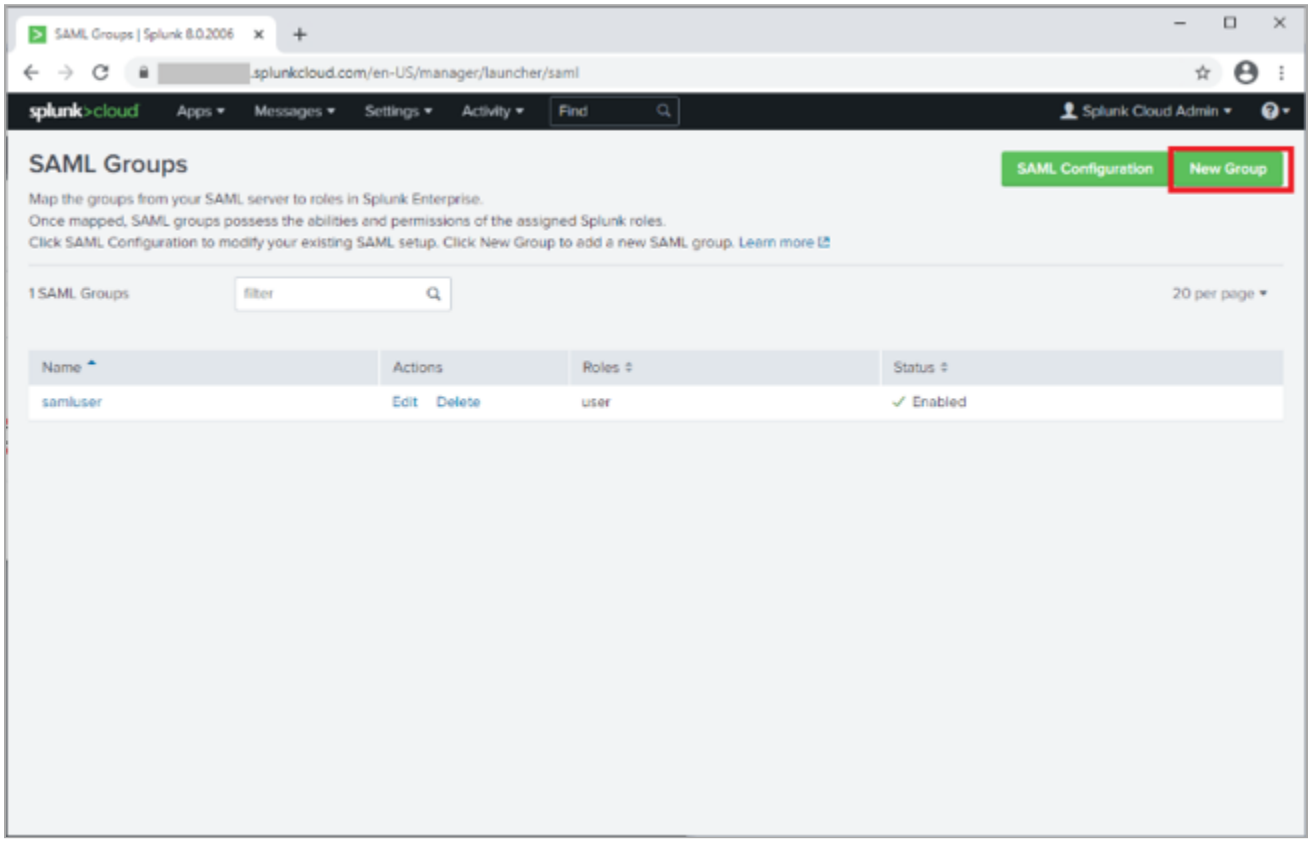
11. Ensure the fully qualified domain name parameter and port parameter match that of your Splunk Cloud instance.

    For example:

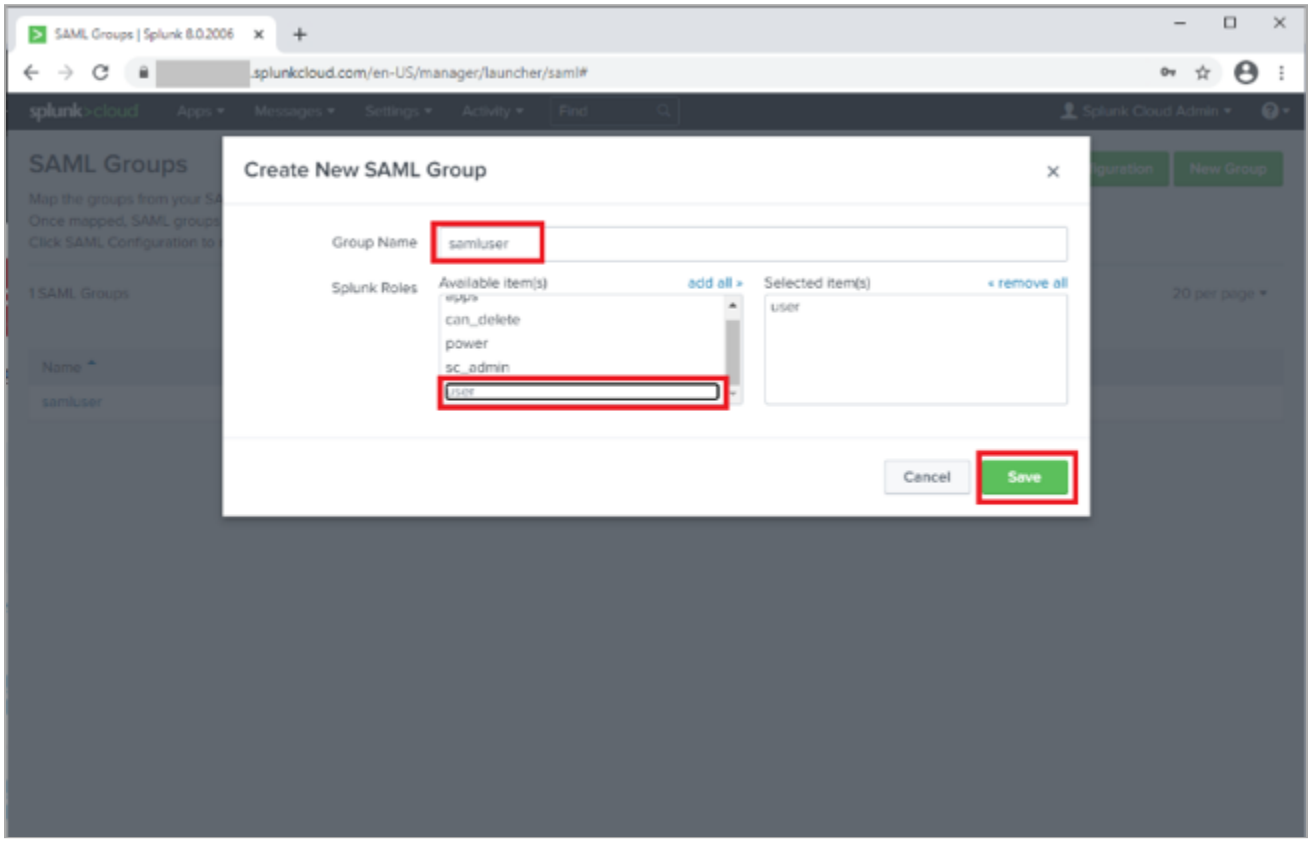
    - **Fully Qualified Domain Name**: `https://tenant.splunkcloud.com`
    - **Port**: 443

12. Click **Save**.
13. Go to **Settings → Authentication Methods → SAML Settings**.
14. Click **New Group** and configure the following settings.

Setting	Value
Name	`samluser` **Note** This value should match the role you are passing from PingFederate in the SSO Attribute Mapping.
Role	`user`



15. Click **Save**.
16. Create additional groups as required to meet requirements.



The configuration is complete.

Configuring SAML SSO with Splunk Cloud and PingOne for Enterprise

Learn how to configure SAML SSO with Splunk Cloud and PingOne for Enterprise.

About this task

> **Note**
>
> An error in configuration could cause users and administrators to be unable to sign on to Splunk Cloud. The following Direct Login link can be used for local authentication:
> `https://tenant.splunkcloud.com/en-US/account/login?loginType=splunk`

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
`SAML_SUBJECT`		Required
`Role`	User role as per SAML Groups. Attribute name is configurable in SAML configuration for application.	Required
`Email`	User email address. Attribute name is configurable in SAML configuration for application.	Optional

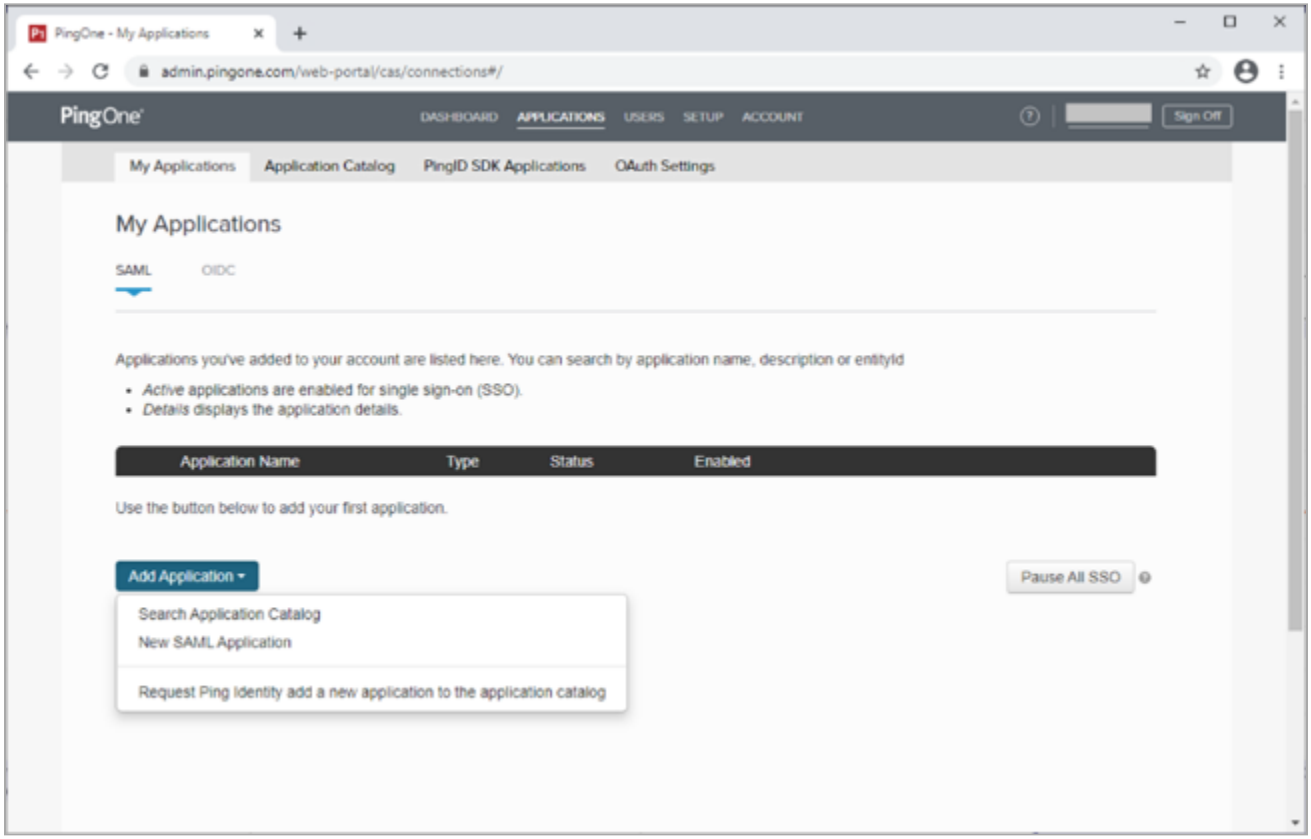
Attribute Name	Description	Required / Optional
`RealName`	User display name. Attribute name is configurable in SAML configuration for application.	Optional

The following table details the references that are used within this guide that are environment-specific. Replace these with the suitable value for your environment.

Reference	Description
`tenant`	The instance name for the Splunk Cloud tenant.

Create a PingOne for Enterprise Application for Splunk Cloud

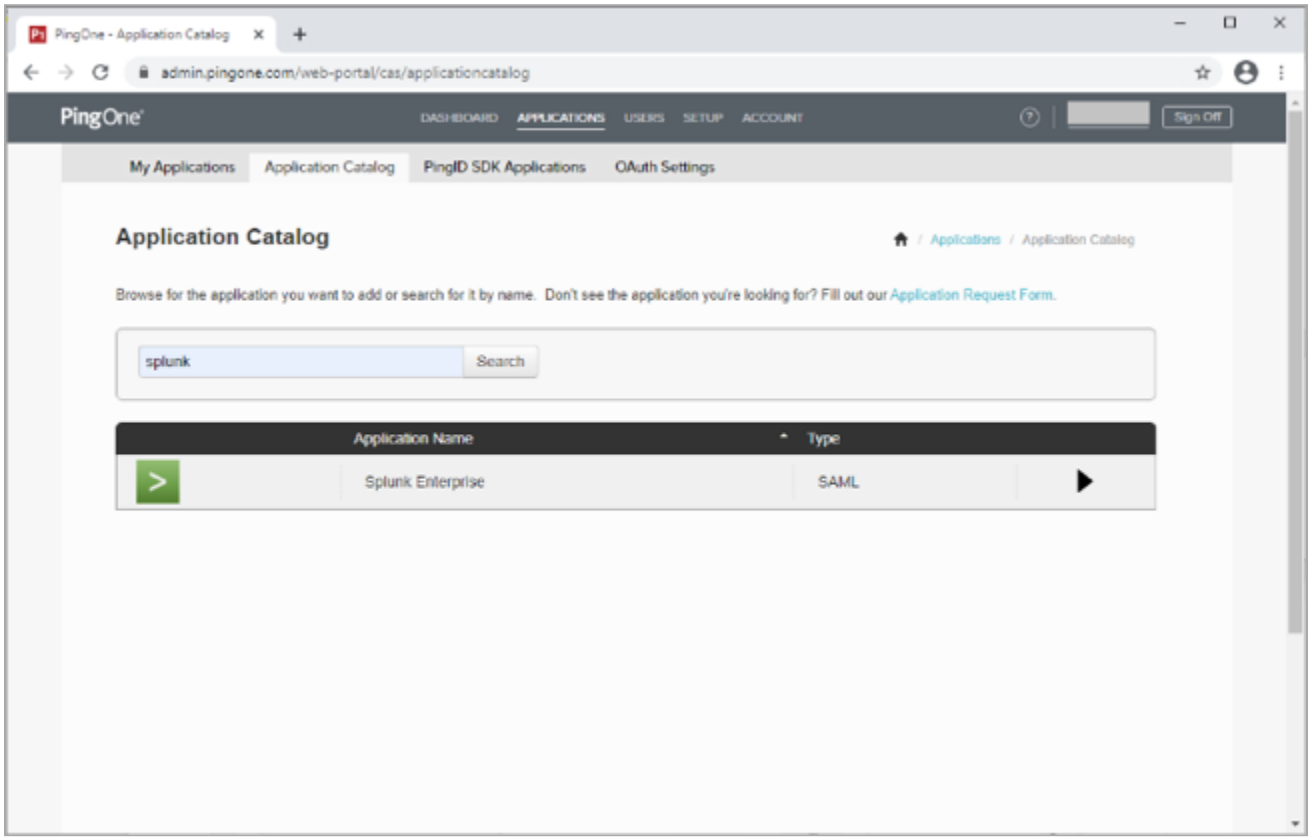
1. Download the Splunk Cloud Metadata from `https://tenant.splunkcloud.com/en-US/saml/spmetadata`.
2. Sign on to PingOne for Enterprise and click **Applications**.
3. On the **SAML** tab, click **Add Application**.



4. Click **Search Application Catalog** and search for `Splunk`.

   The results should show Splunk Enterprise. This is suitable for both Splunk Cloud and Splunk Enterprise.

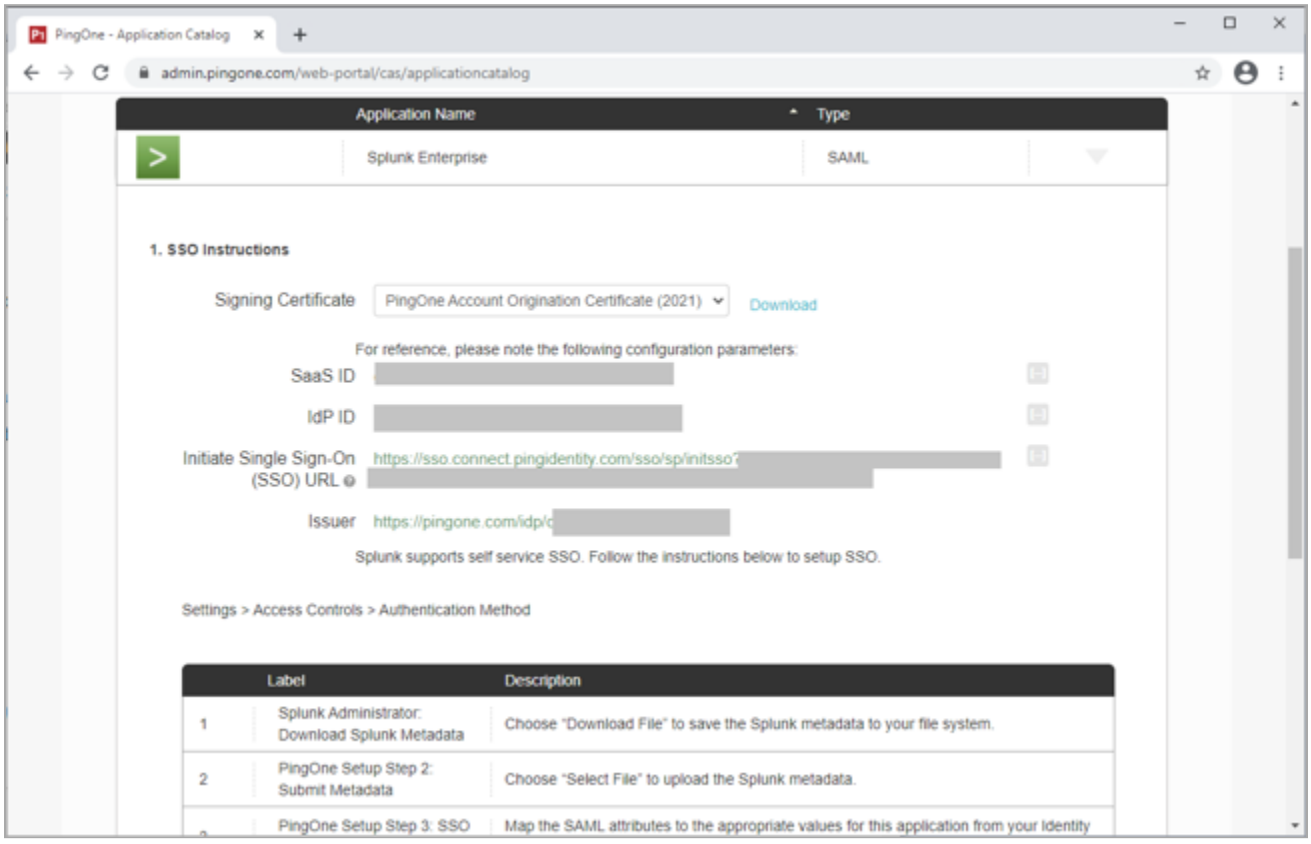
5. Click the **Splunk Enterprise** row.



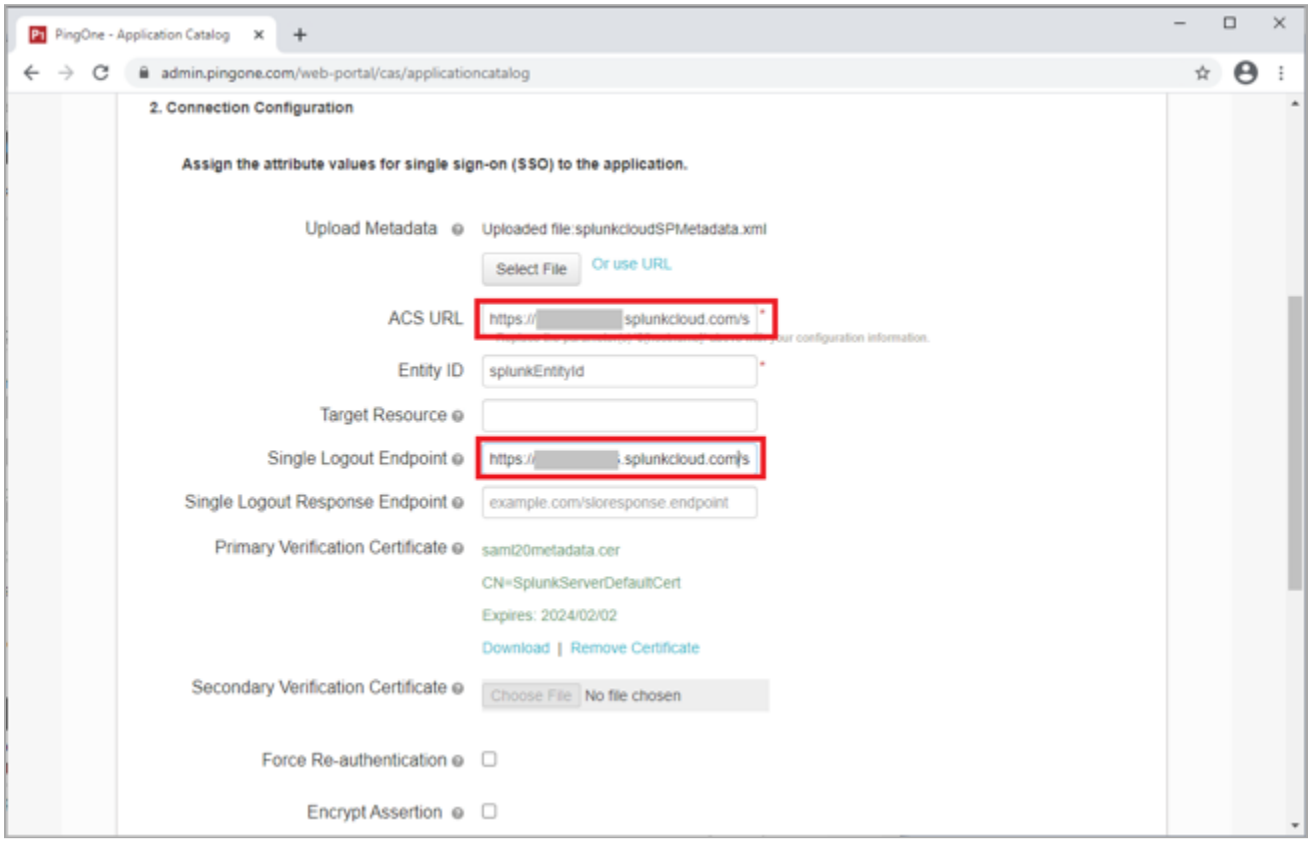
6. Click **Setup**.

7. Select the appropriate signing certificate.

8. Review the steps, and note the **PingOne SaaS ID**, **IdP ID**, **Initiate Single Sign-on (SSO) URL**, and **Issuer** values.



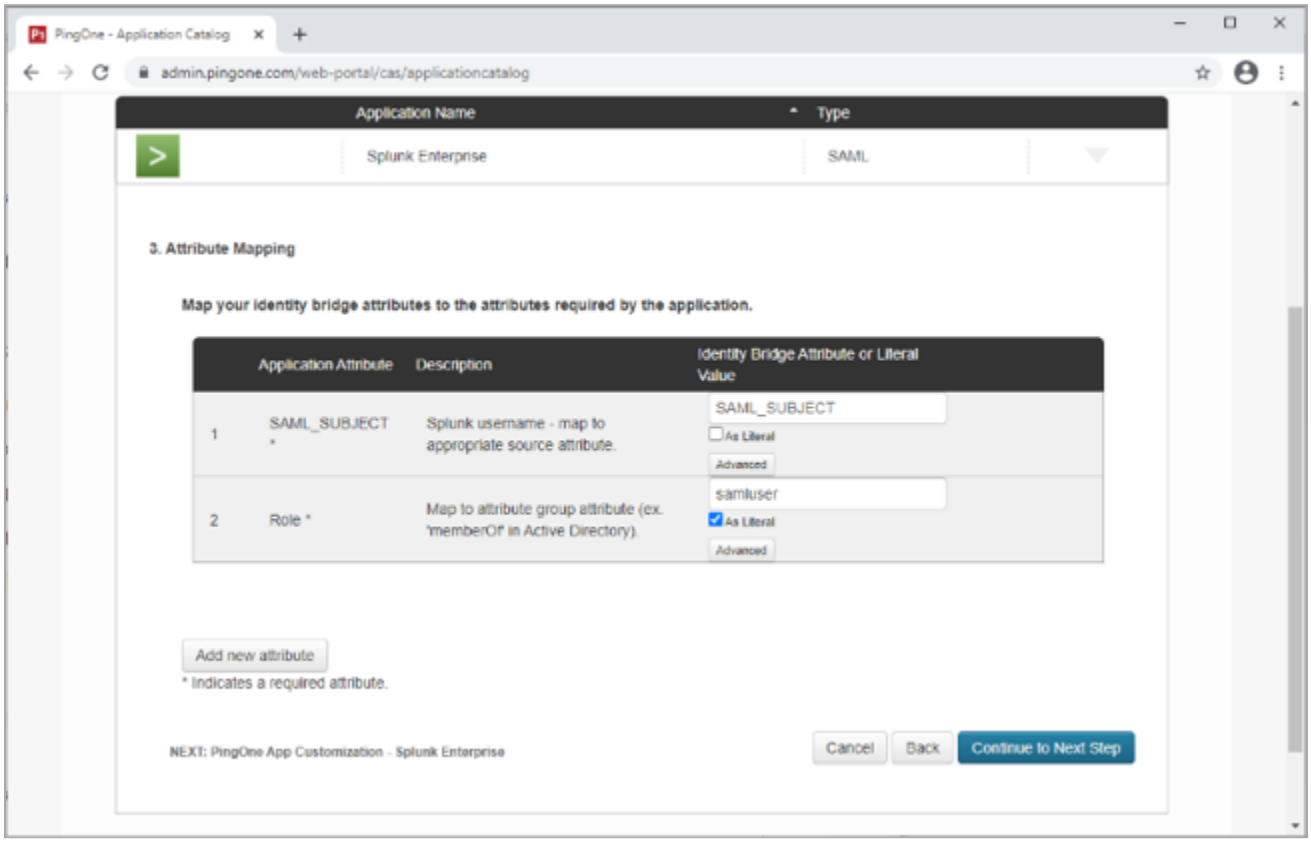
9. Click **Continue to Next Step**.
10. In the **Upload Metadata** section, click **Select File**, and upload the Splunk Cloud metadata file that you downloaded.
11. Make sure the following values are set:
    - **ACS URL** to `https://tenant.splunkcloud.com/saml/acs`
    - **Single Logout Endpoint** to `https://tenant.splunkcloud.com/saml/logout`



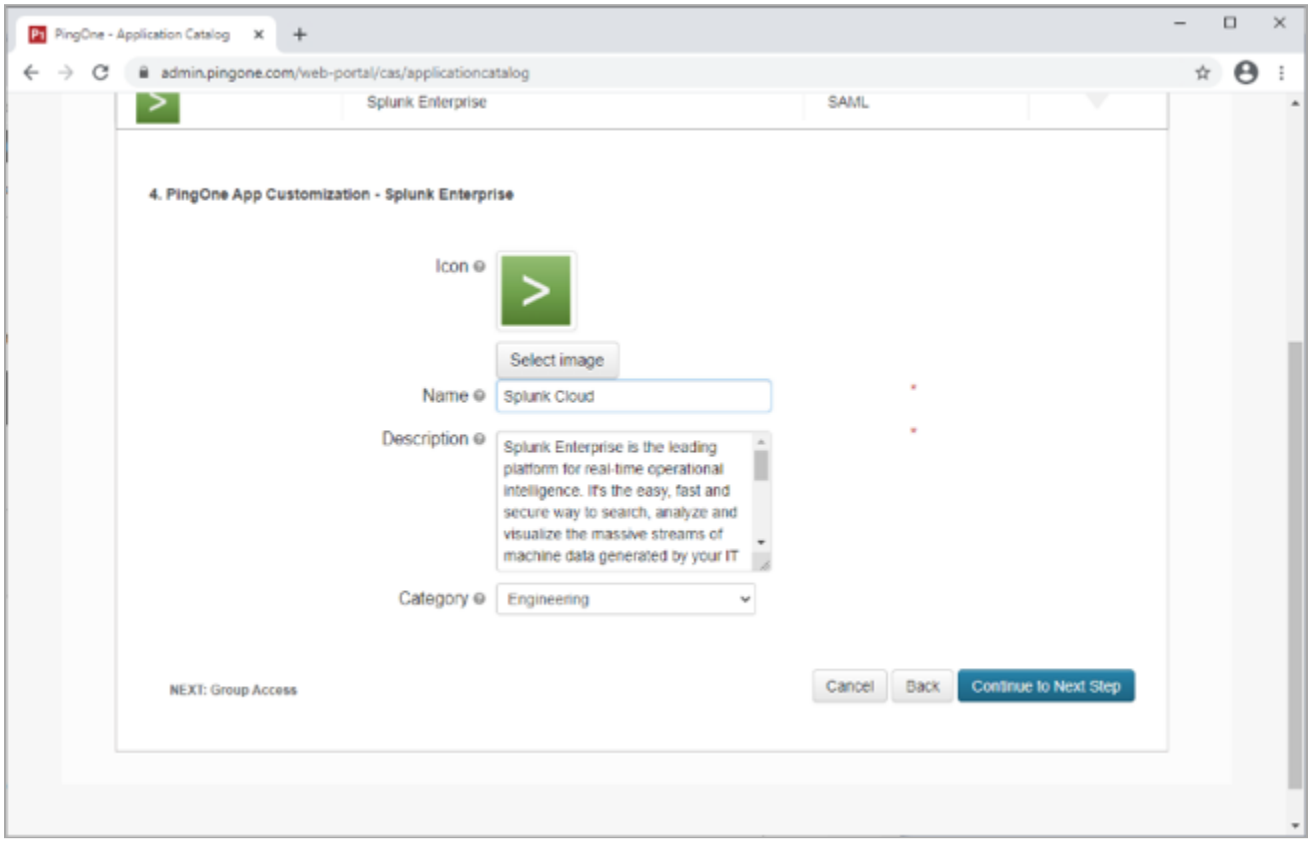
12. Click **Continue to Next Step**.
13. In the **Attribute Mapping** section, complete the attribute mapping for the Splunk role for the user.

> **Note**
>
> For this integration example, all PingOne for Enterprise authenticated users will be mapped to a role with the literal value of samluser, and the **Identity Bridge Attribute** or **Literal Value** check box is selected. However, this could also be retrieved from the user directory.

14. In the **Attribute Mapping** section, in the **Identity Bridge Attribute** or **Literal Value** column of the **SAML_SUBJECT** row, select the attribute **SAML_SUBJECT**.

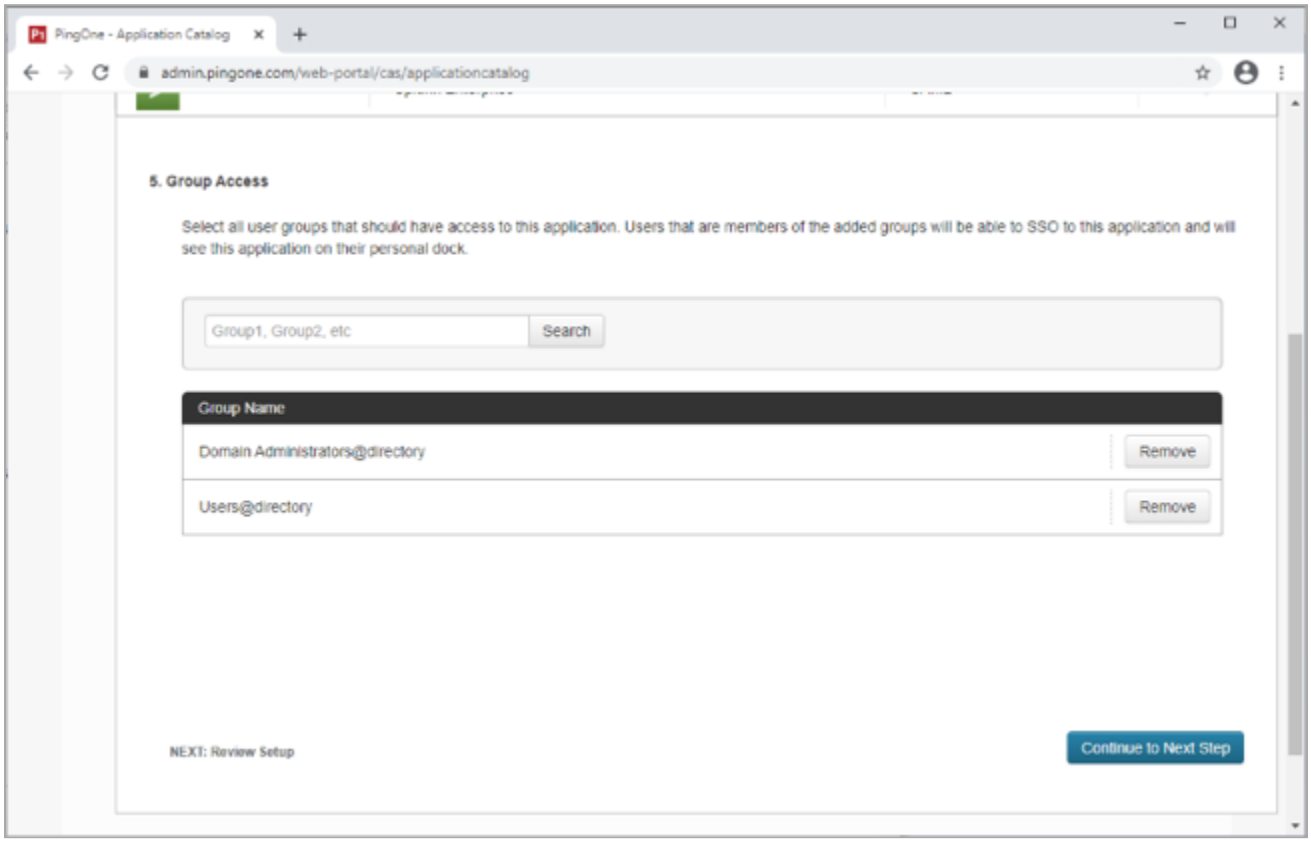


15. Click **Continue to Next Step**.
16. Update the **Name**, **Description**, and **Category** fields as required.

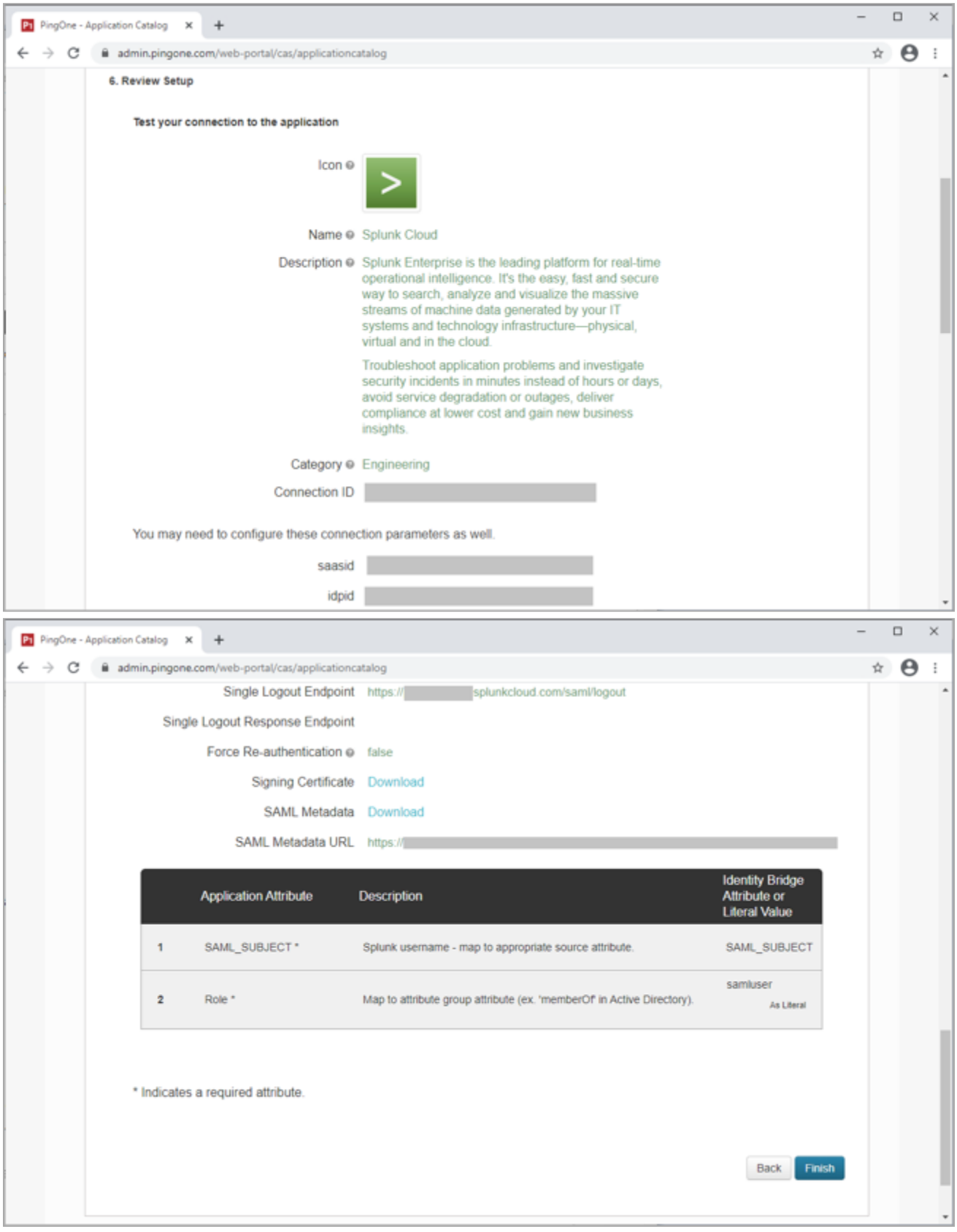


17. Click **Continue to Next Step**.

18. Add suitable user groups for the application.



19. Click **Continue to Next Step**.
20. Review the settings.



21. Copy the **Single Sign-On (SSO) URL** value to a temporary location.

    This is the IdP-initiated SSO URL that you can use for testing.

22. On the **Signing Certificate** row, click **Download**.

    You will use this for the Splunk Cloud configuration.

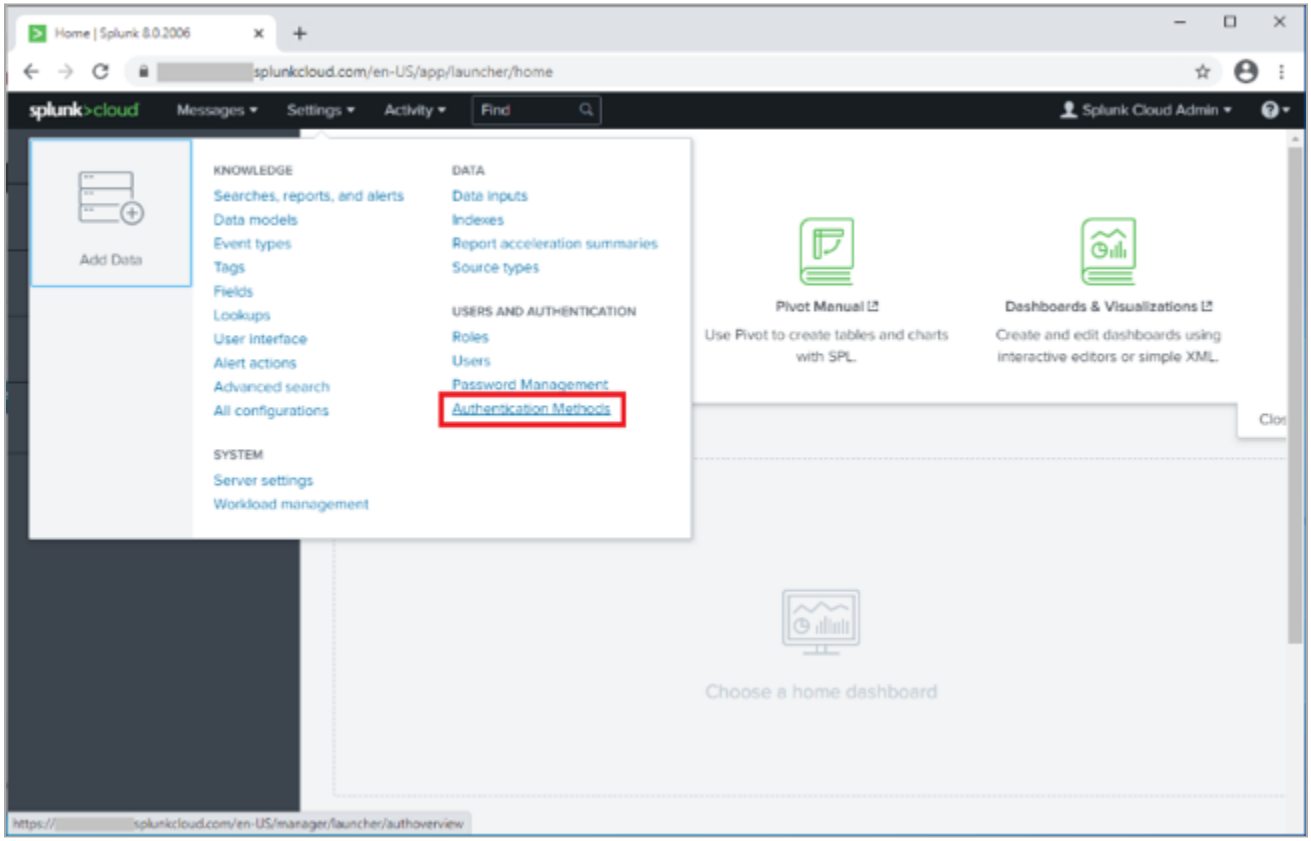
23. On the **SAML Metadata** row, click **Download**.

    You will use this for the Splunk Cloud configuration.

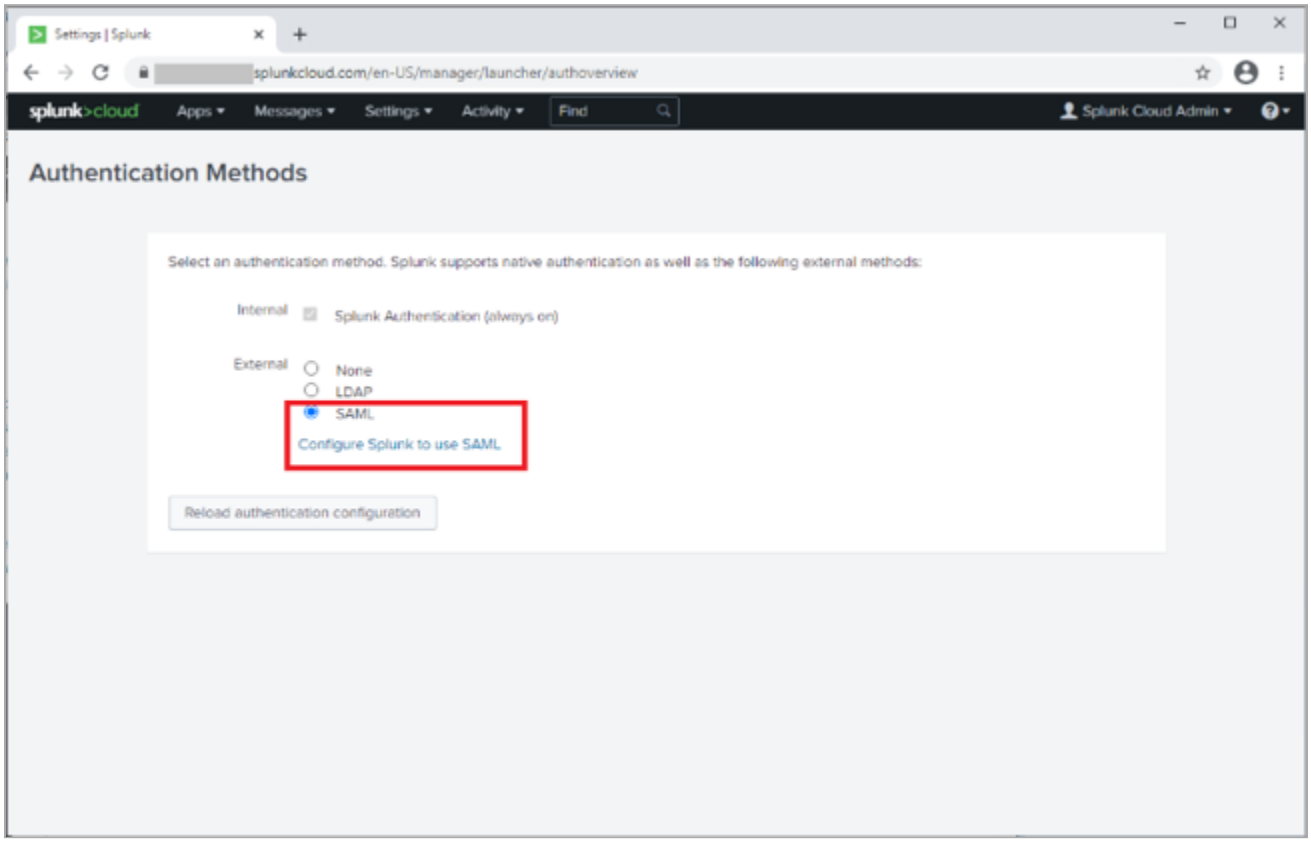
24. Click **Finish**.

Configure the PingOne for Enterprise IdP connection for Splunk Cloud

1. Sign on to Splunk Cloud as an administrator.
2. From the top navigation bar, click **Settings**.
3. Click **Authentication Methods**.

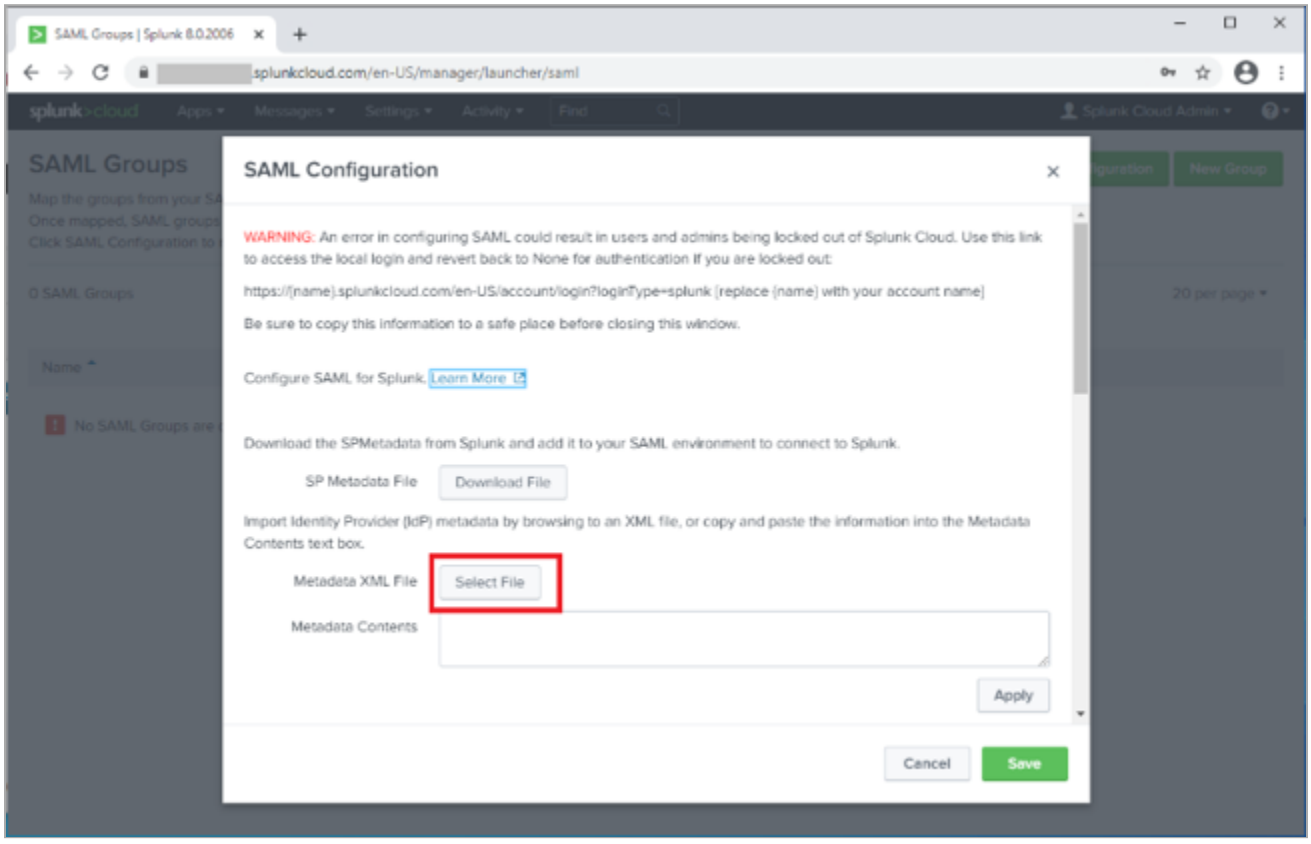


4. Click **SAML**, and then click **Configure Splunk to use SAML**.

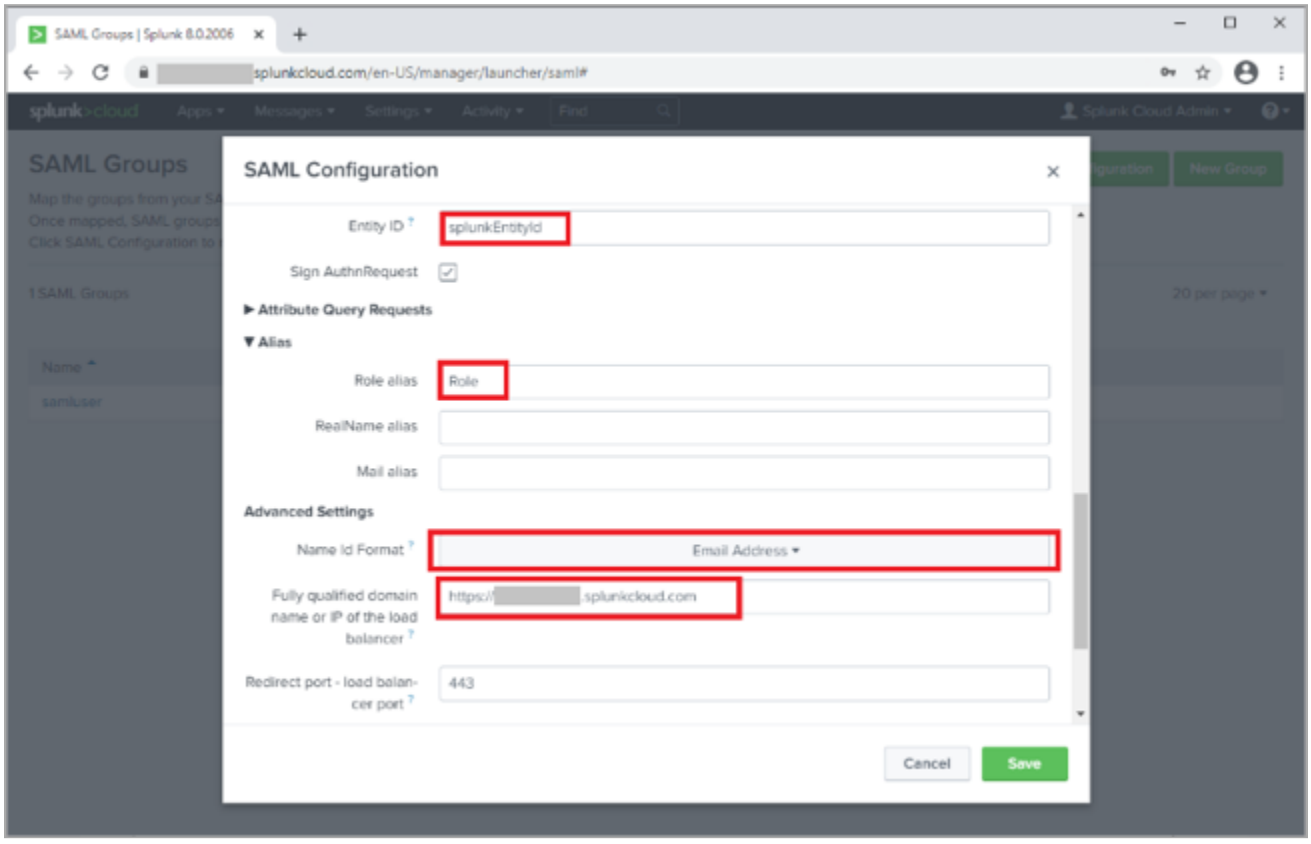


5. Note the warning and save the **Direct Login URL** so that you can use it in the event of integration errors.

6. On the **Metadata XML File** row, click **Select File**, and select the PingOne for Enterprise metadata that you exported.



7. Review the configuration you loaded from the metadata.
8. Set the **Entity ID** to the one that you configured in PingOne for Enterprise when you created the SP configuration, such as `splunkEntityId`.
9. Set the **Role alias** to the value that you configured in PingOne for Enterprise for the **SSO Attribute Mapping**. For example, `Role`.

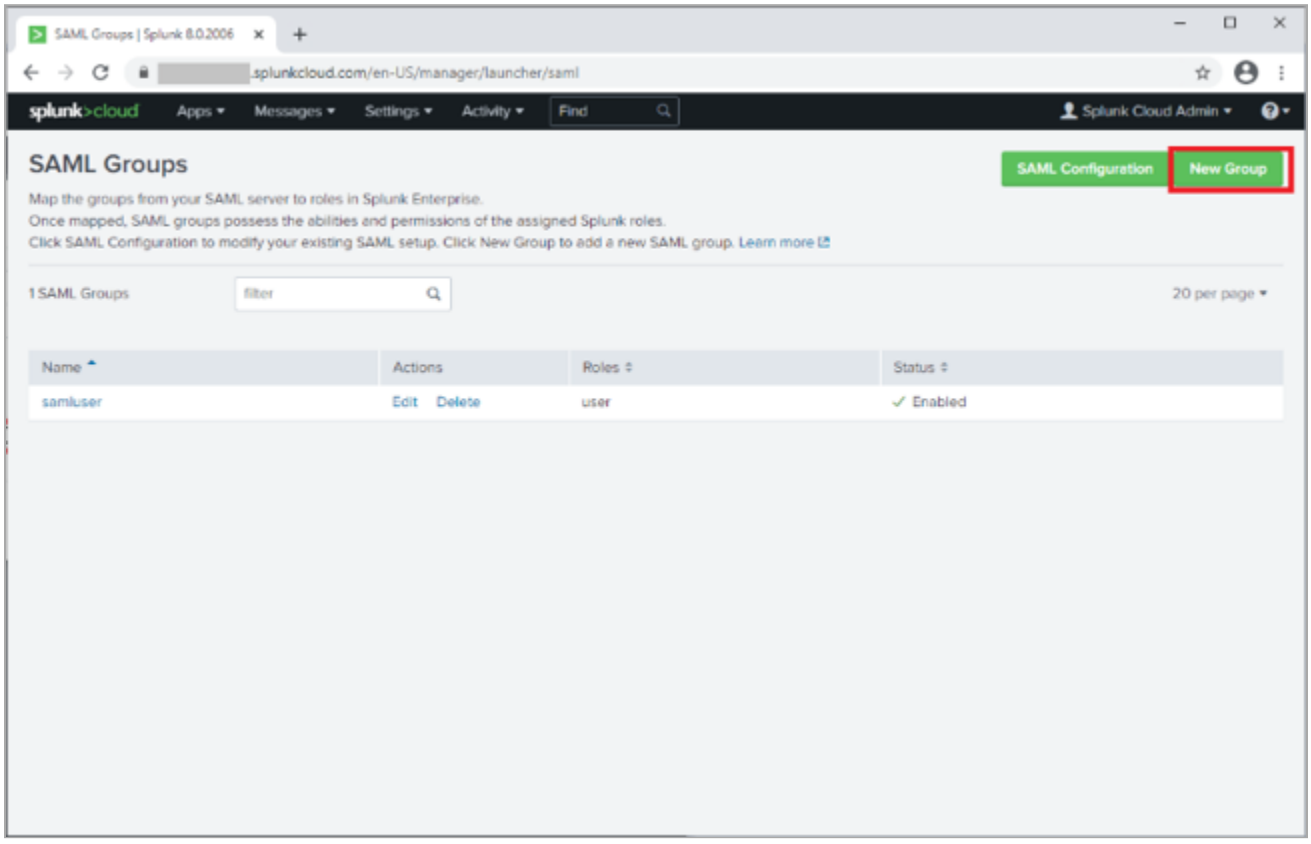


10. Set the **Name ID Format** to **Email Address**.
11. Ensure the fully qualified domain name parameter, and port parameter matches that of your Splunk Cloud instance.

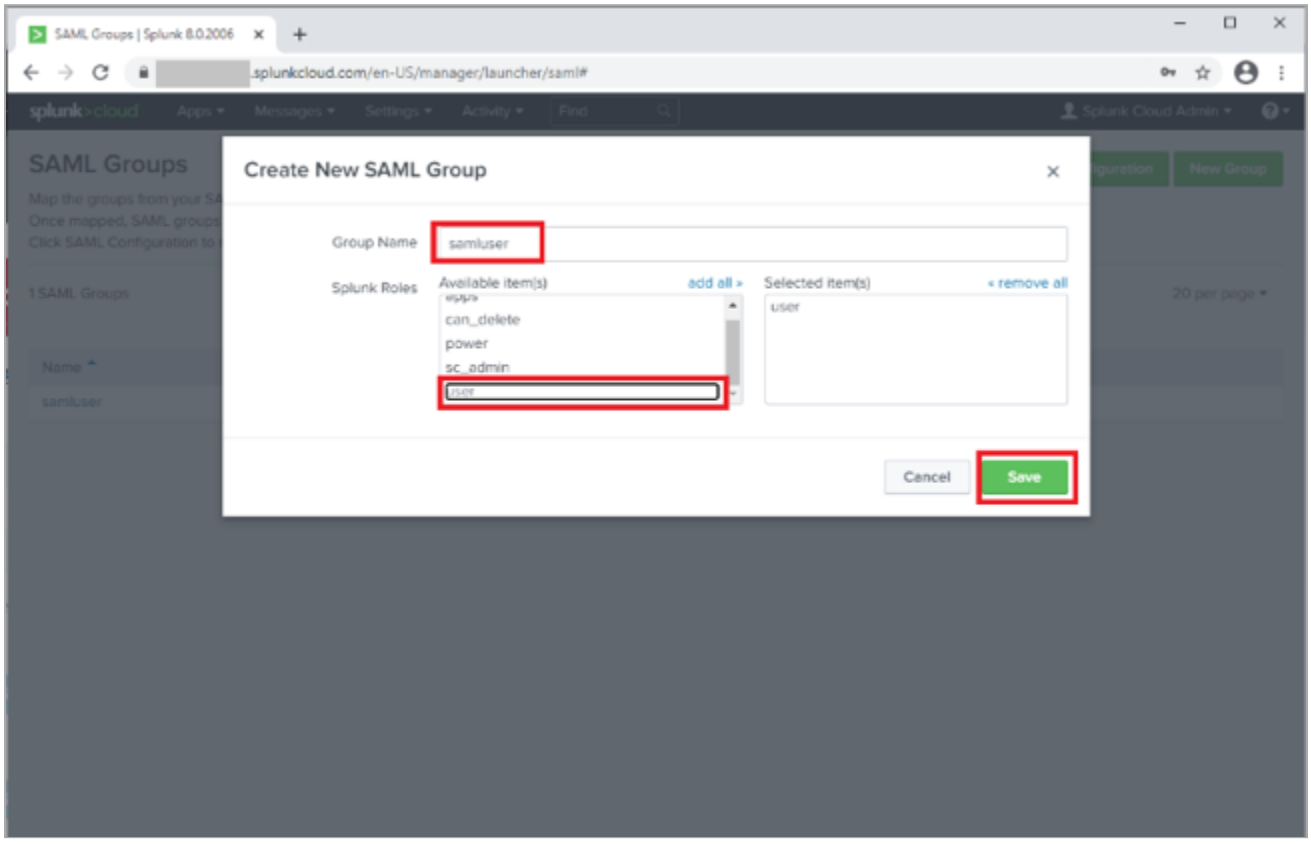
    For example:

    - **Fully Qualified Domain Name**: `https://tenant.splunkcloud.com`
    - **Port**: `443`
12. Click **Save**.
13. Go to **Settings → Authentication Methods → SAML Settings**.
14. Click **New Group** and configure the following settings:

Setting	Value
Name	`samluser` **Note** This value should match the role you're passing from PingOne for Enterprise in the SSO Attribute Mapping.
Role	`user`



15. Click **Save**.
16. Create additional groups as required to meet requirements.



The configuration is complete.

Test the PingOne for Enterprise IdP-Initiated SSO integration

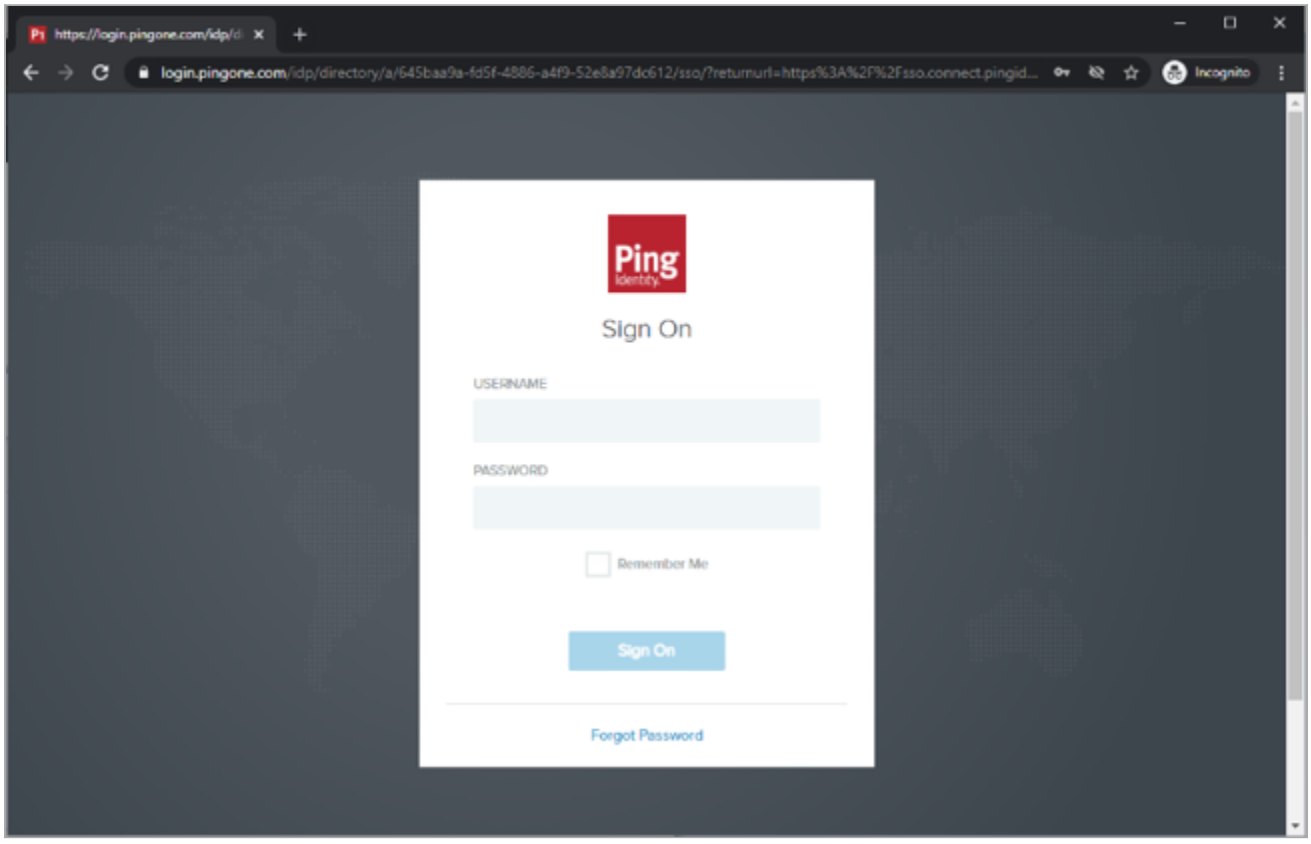
1. Go to the **Single Sign-On (SSO) URL** in the PingOne for Enterprise application configuration and perform IDP initiated SSO.

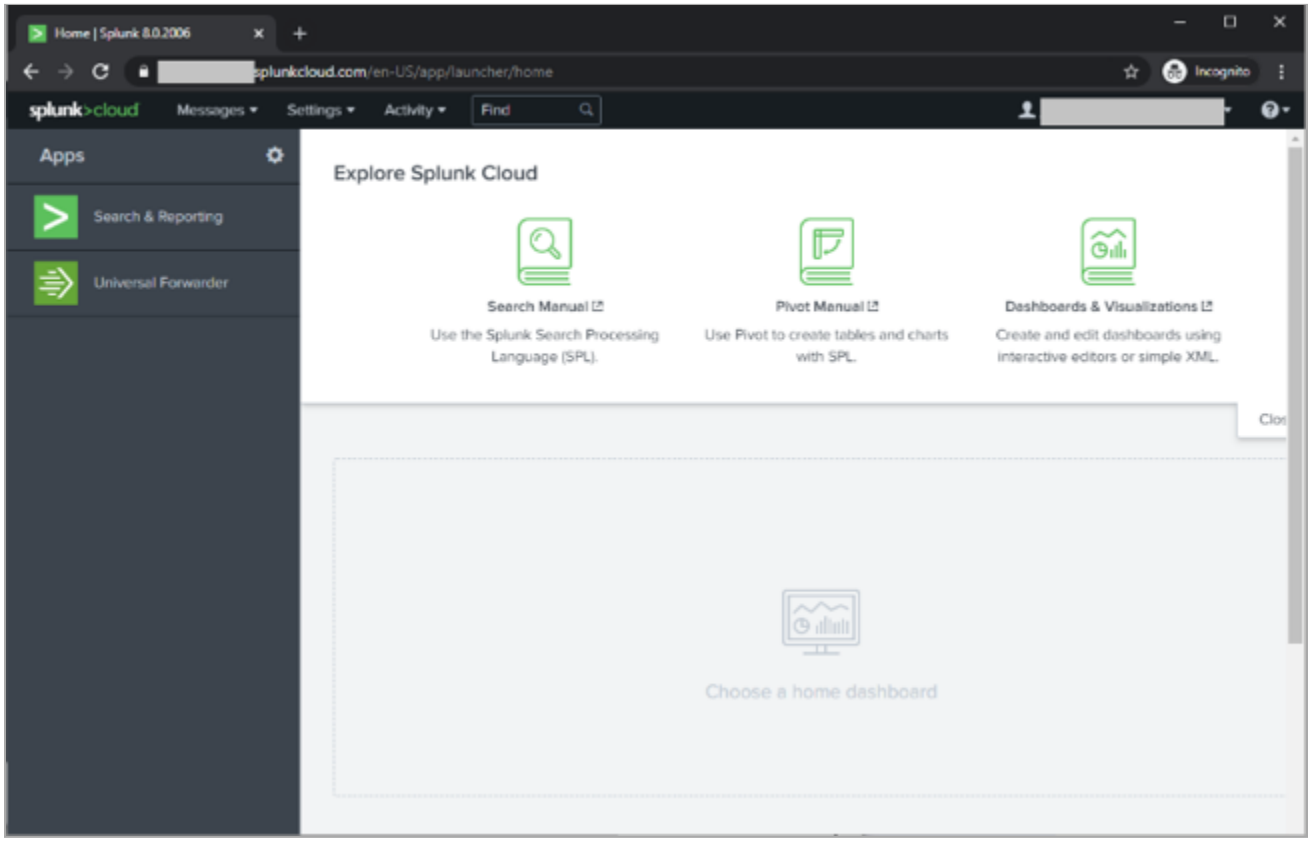
   `https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=saasid&idpid=idpid`

Test the PingOne for Enterprise SP-initiated SSO integration

1. Go to the URL for your Splunk Cloud tenant, `https://tenant.splunkcloud.com`.

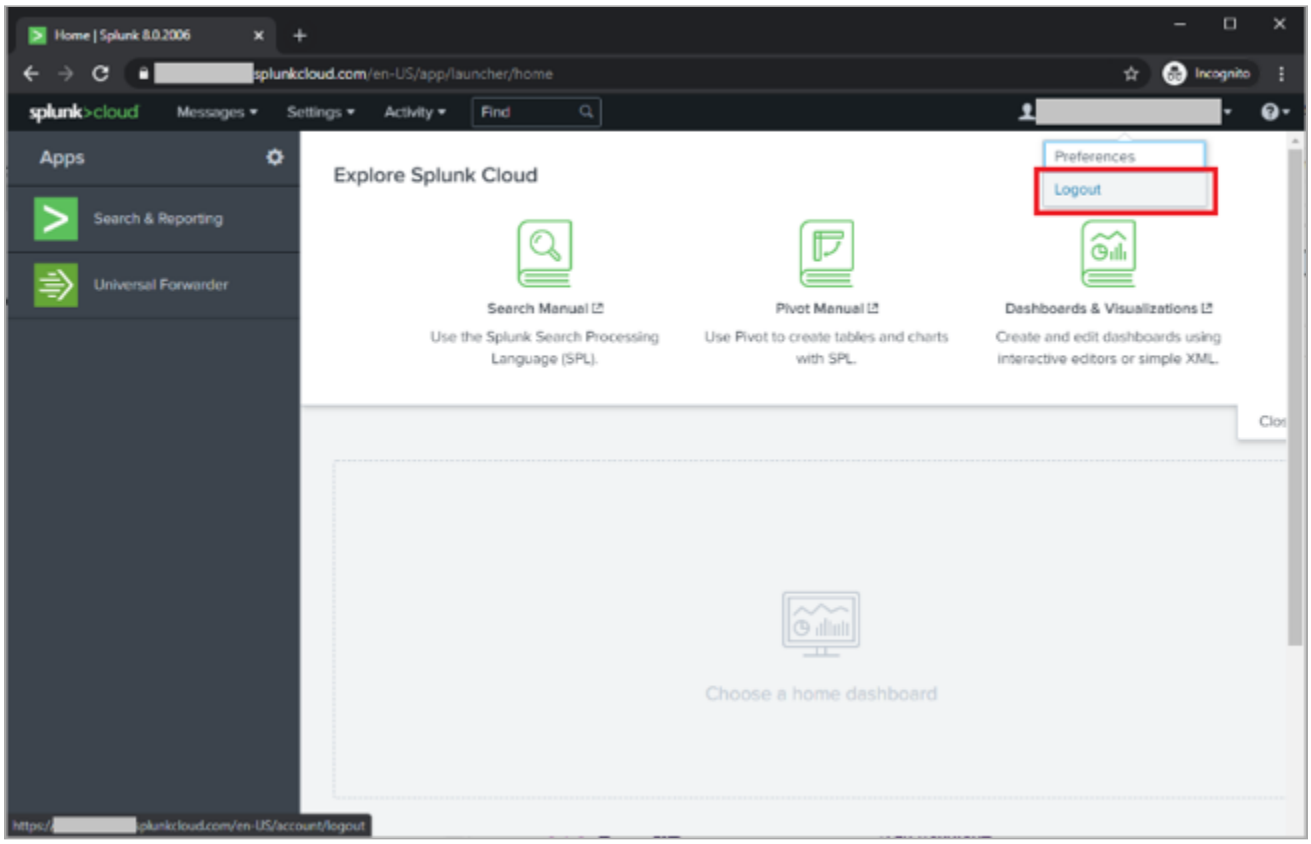
   You're redirected to PingOne for Enterprise for authentication.

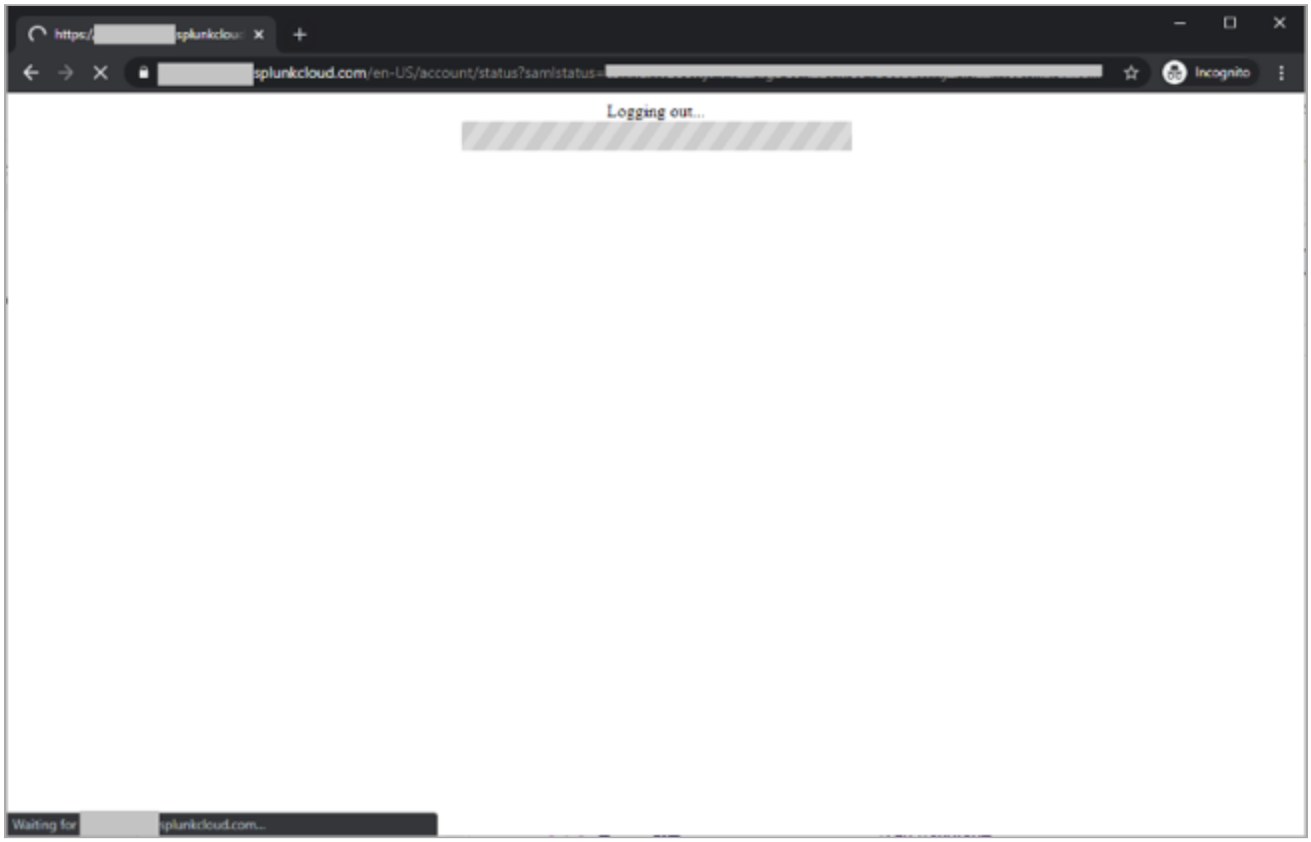

Ping Identity
Sign On
USERNAME
PASSWORD
Remember Me
Sign On
Forgot Password

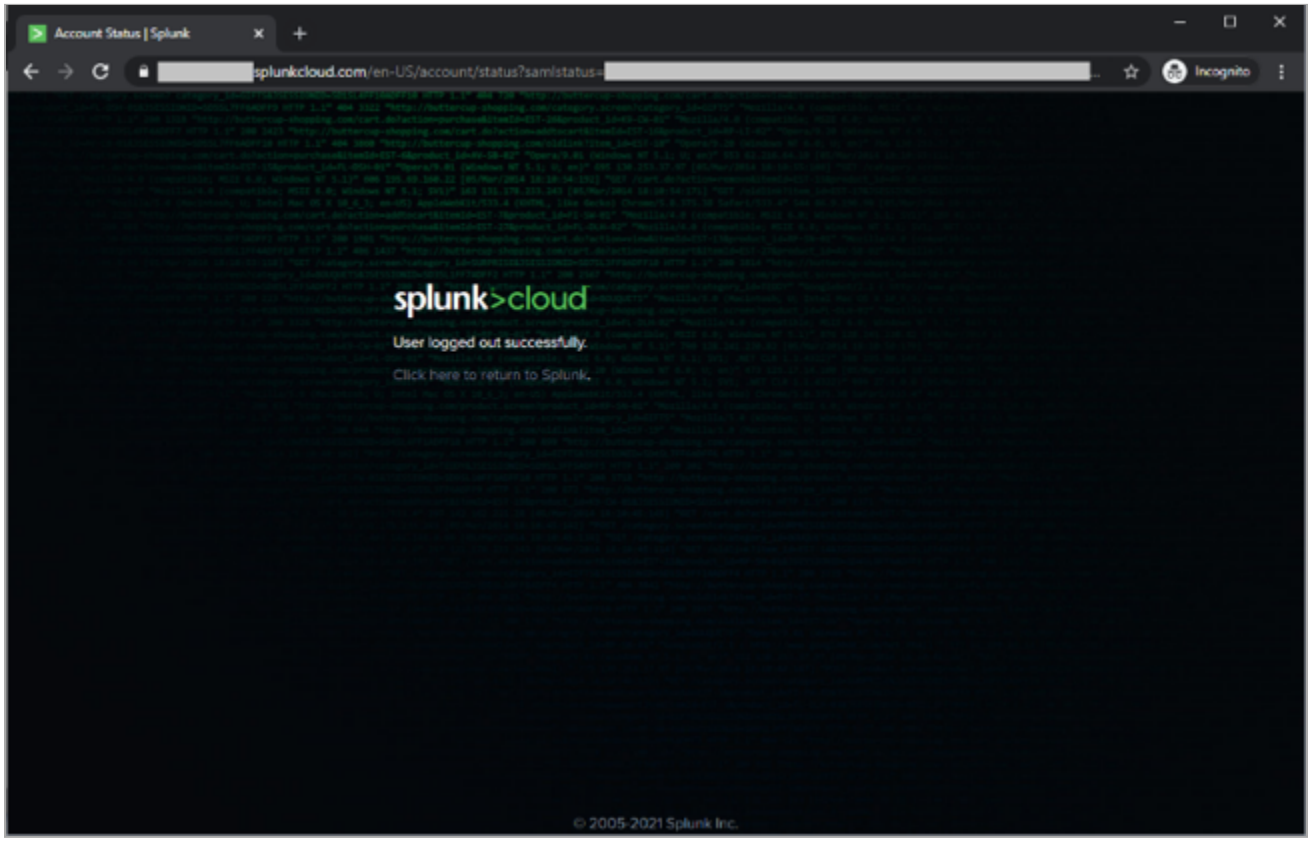

splunk>cloud
Messages
Settings
Activity
Find
Apps
Search & Reporting
Universal Forwarder
Explore Splunk Cloud
Search Manual
Use the Splunk Search Processing Language (SPL).
Pivot Manual
Use Pivot to create tables and charts with SPL.
Dashboards & Visualizations
Create and edit dashboards using interactive editors or simple XML.
Choose a home dashboard

Test PingOne for Enterprise SP-initiated SLO

1. Click the username in the top right corner.
2. Click **Logout**.







SuccessFactors

Configuring SAML SSO with SuccessFactors and PingFederate

Learn how to enable SuccessFactors sign-on from a PingFederate URL (IdP-initiated sign-on) and direct SuccessFactors sign-on using PingFederate (SP-initiated sign-on).

Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate SuccessFactors with at least one user to test access.
- You must have administrative access to PingFederate.
- You must have access to either SuccessFactors Customer Support or the SuccessFactors Provisioning tool.

Create a PingFederate SP connection for SuccessFactors

1. Sign on to the PingFederate administrative console.
2. Create an SP connection for SuccessFactors in PingFederate:
    1. Configure using**Browser SSO** profile **SAML 2.0**.
    2. Set **Partner's Entity ID** to `https://www.successfactors.com`.
    3. Enable the following **SAML Profiles**:
        - **IdP-Initiated SSO**
        - **SP-Initiated SSO**
    4. In **Assertion Creation: Attribute Contract**, extend the contract to add an attribute named **SAML_NAME_FORMAT**.
    5. In **Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment**, map **SAML_SUBJECT** and map **SAML_NAME_FORMAT** to `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`.
    6. In **Protocol Settings: Assertion Consumer Service URL**, set **binding** to **POST**, and set **Endpoint URL** to `http://placeholder`.

        You will update this value later.
    7. In **Protocol Settings: Allowable SAML Bindings**, enable **POST**.
    8. In **Credentials: Digital Signature Settings**, select the PingFederate signing certificate.
3. Save the configuration.

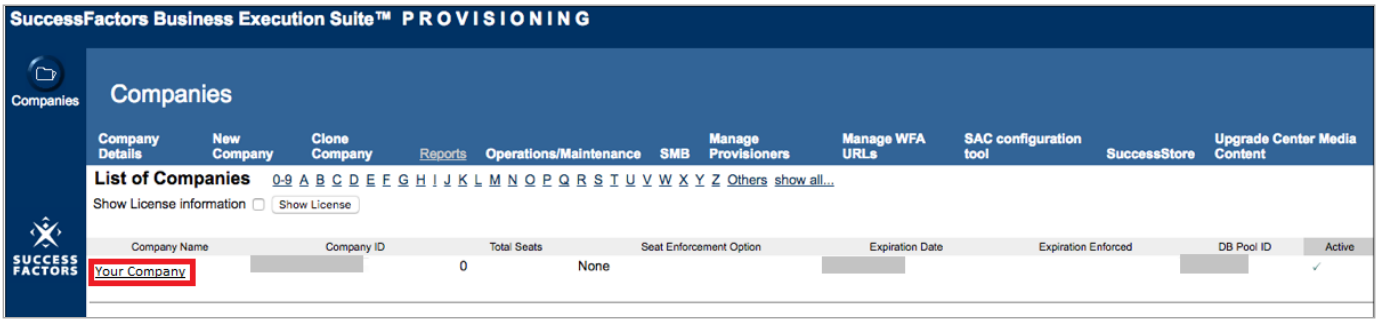
4. Export the signing certificate.
5. Export and then open the metadata file, and copy the following values:
    - The entityID
    - The Location entry (`https://your-value/idp/SSO.saml2`)

Add the PingFederate IdP Connection to SuccessFactors

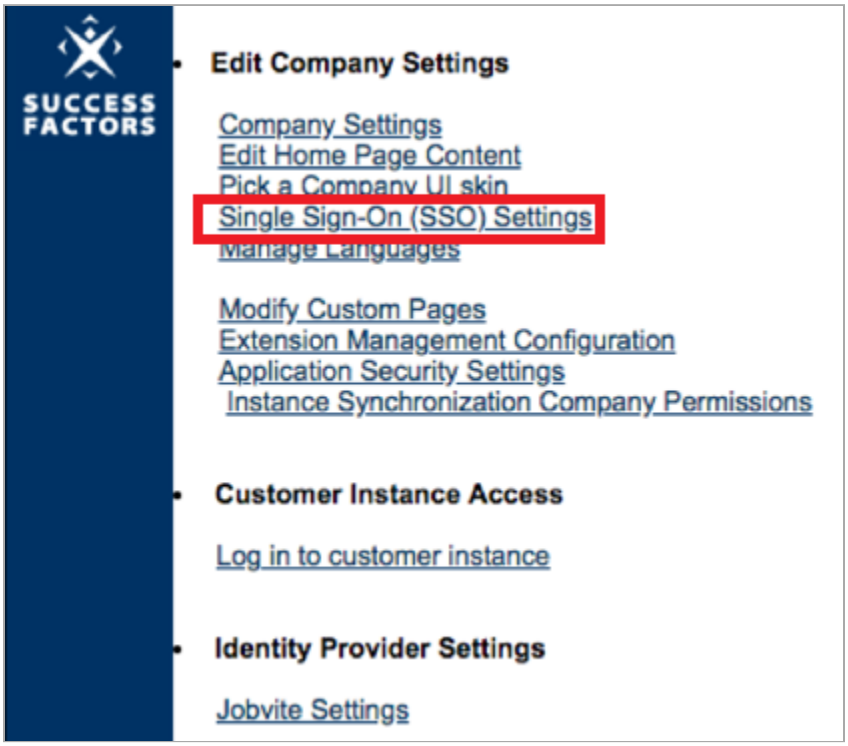
1. Sign on to the SuccessFactors Provisioning application.

> **Note**
>
> If you do not have access to this application, you will need to contact SuccessFactors' Customer Support.

2. Search for your company and click its name link.



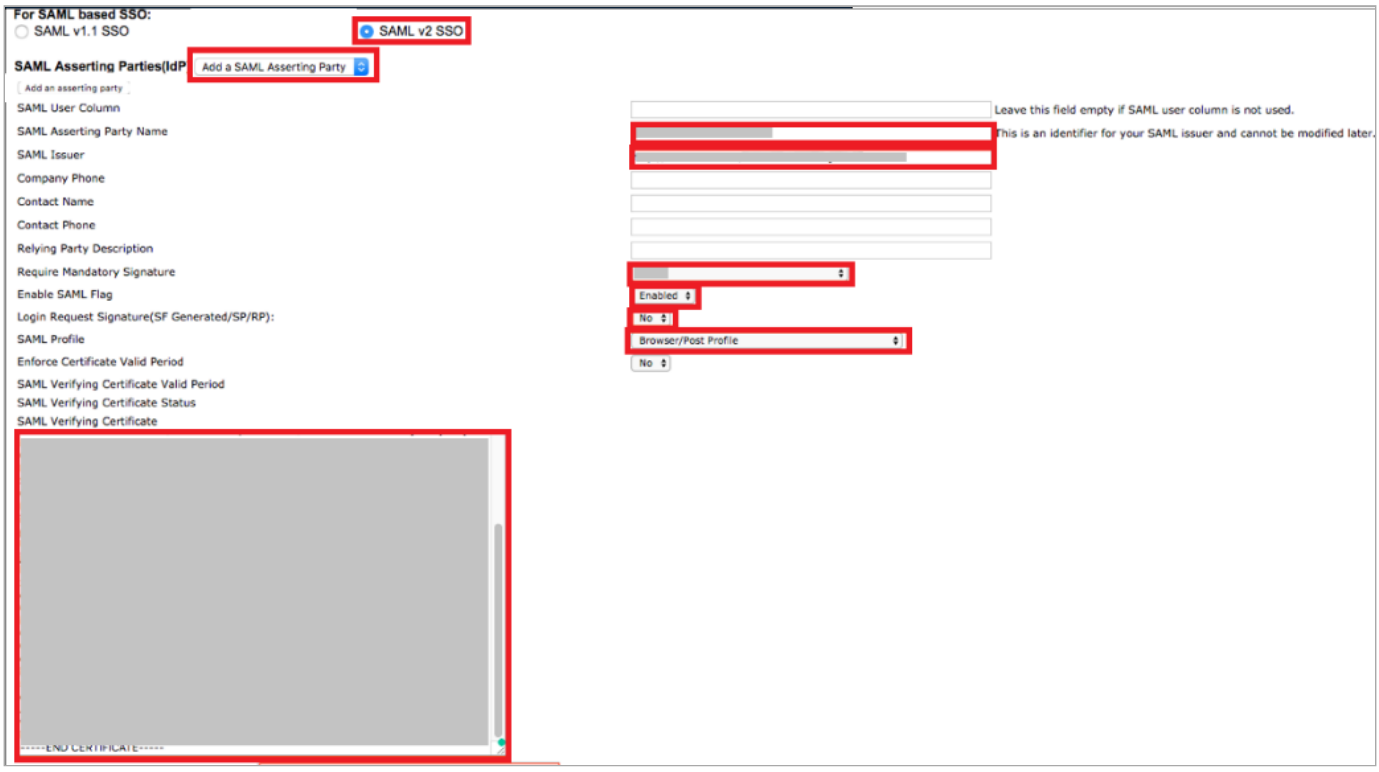
3. Click **Single Sign-On (SSO) Settings**.



4. In the **For SAML based SSO** section, click **SAML v2 SSO**.

5. In the **SAML Asserting Parties (IdP)** list, select **Add a SAML Asserting Party**, and enter the following values:

Field	Value
SAML Asserting Party Name	PingFederate
SAML Issuer	The PingFederate **Issuer** value
Require Mandatory Signature	**Assertion**
Enable SAML Flag	**Enabled**
Login Requested Signature (SF Generated/SP/RP)	Select **No**.
SAML Profile	**Browser/Post Profile**
SAML Verifying Certificate	Paste the PingFederate signing certificate contents.

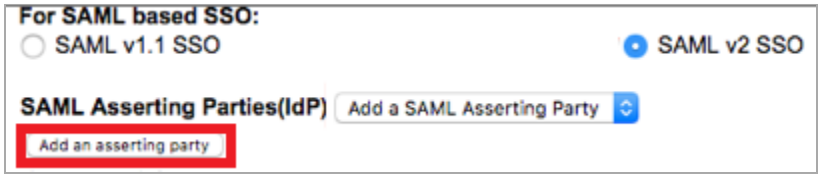


6. In the **SAML v2: SP-initiated login** section, enter the following values:

Field	Value
Enable sp initiated login (AuthnRequest)	Select **Yes**.
Default issuer	Selected.

Field	Value
single sign on redirect service location (to be provided by idp)	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=IdP-ID-value`
Send request as Company-Wide issuer	Select **Yes**.

7. Click **Add an asserting party** to save the configuration.



8. In the **SAML Asserting Parties (IdP)** list, select the asserting party that you created.

9. Go to **Single Sign On Features**.
10. In the **Single Sign On Features** section, enter any text value in the **Reset Token** field.

    A value is required only to switch on SSO.

11. Click **Save Token**.

12. Record the SuccessFactors **Assertion Consumer Service URL** value containing your SuccessFactors **Hostname** and **Company ID**.

    (`https://your-hostname.successfactors.com/saml2/SAMLAssertionConsumer?company=your-company-ID`)

Update the ACS URL values in PingFederate

1. Sign on to the PingFederate administrative console.

2. Edit the SP connection for SuccessFactors.
3. Set **Assertion Consumer Service URL → Endpoint URL** to the SuccessFactors **Assertion Consumer Service URL** value.

   (`https://your-hostname.successfactors.com/saml2/SAMLAssertionConsumer?company=your-company-ID`)
4. Save the changes.

Test the PingFederate IdP-initiated SSO integration

1. Go to the PingFederate SSO Application Endpoint for the SuccessFactors SP connection.
2. Complete PingFederate authentication.

   You're redirected to your SuccessFactors domain.

Configuring SAML SSO with SuccessFactors and PingOne for Enterprise

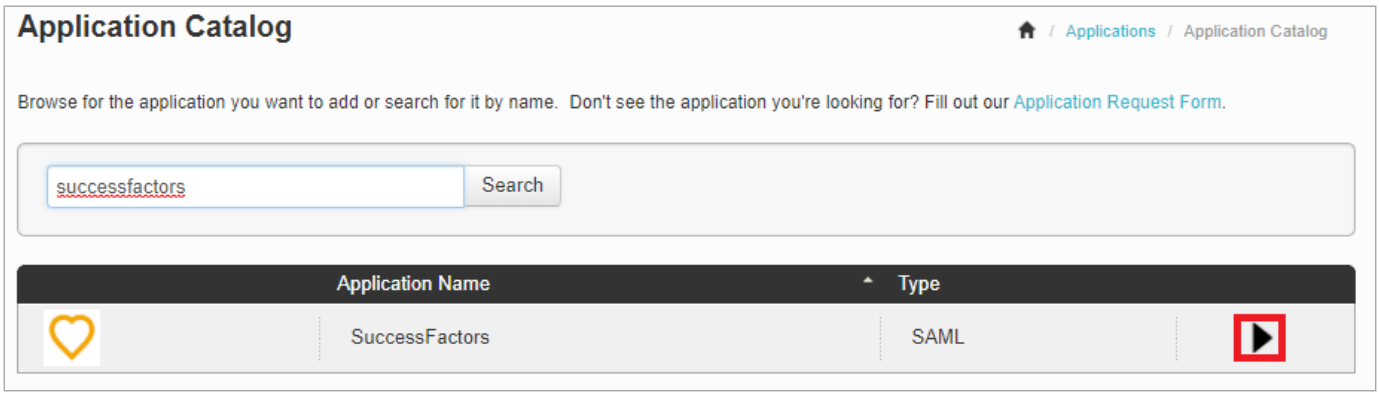
Learn how to enable SuccessFactors sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct SuccessFactors sign-on using PingOne for Enterprise (SP-initiated sign-on).

Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate SuccessFactors with at least one user to test access.
- You must have administrative access to PingOne for Enterprise.
- You must have access to either SuccessFactors Customer Support or the SuccessFactors Provisioning tool.

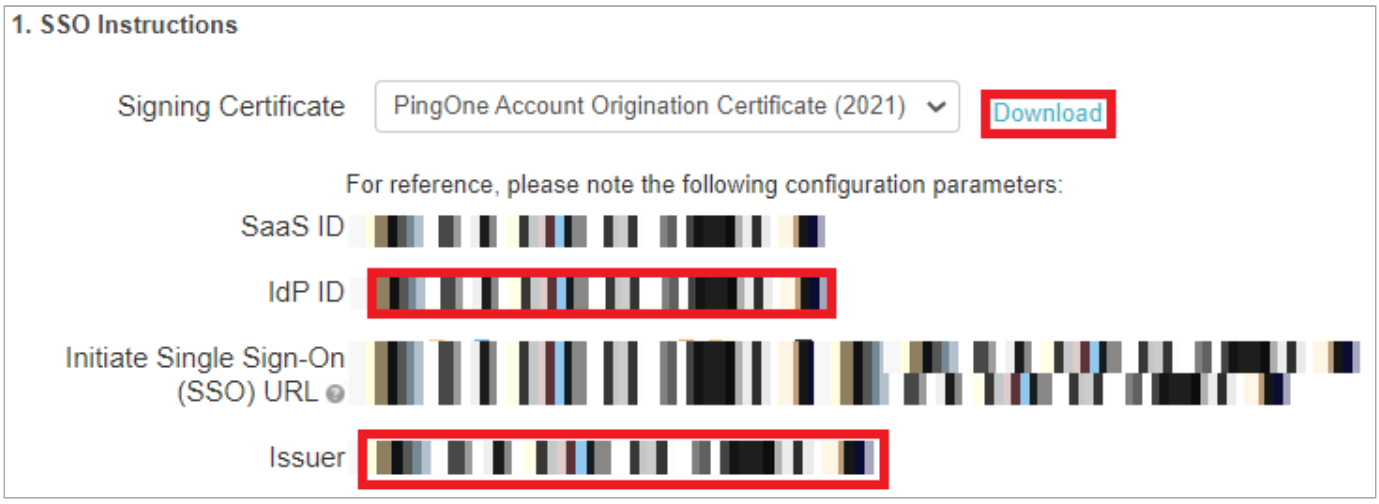
Obtain the PingOne for Enterprise values for the SuccessFactors application

1. Sign on to PingOne for Enterprise and go to **Applications → Application Catalog**.
2. Search for `SuccessFactors` .



3. Expand the SuccessFactors entry and click the **Setup** icon.
4. Copy the **Issuer** and **IdP ID** values.

5. Download the signing certificate.

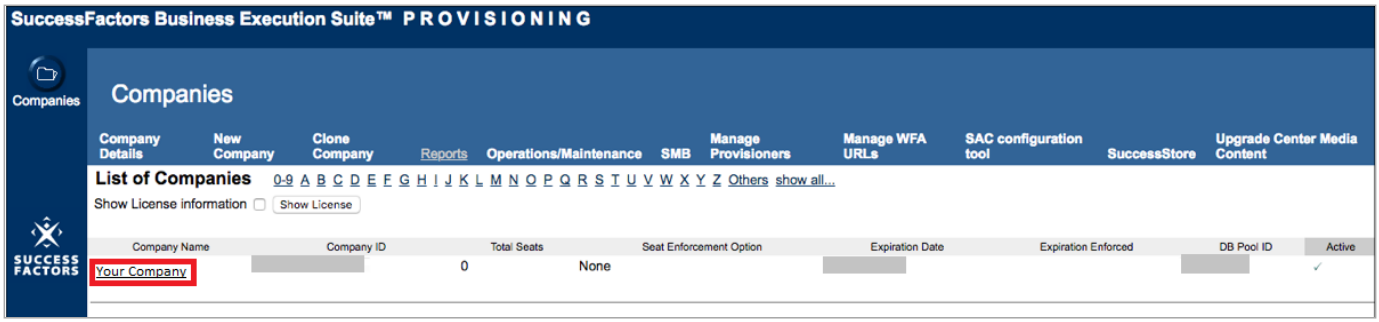


Add the PingOne for Enterprise IdP connection to SuccessFactors

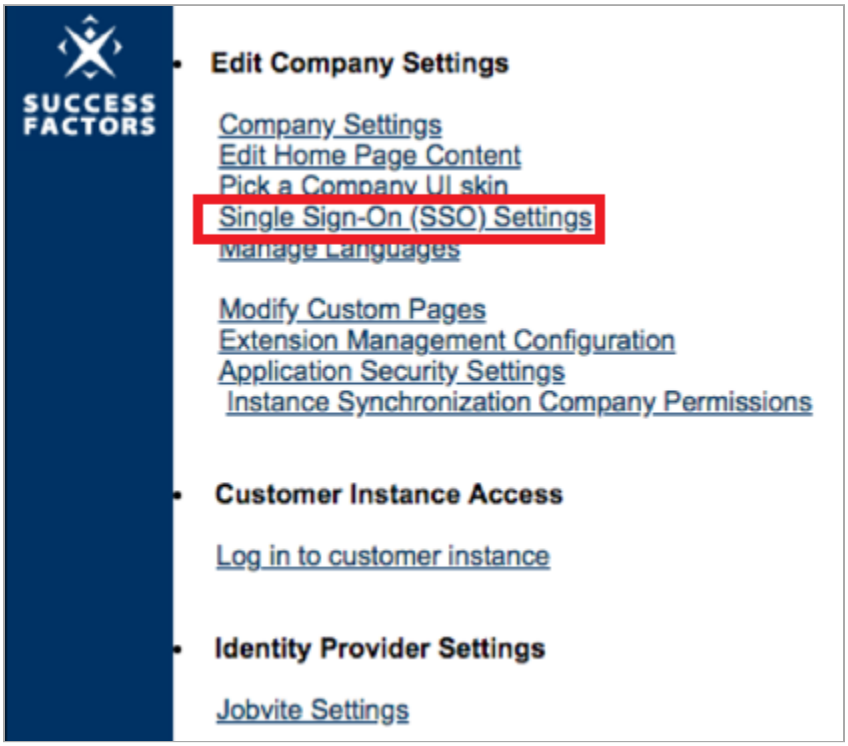
1. Sign on to the SuccessFactors Provisioning application.

> **Note**
>
> If you do not have access to this application, you will need to contact SuccessFactors' Customer Support.

2. Search for your company and click its name link.

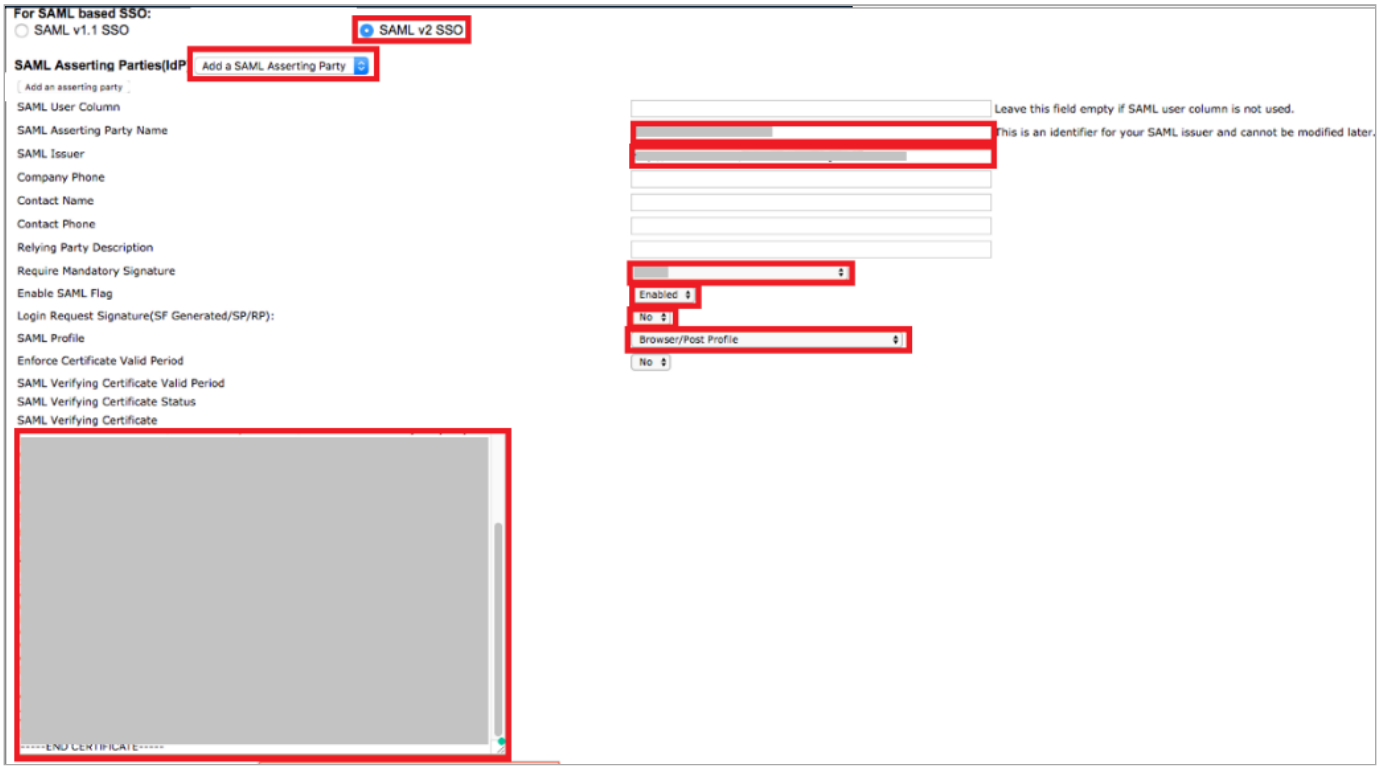


3. Click **Single Sign-On (SSO) Settings**.



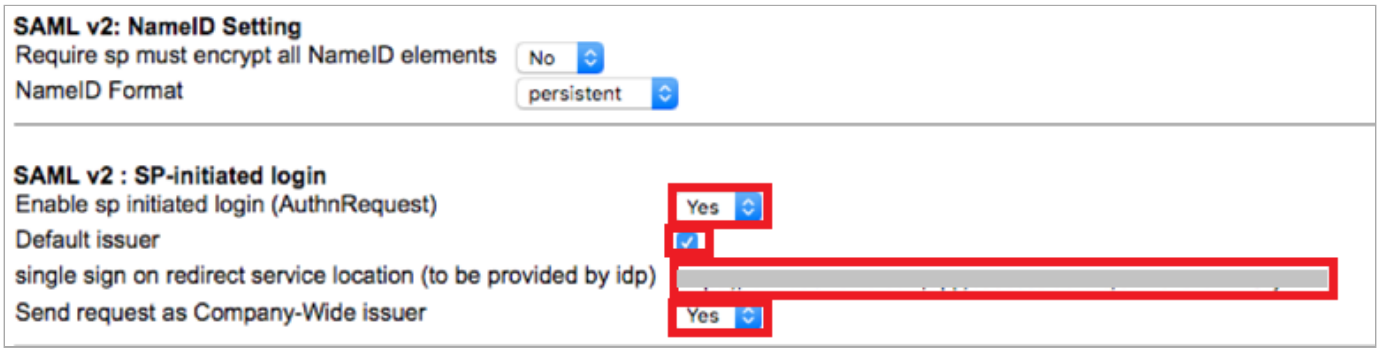
4. In the **For SAML based SSO** section, click **SAML v2 SSO**.
5. In the **SAML Asserting Parties (IdP)** list, select **Add a SAML Asserting Party**, and enter the following.

Field	Value
SAML Asserting Party Name	PingOne for Enterprise
SAML Issuer	The PingOne for Enterprise **Issuer** value.
Require Mandatory Signature	**Assertion**
Enable SAML Flag	**Enabled**
Login Request Signature (SF Generated/SP/RP)	Select **No.**
SAML Profile	**Browser/Post Profile**
SAML Verifying Certificate	Paste the PingOne for Enterprise signing certificate contents.



6. In the **SAML v2: SP-initiated login** section, enter the following.

Field	Value
Enable sp initiated login (AuthnRequest)	Select **Yes**.
Default Issuer	Selected.
single sign on redirect service location (to be provided by idp)	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=IdP-ID-value`
Send request as Company-Wide issuer	Select **Yes**.



7. Click **Add an asserting party** to save the configuration.

8. In the **SAML Asserting Parties (IdP)** list, select the asserting party that you created.

9. In the **Single Sign On Features** section, enter any text value in the **Reset Token** field.

   A value is required only to switch on SSO.

10. Click **Save Token**.

11. Record the SuccessFactors **Assertion Consumer Service URL** value containing your SuccessFactors **Hostname** and **Company ID**.

   (`https://*your-hostname*.successfactors.com/saml2/SAMLAssertionConsumer?company=*your-company-ID*)

Complete the SuccessFactors setup in PingOne for Enterprise

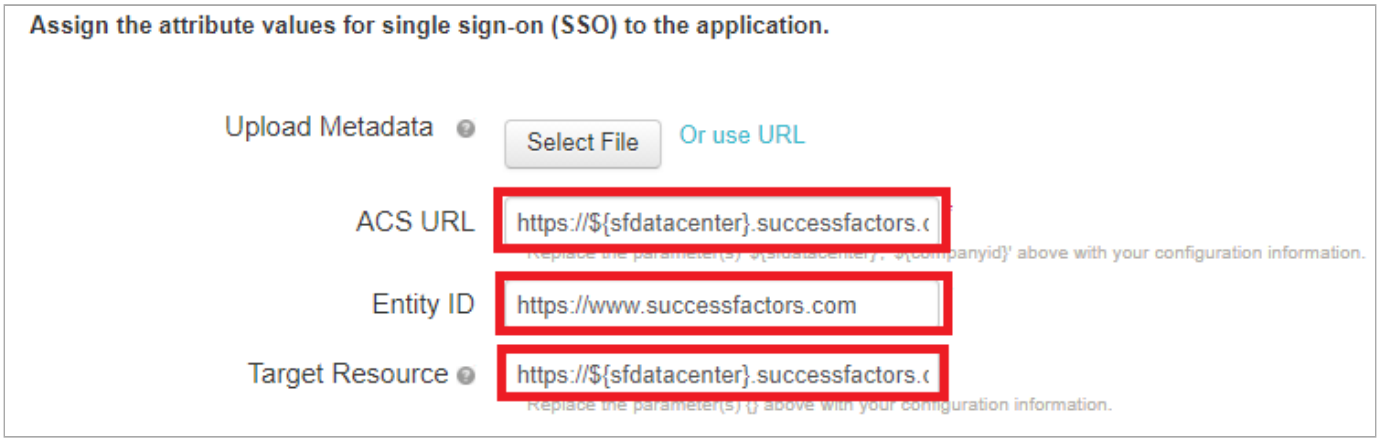
1. Continue editing the SuccessFactors entry in PingOne for Enterprise for Enterprise.

> **Note**
>
> If the session has timed out, complete the initial steps to the point of clicking **Setup**.

2. Click **Continue to Next Step**.
3. Set the **ACS URL** to be the SuccessFactors **Assertion Consumer Service URL** value.

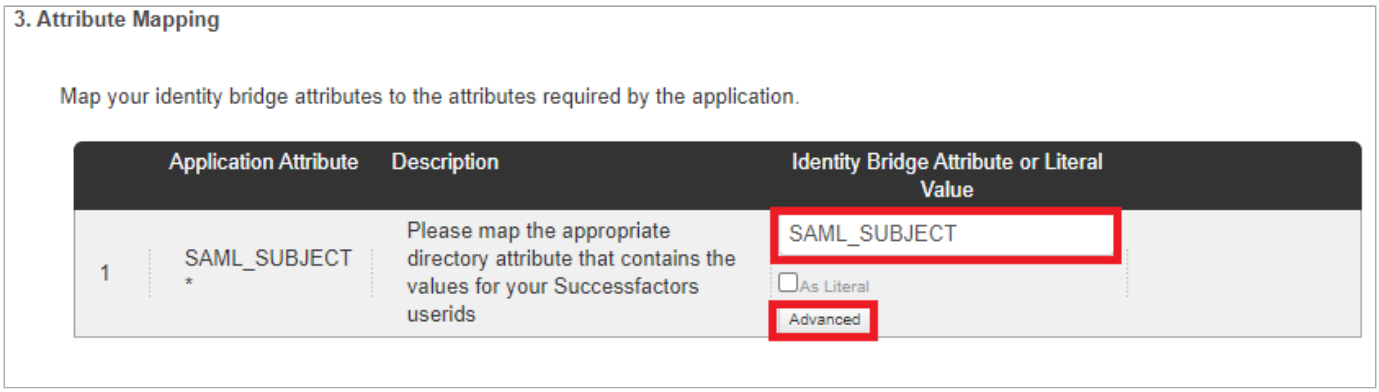
   (`https://your-hostname.successfactors.com/saml2/SAMLAssertionConsumer?company=your-company-ID`)

4. Leave the preset **Entity ID**.
5. In the **Target Resource** field, replace `${sfdatacenter}` with the hostname from the **ACS URL** value.

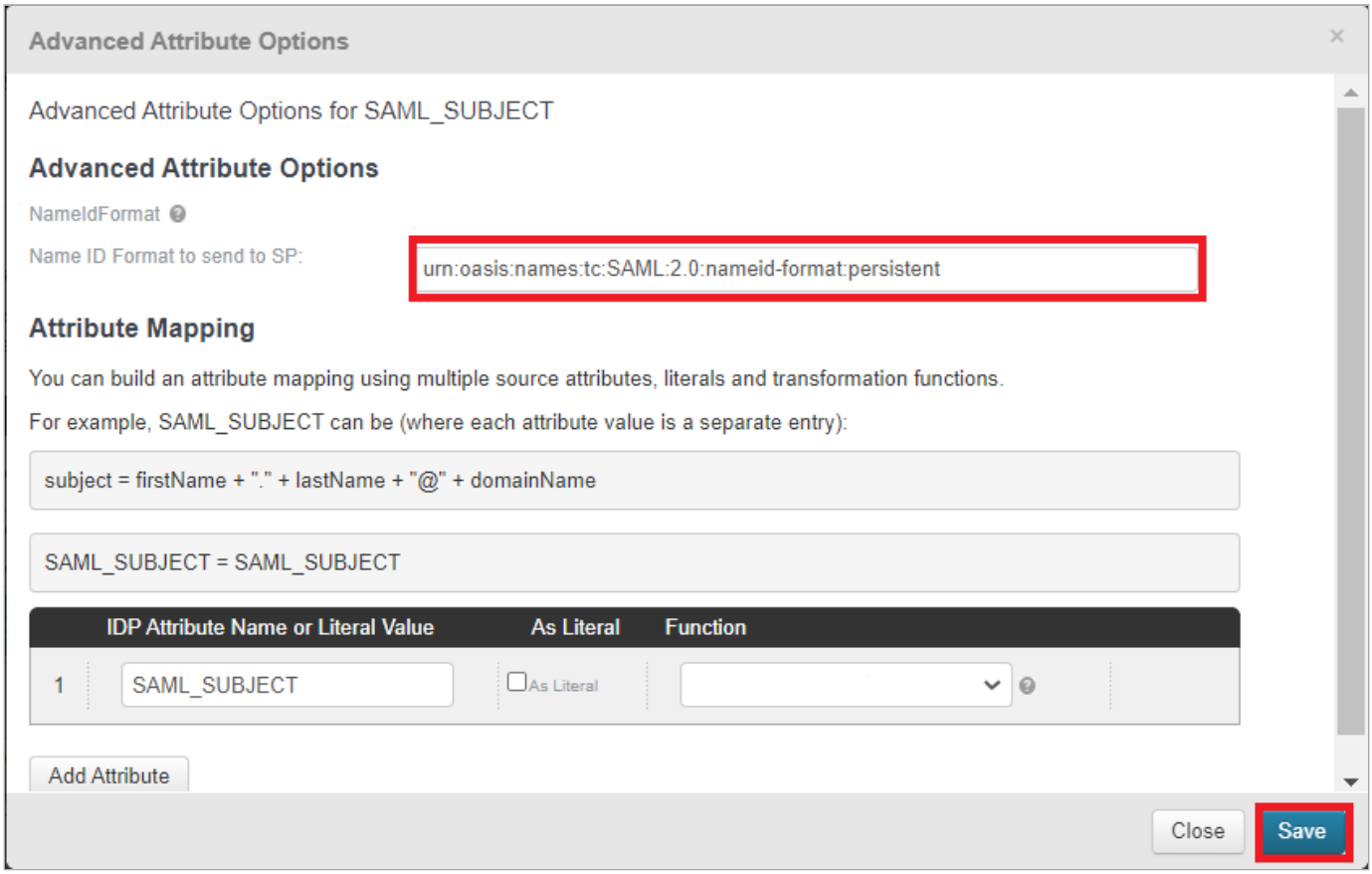


6. Click **Continue to Next Step**.

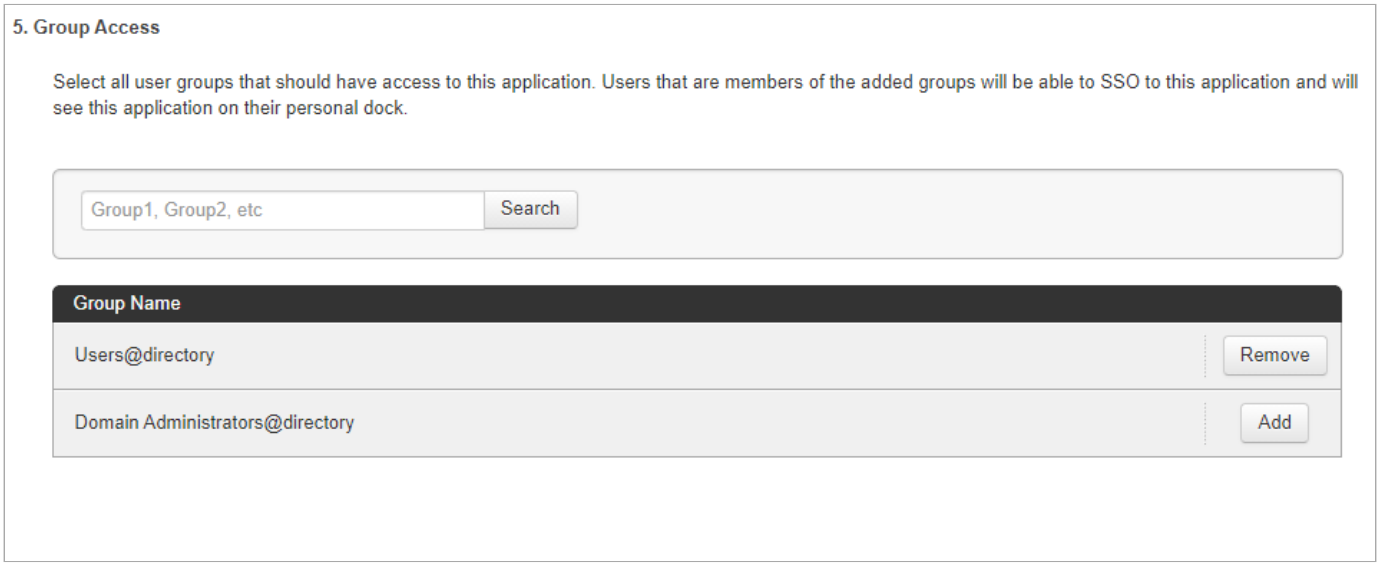
7. Map the **SAML_SUBJECT** attribute to the similar attribute names in your environment and click **Advanced**.



8. Set the **Name ID Format to send to SP** to **urn:oasis:names:tc:SAML:2.0:nameid-format:persistent**. Click **Save**.



9. Click **Continue to Next Step** twice.
10. Click **Add** for all user groups that should have access to SuccessFactors.



11. Click **Continue to Next Step**.
12. Click **Finish**.

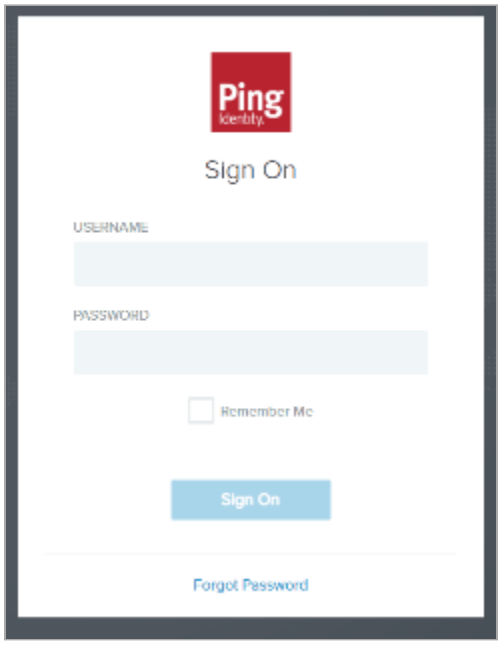
Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with SuccessFactors access.

   > **Note**
   >
   > To find the Ping desktop URL in the Admin console, go to **Setup → Dock → PingOne Dock URL**.

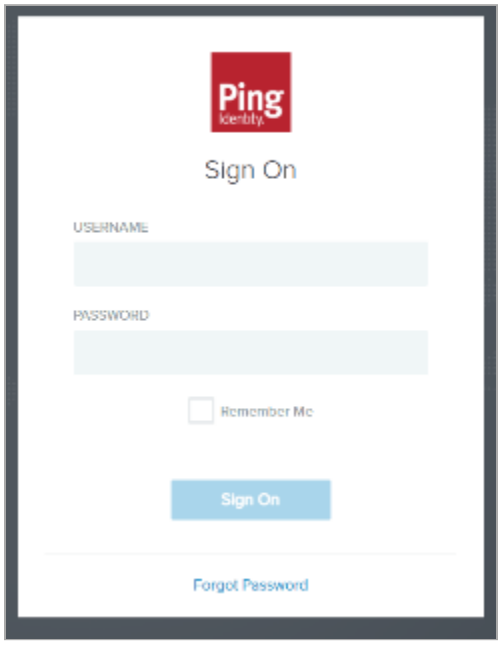
2. Complete the PingOne for Enterprise authentication.

   You're redirected to your SuccessFactors account.



Test the PingOne SP-initiated SSO integration

1. Go to your SuccessFactors URL.
2. When you're redirected to PingOne for Enterprise, enter your PingOne username and password.



You’re redirected back to SuccessFactors.

SumoLogic

Configuring SAML SSO with SumoLogic and PingFederate

Learn how to enable SumoLogic sign-on from a PingFederate URL (IdP-initiated sign-on) and direct SumoLogic sign-on using PingFederate (SP-initiated sign-on).

Before you begin

- Configure PingFederate to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- PingFederate's X.509 certificate should be exchanged to verify the signature in SAML assertions.
- An email attribute is required in the assertion, either the SAML Subject or another SAML attribute per the SAML configuration. The value of the email attribute must be a valid email address. It is used to uniquely identify the user in the organization.
- Populate SumoLogic with at least one user to test access.

Create a PingFederate service provider (SP) connection for SumoLogic

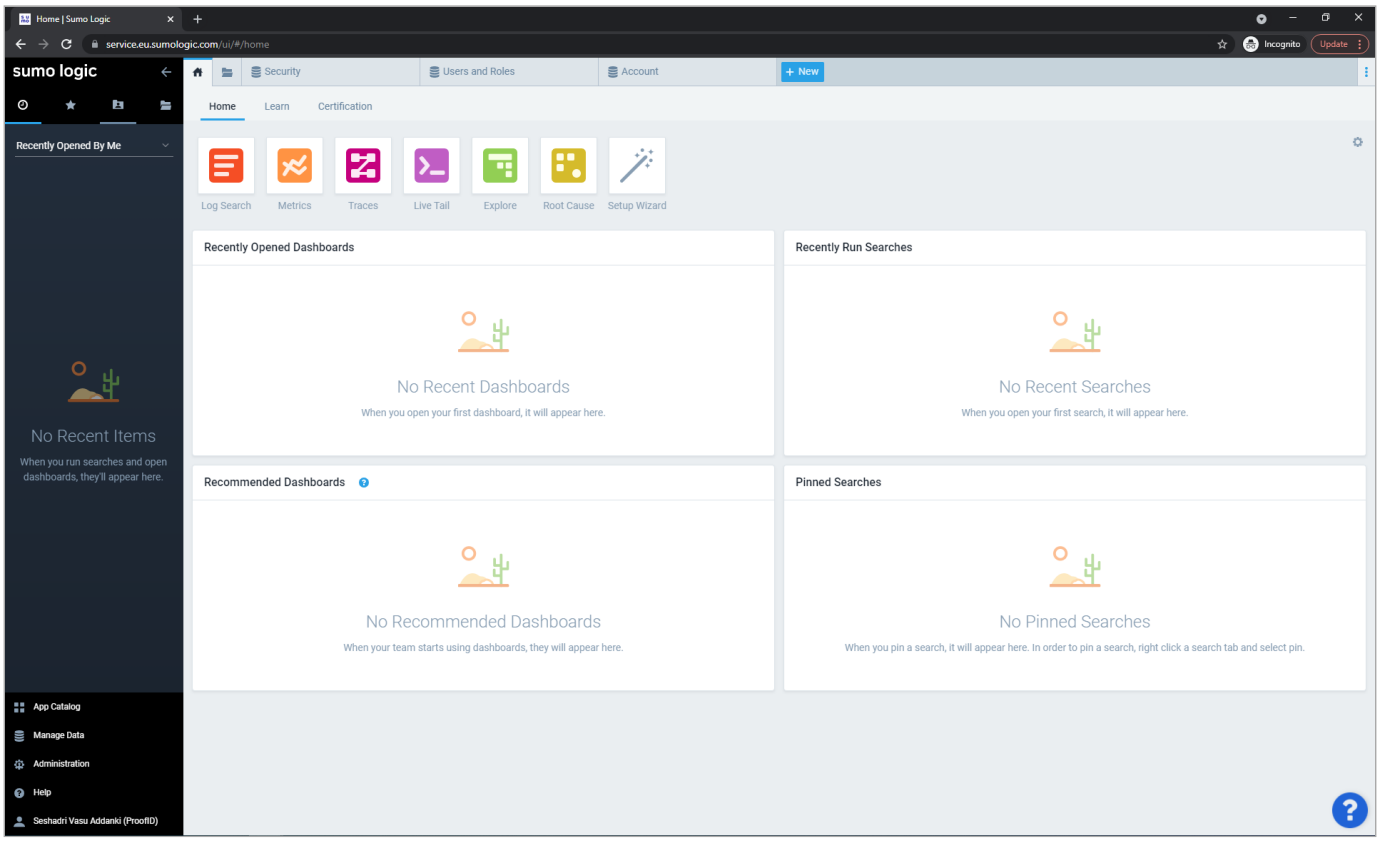
1. Sign on to the PingFederate admin console.
2. Configure using **Browser SSO** profile **SAML 2.0**.
3. Set **Partner's Entity ID** to `https://service.eu.sumologic.com/`.
4. Enable the following SAML Profiles:
    - **IdP-Initiated SSO**
    - **SP-Initiated SSO**
5. In **Assertion Creation: Attribute Contract**, select **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified**.
6. In **Assertion Creation: Authentication Source Mapping: Authentication Source Mapping**, map a new **Adapter Instance → HTML Form**.
7. In **Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfilment**, map `SAML_SUBJECT`.
8. In **Protocol Settings: Assertion Consumer Service URL**, set **Binding** to **POST** and set **Endpoint URL** to `https://service.eu.sumologic.com/sumo/saml/consume/596910108`. This value is received and updated from SumoLogic.
9. In **Protocol Settings: Allowable SAML Bindings**, enable **POST**.
10. In **Credentials: Digital Signature Settings**, select the **PingFederate Signing Certificate**.
11. Save the configuration.

12. Export the signing certificate.
13. Export and then open the metadata file and copy the value of:
    - The **entityID**
    - The **Location** entry (`https://your-value/idp/SSO.saml2`)

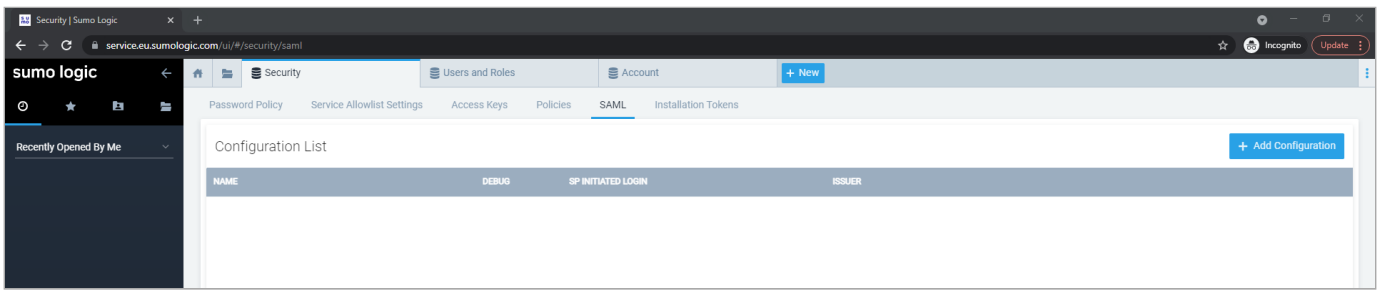
Add the PingFederate IdP Connection to SumoLogic

1. Sign on to the SumoLogic application.

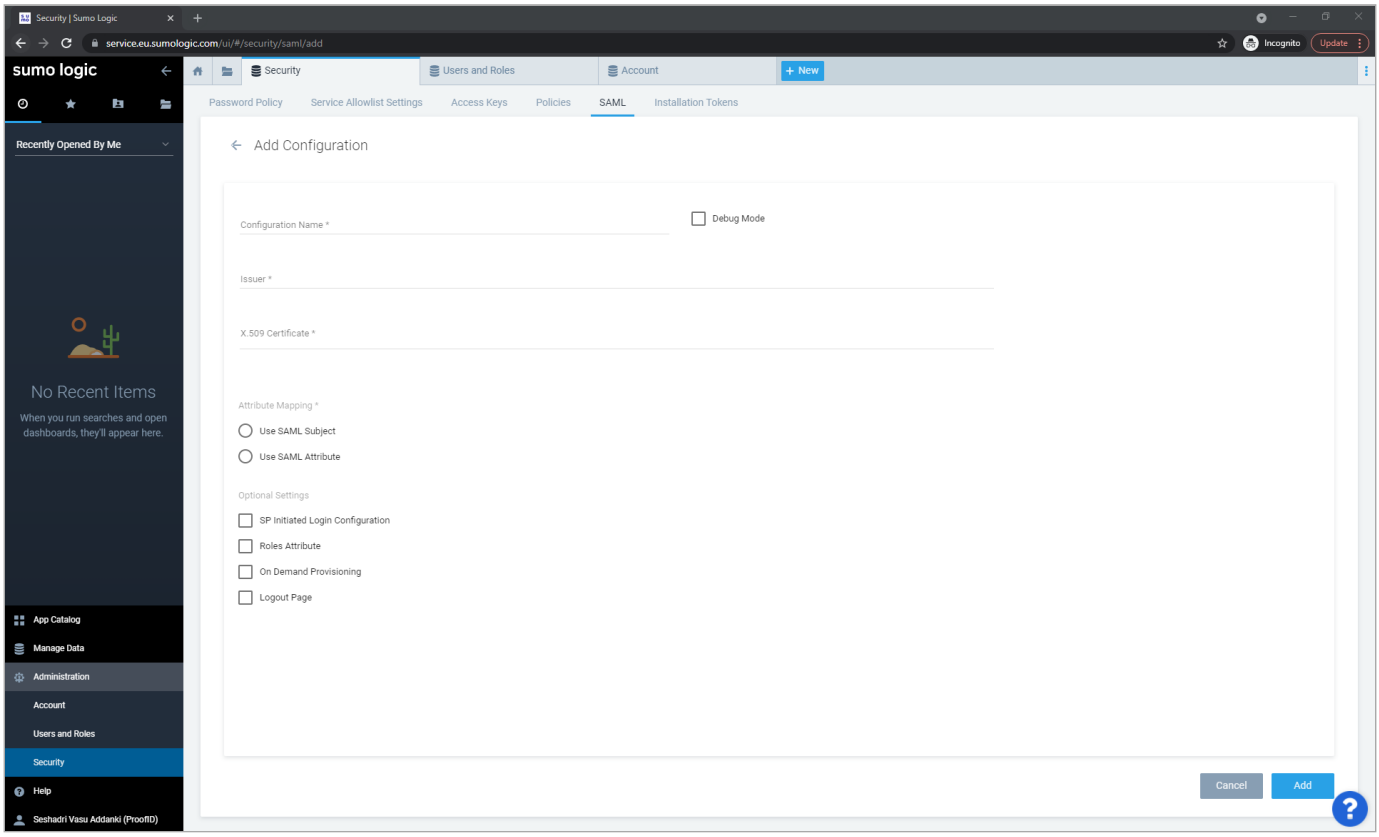
> **Note**
>
> In this example, we have registered and logged in using trial mode.



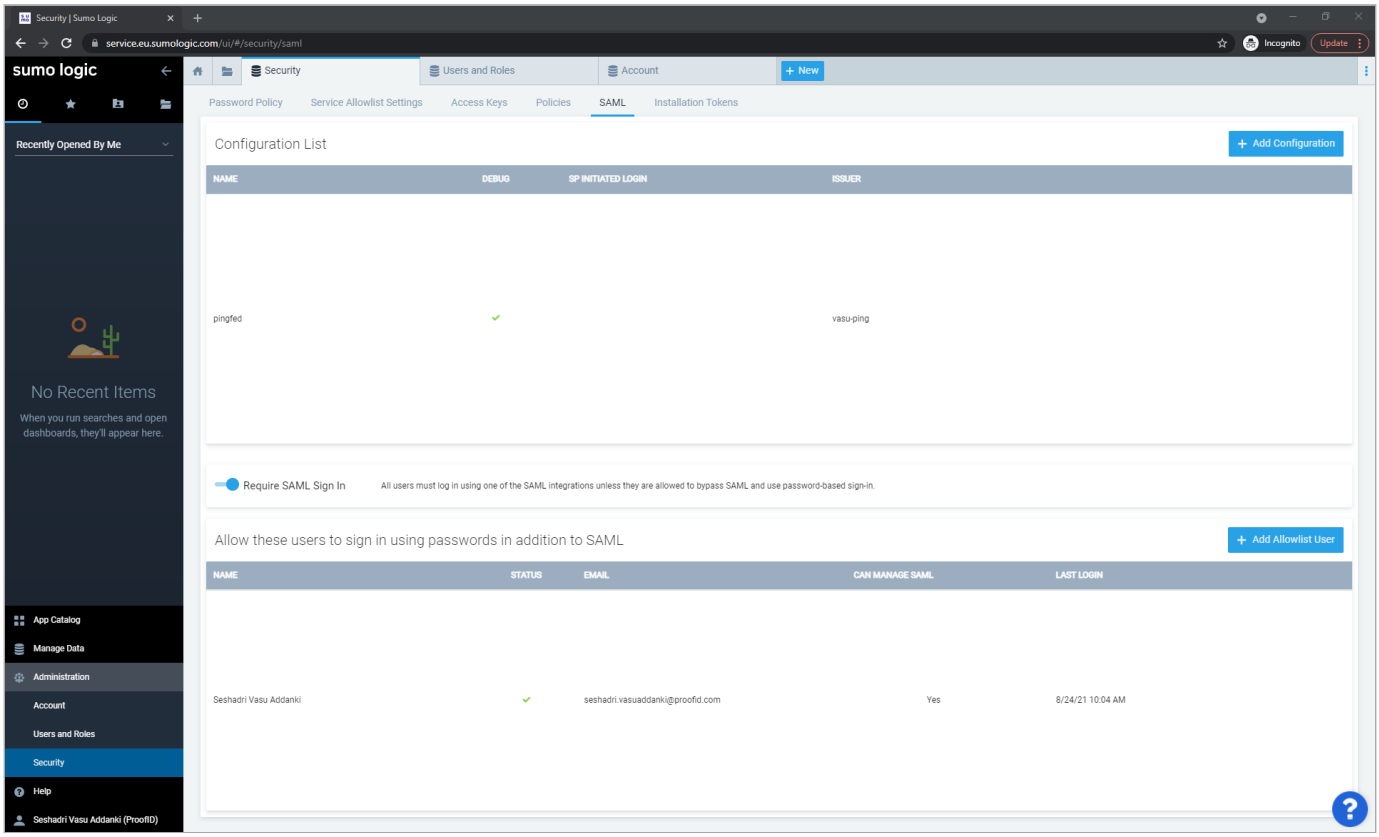
2. Go to **Administration → Security → SAML**.



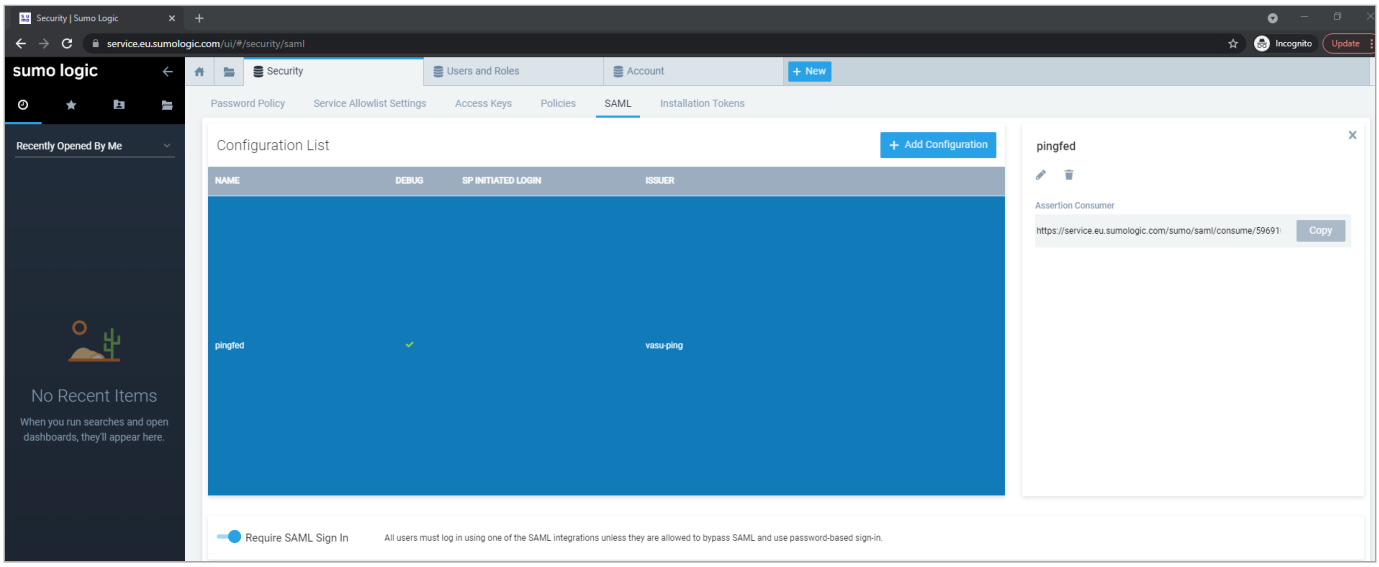
3. Click **Add Configuration**.



4. Add the following values:
    - **Configuration Name** : `pingfed`
    - Select the **Debug Mode** check box
    - **Issuer**: The PingFederate Issuer value
    - **X.509 Certificate**: Copy PingFederate's X.509 certificate here for verifying the signature
    - **Attribute Mapping**: Select **Use SAML Subject**
    - **Optional Settings**: Leave the default settings
    - Click **Add**
    - Enable **Require SAML Sign In**.

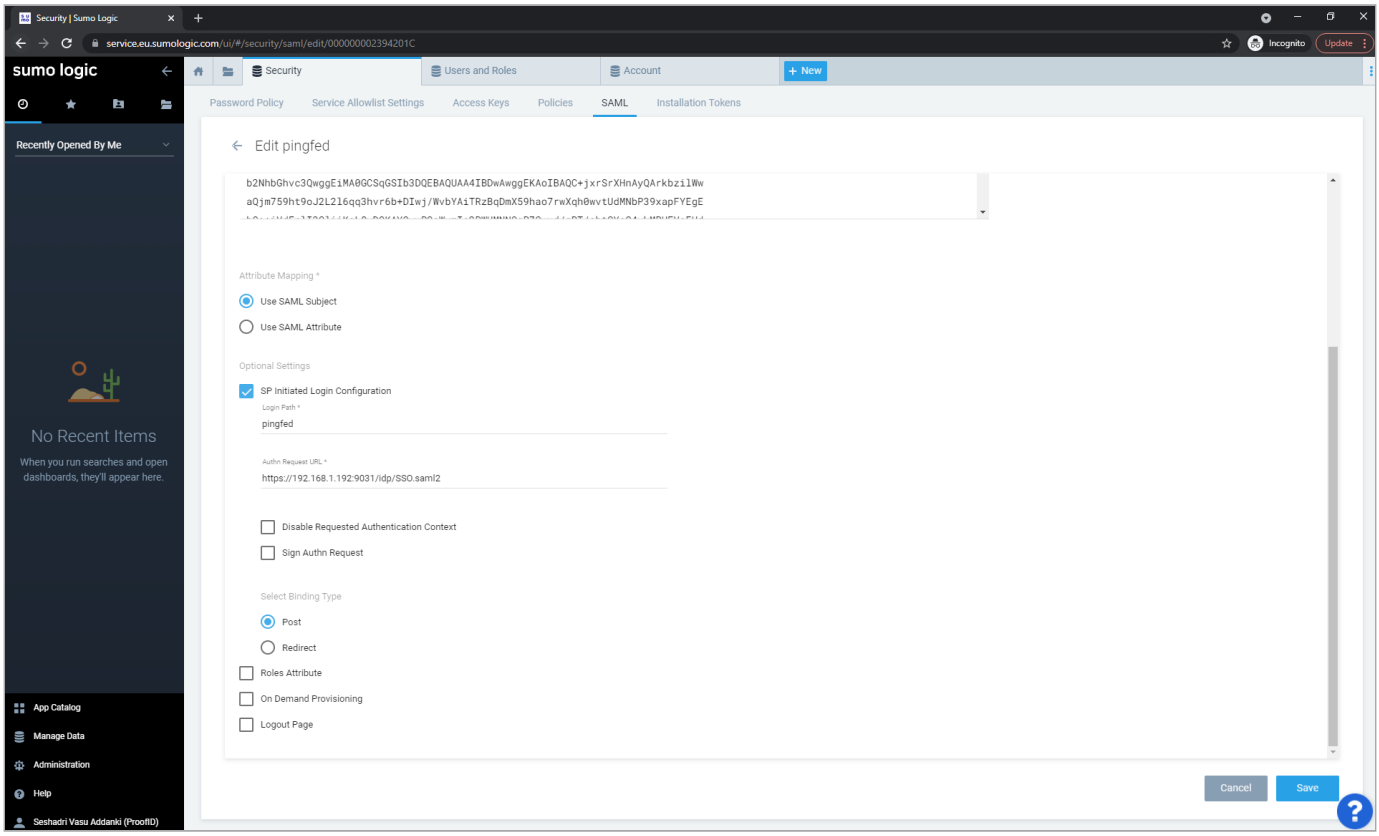


5. Select the **pingfed** configuration you have just created and copy the **Assertion Consumer Service URL**.

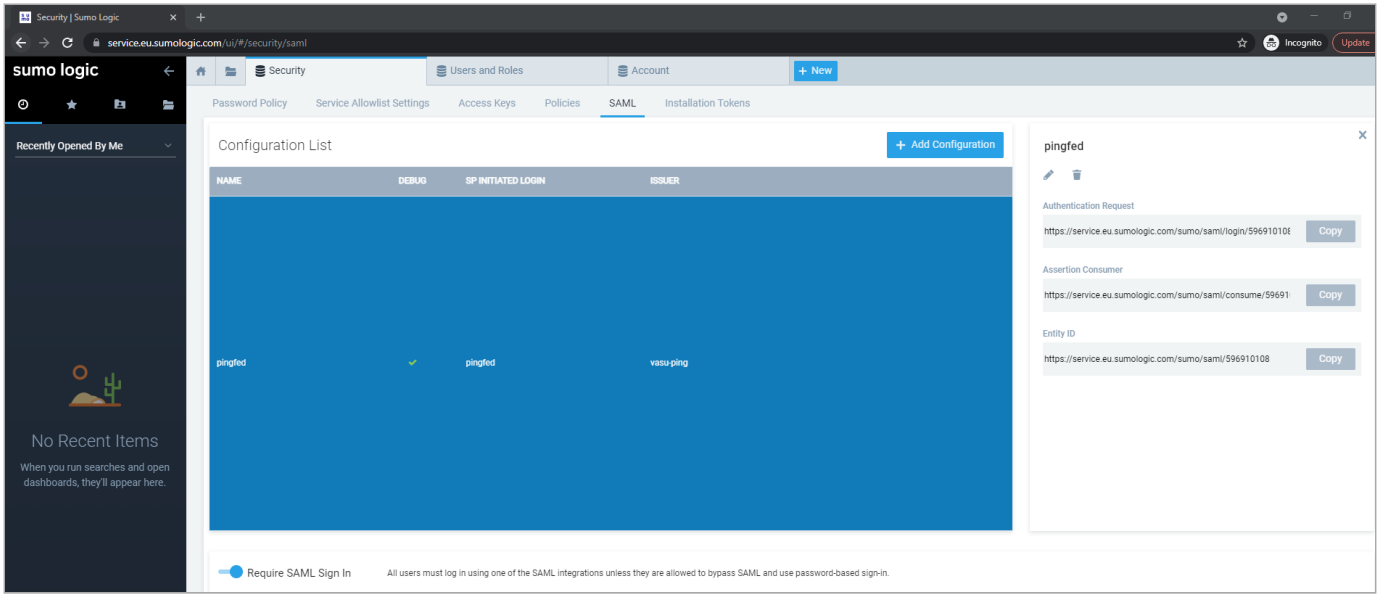


6. To enable SP-initiated SSO, select the **pingfed** configuration and click the **Pencil** icon above the **ACS URL**.
7. Select the **SP Initiated Login Configuration** check box and enter the following values:
    - **Login Path**: enter a unique identifier for your organization. You can specify any alphanumeric string (with no embedded spaces), provided that it is unique to your organization. (You can't configure a **Login Path** that another Sumo customer has already configured).

- **Authn Request URL**: enter the URL that the IdP has assigned for SumoLogic to submit SAML authentication requests to the IdP. For example, `https://idp-server-hostname:9031/sso/idp/SSO.saml2`
- Select **Binding Type: Post**.



8. Click **Save**.
9. Click the saved **pingfed** configuration again and make a note of the **Authentication Request** and **EntityID** URLs.



The SumoLogic connection configuration is now complete.

Update the ACS URL values in PingFederate

1. Sign on to the PingFederate administrative console.
2. Edit the SP connection for SumoLogic.
3. Set the **Partner's Entity ID (Connection ID)** value to SumoLogic's **Entity ID** that you copied previously.
4. Set **Assertion Consumer Service URL : Endpoint URL** to SumoLogic's **Assertion Consumer Service URL** value.
5. Click **Save**.

Test the PingFederate IdP-initiated SSO integration

1. Go to the **PingFederate SSO Application Endpoint** for the SumoLogic SP connection.
2. Authenticate with PingFederate.

   You're redirected to your SumoLogic domain.

Test the PingFederate SP-initiated SSO integration

1. Go to your SumoLogic **Authentication Request URL**.
2. After you're redirected to PingFederate, enter your PingFederate username and password.

   After successful authentication, you're redirected back to SumoLogic.

Tableau

Configuring SAML SSO with Tableau and PingOne

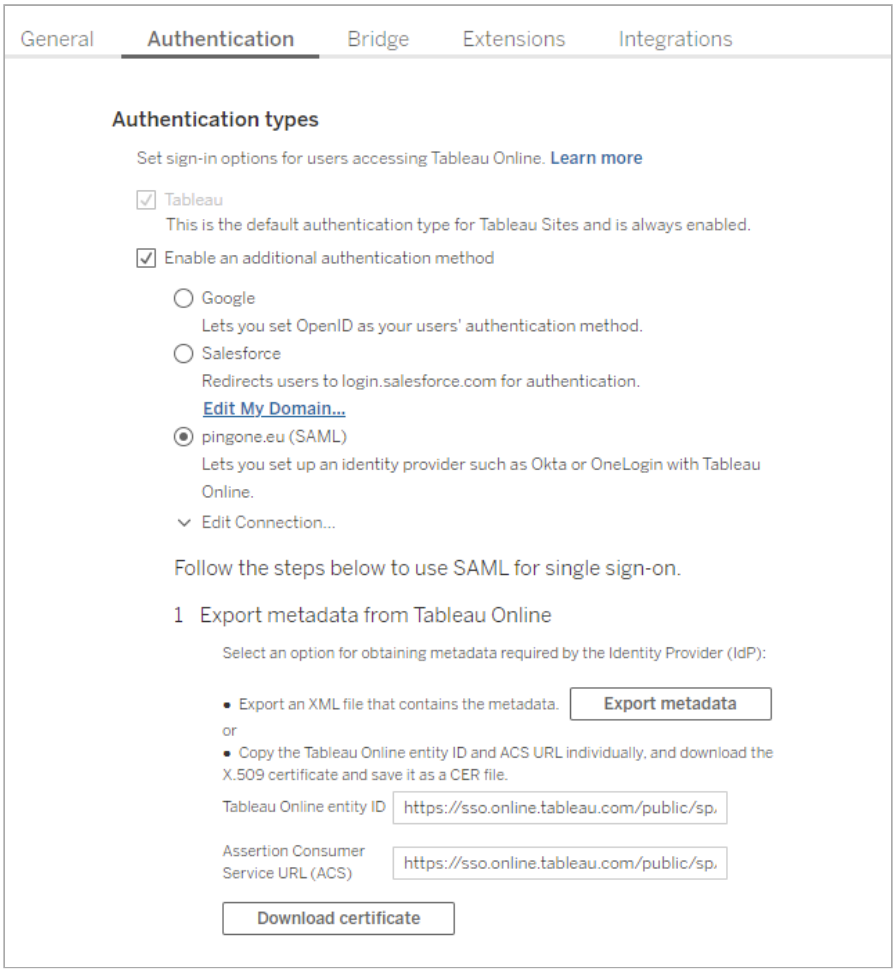
Learn how to enable Tableau SSO in PingOne (IdP and SP-initiated).

Before you begin

- Configure PingOne to authenticate against an identity repository containing the users requiring application access.
- An Email Attribute is required in the assertion, either the SAML Subject or another SAML attribute per the SAML configuration. The value of the Email Attribute must be a valid email address. This attribute is used to uniquely identify the user in the organization.

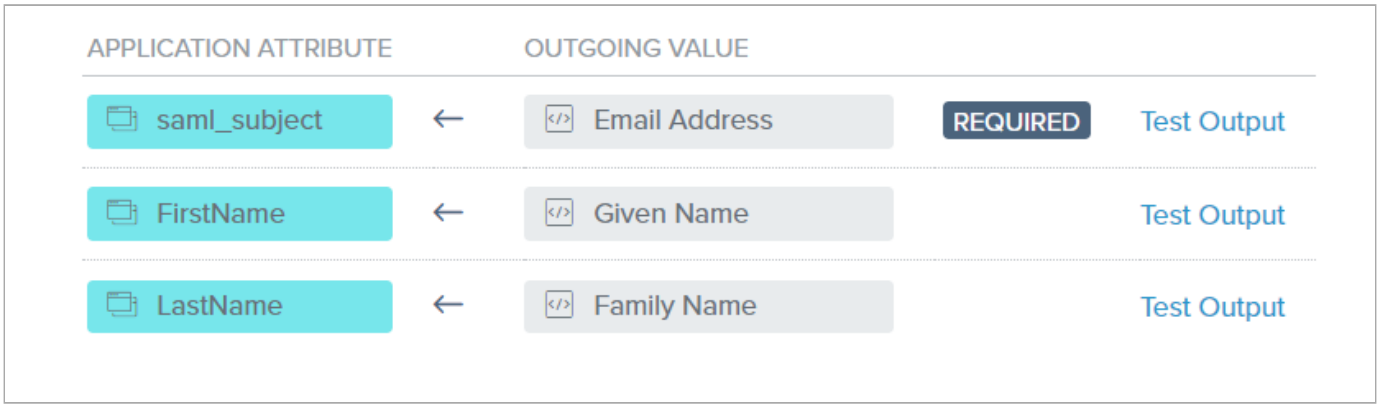
Export the metadata from Tableau

1. Sign on to Tableau with an administration account.
2. Go to **Settings → Authentication**.
3. Select the **Enable an additional authentication method** check box.
4. Select the SAML authentication method.
5. Expand the **Edit Connection** section.
6. Click **Export Metadata**.

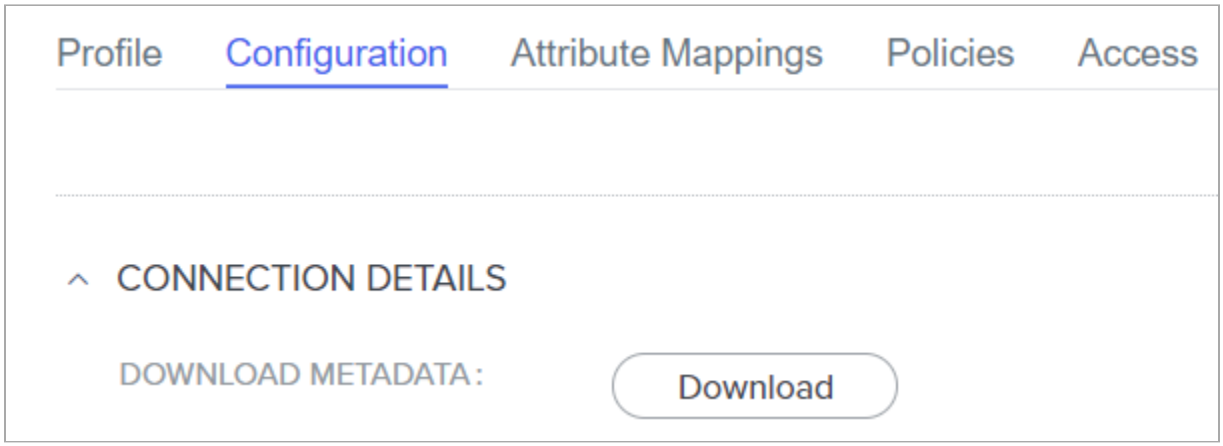


Create the Tableau SP connection

1. In the PingOne admin portal, go to **Connections → Applications**.
2. Create an SP connection for Tableau by selecting **Add application**.
3. When you're prompted to select an application type, select **WEB APP** and then click **Configure** next to **SAML** for the chosen connection type.
4. Enter a unique name for the application.
5. Import the Tableau metadata.
6. Select the signing certificate.
7. Confirm that the **EntityID** and endpoints are correct.
8. Enter a suitable value for **Assertion Validity Duration (in seconds)**. A value of 300 seconds is typical.
9. Click **Save and Continue**.
10. Define the Tableau assertion requirements.

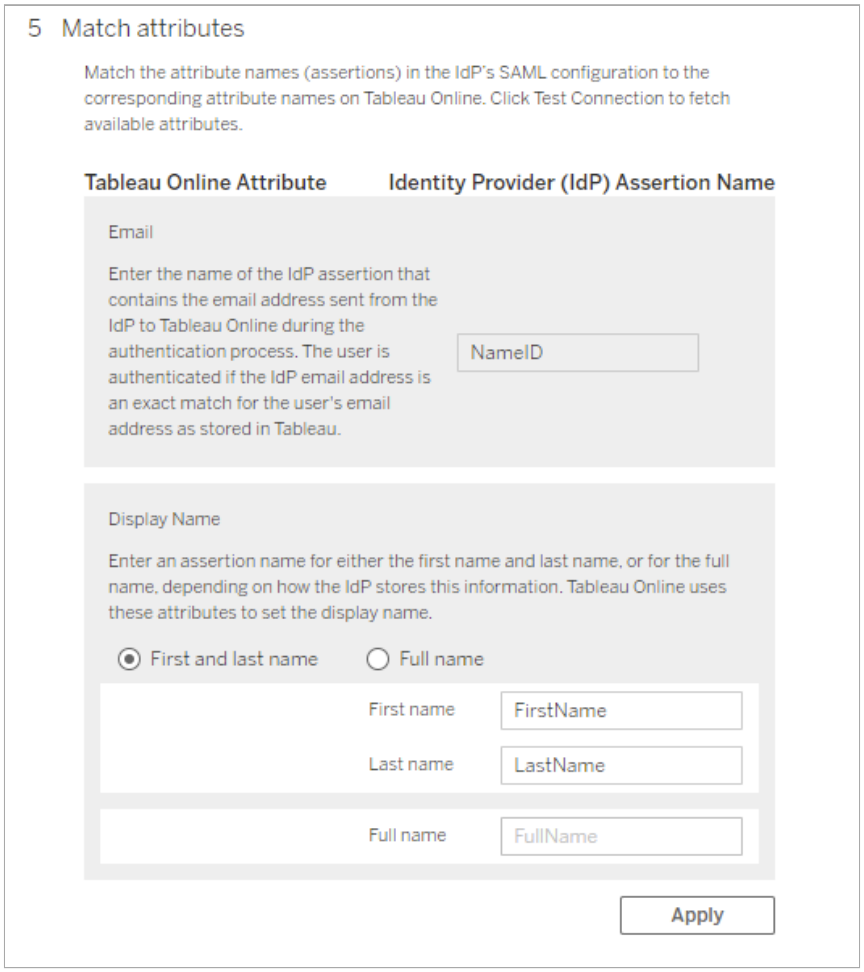


11. Click the toggle to enable the application.
12. On the **Configuration** tab for the Tableau application, on the **Download Metadata** line, click **Download**.



Import the metadata in Tableau

1. Upload the PingOne metadata file and click **Apply**.
2. Confirm that the IdP, entityID, and SSO service URL are correct.
3. Test the connection.
4. Match the Tableau attributes to the assertion attributes and click **Apply**.



Test the IdP-initiated SSO integration

1. Go to the PingOne Application Portal and sign on with a user account.

   > **Note**
   >
   > In the Admin console, go to **Dashboard → Environment Properties** to find the **PingOne Application Portal URL**.

2. Click the Tableau icon.

   You're redirected to the Tableau website and logged in with SSO.

Test the SP-initiated SSO integration

1. Go to the Tableau sign on page and enter the email address that will redirect to PingOne.
2. In the PingOne sign-on prompt, enter your PingOne username and password.

   You're redirected back to Tableau and signed on with SSO.

Configuring SAML SSO with Tableau and PingFederate

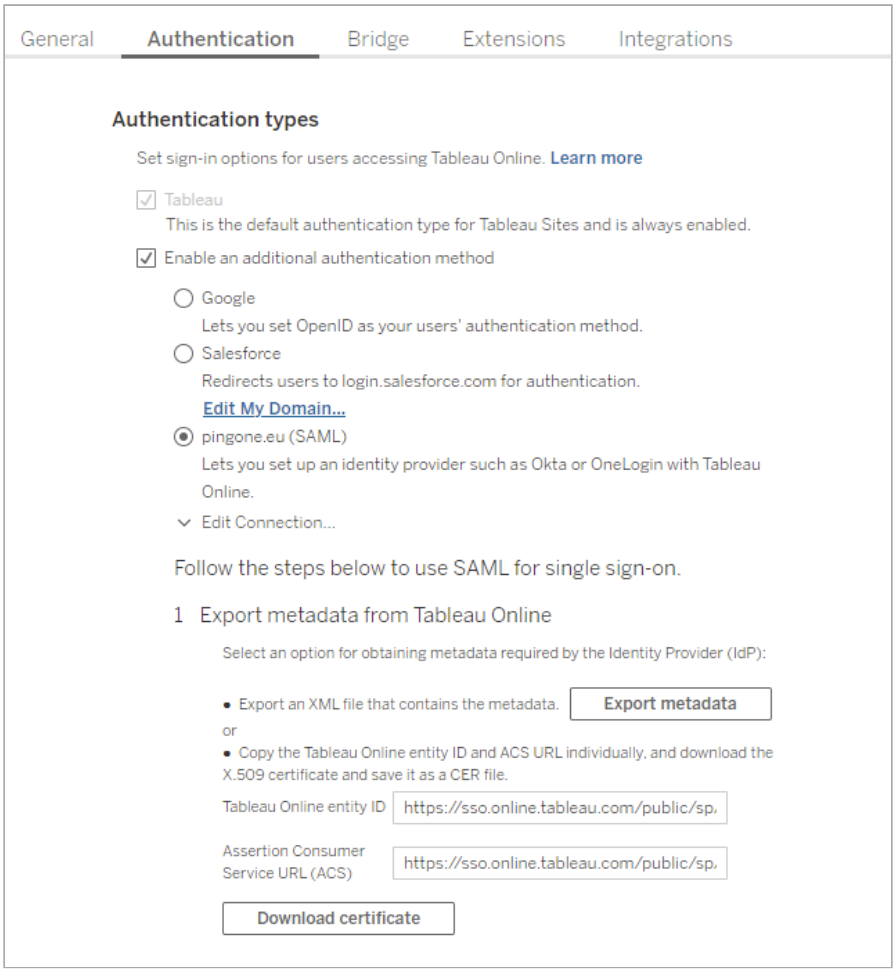
Learn how to enable Tableau SSO in PingFederate (IdP and SP-initiated).

Before you begin

- Configure PingFederate to authenticate against an identity repository containing the users requiring application access.
- An Email Attribute is required in the assertion, either the SAML Subject or another SAML attribute per the SAML configuration. The value of the Email Attribute must be a valid email address. This attribute is used to uniquely identify the user in the organization.

Export the metadata from Tableau

1. Sign on to Tableau with an administration account.
2. Go to **Settings → Authentication**.
3. Select the **Enable an additional authentication method** check box.
4. Select the SAML authentication method.
5. Expand the **Edit Connection** section.
6. Click **Export Metadata**.



Create a Tableau SP Connection

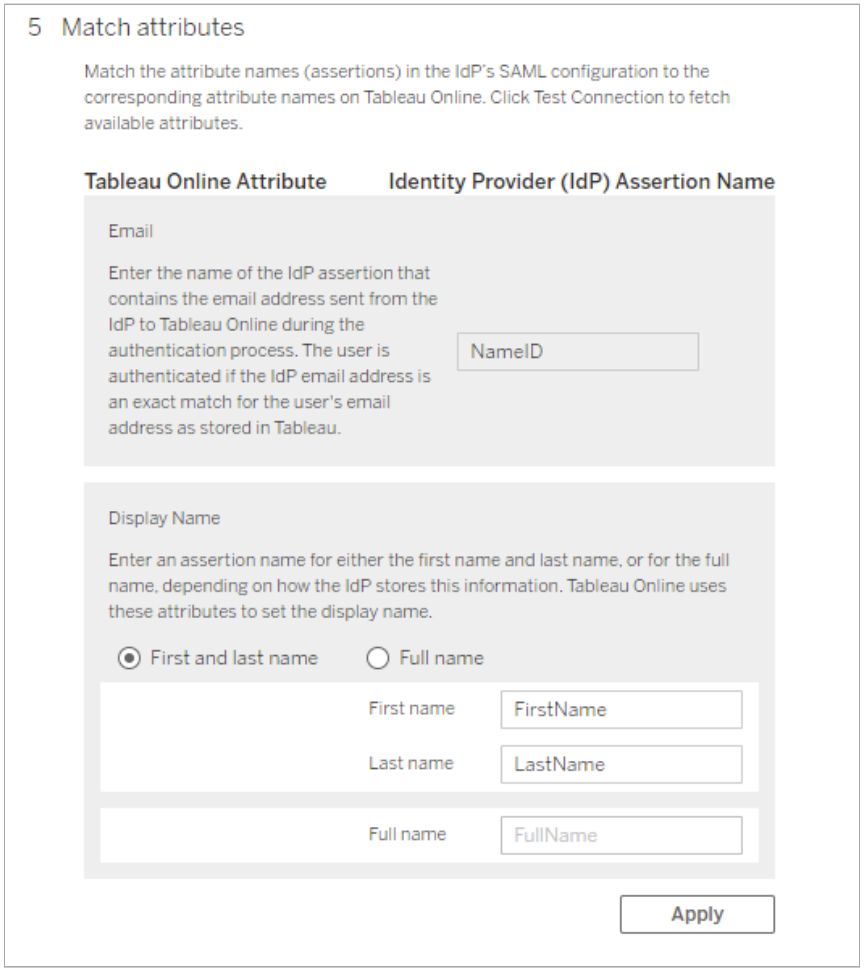
1. In PingFederate, create a service provider (SP) connection for Tableau.
2. Configure using **Browser SSO** profile **SAML 2.0**.
3. Upload the metadata file from Tableau.
4. Enable the following SAML profiles.
    - **IdP-Initiated SSO**
    - **SP-Initiated SSO**
5. Configure the assertion:
    - Select the source mappings.
    - Define the contract fulfillment.

Mapping Method	
Adapter	HTML Form IdP Adapter
Mapping Method	Use only the Adapter Contract values in the mapping
Attribute Contract Fulfillment	
FirstName	givenname (Adapter)
LastName	sn (Adapter)
SAML_SUBJECT	mail (Adapter)

6. In **protocol settings: Allowable SAML Bindings**, enable **POST**.
7. Go to `https://PingFederate-url/pf/federation_metadata.ping?PartnerSpId=Tableau-EntityId` and download the metadata file from PingFederate.

Import the metadata in Tableau

1. Upload the PingFederate metadata file and click **Apply**.
2. Confirm that the IdP entityID and SSO service URL are correct.
3. Test the connection.
4. Match the Tableau attributes to the assertion attributes and click **Apply**.



Test the IdP-initiated SSO integration

1. Go to the PingFederate SSO application endpoint for Tableau, `https://PingFederate-url/idp/startSSO.ping?PartnerSpId=Tableau-EntityId`.

   `https://127.0.0.1:9031/idp/startSSO.ping?PartnerSpId=https://sso.online.tableau.com/public/sp/metadata/5c142f94-8889-491a-816c-e61ae6dc84cb`

2. Authenticate with PingFederate.

   You're redirected to Tableau.

Test the SP-initiated SSO integration

1. Go to the Tableau sign on page.
2. Enter the email address that will redirect to PingFederate.
3. Authenticate with PingFederate.

   You're redirected back to Tableau.

Configuring SCIM 2.0 provisioning with Tableau and PingFederate

Learn how to enable Tableau SCIM 2.0 Provisioning in PingFederate.

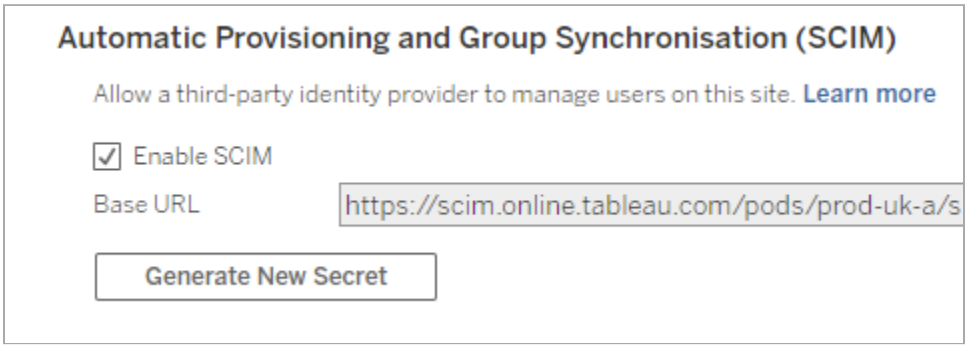
Before you begin

- Configure PingFederate to authenticate against an LDAP identity repository containing the users requiring application access.
- Configure PingFederate with the SCIM provisioning connector to support the SCIM 2.0 protocol.
- Configure PingFederate with the Tableau SP connection.
- Configure the PingFederate `run.properties` file to support provisioning.

Enable SCIM provisioning in Tableau

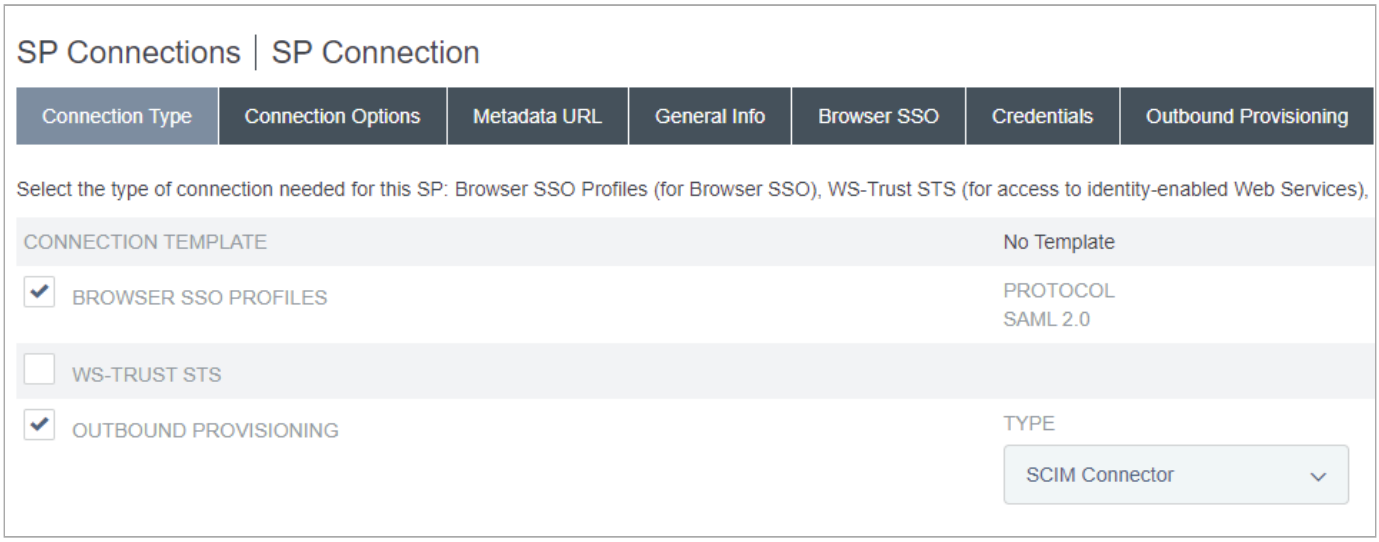
1. Sign on to Tableau with an administration account.
2. Go to **Settings → Authentication**.
3. In the **Automatic Provisioning and Group Synchronisation (SCIM)** section, select the **Enable SCIM** check box.
4. Click **Generate New Secret**.

   This will generate a new API secret that PingFederate will use to authenticate to the Tableau SCIM endpoint.

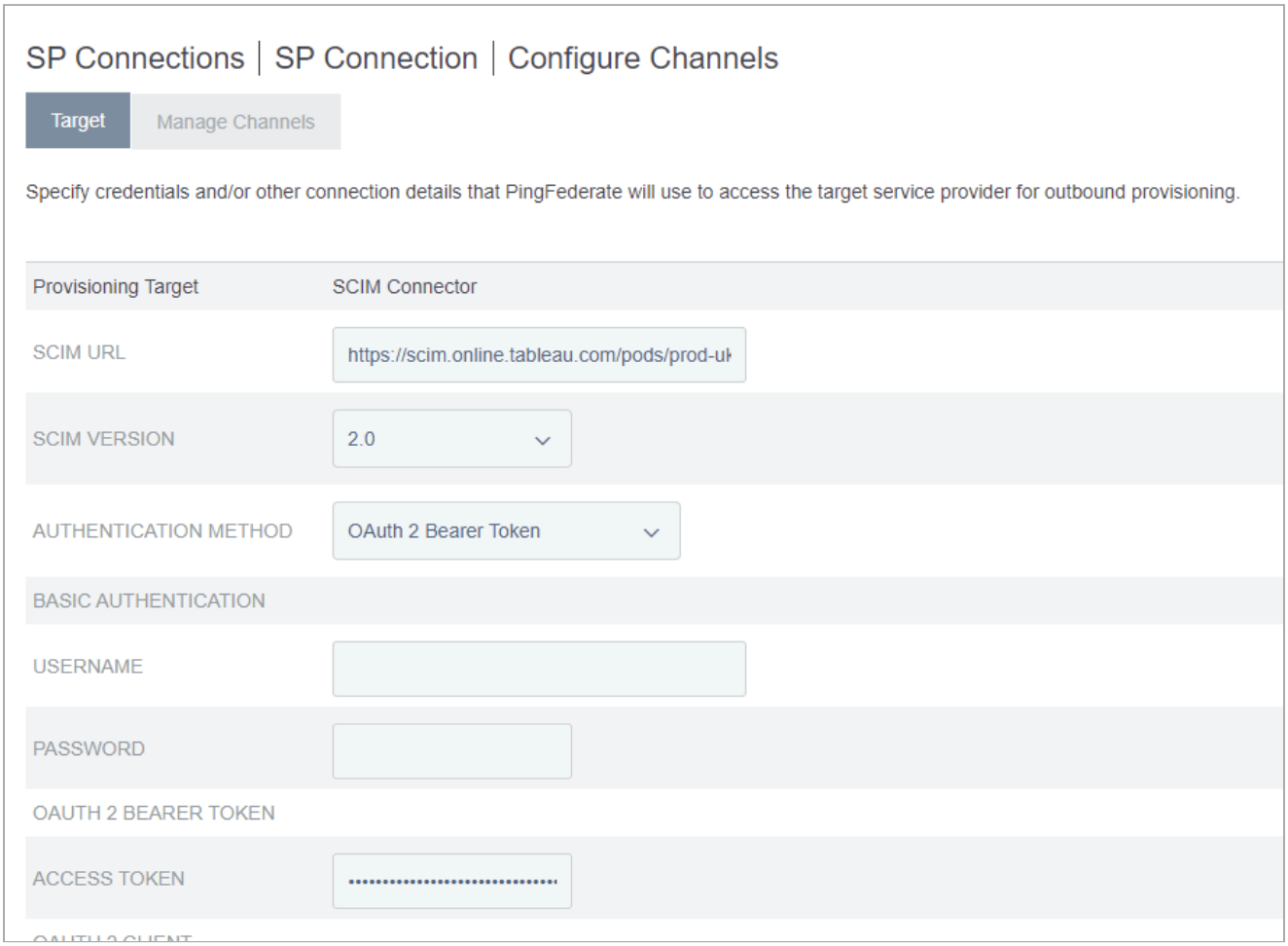


Enable SCIM provisioning in the SP connection

1. In the PingFederate administrative console, select the Tableau SP connector.
2. On the **Connection Type** tab, select the **Outbound Provisioning** check box and in the **Type** list, select **SCIM Connector**.

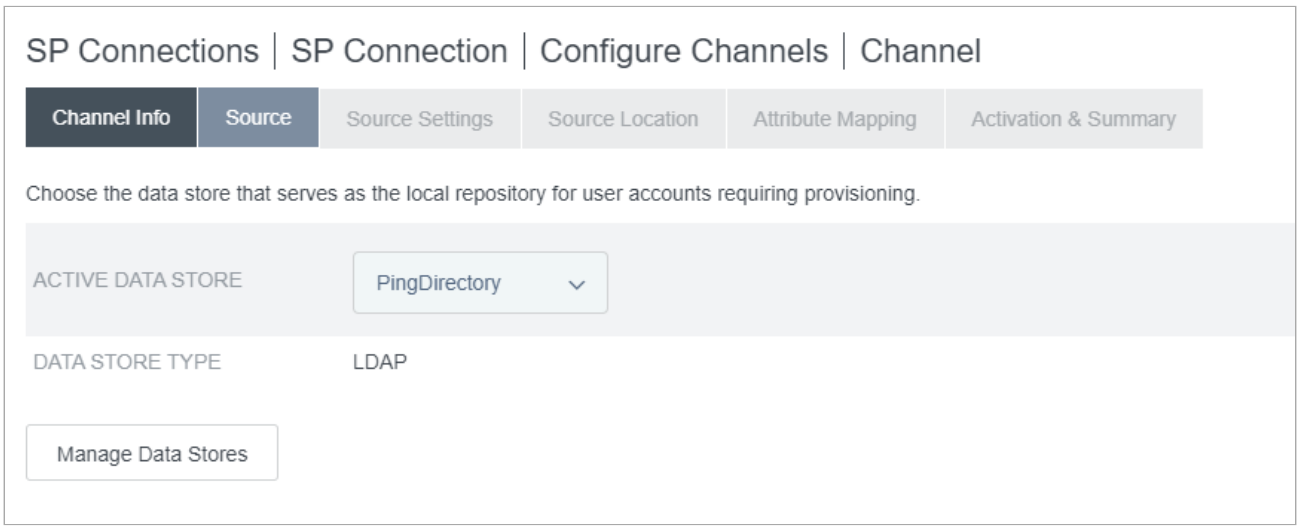


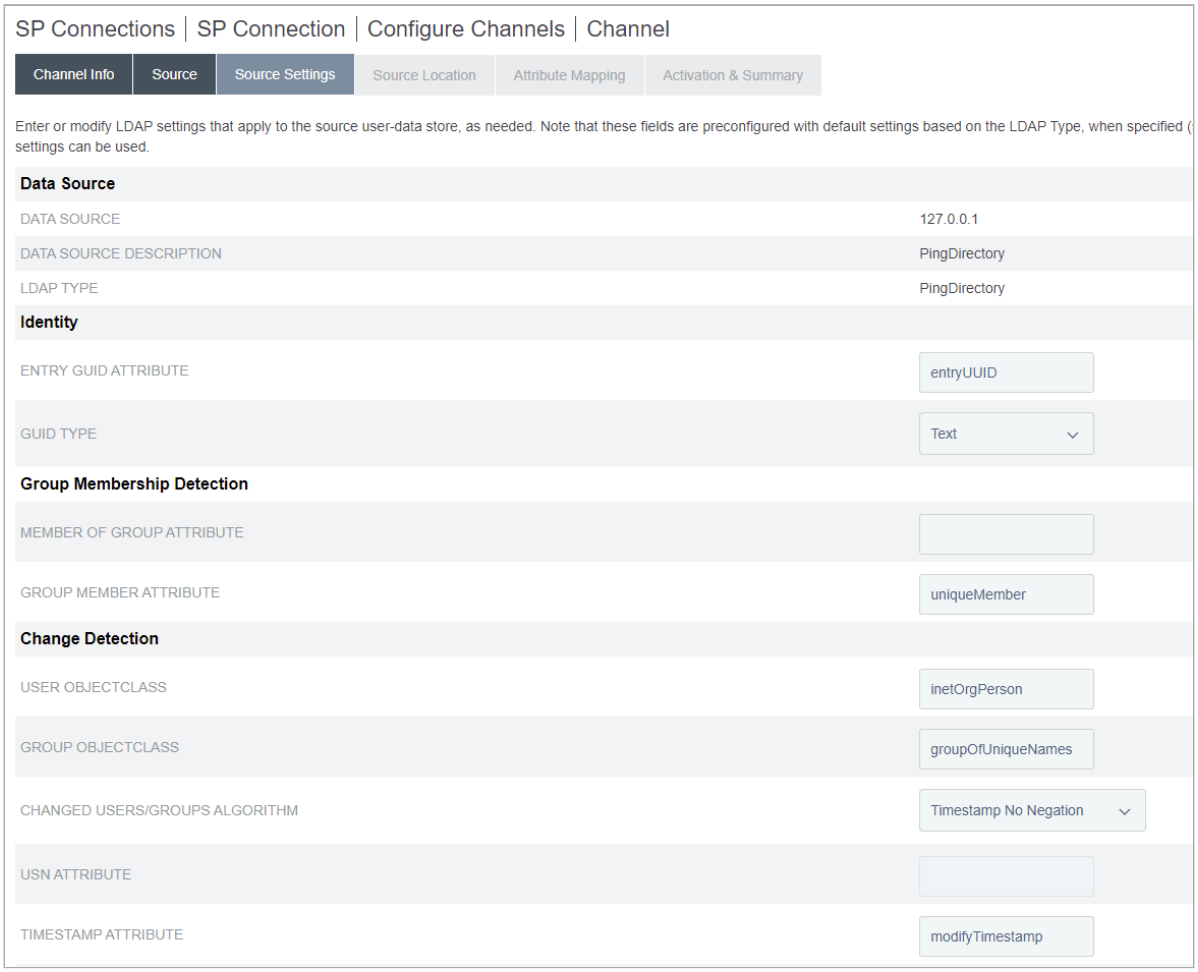
3. On the **Outbound Provisioning** tab, select **Configure Provisioning**.
4. On the **Target** tab, in the **SCIM Version** list, select 2.0 and enter the **SCIM URL** and **OAuth 2 Bearer Token** obtained from Tableau.

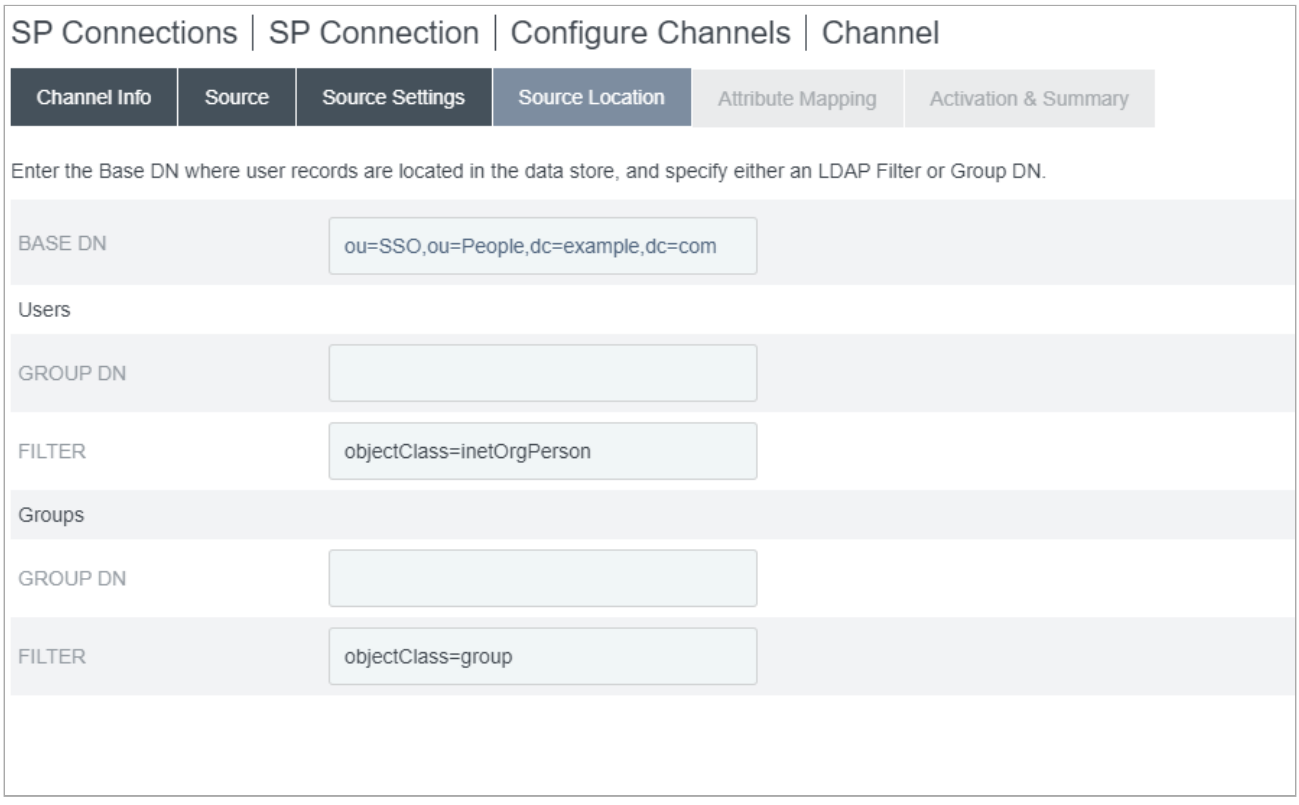


5. Define a channel to obtain the user details:

    1. Add the LDAP source and source location according to your user data source.







2. Configure attribute mappings.

> **Note**
>
> The SCIM **userName** field must map to an email address.
> + image::ixz1640220648501.png[alt="Screen capture of PingFederate SP Connection channel attribute mapping page.",role="border-no-padding"]

3. Enable the channel.

Terraform

Configuring SAML SSO with Terraform and PingOne

Learn how to enable Terraform sign-on from the PingOne SSO console (IdP-initiated sign-on) and direct Terraform login using PingOne SSO (SP-initiated sign-on).

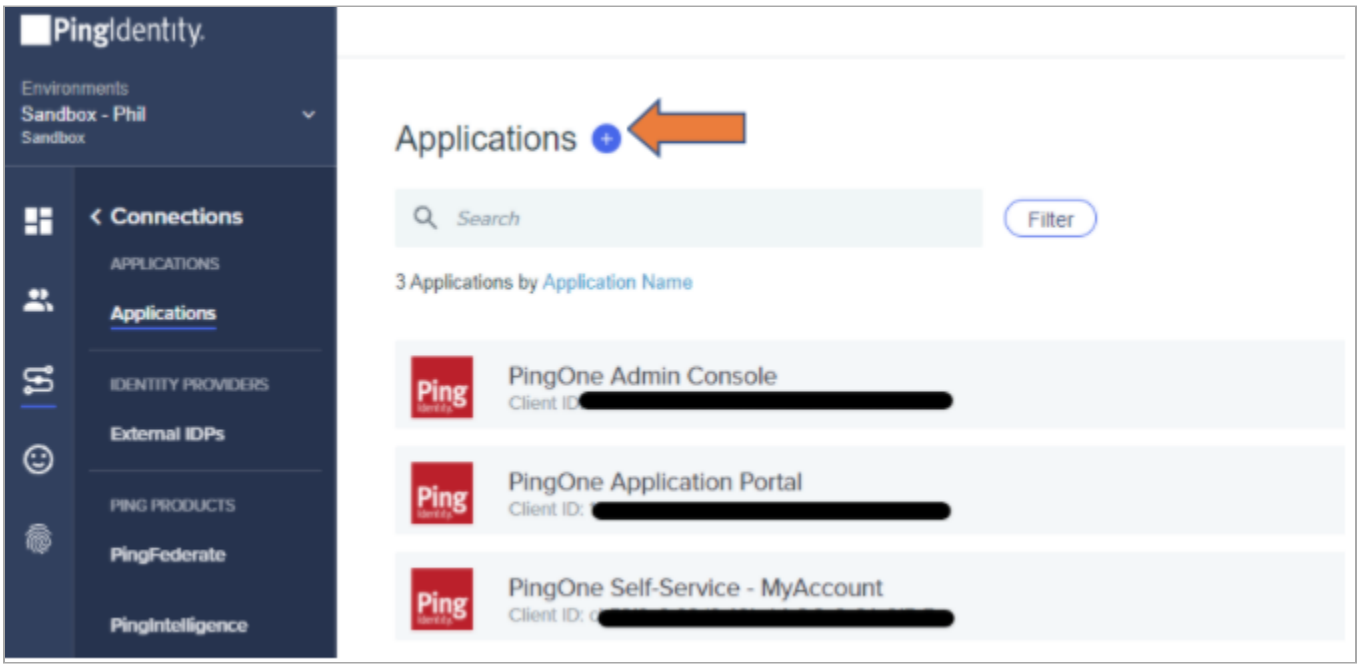
Before you begin

- Link PingOne to an identity repository containing the users requiring application access.
- Populate Terraform with at least one user to test access.
- You must have administrative access to PingOne and an administrative account with site-admin permission on Terraform.

> **Note**
>
> Whenever *TFE-HOSTNAME* is specified throughout this document, replace it with the actual value of your Terraform instance hostname.

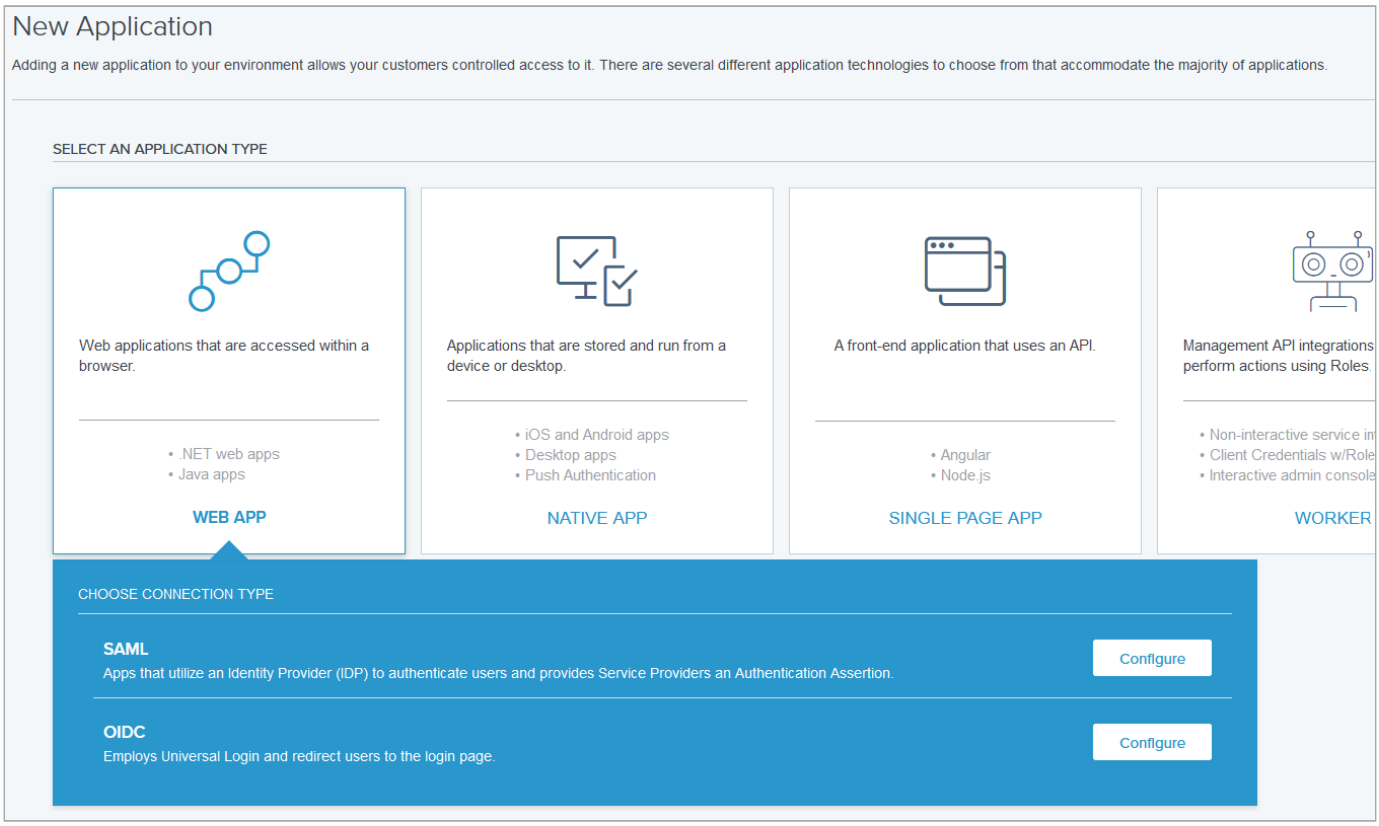
Add the Terraform application to PingOne

1. In PingOne, go to **Connections → Applications** and click + to add a new application.



2. In **Select an Application Type**, click **Web App**.

3. In **Choose Connection Type**, click **Configure** next to **SAML.**

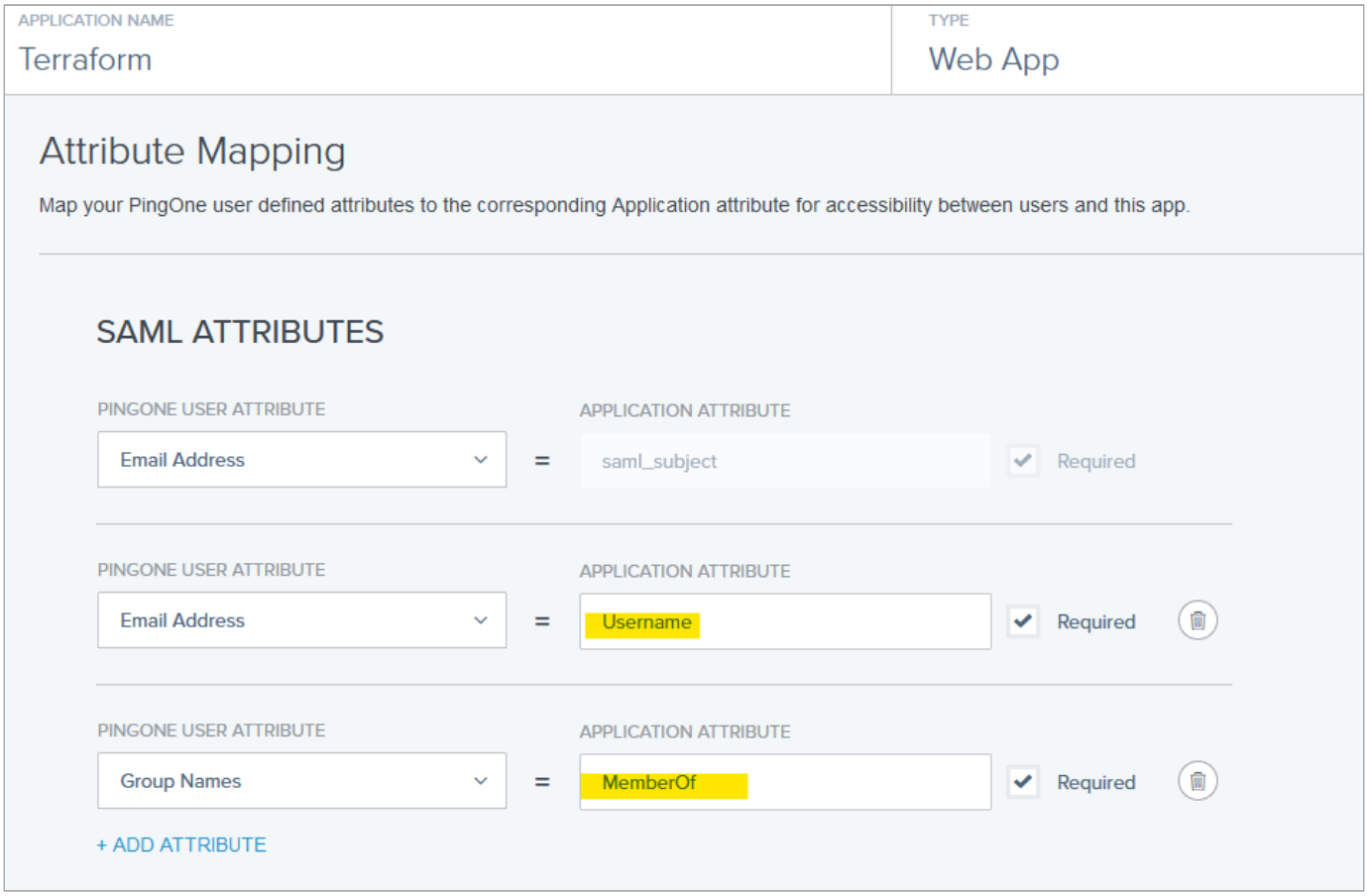


4. Enter Terraform as the application name.
5. **Optional:** Enter a suitable description.
6. **Optional:** Upload an icon.
7. Click **Next**.
8. For **Provide App Metadata**, select **Manually Enter**.
9. For **ACS URLs**, enter `https://TFE-HOSTNAME/users/saml/auth`
10. Choose the **Signing Key** to use and then click **Download Signing Certificate** to download it as X509 PEM (`.crt`).
11. For **Entity ID,** enter `https://TFE-HOSTNAME/users/saml/metadata`
12. Leave **SLO Endpoint** and **SLO Response Endpoint** blank. Terraform does not support single logout (SLO).
13. In the **Subject NameID Format** list, select **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.
14. Set a suitable value for **Assertion Validity Duration (in seconds)**. A value of 300 seconds is typical.
15. Click **Save and Continue**.

> **Note**
>
> By default, Terraform generates a **Username** when an account is first created upon initial SSO. This is based on the user email address.

16. **Optional:** If you want to dictate the **Username** created for a user, you can include the **Username** attribute in the security assertion.

    You can include the **MemberOF** attribute to automatically add users to specific **Teams** in the Terraform platform. Configure which **PingOne User Attribute** to map to each of these Terraform attributes.



17. Click **Save and Close**.

18. Enable user access to this new application by moving the toggle to the right.

19. On the **Configuration** tab of the newly created Terraform application, copy and save the **Issuer ID** and **Initiate Single Sign-On URL** values. You will use these for configuring SAML on Terraform.

Add PingOne as an identity provider (IdP) to Terraform

1. Go to `https://TFE-HOSTNAME/app/admin/saml` and sign on with an administrator account that has site-admin permissions.
2. Paste the **Initiate Single Sign-On URL** value that you saved previously into the **Single Sign-On URL** field.
3. Open the `.crt` file that downloaded previously in a text editor and copy and paste the entire contents into the **IDP Certificate** field.
4. Click **Save SAML settings**.

Test the PingOne IdP integration

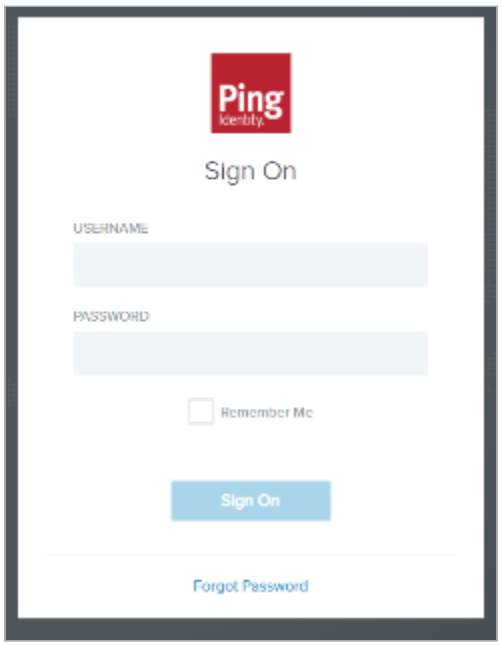
1. Go to the PingOne application portal and sign on with a user account.

   > **Note**
   >
   > You can find the PingOne Application Portal URL in **Dashboard → Environment Properties**.

2. Click the Terraform icon.

   You're redirected and presented with a PingOne sign on prompt.

3. Enter your PingOne username and password.



   After successful authentication, you're redirected back to Terraform as a signed-on user.

UltiPro

Configuring SAML SSO with UltiPro and PingFederate

Learn how to enable UltiPro sign-on from the PingFederate console (IdP-initiated sign-on) and direct UltiPro sign-on using PingFederate (SP-initiated sign-on).

Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate UltiPro with at least one user to test access.
- You must have administrative access to PingFederate.

Create a PingFederate SP connection for UltiPro

1. Sign on to the PingFederate administrative console.
2. Create an SP connection for UltiPro in Ping Federate:
    1. Configure using **Browser SSO** profile **SAML 2.0**.
    2. Set **Partner's Entity ID** to `placeholder`.

       You'll change this later.
    3. Enable the following **SAML Profiles**:
        - **IdP-Initiated SSO**
        - **SP Initiated SSO**
    4. In **Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment,** map the **SAML_SUBJECT**.
    5. In **Protocol Settings: Assertion Consumer Service URL**, set **Binding** to **POST**, and set **Endpoint URL** to `https://placeholder`.

       You'll change the **Endpoint URL** later.
    6. In **Protocol Settings: Allowable SAML Bindings**, enable **POST.**
    7. In **Credentials: Digital Signature Settings**, select the PingFederate signing certificate.
3. Export the metadata for the newly created UltiPro SP connection.
4. Export the signing certificate.

Add the PingFederate connection to UltiPro

1. Contact UltiPro Customer Support and request that SAML 2 be enabled for your organization.
2. Provide them with the downloaded PingFederate signing certificate and metadata.
3. Request their ACS URL and EntityID values.

Update the ACS URL values in PingFederate

1. Sign on to the PingFederate administrative console.
2. Edit the SP connection for UltiPro.
3. Set **Partner's Entity ID** to the UltiPro **Entity ID** value.
4. In **Protocol Settings: Assertion Consumer Service URL**, set **Endpoint URL** to the UltiPro **Assertion Consumer Service URL** value.
5. Save the changes.

Test the PingFederate IdP-initiated SSO integration

1. Go to the PingFederate SSO application endpoint for the UltiPro SP connection.
2. Complete the PingFederate authentication.

   You're redirected to your UltiPro domain.

Test the PingFederate SP-initiated SSO integration

1. Go to your UltiPro application.
2. After you're redirected to PingFederate, enter your PingFederate username and password.

   You're redirected back to UltiPro.

Configuring SAML SSO with UltiPro and PingOne for Enterprise

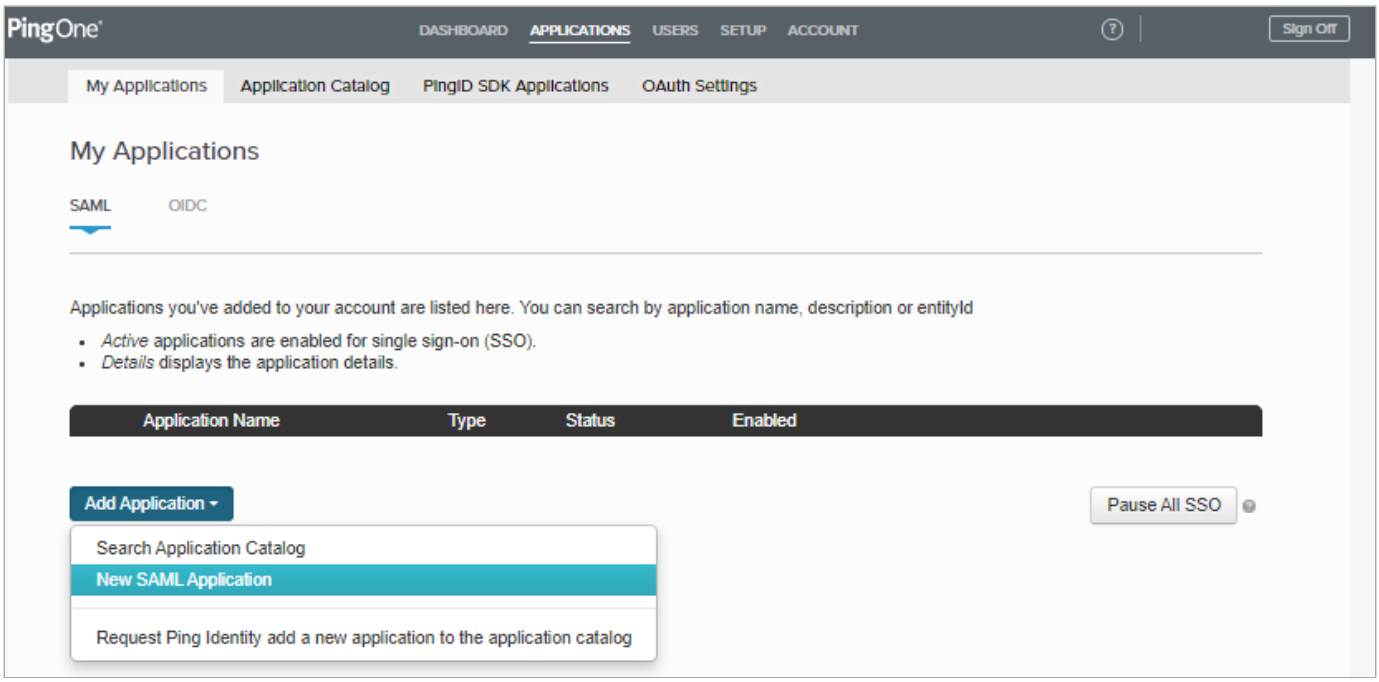
Learn how to enable UltiPro sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct UltiPro sign-on using PingOne for Enterprise (SP-initiated sign-on).

Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate UltiPro with at least one user to test access.
- You must have administrative access to PingOne for Enterprise.

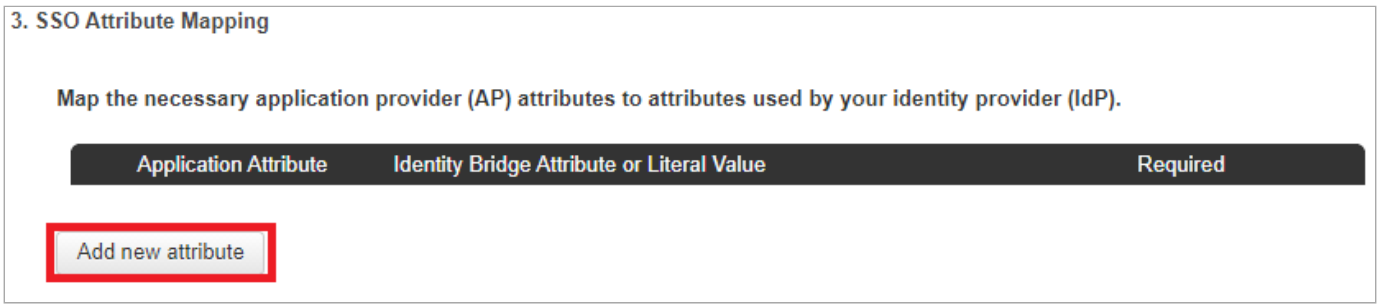
Add the UltiPro application to PingOne for Enterprise

1. Sign on to PingOne for Enterprise and go to **Applications → My Applications**.
2. On the **SAML** tab, click **Add Application**.

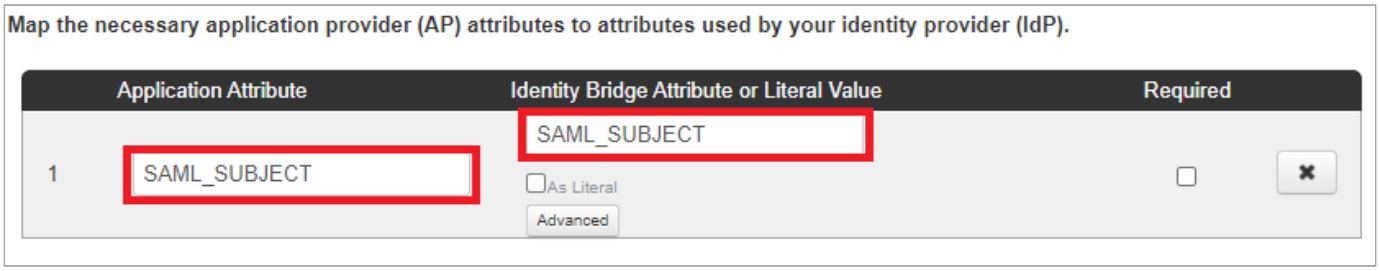


3. Enter `UltiPro` as the application name.
4. Enter a suitable description.
5. For the category, select **Human Resources**.
6. Click **Continue to Next Step**.
7. Set **Assertion Consumer Service (ACS)** to `https://placeholder` and set **Entity ID** to `placeholder`.

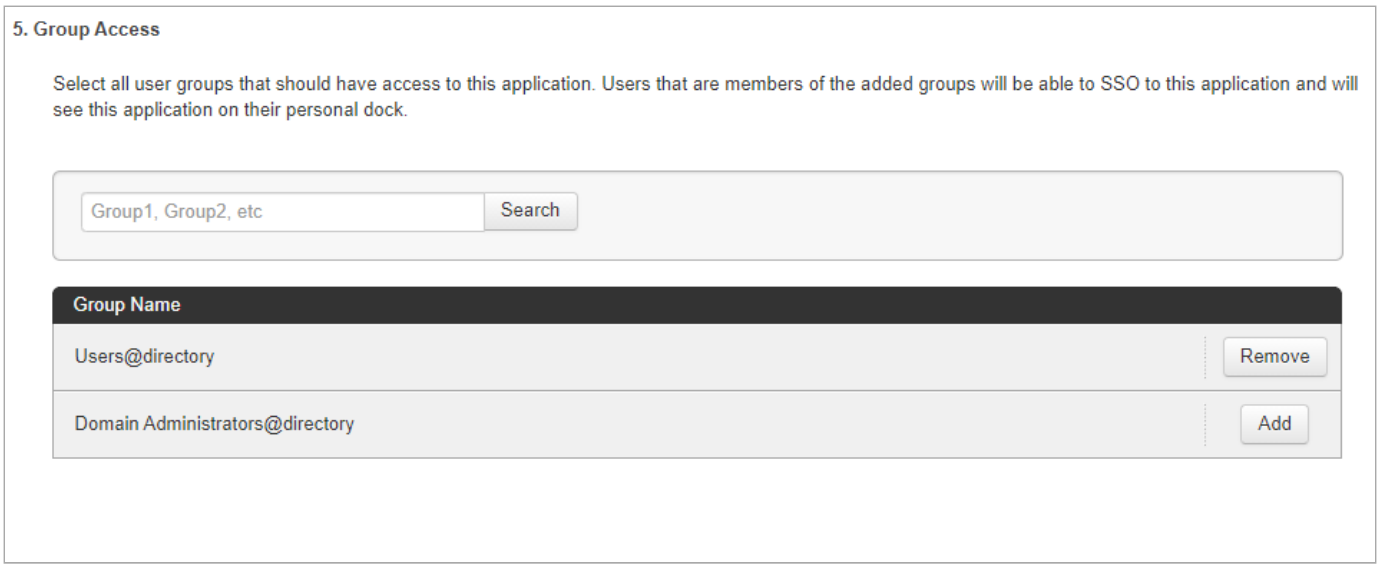
   You'll update these values later.
8. Click **Continue to Next Step**.
9. Click **Add new attribute**.



10. Add the **SAML_SUBJECT** attribute and map it to the value required by UltiPro.



11. Click **Continue to Next Step**.
12. Click **Add** for all user groups that should have access to UltiPro.



13. Click **Continue to Next Step**.
14. Download the PingOne for Enterprise signing certificate and metadata.

15. Click **Finish**.

Add the PingOne for Enterprise connection to UltiPro

1. Contact UltiPro Customer Support and request that SAML 2 be enabled for your organization.
2. Provide them with the downloaded PingOne for Enterprise signing certificate and metadata.
3. Request their ACS URL and EntityID values.

Complete the UltiPro PingOne for Enterprise setup in UltiPro

1. Continue editing the UltiPro entry in PingOne for Enterprise for Enterprise.

> **Note**
>
> If the session has timed out, complete the initial steps to the point of clicking **Setup**.

2. Click **Continue to Next Step**.
3. Set the **ACS URL** to the UltiPro **ACS URL** value.
4. Set the **Entity ID** to the UltiPro **Entity ID** value.
5. Click **Continue to Next Step** until you reach the final page, then click **Finish**.

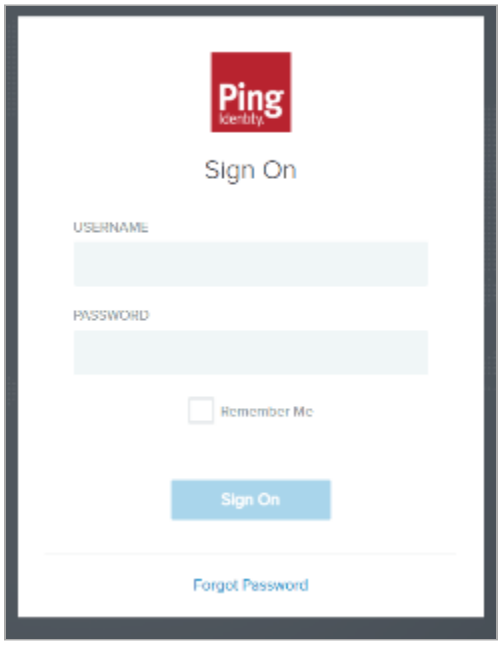
Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with UltiPro access.

> **Note**
>
> To find the Ping desktop URL in the Admin console, go to **Setup → Dock → PingOne Dock URL**.

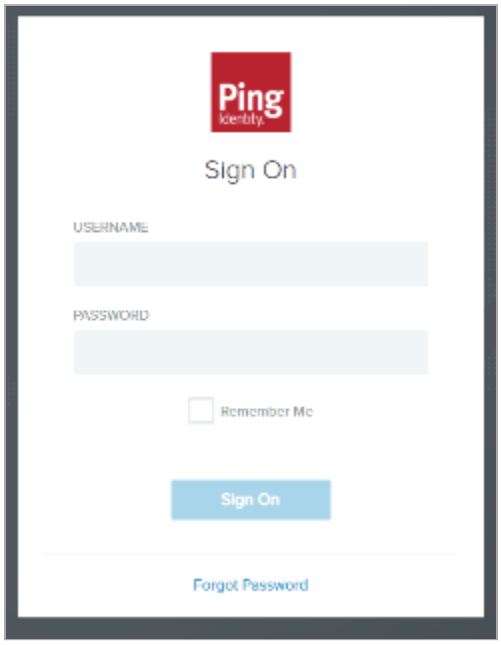
2. Complete the PingOne for Enterprise authentication.

   You're redirected to your UltiPro application.



Test the PingOne for Enterprise SP-initiated SSO integration

1. Go to your UltiPro application.
2. After you're redirected to PingOne for Enterprise, enter your PingOne for Enterprise username and password.



You’re redirected back to UltiPro.

Workato

Configuring SAML SSO with Workato and PingFederate

Learn how to enable Workato sign-on from the PingFederate console (IdP-initiated sign-on) and direct Workato sign-on using PingFederate (SP-initiated sign-on).

Before you begin

- Configure PingFederate to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- Populate Workato with at least one user to test access.
- You must have administrative access to PingFederate.

Create the Workato metadata

1. In PingFederate, create a service provider (SP) connection for Workato:
    1. Configure using **Browser SSO** profile **SAML 2.0**.
    2. Set Partner's Entity ID to `https://www.workato.com/saml/metadata?id=Workato ID`.

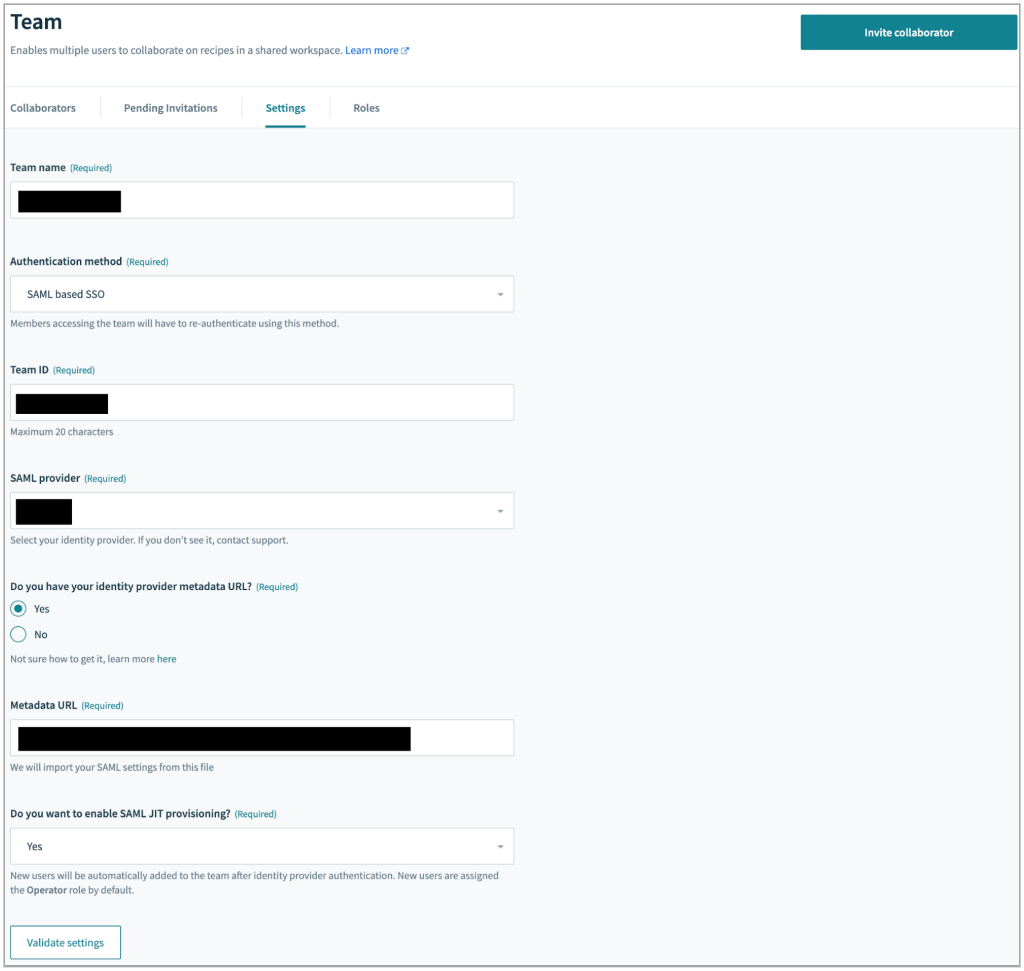
        > **Note**
        > This value is provided by Workato on the **Tools → Team → Settings** tab.

    3. Enable the following SAML profiles.
        - **IdP-Initiated SSO**
        - **SP-Initiated SSO**
    4. In **Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfilment,** map the **SAML_SUBJECT** to your email attribute.
    5. In **Protocol Settings: Assertion Consumer Service URL**, set **Binding** to **POST** and set **Endpoint URL** to `https://www.workato.com/saml/consume/`.
    6. In **Protocol Settings: Allowable SAML Bindings**, enable **POST**.
    7. In **Credentials: Digital Signature Settings**, select the **PingFederate Signing Certificate**.

        > **Note**
        > Note the metadata URL for the newly-created Workato SP connection.

Add the PingFederate connection to Workato

1. Sign on to the Workato console as an administrator.
2. Select **Tools** in the left navigation pane.
3. Click the **Members** tab.
4. Select **Team**.
5. Select the **Settings** tab.



6. Enter a **Team name** for the team or company.
7. In the **Authentication method** list, select **SAML based SSO**.
8. In the **SAML_provider** list, select **Other**.
9. Enter the **Metadata URL** value for the Workato SP connector in PingFederate.

Test the PingFederate IdP-initiated SSO integration

1. Go to the PingFederate SSO Application Endpoint for the Workato SP connection.

2. Authenticate with PingFederate.

   You're redirected to your Workato domain.

Test the PingFederate SP-initiated SSO integration

1. Go to https://app.workato.com/users/sign_in.
2. After you're redirected to PingFederate, enter your PingFederate username and password.

   You're redirected back to Workato.

Configuring SAML SSO with Workato and PingOne

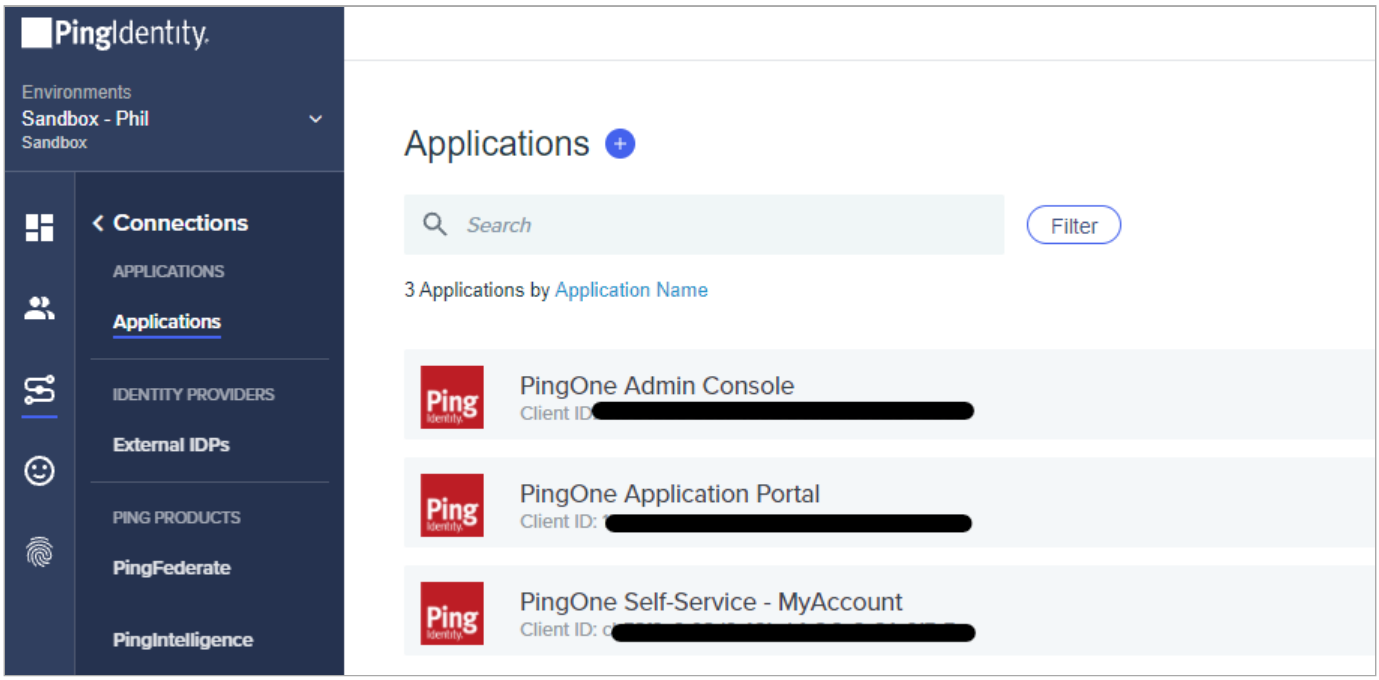
Learn how to enable Workato sign-on from the PingOne console (IdP-initiated sign-on) and direct Workato sign-on using PingOne (SP-initiated sign-on).

Before you begin

- Link PingOne to an identity repository containing the users requiring application access.
- Populate Workato with at least one user to test access.
- You must have administrative access to PingOne and an Admin account on Workato.

Add the Workato application to PingOne

1. In PingOne, go to **Connections → Applications** and click the + icon.



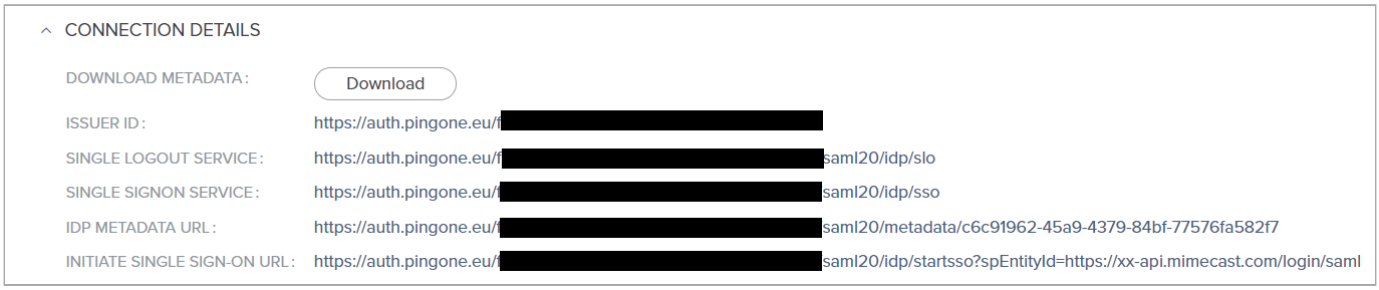
2. When you're prompted to select an application type, select **WEB APP** and then click **Configure** next to **SAML** for the chosen connection type.

3. Enter **Workato** as the application name.
4. Enter a suitable description.
5. **Optional:** Upload an icon.
6. For **Provide App Metadata**, select **Enter from URL**.
7. In the **Import URL** field, enter `https://www.workato.com/saml/metadata?id=your-Workato-ID`.

> **Note**
>
> *your-Workato-ID* is a unique value to your Workato account and can be found in the Workato Portal.

8. In the **ACS URLS** field, enter `https://www.workato.com/saml/consume`.
9. Select the **Signing Key** to use and then click **Download Signing Certificate** to download as X509 PEM (.crt).
10. Leave **SLO Endpoint** and **SLO Response Endpoint** blank.
11. In the **Subject NameID Format** list, select **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.
12. Enter a suitable value for **Assertion Validity Duration (in seconds)**. A value of 300 seconds is typical.
13. Click **Save and Continue**.
14. Workato expects an email address to identify a user in the SSO security assertion:
    - If you use an email address to sign on through PingOne, click **Save and Close**.
    - If you sign on with a username, in the **PingOne User Attribute** list, select **Email Address** to map that to the **SAML_SUBJECT**, then click **Save and Close**.
15. Click the toggle to enable the application.
16. On the **Configuration** tab of the newly-created Workato application, copy and save the **IDP Metadata URL** value.

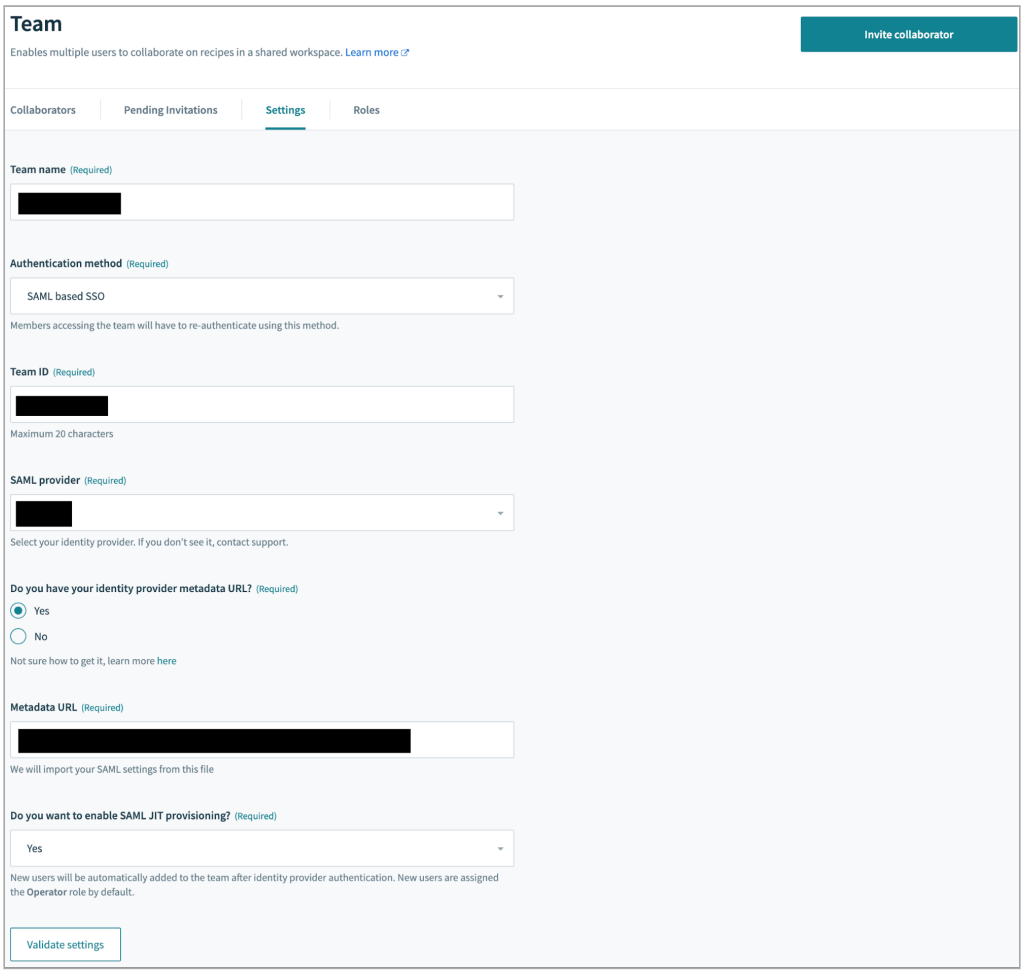
    You'll need this when configuring SAML on Workato.



Add PingOne as an identity provider (IdP) to Workato

1. Sign on to the Workato console as an administrator.
2. In the left navigation pane, click **Tools**.
3. Click the **Members** tab.

4. Select **Team**.
5. Click the **Settings** tab.



6. Enter a **Team name** for the team or company.
7. In the **Authentication method** list, select **SAML based SSO**.
8. In the **SAML_provider** list, select **Other**.
9. Enter the **Metadata URL** for the Workato SP Connector in PingOne.

Test the PingOne IdP integration

1. Go to the PingOne Application Portal and sign on with a user account.

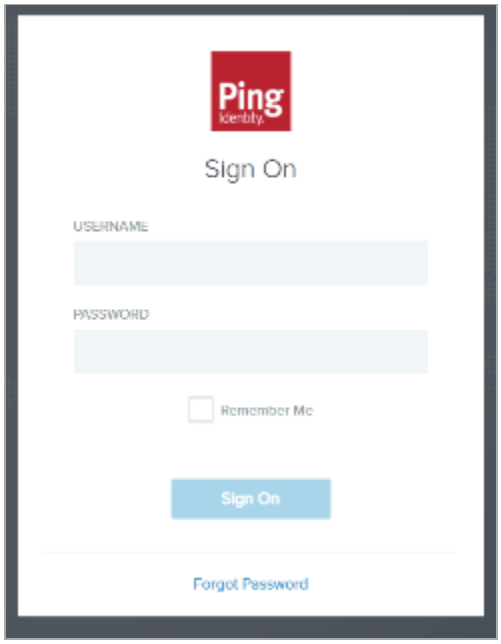
> **Note**
>
> In the Admin console, go to **Dashboard → Environment Properties** to find the **PingOne Application Portal URL**.

2. Click the Workato icon.

   You're redirected to Workato and signed on with SSO.

Test the PingOne SP integration

1. Go to https://app.workato.com/users/sign_in and enter your email address only.
2. In the PingOne sign-on prompt, enter your PingOne username and password.



You're redirected back to Workato and signed on.

Workday

Configuring SAML SSO with Workday and PingFederate

Enable Workday sign-on from a PingFederate URL (IdP-initiated sign-on) and direct Workday sign-on using PingFederate (SP-initiated sign-on), with single logout (SLO).

Before you begin

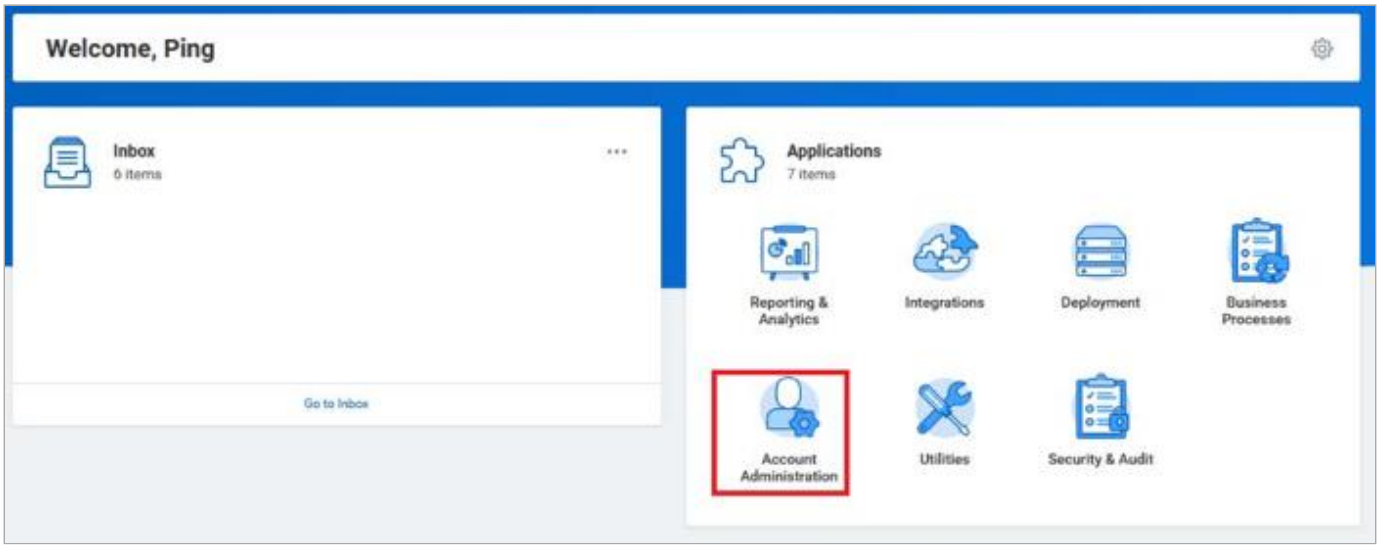
- Configure PingFederate to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- Populate Workday with at least one user to test access.
- You must have administrative access to PingFederate and Workday.

Create a PingFederate service provider (SP) connection for Workday

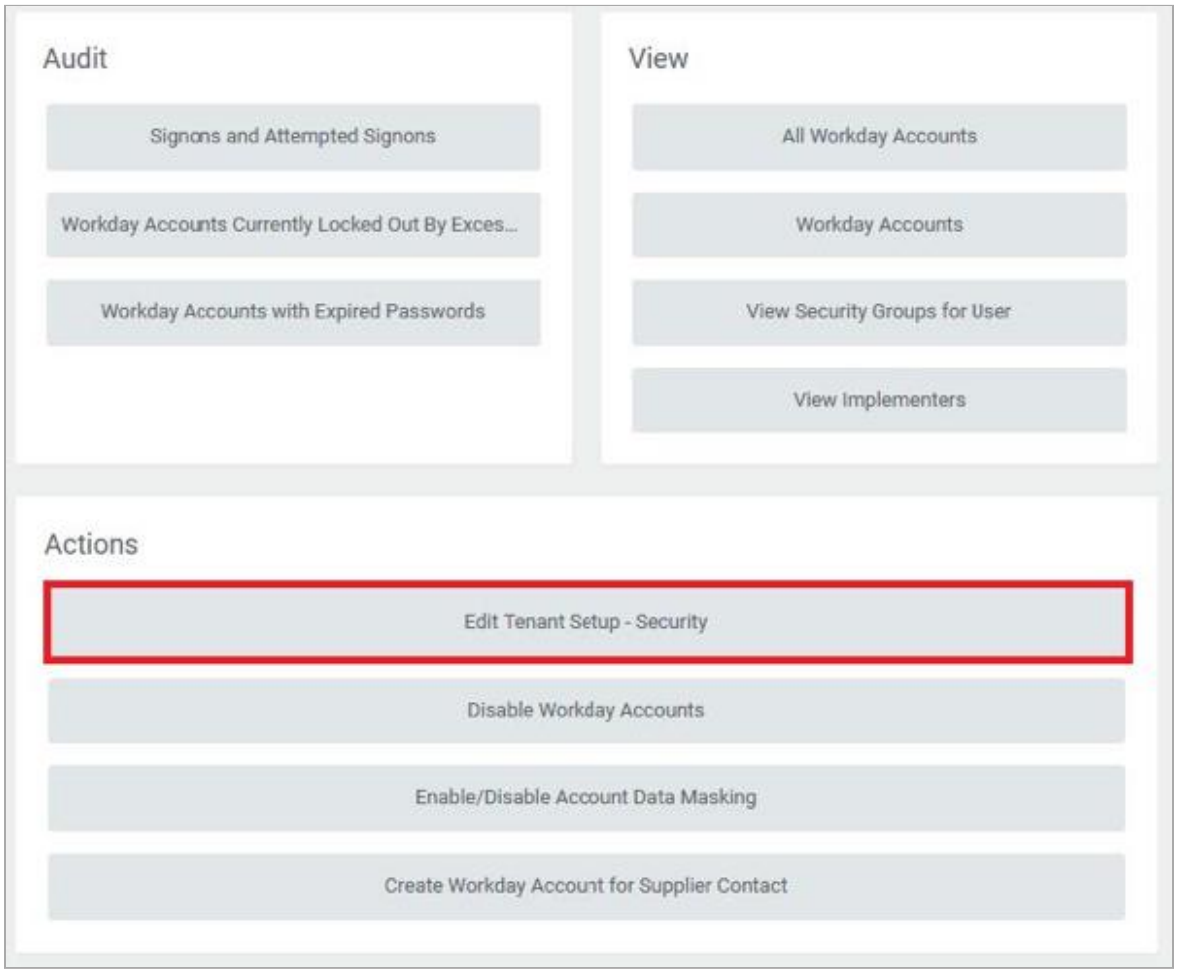
1. Sign on to the PingFederate administrative console.
2. Create an SP connection for Workday in PingFederate.
3. Set **Partner's Entity ID** to `http://www.workday.com`.
4. Enable the **IdP-Initiated SSO** and **SP Initiated SSO** SAML profiles.
5. In **Assertion Creation → Authentication Source Mapping → Attribute Contract Fulfillment**, map **SAML_SUBJECT**.
6. In **Protocol Settings → Assertion Consumer Service URL**:
    1. Set **Binding** to **POST**.
    2. In the **Endpoint URL** field, enter `https://your-environment.workday.com/your-tenant-name/login-saml.flex`
    3. In **Protocol Settings → Allowable SAML Bindings**, enable **POST**.
    4. In **Credentials → Digital Signature Settings**, select the **PingFederate Signing Certificate**.
7. Click **Save**.
8. Export the signing certificate.
9. Export the metadata file, open it in a text editor, and copy:
    - The entityID
    - The SSO Location entry `https://your value/idp/SSO.saml2`
    - The SLO Location entry `https://your value/idp/SLO.saml2`

Add the PingFederate IdP Connection to Workday

1. Sign on to Workday as an administrator and click **Account Administration**.



2. Click **Edit Tenant Setup – Security**.



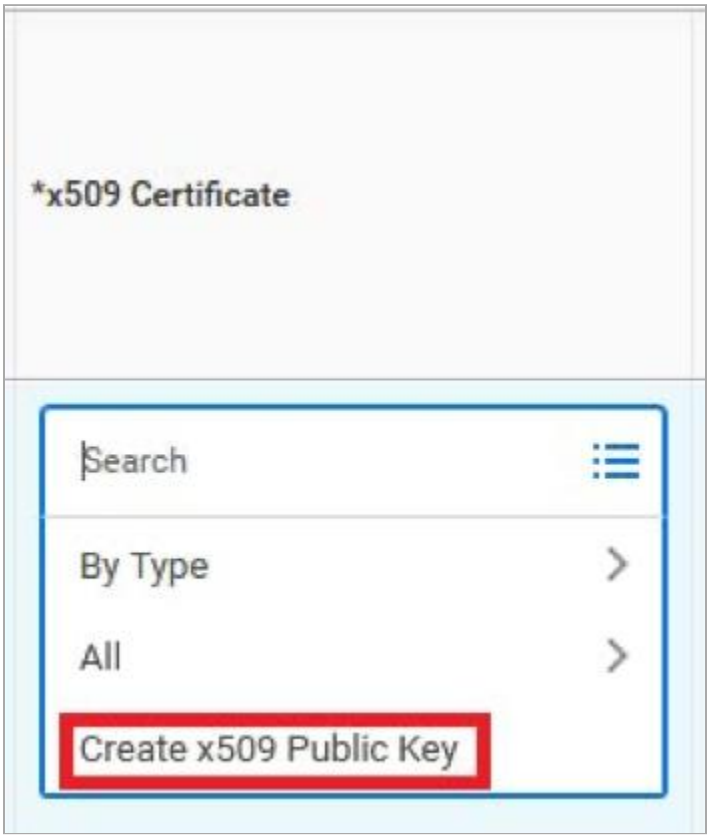
3. In the **Single Sign On** section, click the + icon under **Redirection URLs**.
4. Configure the redirection URLs:

Redirect Type	Single URL
Login Redirect URL	`https://your-environment.workday.com/your-tenant-name/login-saml2.flex`
Logout Redirect URL	Single logout (SLO) location from previous procedure `https://your value/idp/SLO.saml2`
Mobile App Login Redirect URL	`https://your-environment.workday.com/your-tenant-name/login-saml2.flex`
Mobile Browser Login Redirect URL	`https://your-environment.workday.com/your-tenant-name/login-saml2.flex`
Environment	Select environment

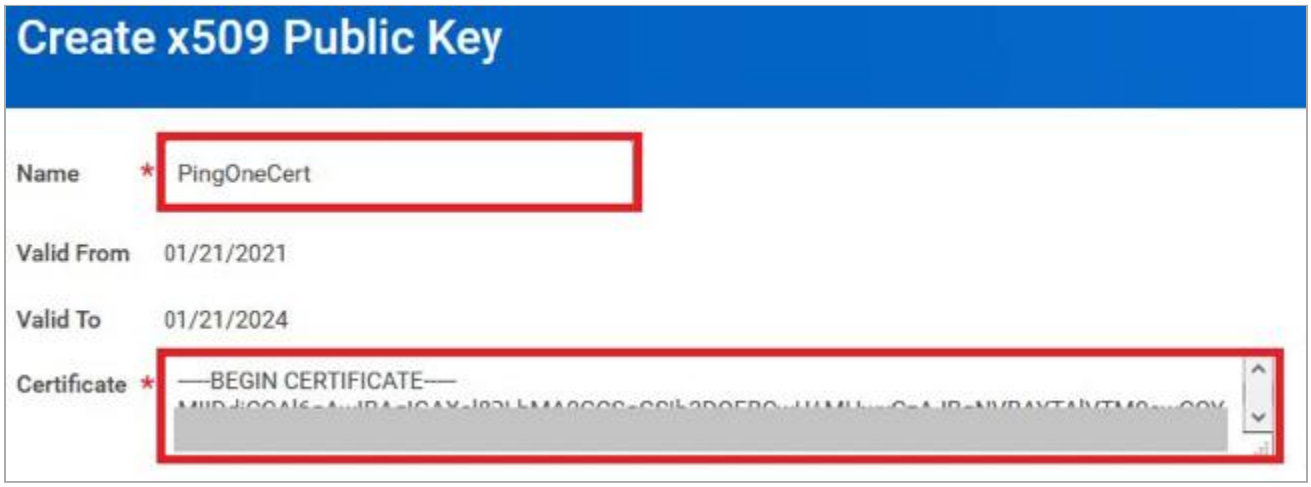
5. In the **SAML Setup** section, select the **Enable SAML Authentication** check box.

6. Click the + icon.

7. Set the **Identity Provider Name** to PingFederate, and in the **Issuer** field, enter the entity ID value that you copied from PingFederate.
8. For SLO, in the **x509 certificate** section, click **Create x509 Public Key**.



9. In the **Name** field, enter a name for your PingFederate signing certificate, such as `PingFederateCert`.
10. Open the PingFederate signing certificate in a text editor, copy the contents, and paste them into the **Certificate** field.



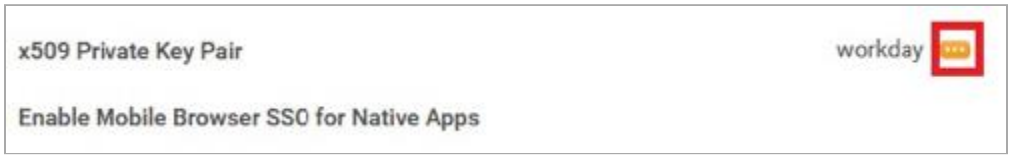
11. Click **OK**.
12. Use the following configuration.

Enable IdP Initiated Logout	Selected
Logout Response URL	Enter the SLO location that you copied from PingFederate. For example, `https://your value/idp/SLO.saml2`.
Enable Workday Initiated Logout	Selected
Logout Request URL	Enter the SLO location that you copied from PingFederate. For example, `https://your value/idp/SLO.saml2.`
Service Provider ID	Enter `http://www.workday.com`.
SP Initiated	Selected
Do Not Deflate SP-initiated Authentication Request	Selected
IdP SSO Service URL	Enter the SLO location you copied from PingFederate. For example, `https://your-value/idp/SLO.saml2`.

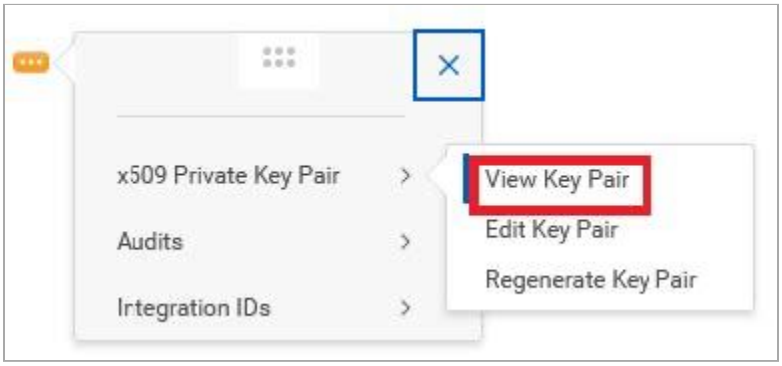
13. Click **OK**.
14. For SLO, in the **x509 Private Key Pair** menu, select **Create x509 Private Key Pair**.

15. In the **Name** field, enter a name for the key pair.

16. Click **OK**.
17. Hover next to the key pair name and click the **...** icon.



18. In **x509 Private Key Pair**, select **View Key Pair**.



19. Copy the contents of the public key and save them in a text editor.

20. Set the **Authentication Request Signature Method** to **SHA-256**.

> **Note**
>
> Leave all the other values in this section blank.

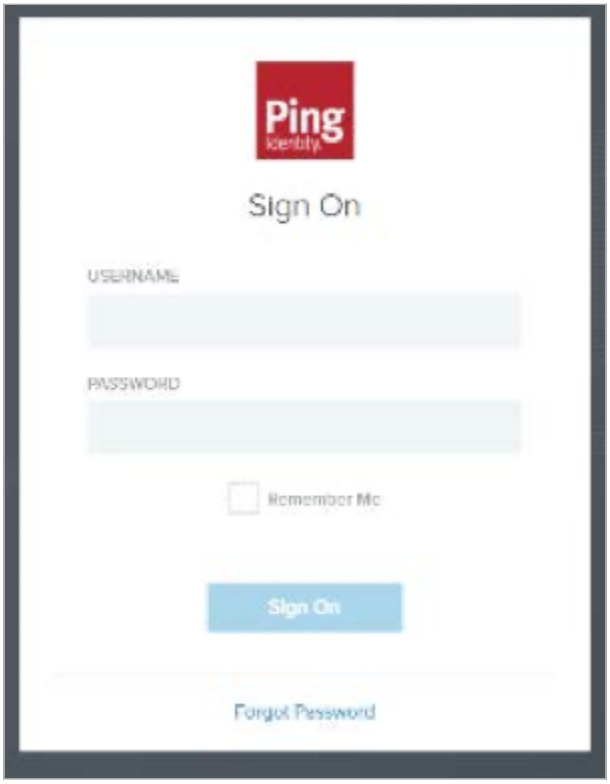
21. Click **Done**.

Update the PingFederate Workday IdP for SLO

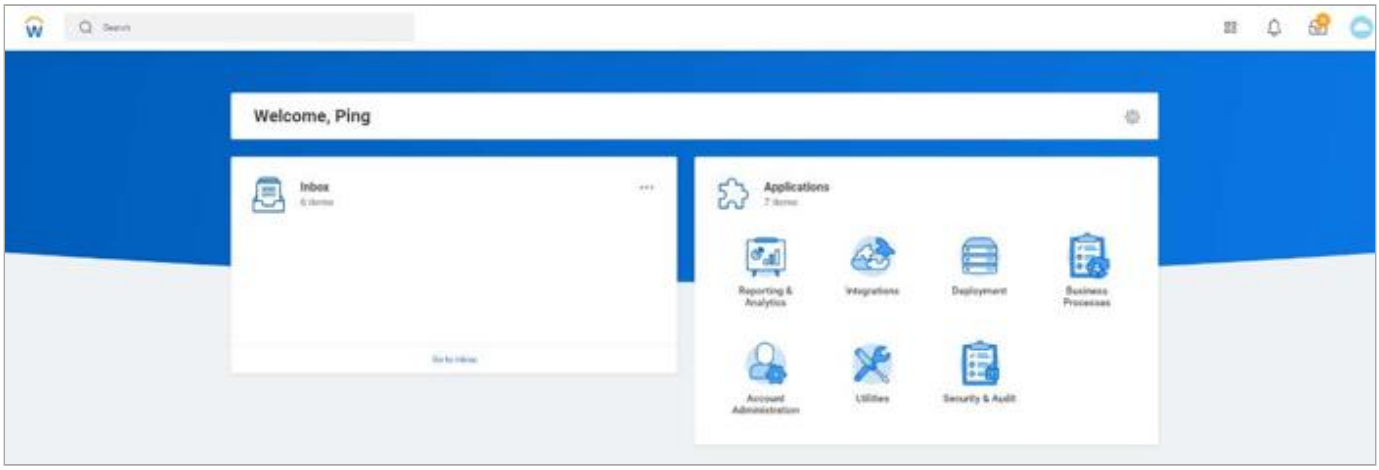
1. Sign on to the PingFederate administrative console.
2. Edit the SP connection for Workday and add the following extra SAML profiles:
    - **IDP-Initiated SLO**
    - **SP Initiated SLO**
3. In **Protocol Settings → SLO Service URL**:
    1. Set **Binding** to **POST**
    2. Set **Endpoint URL** to `https://your-environment.workday.com/your-tenant-name/logout-saml.htmld`.
    3. Set **Response URL** to `https://your-environment.workday.com/your-tenant-name/logout-saml.htmld`.
4. In **Credentials → Signature Verification Settings**, select the saved Workday public key.

Test the PingFederate IdP-initiated SSO

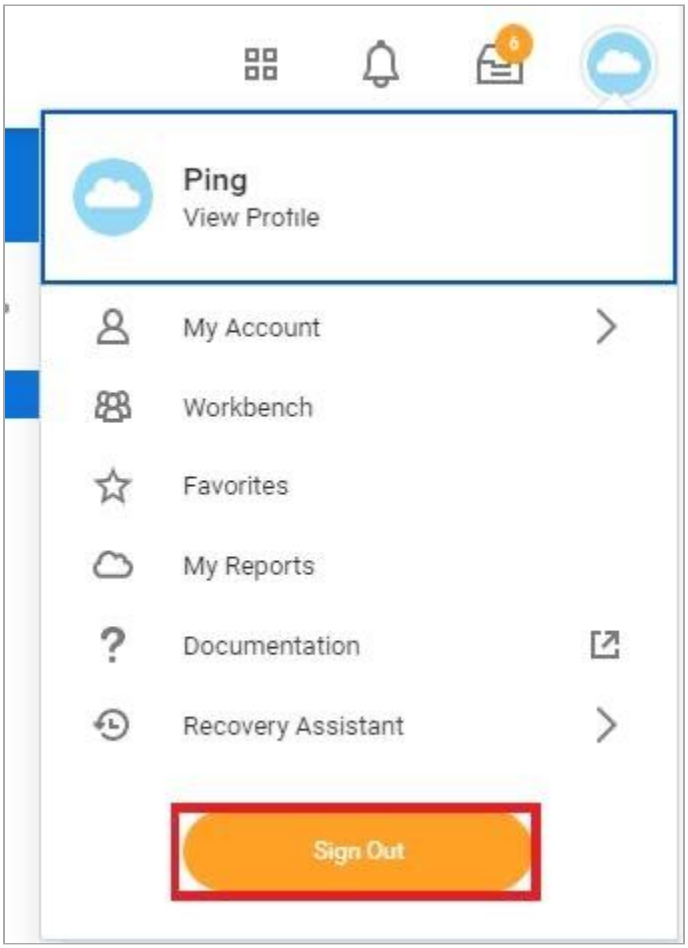
1. Go to the PingFederate SSO Application Endpoint for the Workday SP connection.
2. Complete the PingFederate authentication.



You are redirected to your Workday domain.



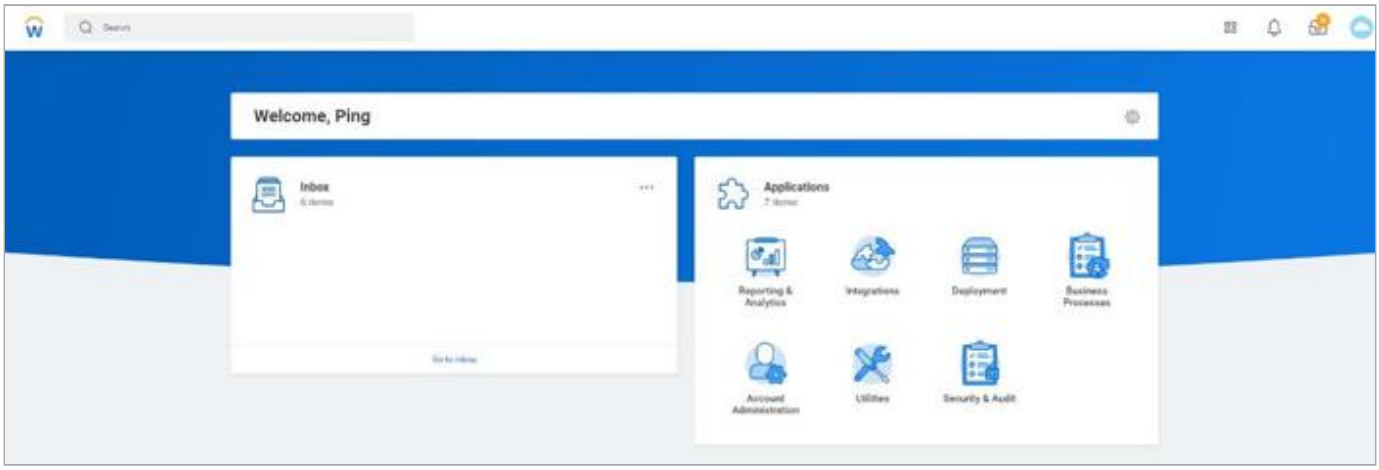
3. Click **Sign Out**.



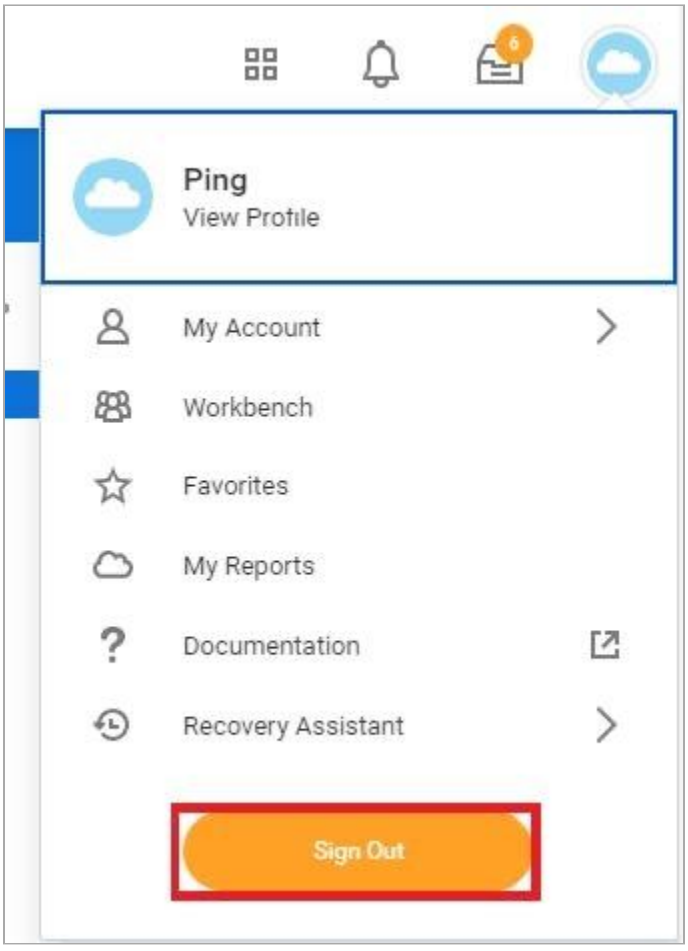
Test the PingFederate SP-initiated SSO integration

1. Go to your Workday URL.
2. After you're redirected to PingFederate, enter your PingFederate username and password.

   After successful authentication, you are redirected back to Workday.



3. Click **Sign Out**.



You are signed out.

Configuring SAML SSO with Workday and PingOne for Enterprise

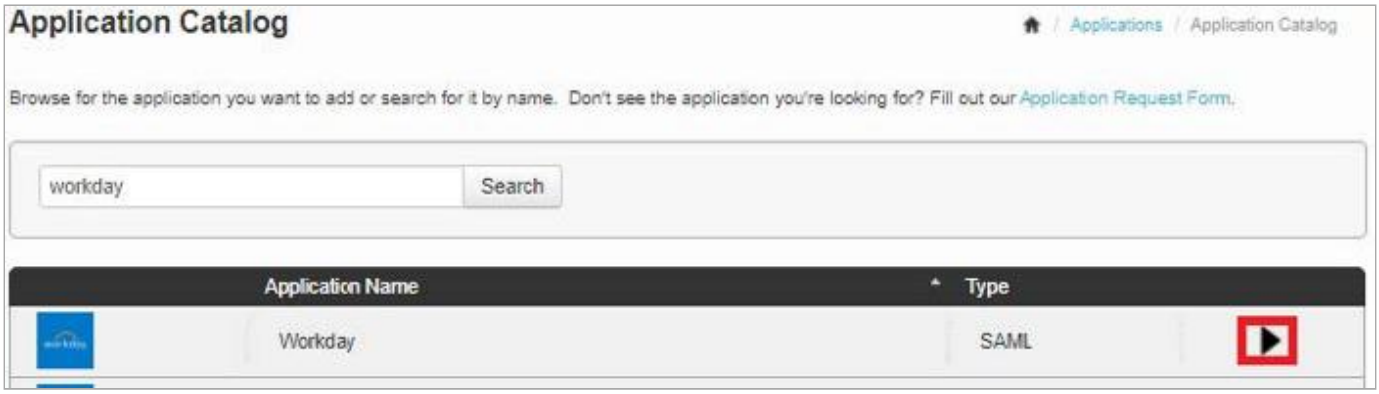
Enable Workday sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct WorkDay sign-on using PingOne for Enterprise (SP-initiated sign-on), with single logout (SLO).

Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate Workday with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and Workday.

Setup the Workday application in PingOne for Enterprise

1. Sign on to PingOne for Enterprise and go to **Applications → Application Catalog**.
2. In the **Application Catalog**, search for `Workday`.

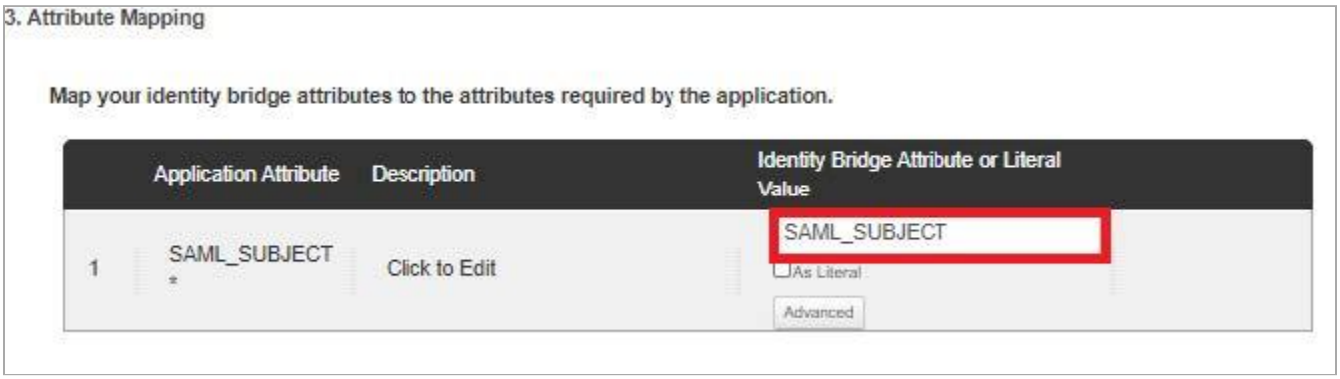


3. Expand the Workday entry and click **Setup**.
4. Copy the **Issuer** and **IdP ID** values.
5. Download the signing certificate.

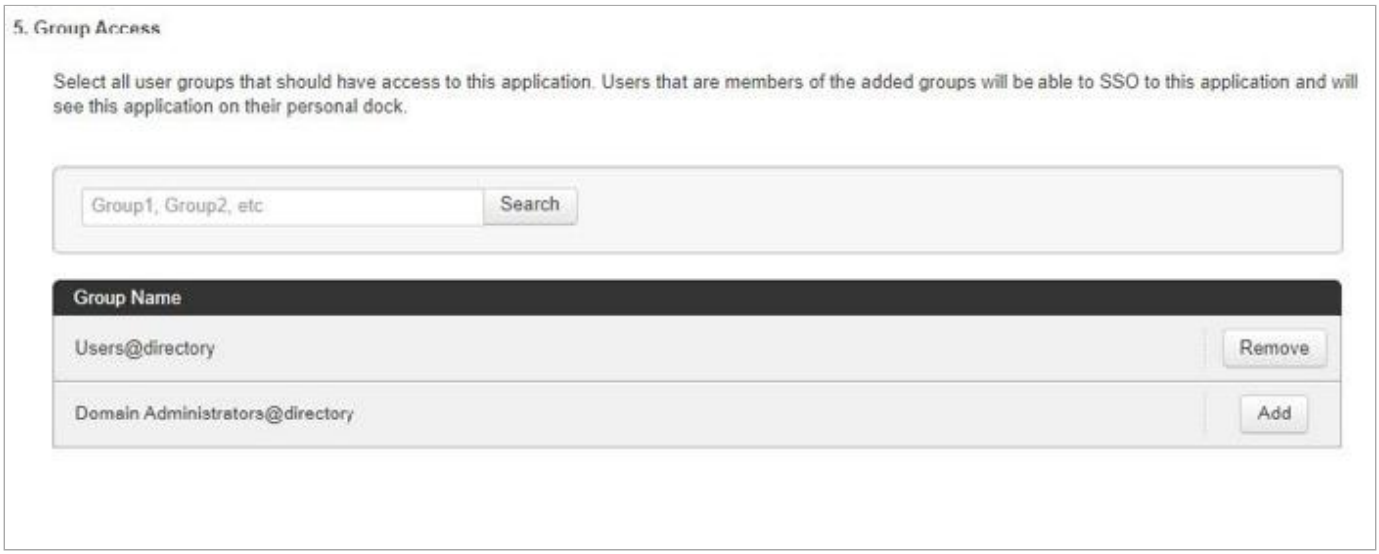
6. Click **Continue to Next Step**.
7. Enter the following values.

Field	Entry
ACS URL	`https://your-environment.workday.com/your-tenant-name/login-saml.flex`
Entity ID	`http://www.workday.com`
Target Resource	`https://your-tenant-name/fx/home.flex`
Single Logout Endpoint	`https://your-environment.workday.com/your-tenant-name/logout-saml.htmld`
Single Logout Response Endpoint	`https://your-environment.workday.com/your-tenant-name/logout-saml.htmld`

8. Click **Continue to Next Step**.
9. Map the **SAML_SUBJECT** attribute.



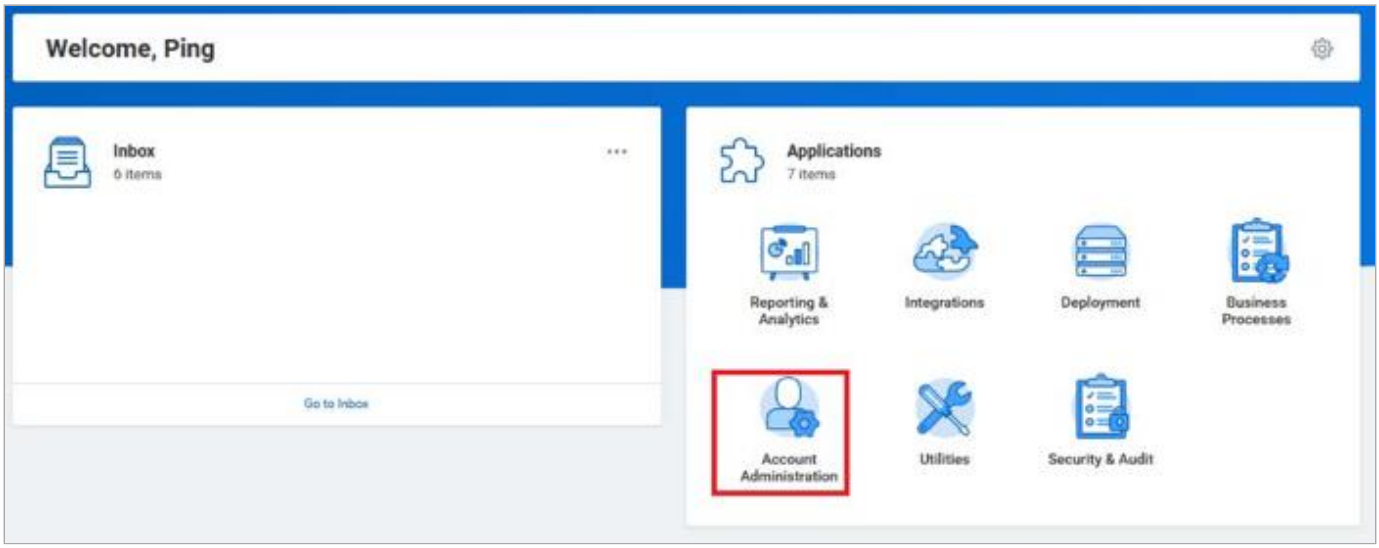
10. Click **Continue to Next Step** twice.
11. Click **Add** for each user group that should have access to Workday.



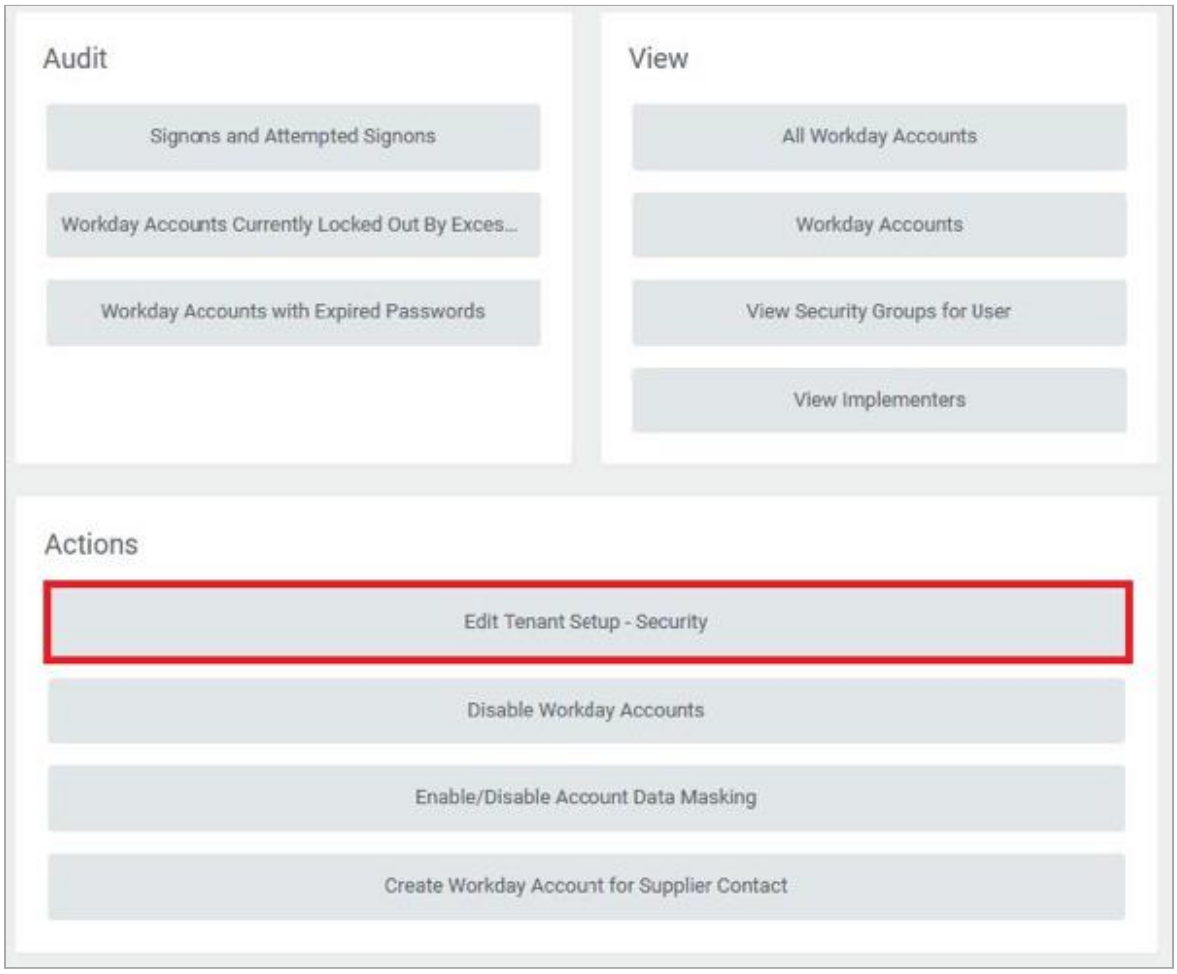
12. Click **Continue to Next Step**.
13. Click **Finish**.

Add the PingOne for Enterprise identity provider (IdP) connection to Workday

1. Sign on to Workday as an administrator and click **Account Administration**.



2. Click **Edit Tenant Setup – Security**.



3. In the **Single Sign On** section, click the + icon under **Redirection URLs**.

4. Set the following properties:

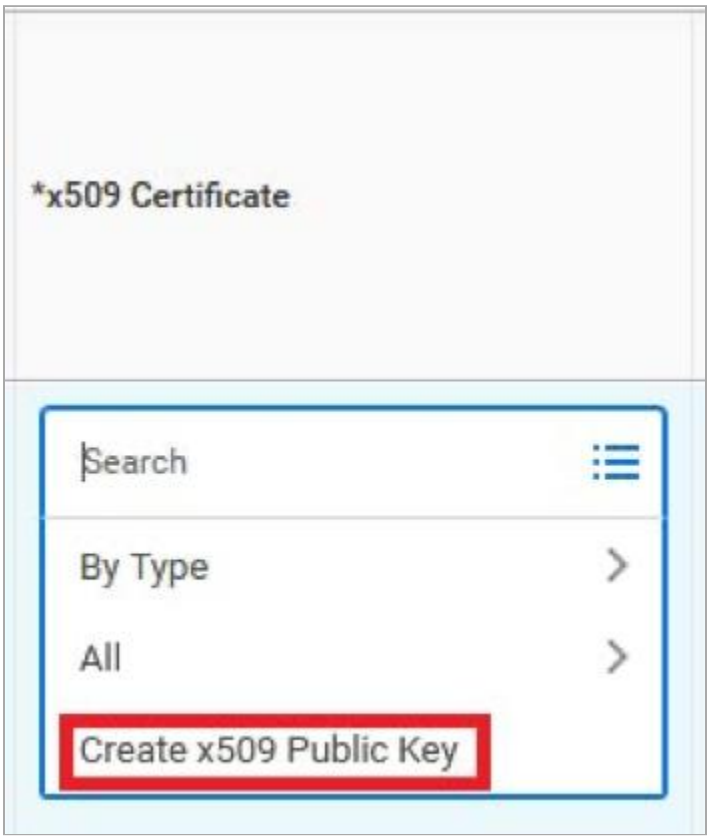
Field	Entry
***Redirect Type**	**Single URL**
Login Redirect URL	`https://your-environment.workday.com/your-tenant-name/login-saml2.flex`
Logout Redirect URL	`https://sso.connect.pingidentity.com/sso/SLO.saml2.workday.com/your-tenant-name/login-saml2.flex`
Mobile App Login Redirect URL	`https://your-environment.workday.com/your-tenant-name/logout-saml.htmld`
Mobile Browser Login Redirect URL	`https://your-environment.workday.com/your-tenant-name/logout-saml.htmld`
Environment	Select your environment.

5. In the **SAML Setup** section, select the **Enable SAML Authentication** check box.

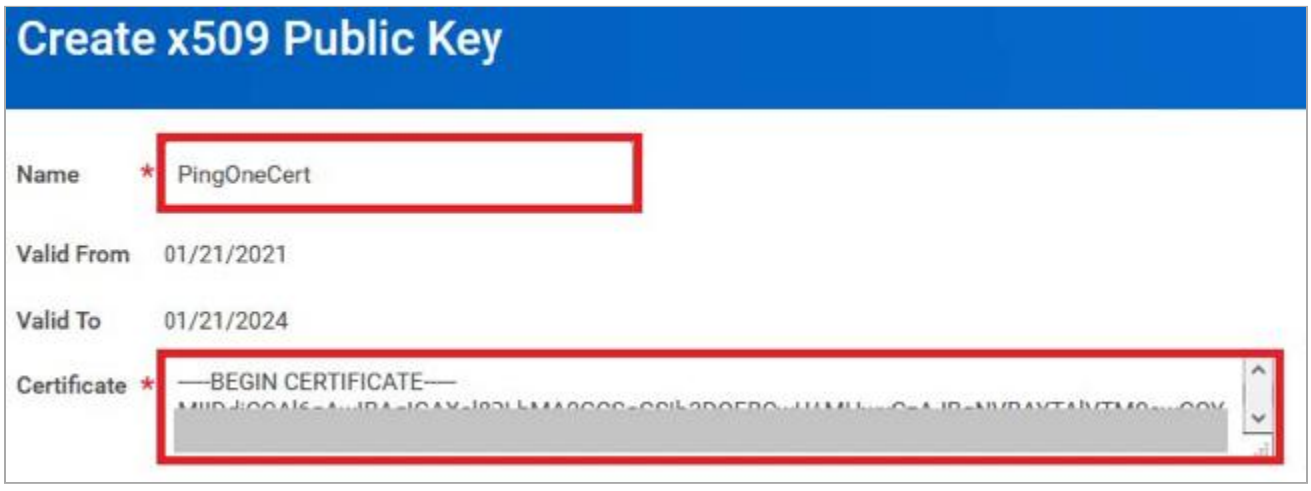
6. Click the + icon.

7. Set the **Identity Provider Name** to **PingOne** and enter the **Issuer** value you copied previously.

8. In the **x509 Certificate** section, click **Create x509 Public Key**.



9. Enter a name for your PingOne for Enterprise signing certificate, such as `PingOneCert`.
10. Open the PingOne for Enterprise signing certificate in a text editor and paste the contents of the certificate into the **Certificate** field.



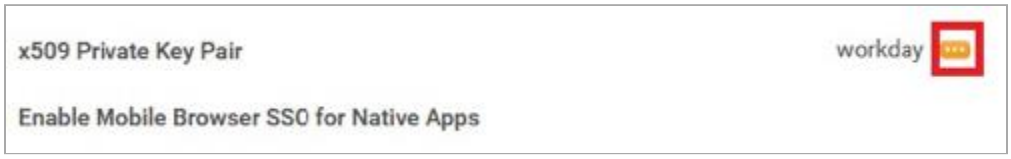
11. Click **OK**.
12. Set the following properties.

Property	Value
Enable IdP Initiated Logout	Selected
Logout Response URL	`https://sso.connect.pingidentity.com/sso/SLO.saml2`
Enable Workday Initiated Logout	Selected
Logout Request URL	`https://sso.connect.pingidentity.com/sso/SLO.saml2`
Service Provider ID	`http://www.workday.com`
SP Initiated	Selected
Do Not Deflate SP-initiated Authentication Request	Selected
IdP SSO Service URL	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=IdP-ID-value-from-PingOne`

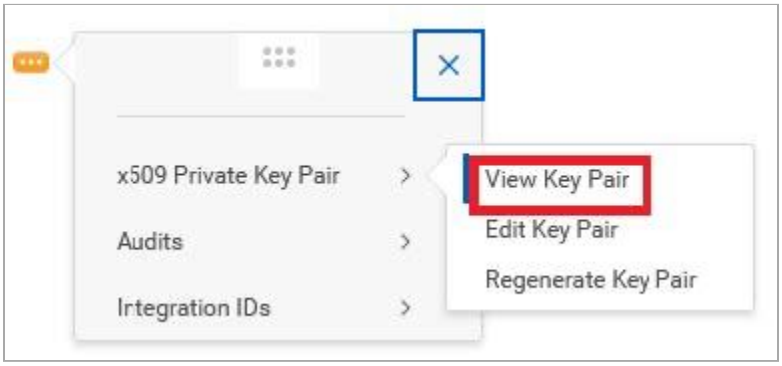
13. Click **OK**.
14. For SLO, in the **x509 Private Key Pair** menu, select **Create x509 Private Key Pair**.

15. Enter a name for the key pair.

16. Click **OK**.
17. Hover next to the key pair name and click the **Menu** icon.



18. Click **View Key Pair**.



19. Copy the contents of the public key and save them in a text editor.

20. Set **Authentication Request Signature Method** to **SHA-256**.

> **Note**
>
> Leave all other values in this section blank.

21. Click **Done**.

Complete the Workday SLO setup in PingOne

1. Go to PingOne for Enterprise and continue editing the Workday entry.

> **Note**
>
> If the session has timed out, complete the initial steps to the point of clicking **Setup**.

2. Click **Continue to Next Step**.
3. Click **Choose File**, and select the saved Workday public key file.

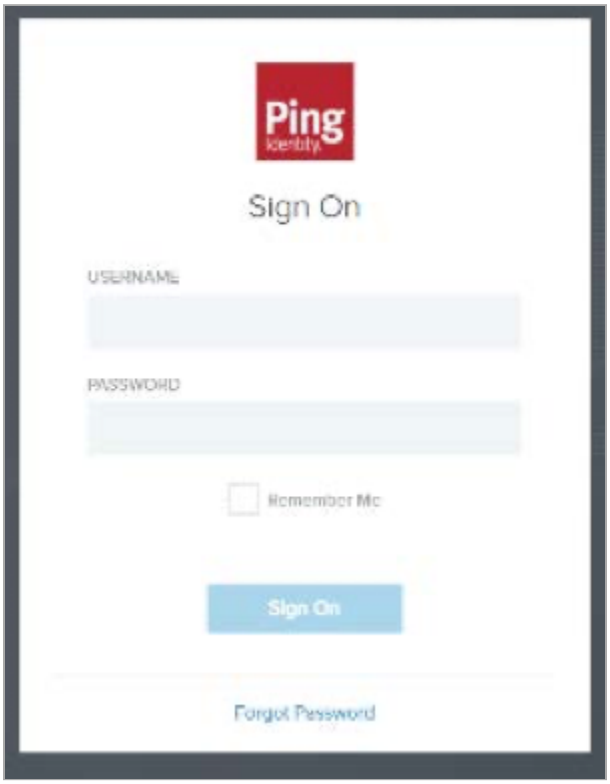
4. Click **Continue to Next Step** until the final screen. Click **Finish**.

Test the PingOne for Enterprise IdP-initiated SSO integration

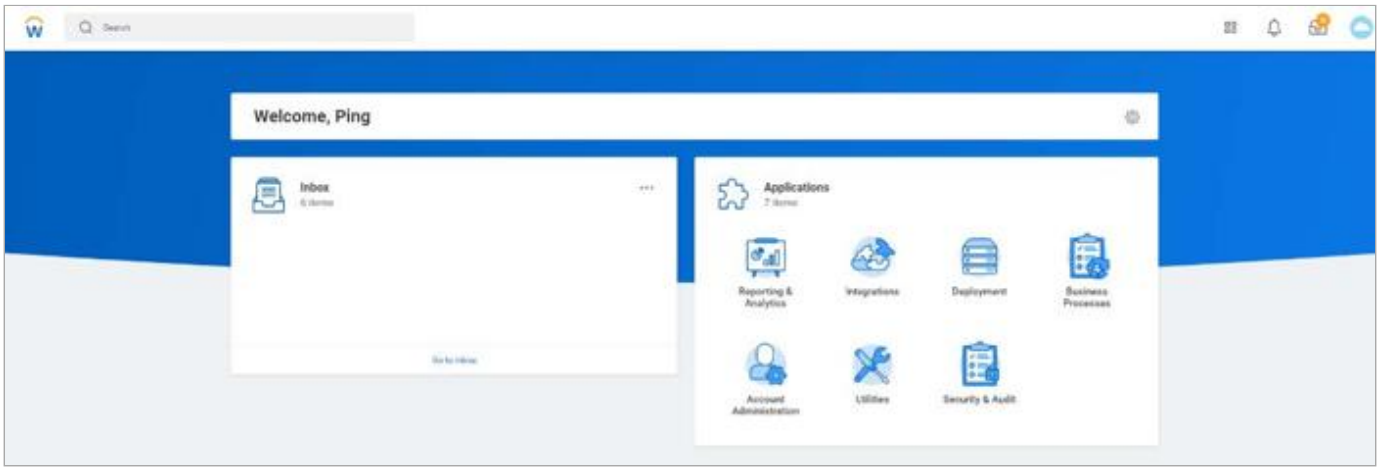
1. Go to your Ping desktop as a user with Workday access.

> **Note**
>
> To find the Ping desktop URL in the admin console, go to **Setup → Dock → PingOne Dock URL**.

2. Complete the PingOne authentication.

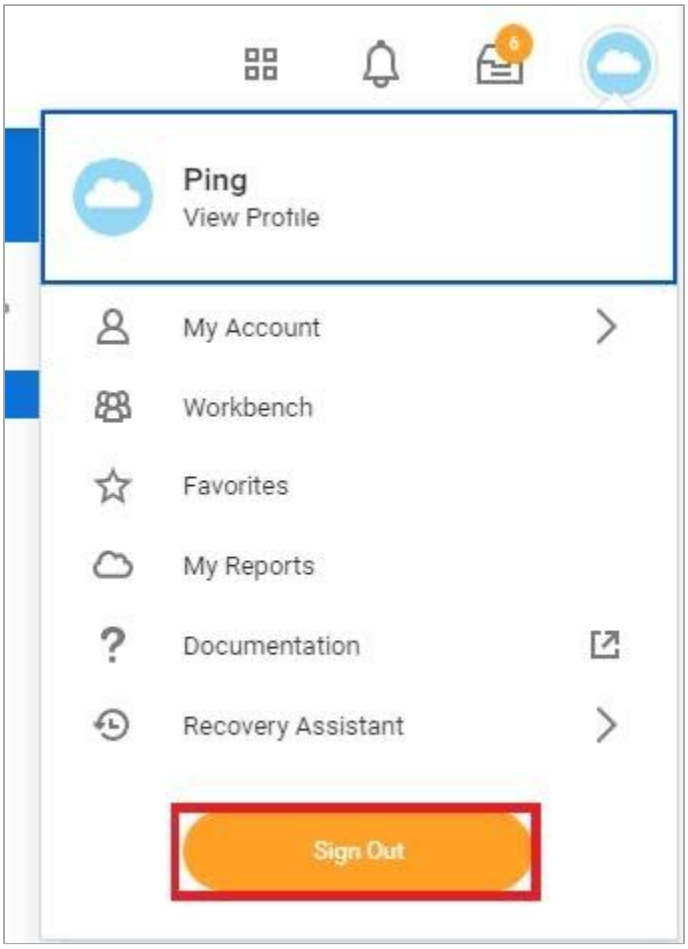


You are redirected to your Workday environment.



3. Click **Sign Out**.

   You are signed out.



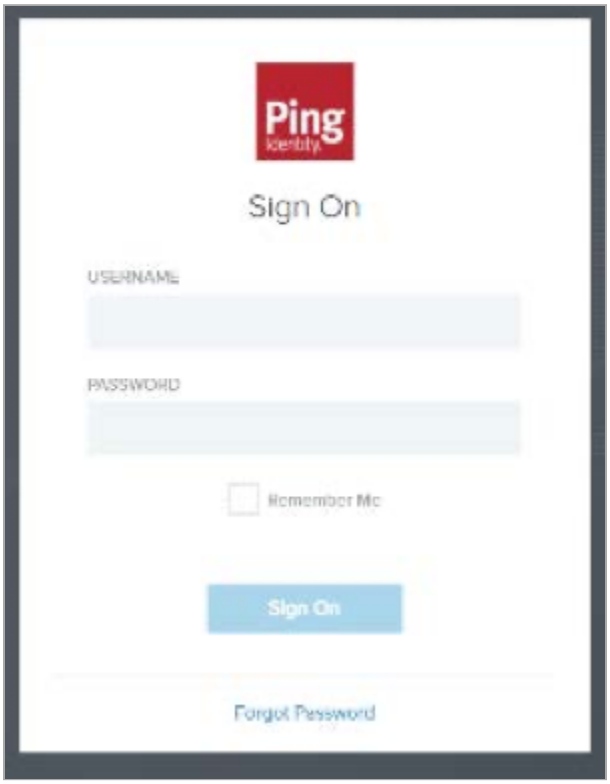
Test the PingOne for Enterprise SP-initiated SSO integration

1. Go to your Workday URL.

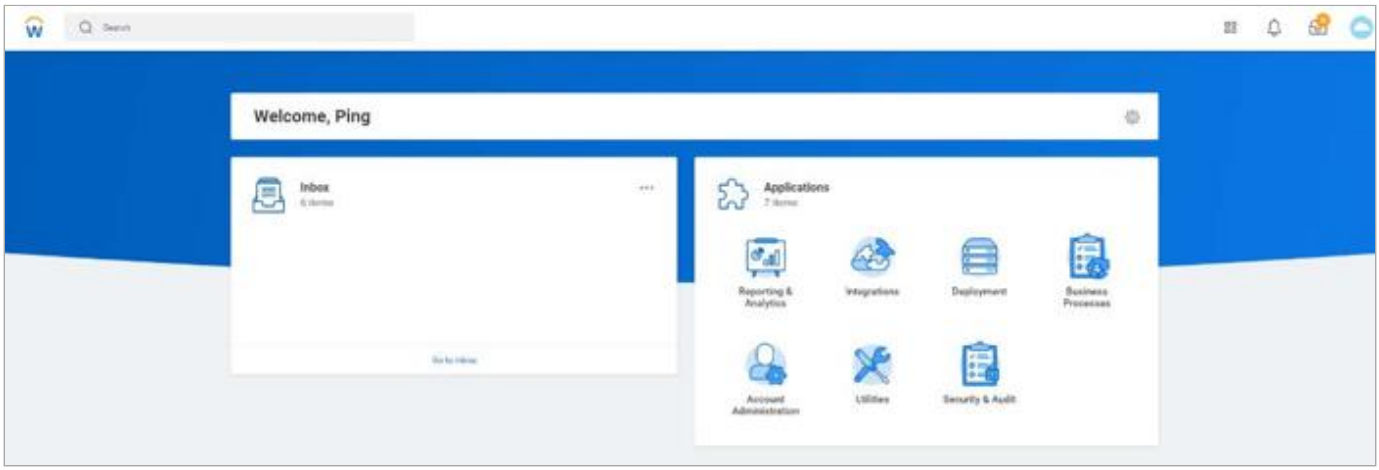
   For example:

   ```
   https://your-environment.workday.com/Your tenant/login-saml2.flex
   ```

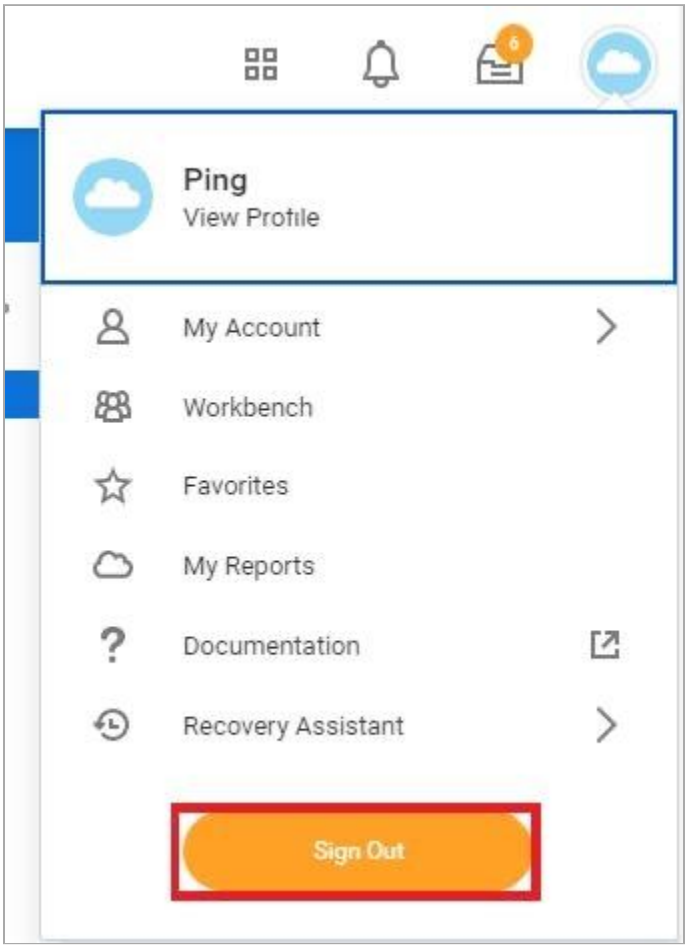
2. After you're redirected to PingOne for Enterprise, enter your PingOne for Enterprise username and password.



After successful authentication, you are redirected back to Workday.



3. Click **Sign Out**.



You are signed out.

Workplace by Facebook

Configuring SAML SSO with Workplace by Facebook and PingOne for Enterprise

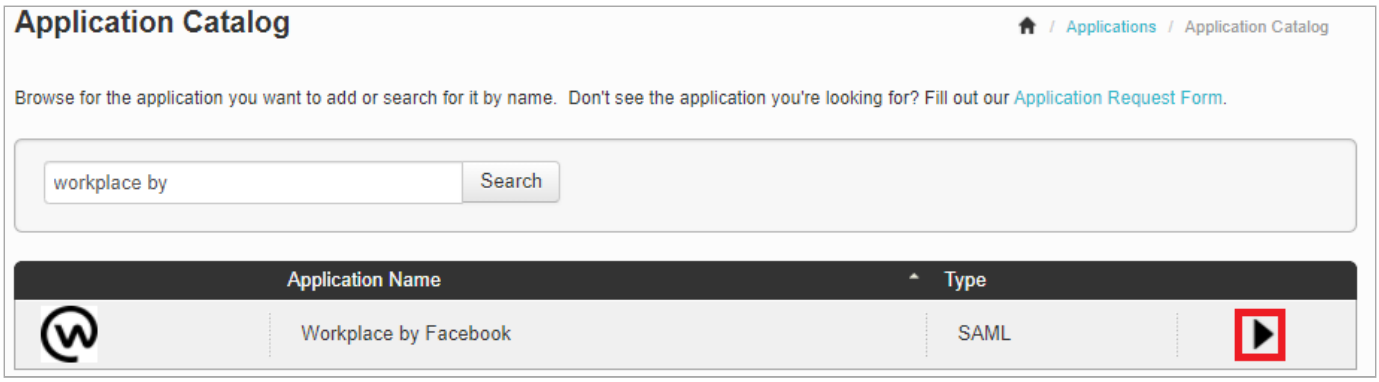
Learn how to enable Workplace by Facebook sign-on from the PingOne for Enterprise console (IdP initiated sign-on) and direct Workplace by Facebook sign-on using PingOne for Enterprise (SP-initiated sign-on).

Before you begin

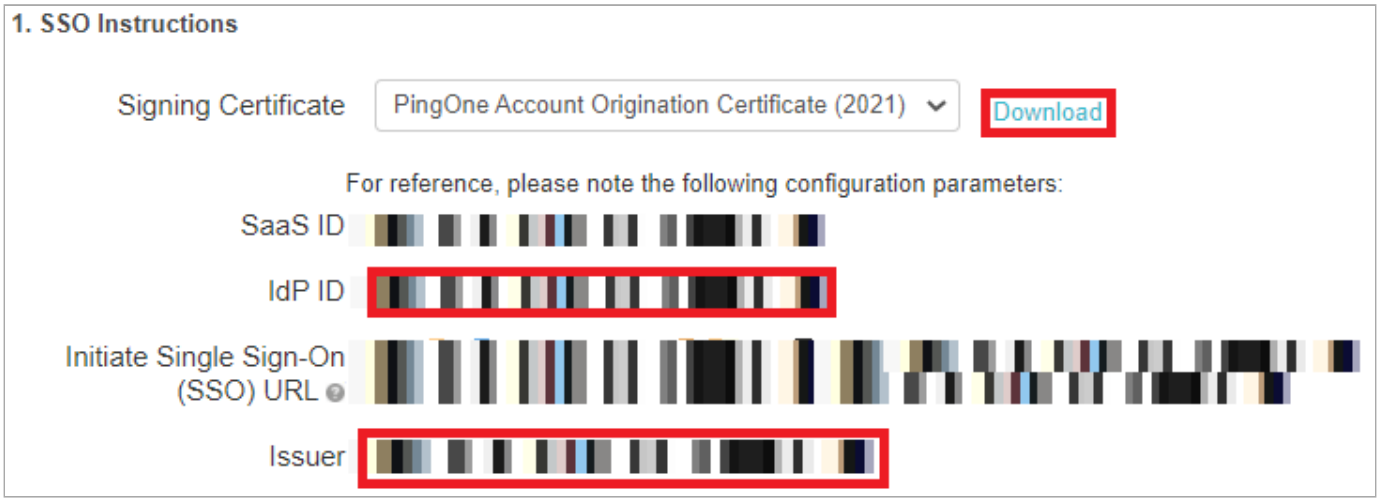
- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate Workplace by Facebook with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and Workplace by Facebook.

Set up the supplied Workplace by Facebook Application in PingOne for Enterprise

1. Make a note of your Workplace by Facebook Organization ID and subdomain, for example, `https://my-org.workplace.com`.
2. Sign on to PingOne for Enterprise and go to **Applications → Application Catalog**.
3. Search for `Workplace by Facebook`.
4. Expand the Workplace by Facebook entry and click the **Setup** icon.

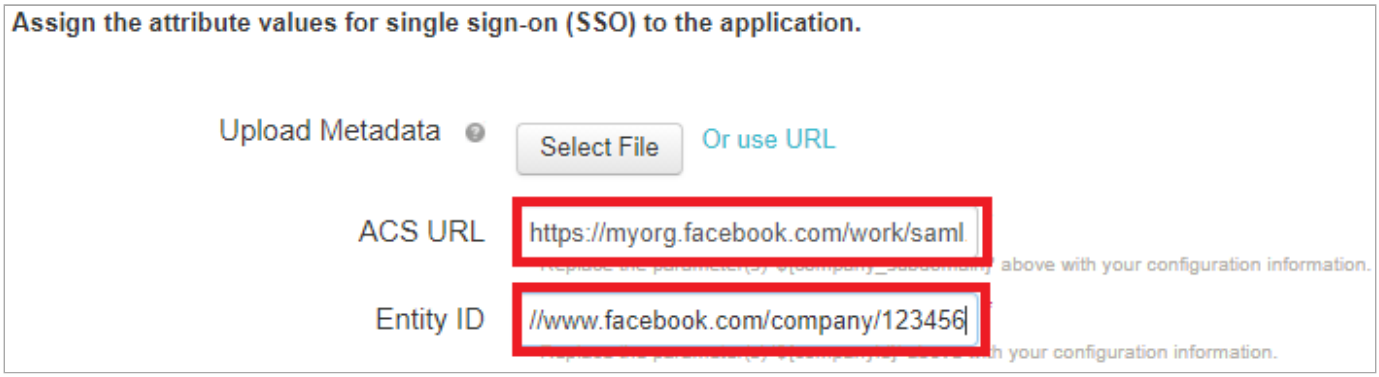


5. Copy the **Issuer** and **IdP ID** values.
6. Download the signing certificate.

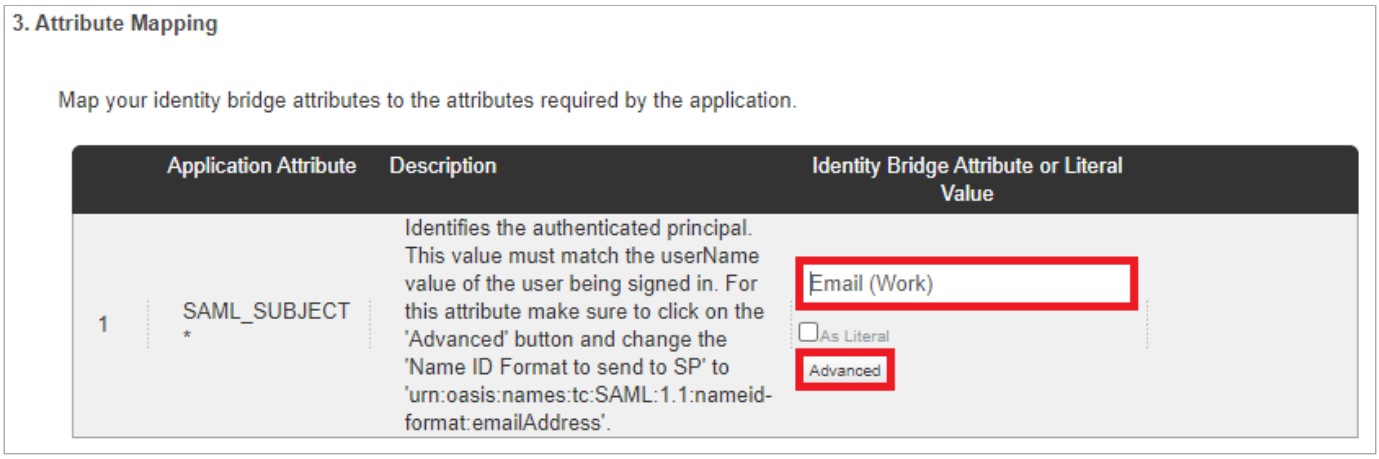


7. Click **Continue to Next Step**.
8. Set **ACS URL** to `https://your-subdomain.facebook.com/work/saml.php`.

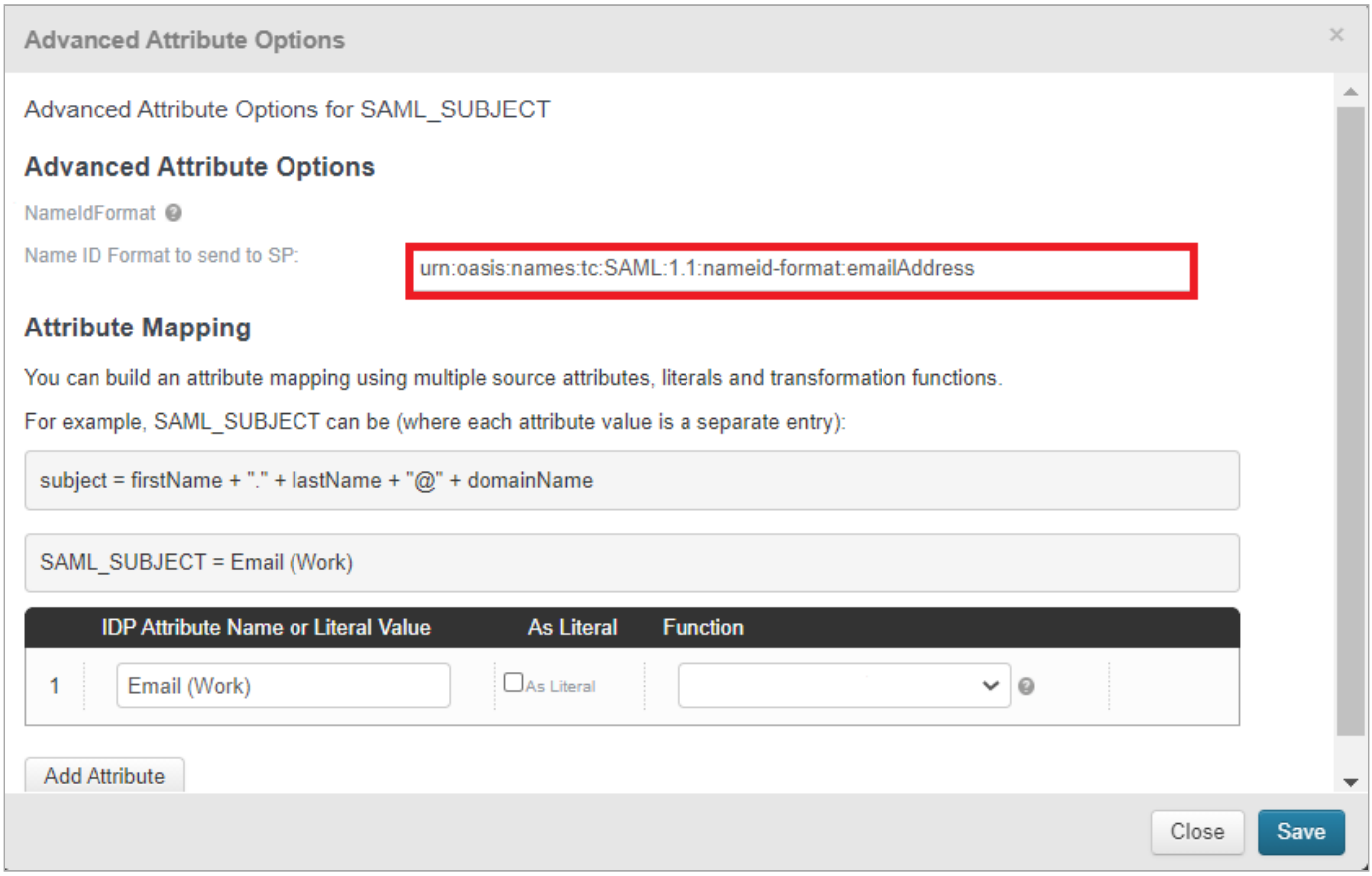
   Set **EntityID** to `https://www.facebook.com/company/your-organization-ID`.



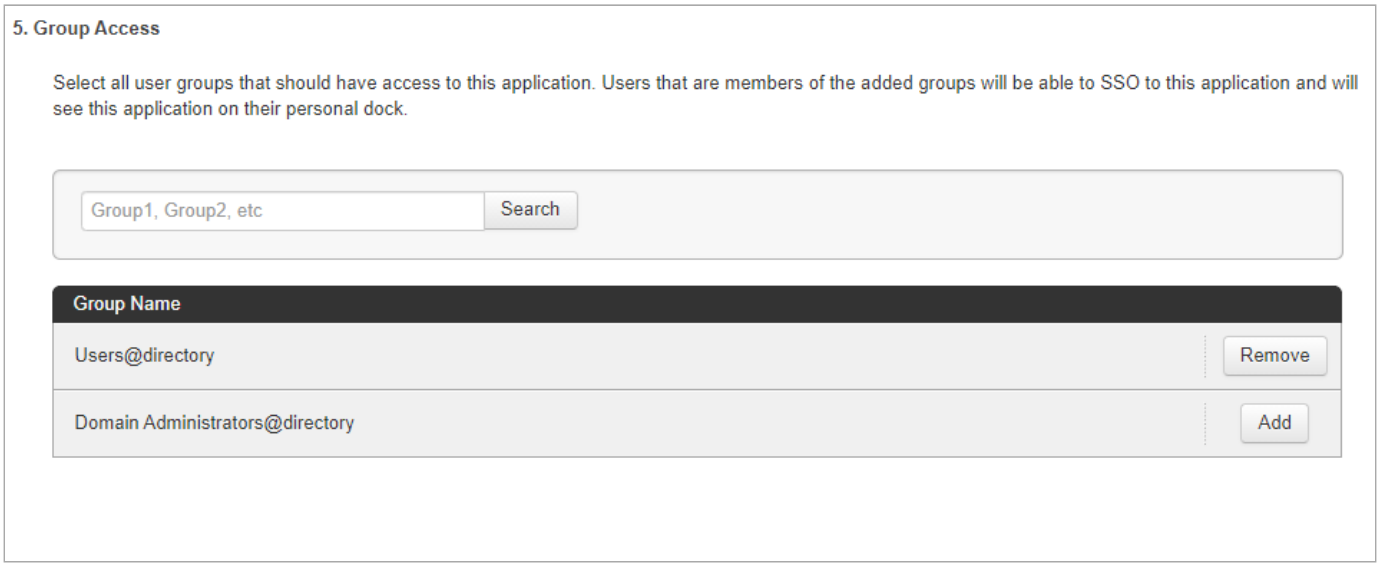
9. Click **Continue to Next Step**.
10. Map **SAML_SUBJECT** to the attribute containing the Facebook username value (an email address).



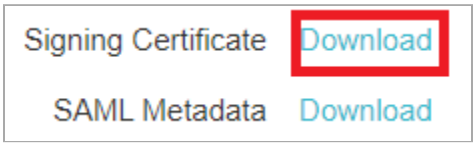
11. Click **Advanced**.
12. Set **Name ID Format** to **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.



13. Click **Save**.
14. Click **Continue to Next Step** twice.
15. Click **Add** for all user groups that should have access to Workplace by Facebook.



16. Click **Continue to Next Step**.
17. Download the signing certificate.

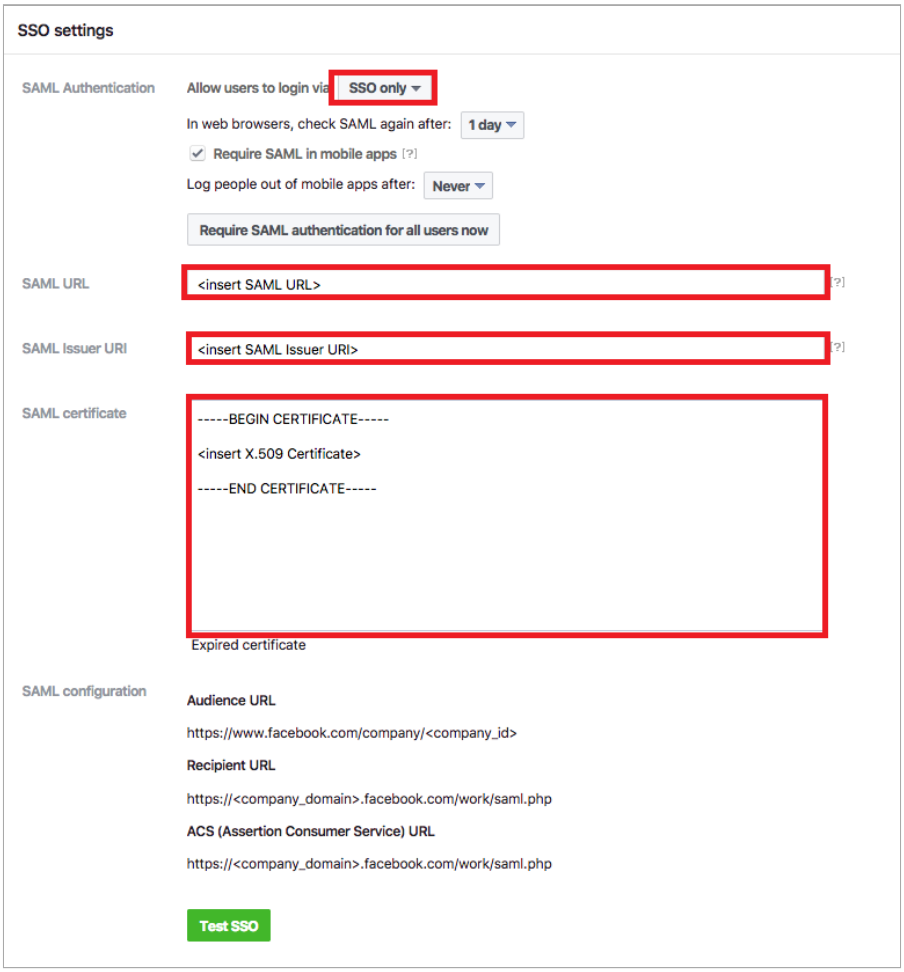


18. Click **Finish**.

Add the PingOne for Enterprise IdP connection to Workplace by Facebook

1. Sign on to your Workplace by Facebook console as an administrator.
2. Go to **Admin Panel → Security**.
3. Click the **Authentication** tab.
4. For **Log in**, select **Single Sign-On (SSO)**.
5. Click **Add New SSO Provider**.
6. Set the following field values:

Field	Setting
Allow users to login via	**SSO only**
SAML URL	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=IdP-ID-value` (from Set up the supplied Workplace by Facebook Application in PingOne for Enterprise)
SAML Issuer URL	`Issuer-value` (from Set up the supplied Workplace by Facebook Application in PingOne for Enterprise)
SAML Certificate	Paste in the contents of the signing certificate that you downloaded.



7. Click **Test SSO**.
8. After a successful test, save the changes.
9. Go to **Admin panel → People** and search for the user to use SSO.
10. Edit the user and select **SSO** for **Log in with**.

> **Note**
>
> See Workplace documentation for setting this value on users in bulk.

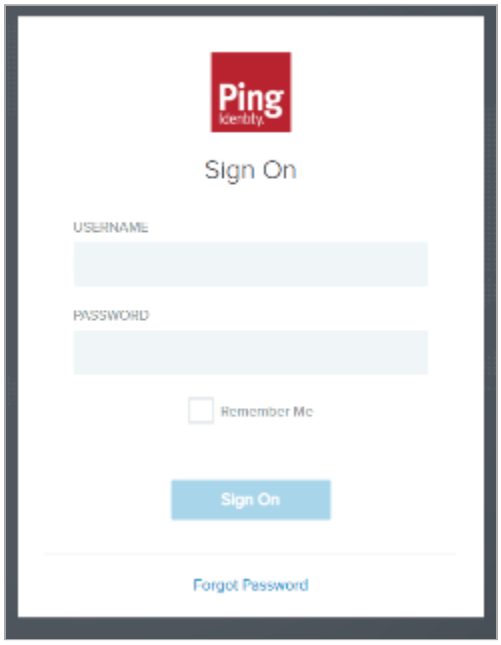
Test the PingOne for Enterprise IdP-Initiated SSO integration

1. Go to your Ping desktop as a user with Workplace by Facebook access.

> **Note**
>
> To find the Ping desktop URL in the Admin console, go to **Setup → Dock → PingOne Dock URL**.

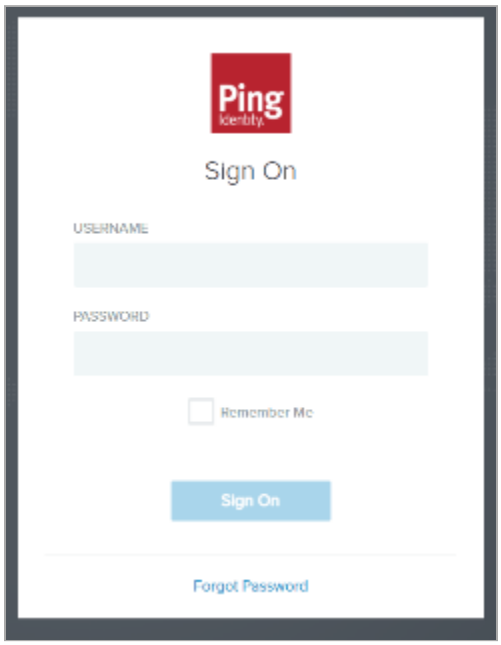
2. Complete PingOne for Enterprise authentication.

   You are redirected to your Workplace by Facebook domain.



Test the PingOne for Enterprise SP-initiated SSO integration

1. Go to https://*your subdomain*.workplace.com.
2. Enter your email address.
3. When you are redirected to PingOne for Enterprise, enter your PingOne for Enterprise username and password.



After successful authentication, you're redirected back to Workplace by Facebook.

Wrike

Configuring SAML SSO with Wrike and PingOne

Learn how to configure SAML SSO with Wrike and PingOne.

Before you begin

You must have Business Level permissions to configure SAML.

About this task

Learn more about Wrike and SSO in the SAML SSO: Implementation Guide in the Wrike documentation.

> **Note**
>
> This is a tested integration

Download the Wrike metadata

1. Sign on to your Wrike admin account and in the upper right-hand corner, select your name and then **Settings**.
2. Go to **Security → Setup SAML SSO**.
3. In the **Set up your identity provider** list, select **Other**.
4. Download the service provider (SP) metadata:

   Choose from:

   - Click **Download XML file**.
   - Copy the metadata link.
5. Click **Next**.

Import the metadata into PingOne

1. In a new tab, sign on to your PingOne SSO admin account and go to **Connections → Applications** and click the **+** icon.
2. On the **New Application** page, click **Advanced Configuration**, and on the **SAML** line, click **Configure**.
3. On the **Create App Profile** page, enter the following information:
   - **Application Name**
   - Optional: **Description**

- Optional: **Icon**

4. Click **Save and Continue**.
5. The **Configure SAML Connection** page allows for a few options to configure the SP metadata in PingOne. Only one of the following is required to import the metadata:

   Choose from:

   - Click **Import Metadata** to import the metadata file that you downloaded in the previous procedure.
   - Click **Import from URL** to upload the copied link from the previous procedure.
   - If you know the Wrike SP metadata details, manually enter the required information.

> **Important**
>
> All required information is filled out if you choose **Import Metadata** or **Import From URL** except for the **SUBJECT NAMEID FORMAT**.
> You must update the **SUBJECT NAMEID FORMAT** to `urn:oasis:nams:tc:SAML:1.1:nameid-format:emailAddress`. If you set this to something else, you'll get a connection error.

6. Click **Save and Continue**.
7. On the **Attribute** mapping page, add the following attributes and mark all as **Required**.

   - **firstName**
   - **lastName**
   - **NameID**

> **Note**
>
> The PingOne **User Attribute** for the **saml_subject** must be updated to **Email Address** and not **User ID**.

8. Click **Save and Close**.
9. On the **Applications** page, click the **Configuration** tab and copy the URL on the **IDP METADATA URL** line.
10. On your Wrike tab, paste the URL that you copied in the previous step into the **Use URL to provide XML** field and click **Next**.
11. Click **Enable SAML settings** to finalize the configuration of the SAML connection.

    You'll receive a verification email providing you with a 6-digit code.
12. Copy and paste the 6-digit code into the confirmation box to verify the connection and then click **Confirm** to finalize set up.

    A page with information on testing opens.

> **Note**
>
> Although this page provides you with information on testing the SAML SSO set up, follow Test the integration to test your integration.

13. Click **Save**.

Create and assign identities in PingOne

> **Note**
>
> If you've already assigned identities and groups in PingOne, go to Test the integration.

1. In PingOne, go to **Identities → Groups** and click the **+** icon next to **Groups.**
2. On the **Create New Group** page, enter values for the following:
    - **Group Name** (Required)
    - **Description** (Optional)
    - **Population** (Optional)
3. Click **Finish & Save**.
4. To add identities to the group, on the **Identities** tab, go to **Users → + Add User**.
5. On the **Add User** page, enter the necessary information for a user.

    > **Important**
    >
    > Verify the first name, last name, and email address are correct, as these are values passed in the SAML assertion.

6. Click **Save**.
7. Assign the user that you created to the group that you created previously.

    Locate the user you created and:

    1. Expand the section for the user.
    2. Select the **Groups** tab.
    3. Click **+ Add**.
8. In the **Available Groups** section, select the group that you created and click the **+** icon to add it to the user's group memberships. Click **Save**.
9. On the **Connections** tab, for the Wrike application:
    - Click the **Access** tab
    - Click the **Pencil** icon to edit the configuration
10. Select the group that you created and add it to the **Applied Groups** section. Click **Save**.

    You're now ready to test the integration.

Test the integration

1. In the PingOne admin console, go to **Dashboard → Environment Properties**.
2. Right-click on the **Application Portal URL** and open it in a private browser session.
3. Sign on as the test user that you created and click the Wrike tile.

   You’re signed on to the user’s Wrike account using SSO and testing is complete.

Zendesk

Configuring SAML SSO with Zendesk and PingFederate

Learn how to configure SAML SSO with Zendesk and PingFederate.

About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
`SAML-SUBJECT`	Email Address	Required

The following table details the references that are used within this guide that are environment specific. Replace these with the suitable value for your environment.

Reference	Description
tenant	Zendesk Tenant name

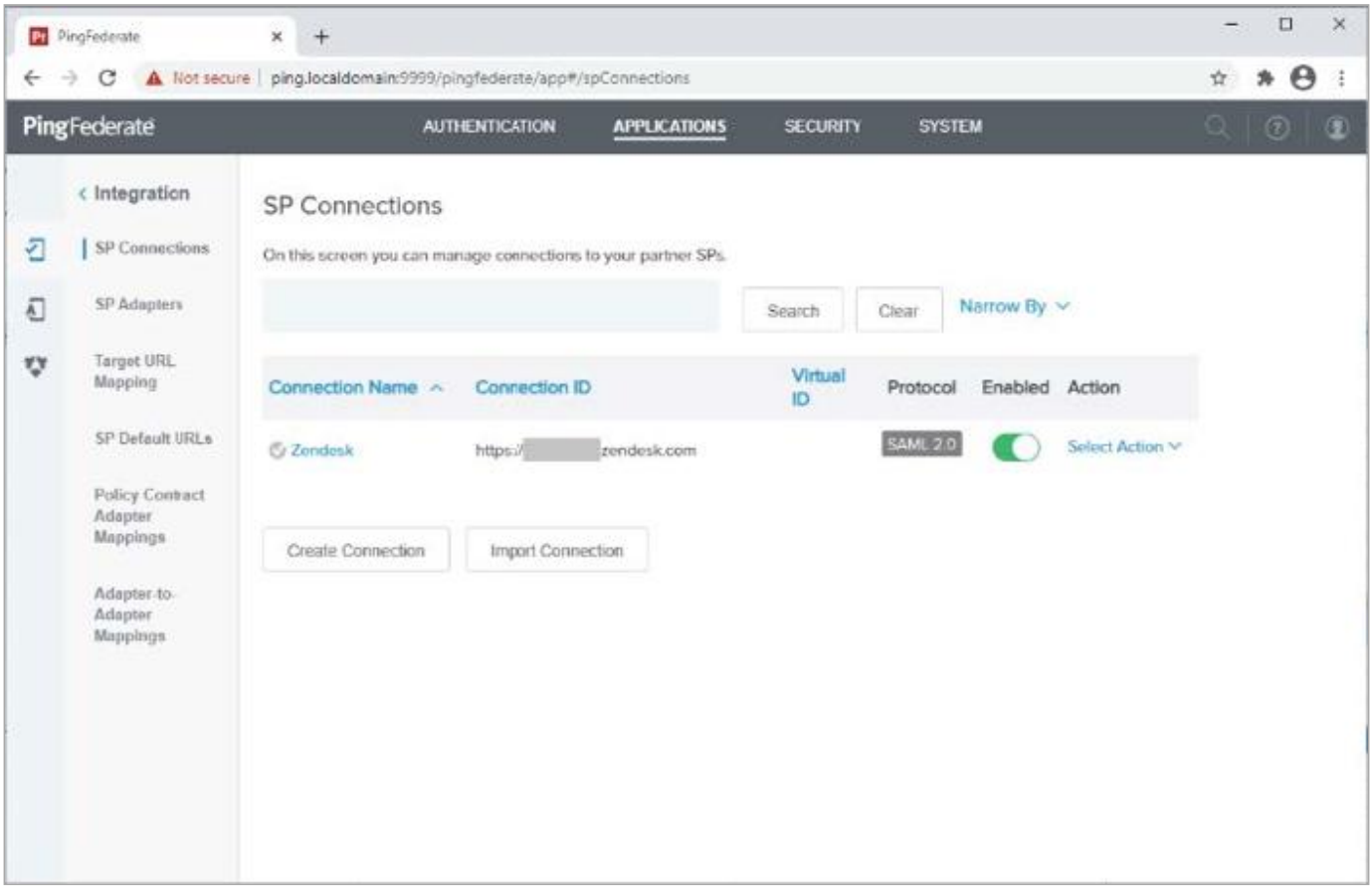
Create the PingFederate service provider (SP) connection for Zendesk

1. Sign on to the PingFederate administrative console.
2. Using the following information, create an SP connection in PingFederate:
    1. Set **Partner's Entity ID** to `https://tenant.zendesk.com`.
    2. Configure using **Browser SSO** profile **SAML 2.0**.
    3. Enable the following **SAML Profiles**.
        - **IdP-Initiated SSO**
        - **SP-Initiated SSO**
    4. In **Assertion Creation → Attribute Contract Fulfillment**, set the **Subject Name Format** to `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`.
    5. In **Assertion Creation → Attribute Contract Fulfillment**, map the attribute **SAML_SUBJECT** to the attribute `mail`.
    6. In **Protocol Settings → Assertion Consumer Service URL**, enter `https://tenant.zendesk.com/access/saml`.
    7. In **Protocol Settings → Allowable SAML Bindings**, enable **Redirect**.

8. In **Credentials**, choose a suitable signing certificate and make sure the **Include the certificate in the signature <KEYINFO> element** check box is selected.

3. Export the metadata for the newly-created SP connection.

4. Export the signing certificate public key.

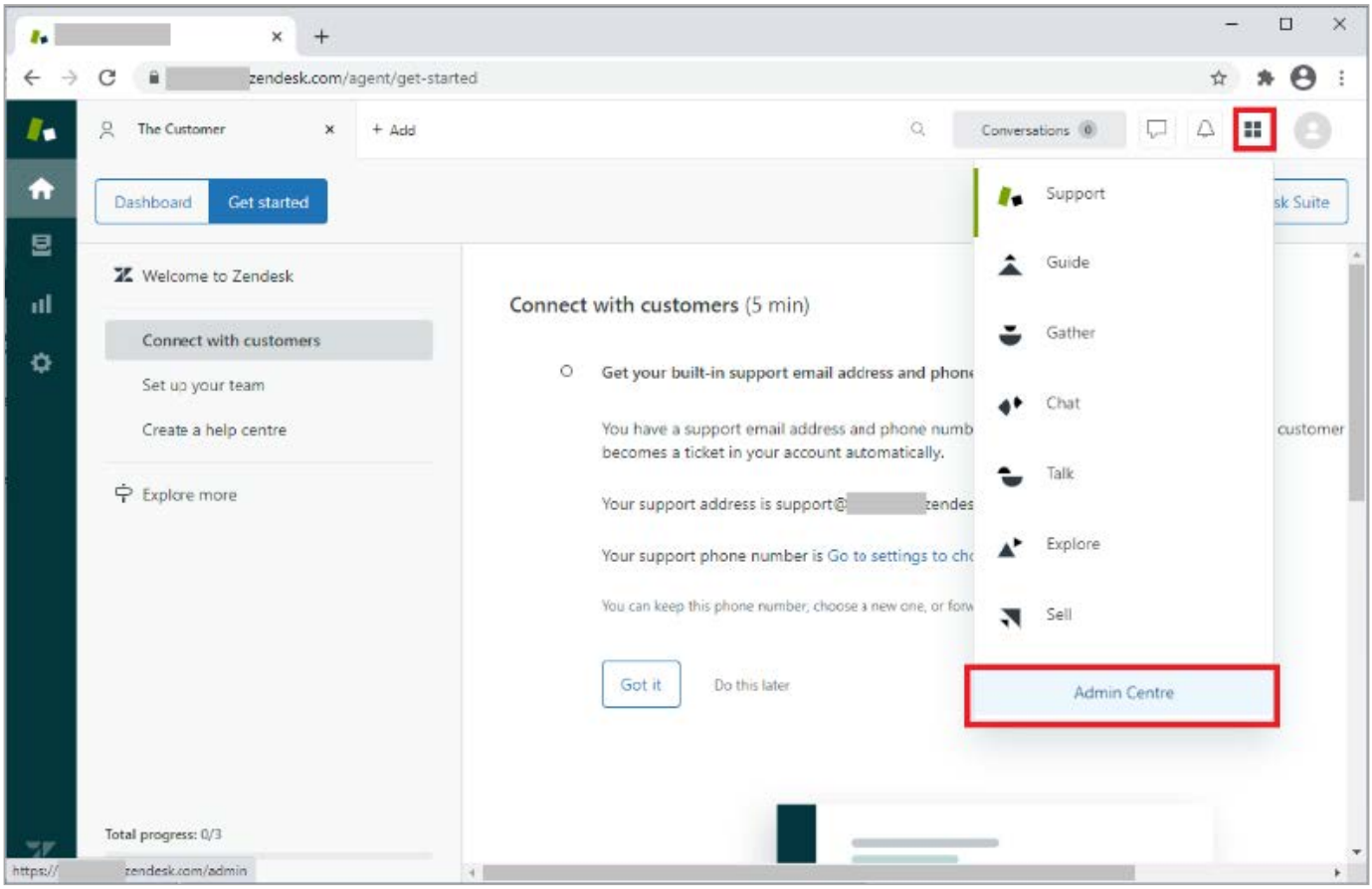


Configure the PingFederate IdP connection for Zendesk

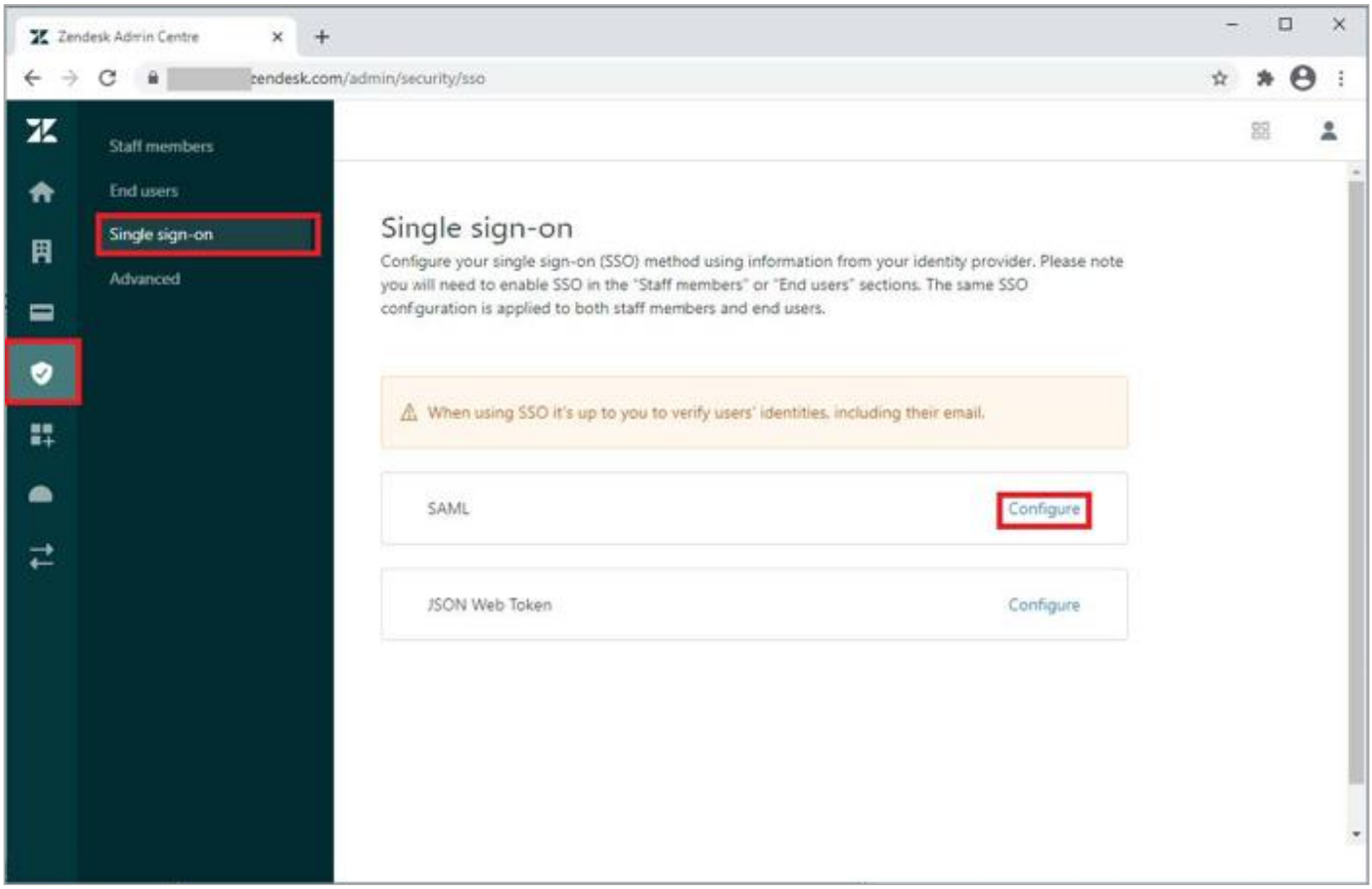
1. Sign on to Zendesk as an administrator.

2. Click on the **Products** icon.

3. Click **Admin Centre**.



4. Click the **Security** icon.
5. Click **Single sign-on**.

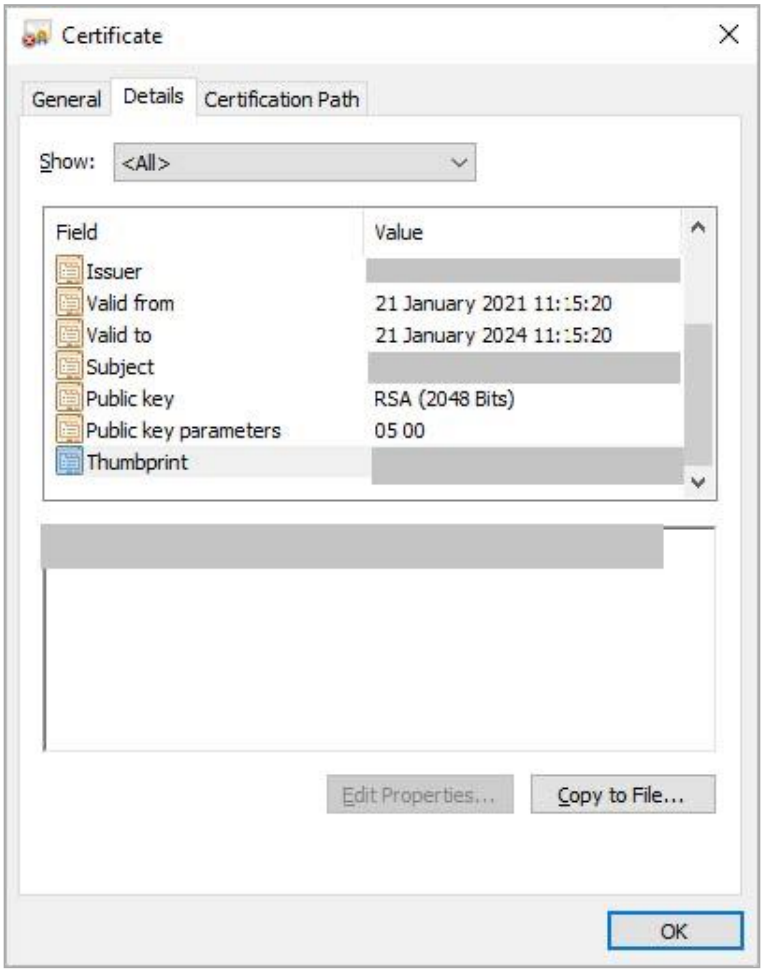


6. In the **SAML SSO URL** field, enter the SSO URL for your PingFederate environment configuration.

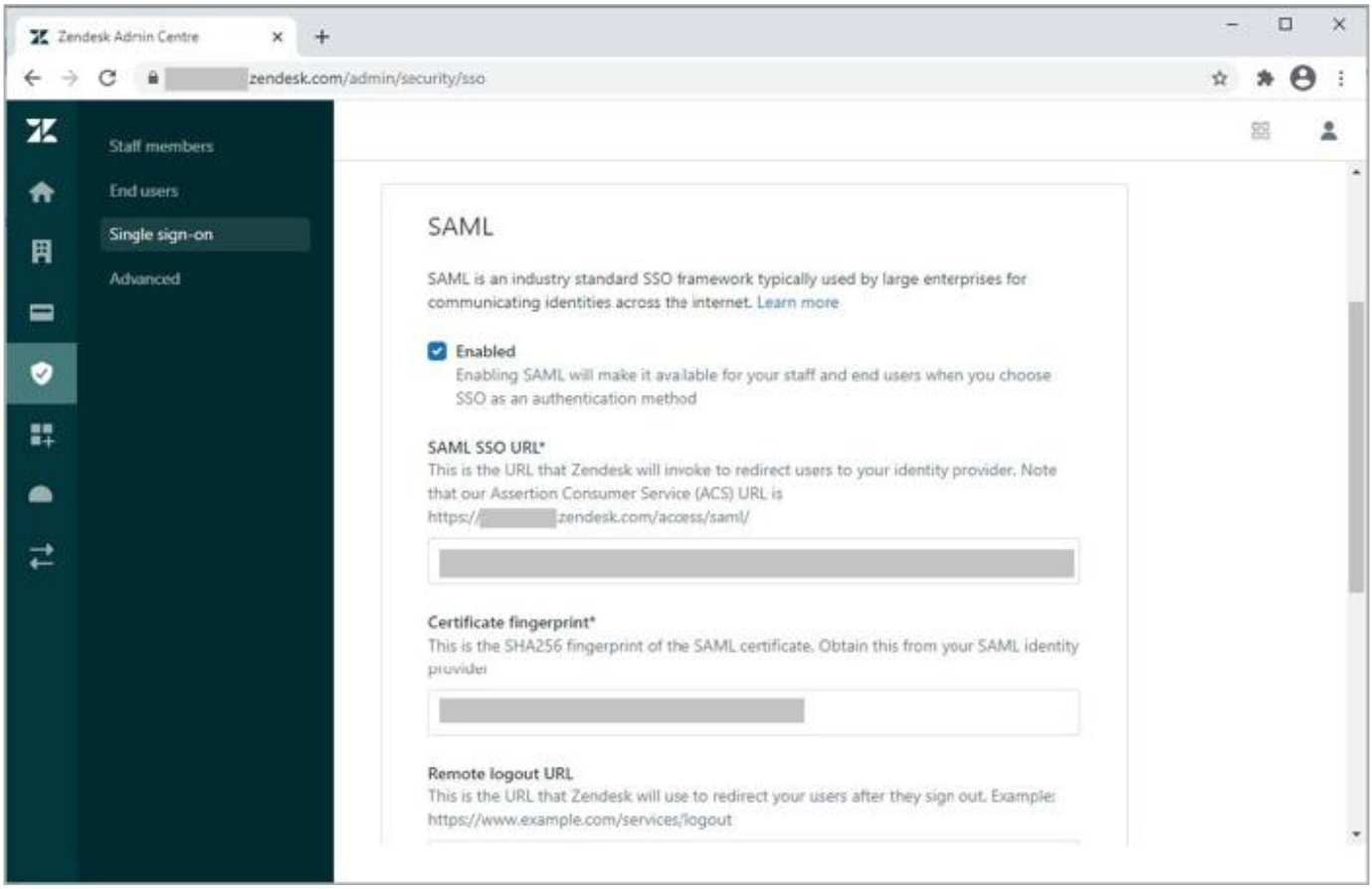
   For example:

   ```
   https://pinghostname/idp/SSO.saml2
   ```

7. Open the **Signing** certificate you downloaded in the PingFederate SP configuration and copy the thumbprint to the **Certificate** fingerprint.



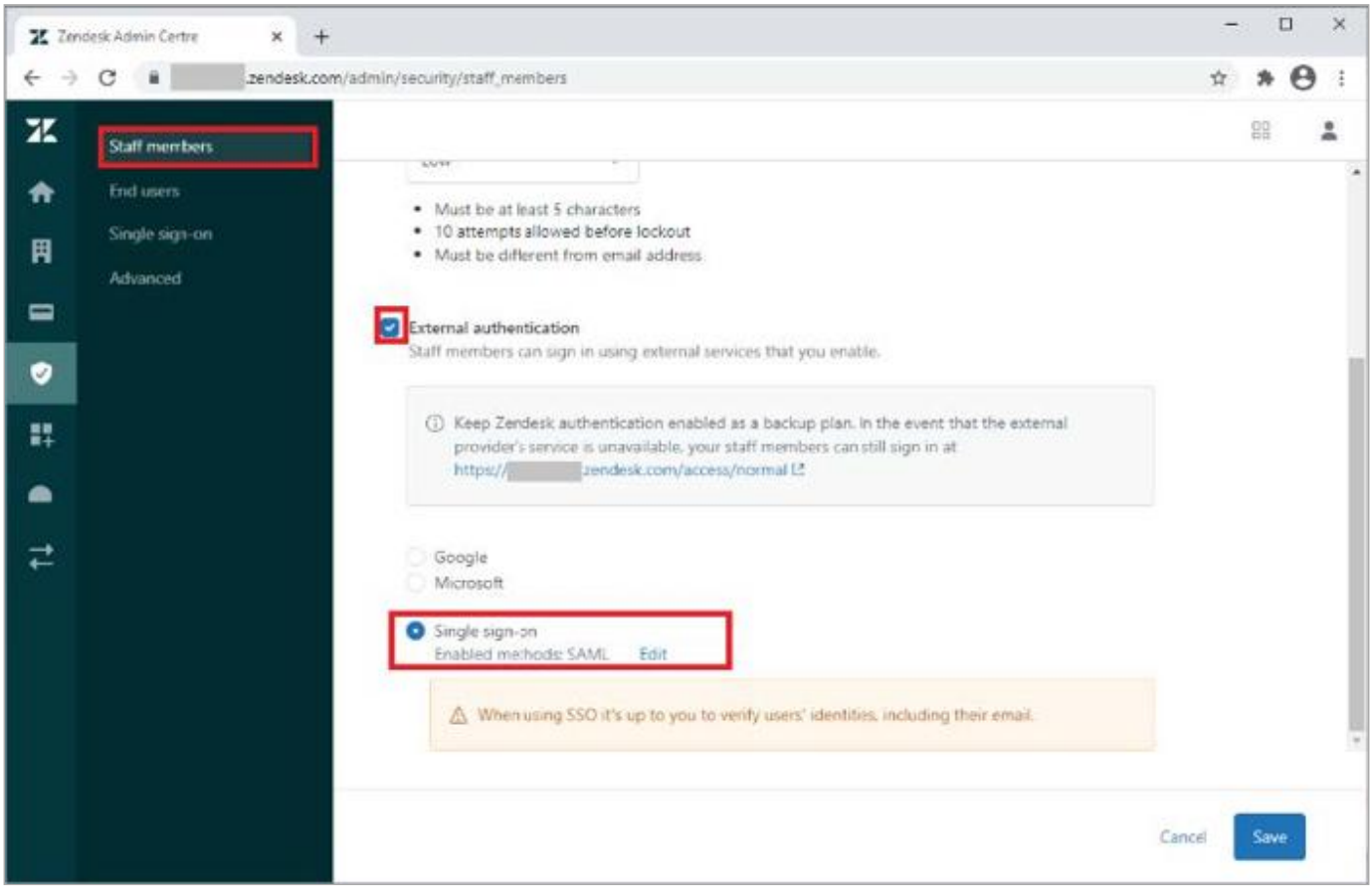
8. Select the **Enabled** check box.



9. Click **Save**.
10. Enable external authentication for **Staff members** or **End users** as required.

> **Note**
>
> The following example enables it for **Staff members** only.

    - Click the **Security** icon.
    - Click **Staff members**.
    - Select the **External Authentication** check box.
    - Click **Single sign-on**.
    - Click **Save**.

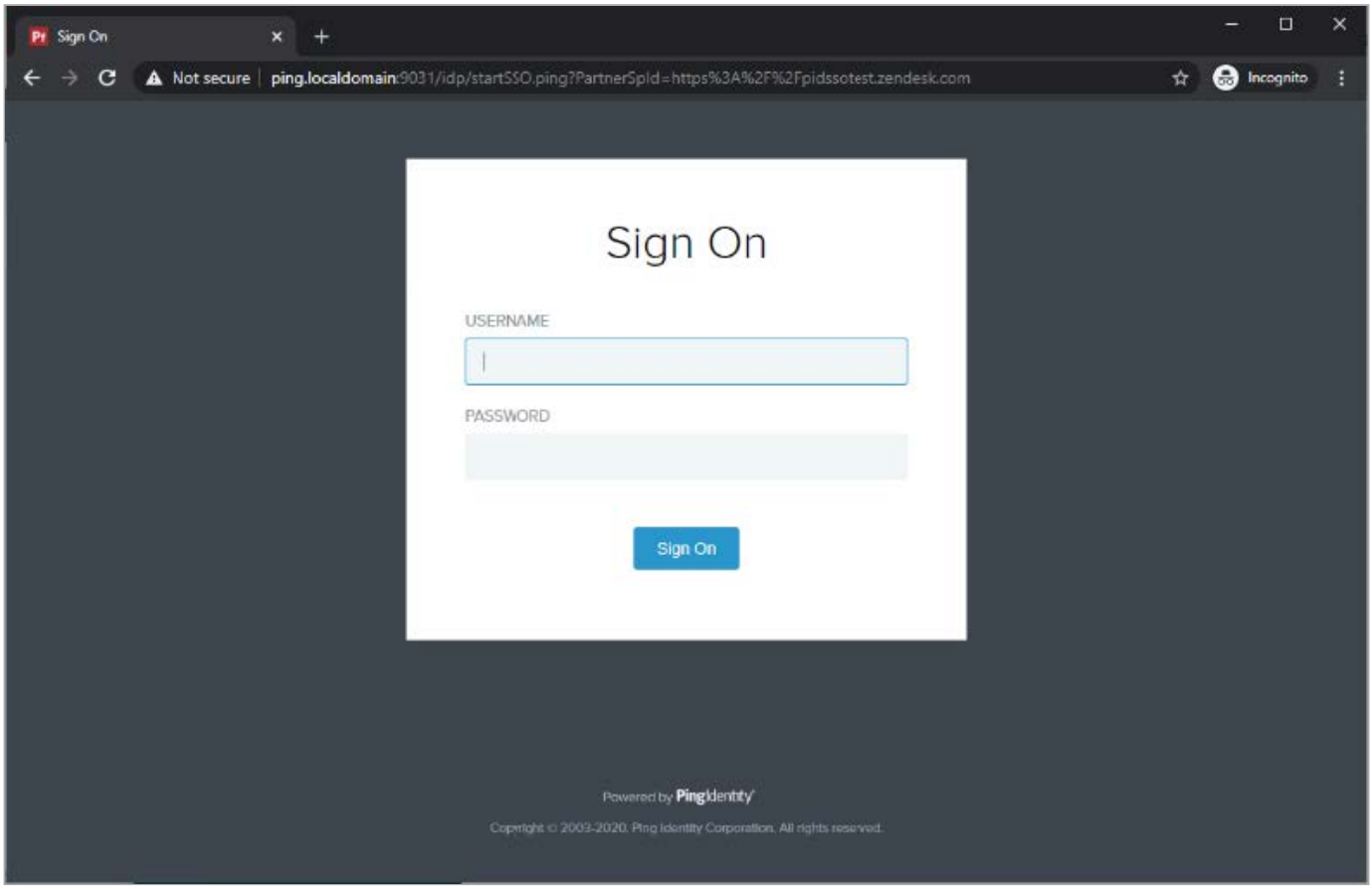


Test the integration

For PingFederate IdP-initiated SSO

Go to the **SSO Application Endpoint** from the PingFederate application configuration to perform IdP-initiated SSO.

For example, `https://PingFederateHostname:PingFederatePort/idp/startSSO.ping?PartnerSpId=Zendesk`.

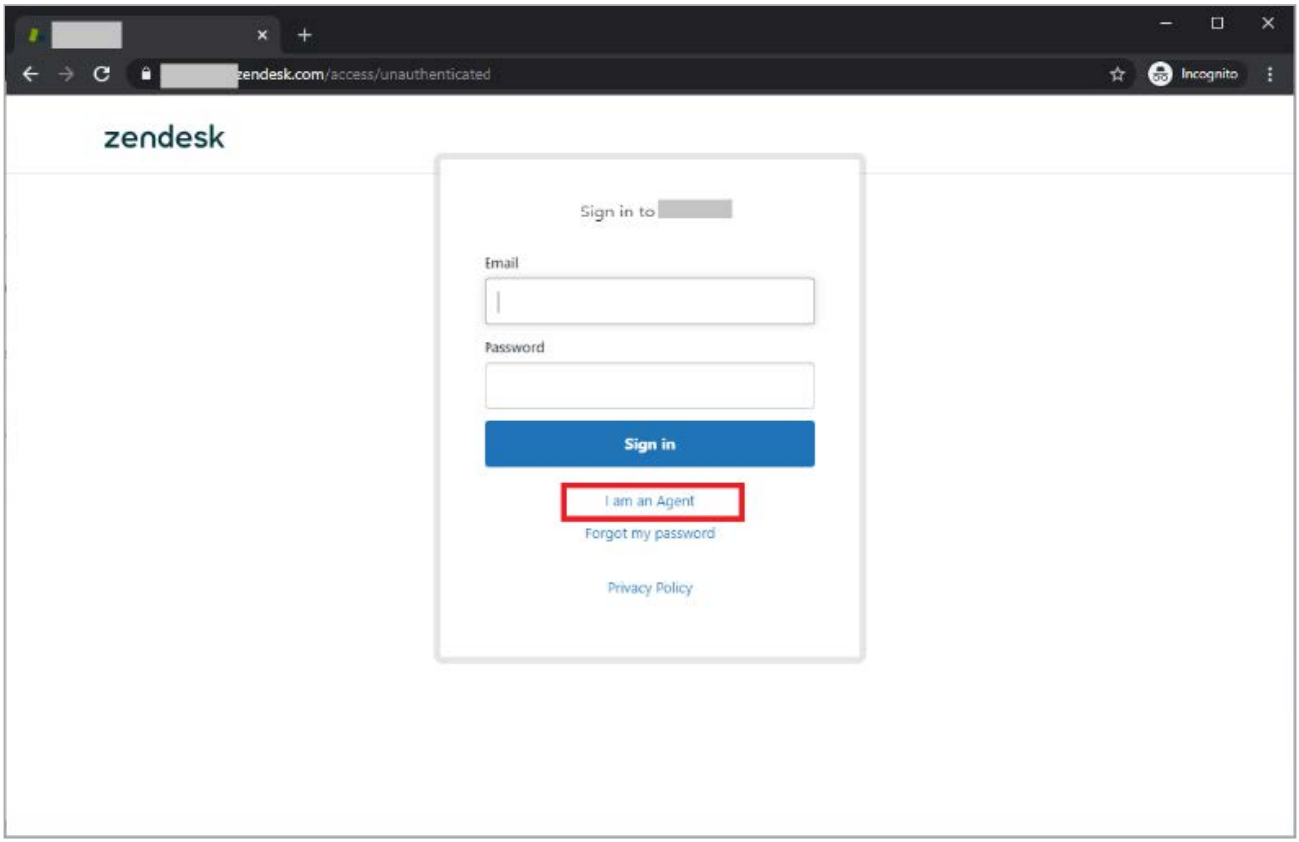


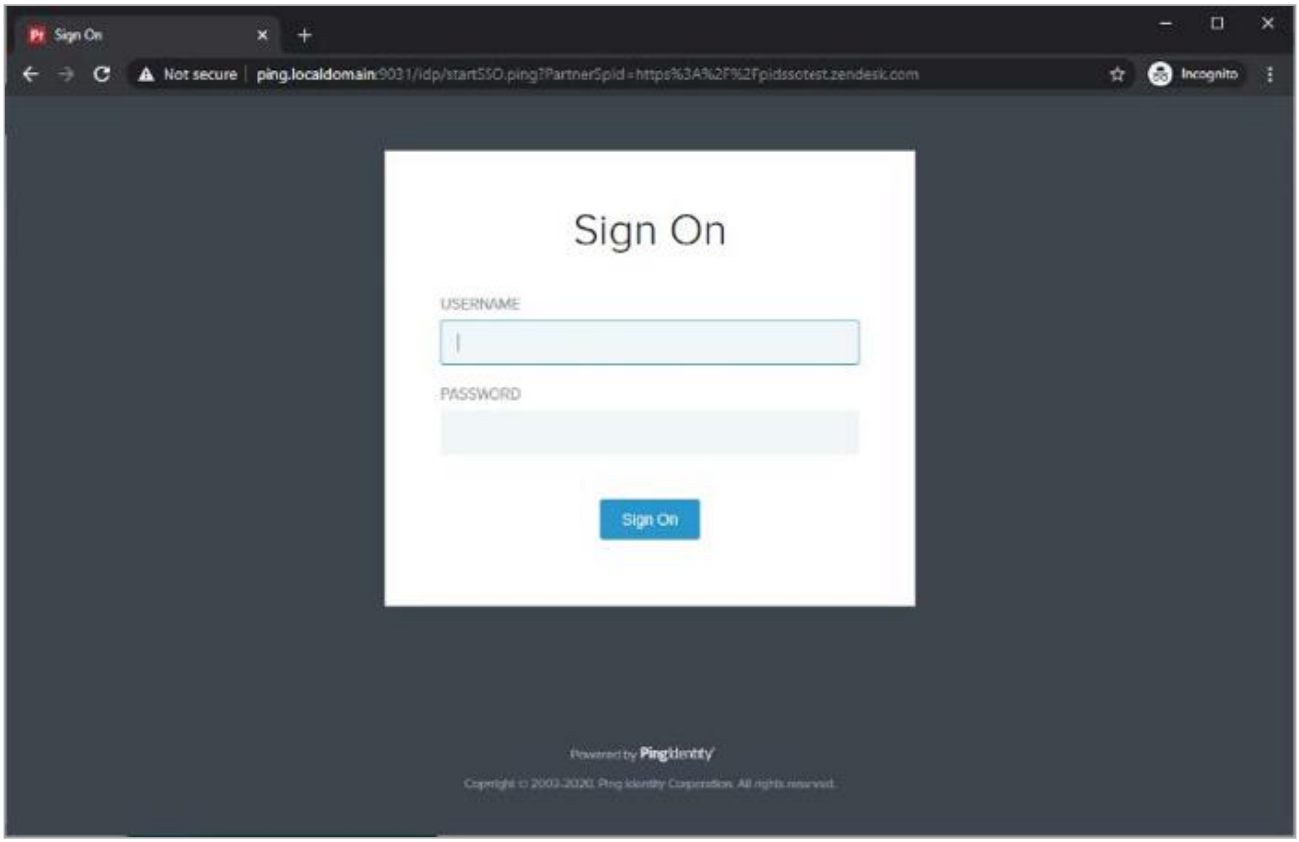
For PingOne SP-initiated SSO

1. Go to the URL for your Zendesk tenant. For example, `https://tenant.zendesk.com`.

> **Note**
>
> Because SSO is only enabled for Staff, you should see a sign on form.

2. Click **I am an Agent** to initiate SSO.





Configuring SAML SSO with Zendesk and PingOne

Learn how to configure SAML SSO with ZenDesk and PingOne.

About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

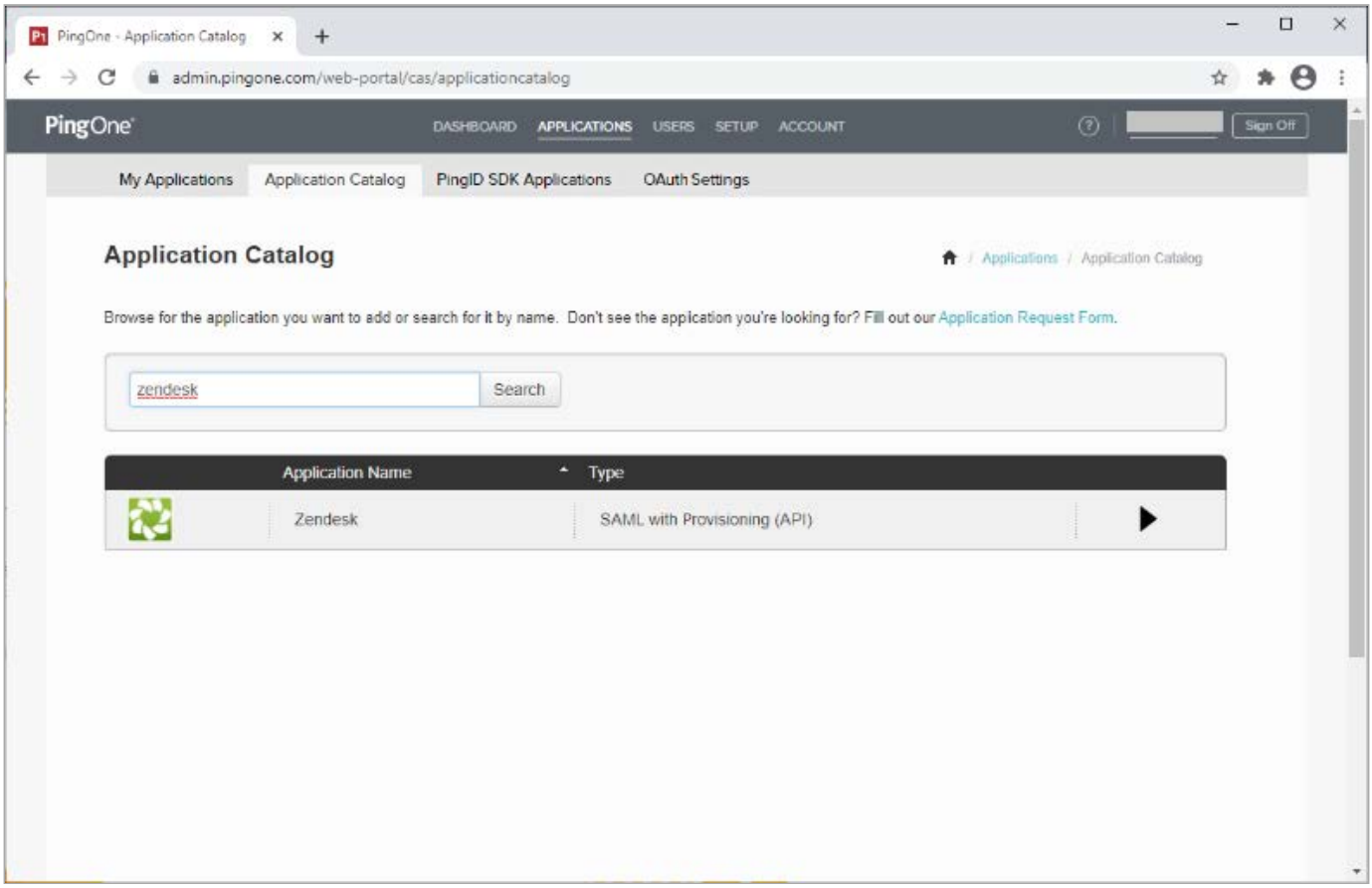
Attribute Name	Description	Required / Optional
`SAML-SUBJECT`	Email Address	Required

The following table details the references that are used within this guide that are environment specific. Replace these with the suitable value for your environment.

Reference	Description
`tenant`	Zendesk Tenant name

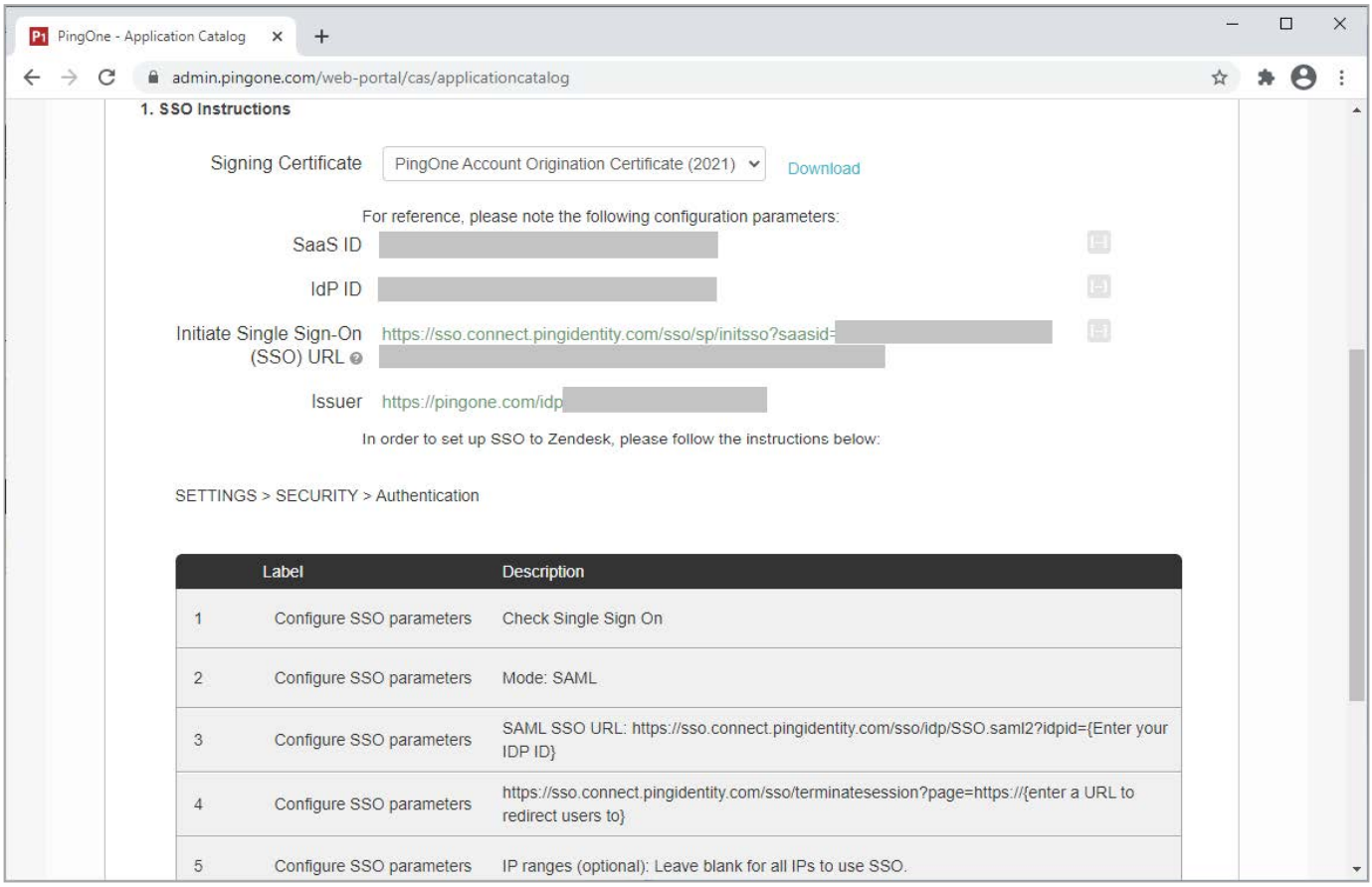
Create a PingOne Application for Zendesk

1. Sign on to PingOne for Enterprise and go to **Applications → Application Catalog**.
2. Search for `Zendesk`.
3. Click the **Zendesk** row.

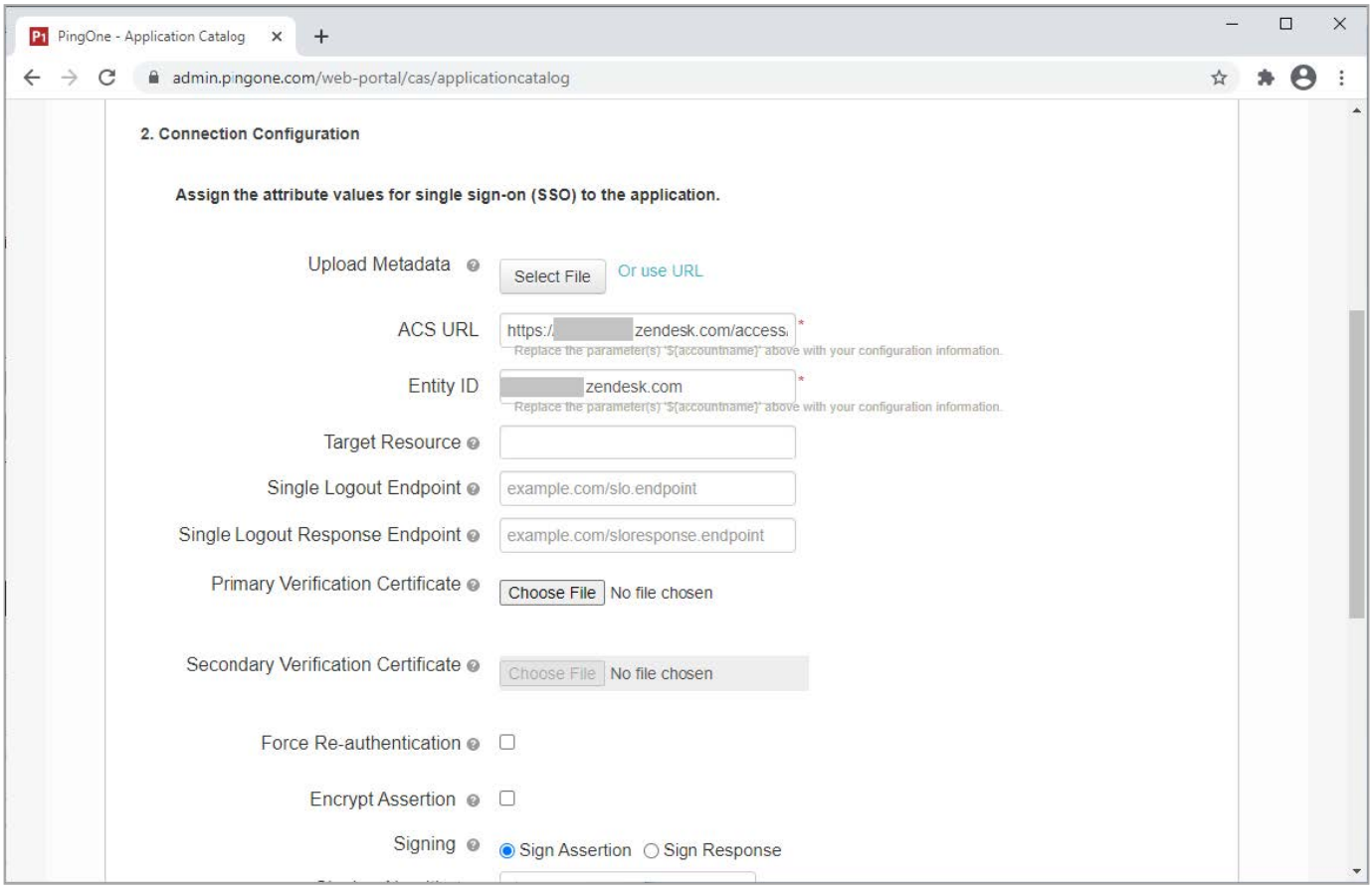


4. Click **Setup**.

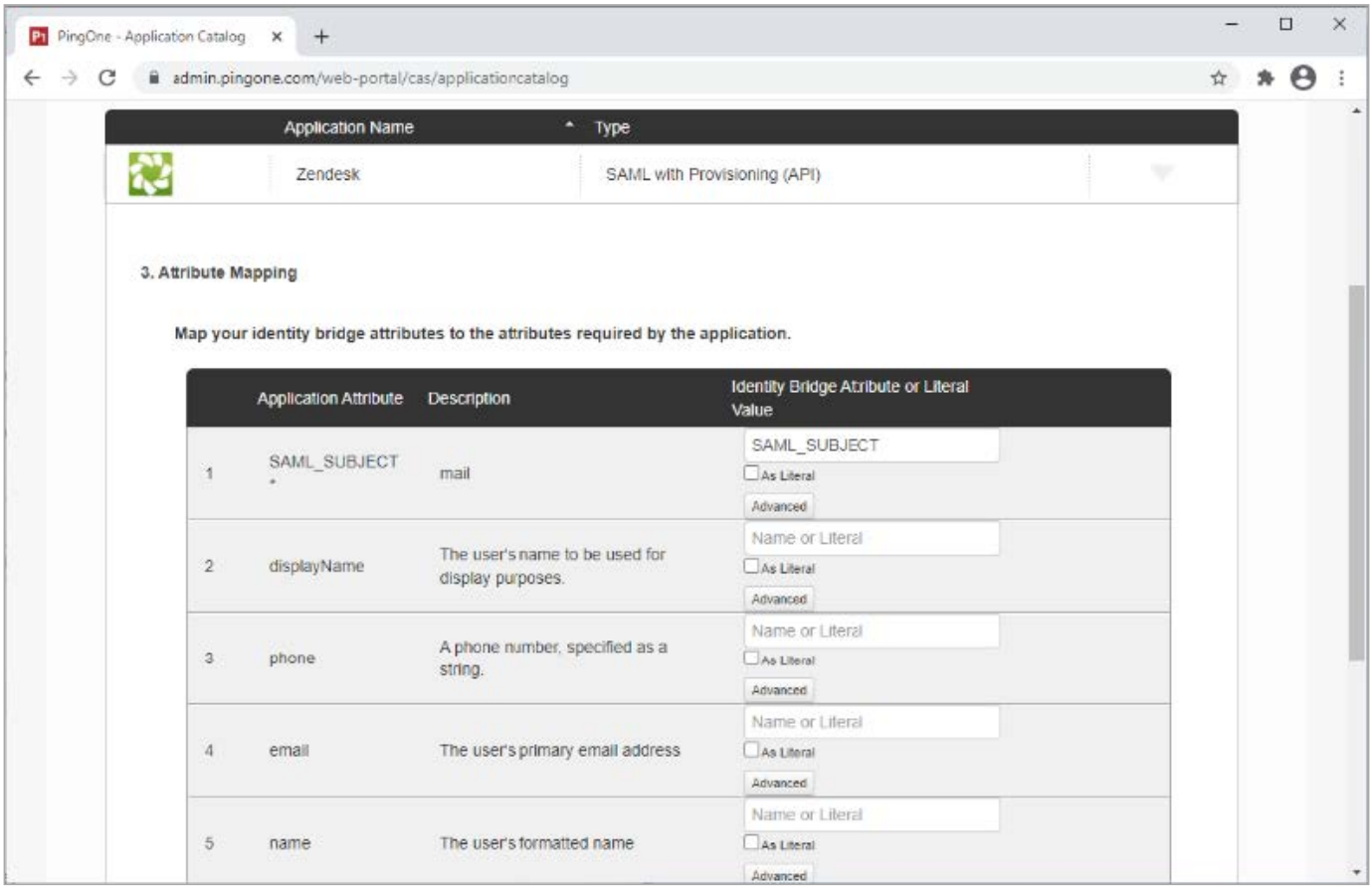
5. In the **Signing Certificate** list, select the appropriate signing certificate.



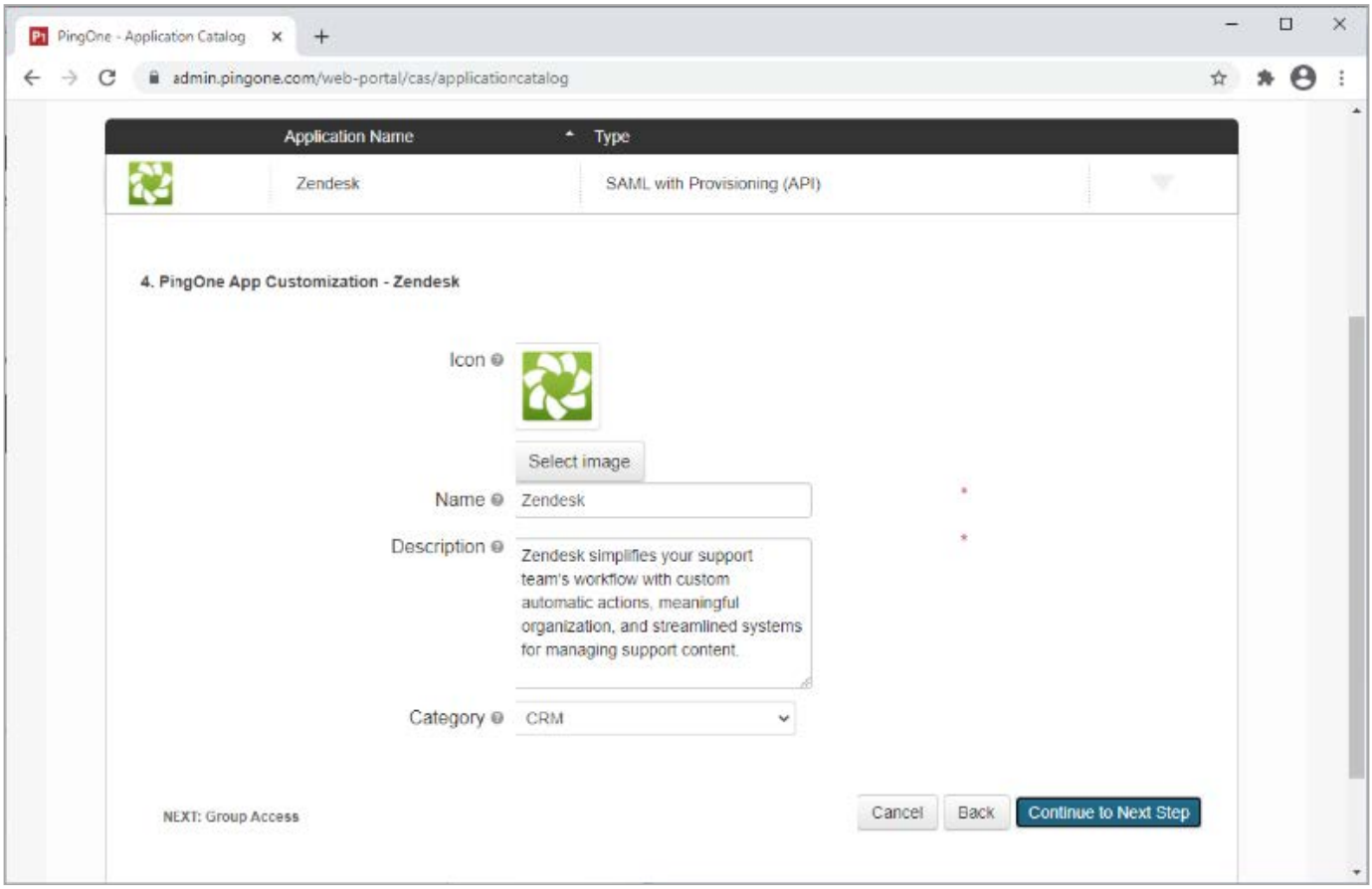
6. Review the steps, and make a note of the **PingOne SaaS ID**, **IdP ID**, **Single Sign-On URL**, and **Issuer** values shown.
7. Click **Continue to Next Step**.
8. Make sure that **ACS URL** is set to `https://tenant.zendesk.com/access/saml`.
9. Make sure that **Entity ID** is set to `https://tenant.zendesk.com`.



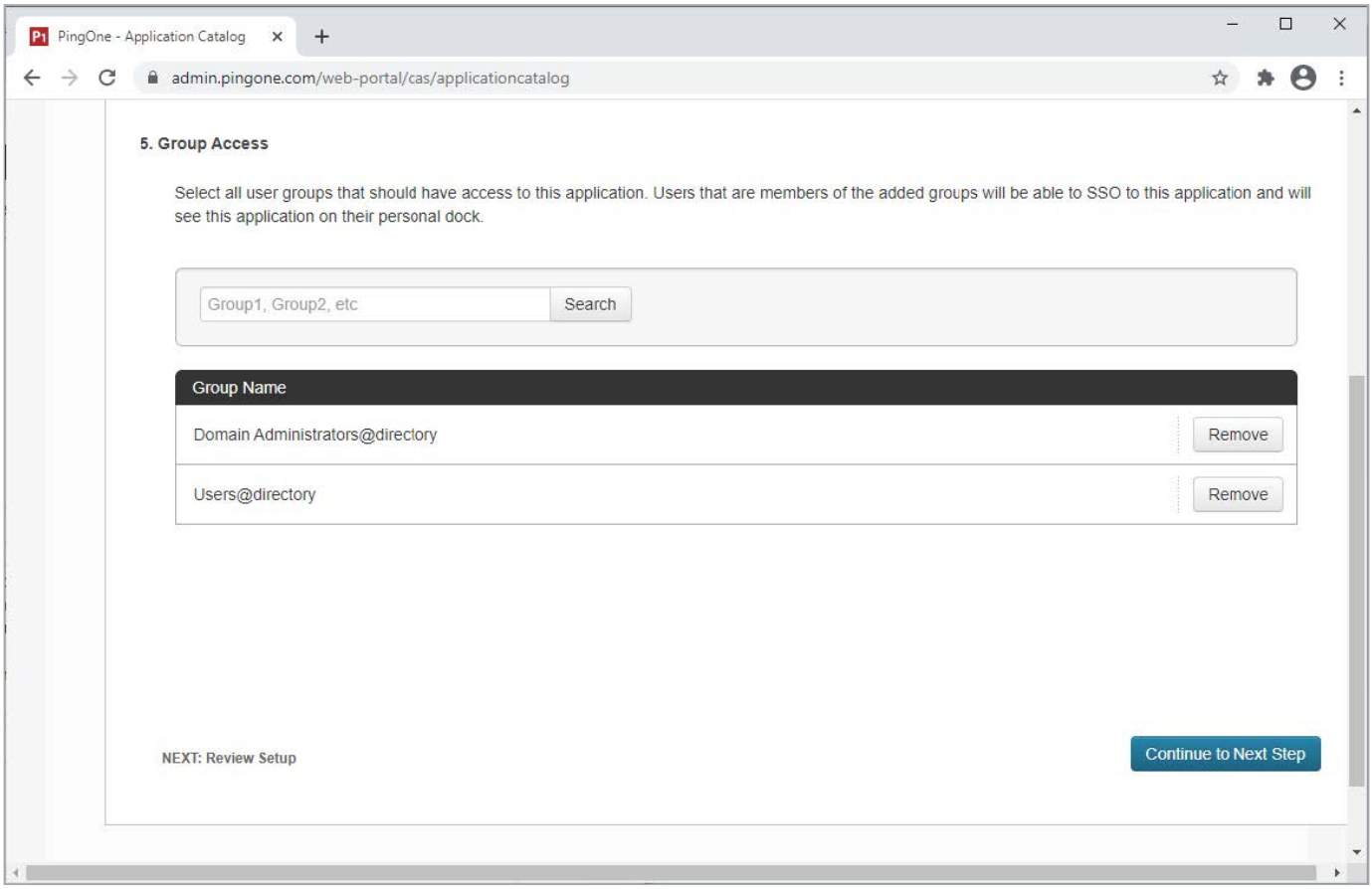
10. Click **Continue to Next Step**.
11. In the **Attribute Mapping** section, in the **Identity Bridge Attribute or Literal Value** column of the **SAML_SUBJECT**row, enter `SAML_SUBJECT`.



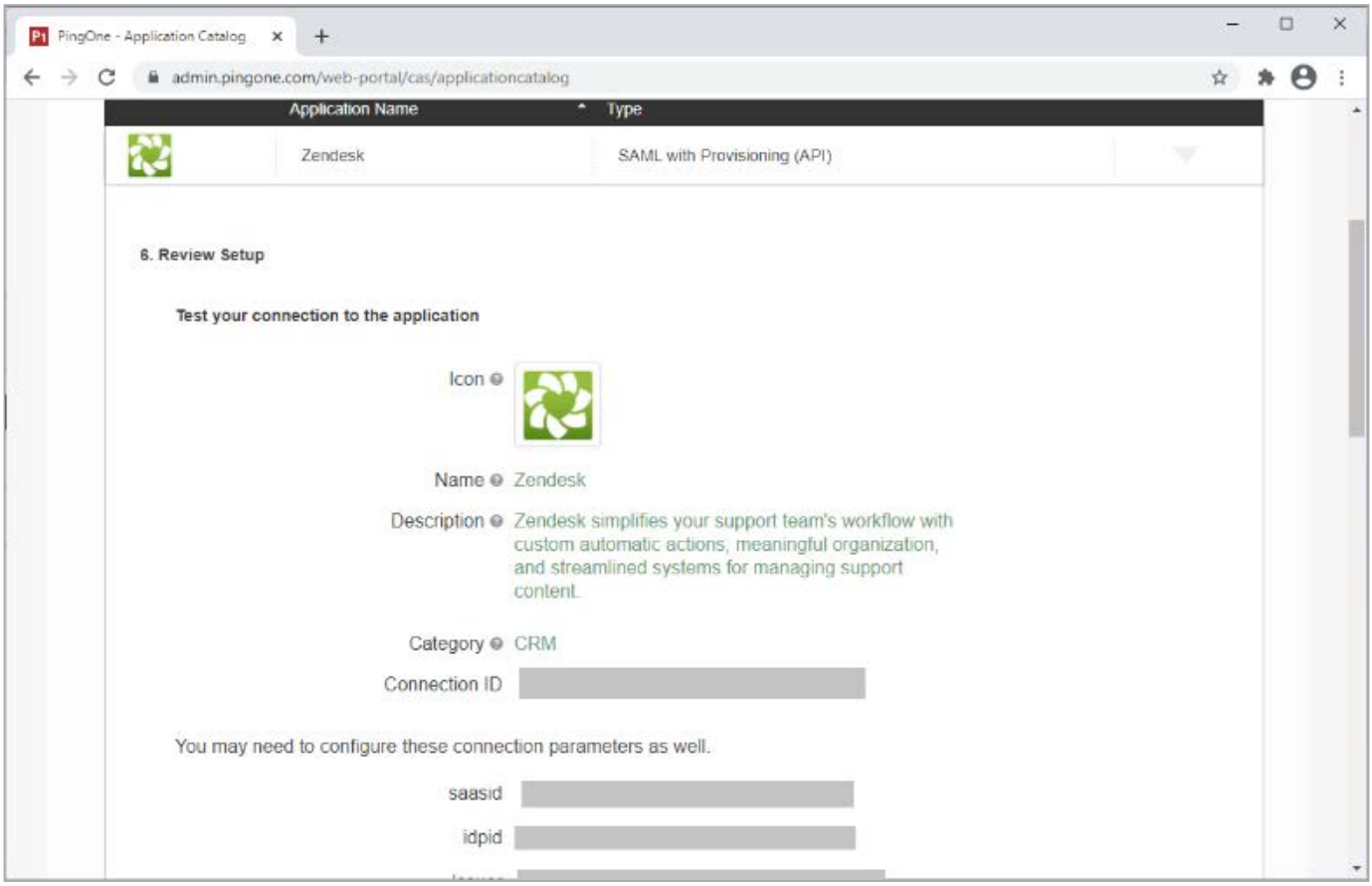
12. Enter the values for the other attributes as required.
13. Click **Continue to Next Step**.
14. Update the **Name**, **Description**, and **Category** fields as required.



15. Click **Continue to Next Step**.
16. Add the user groups for the application.



17. Click **Continue to Next Step**.
18. Review the settings.



19. Copy the **Single Sign-On (SSO) URL** value to a temporary location.

    This is the IdP-initiated SSO URL that you can use for testing.

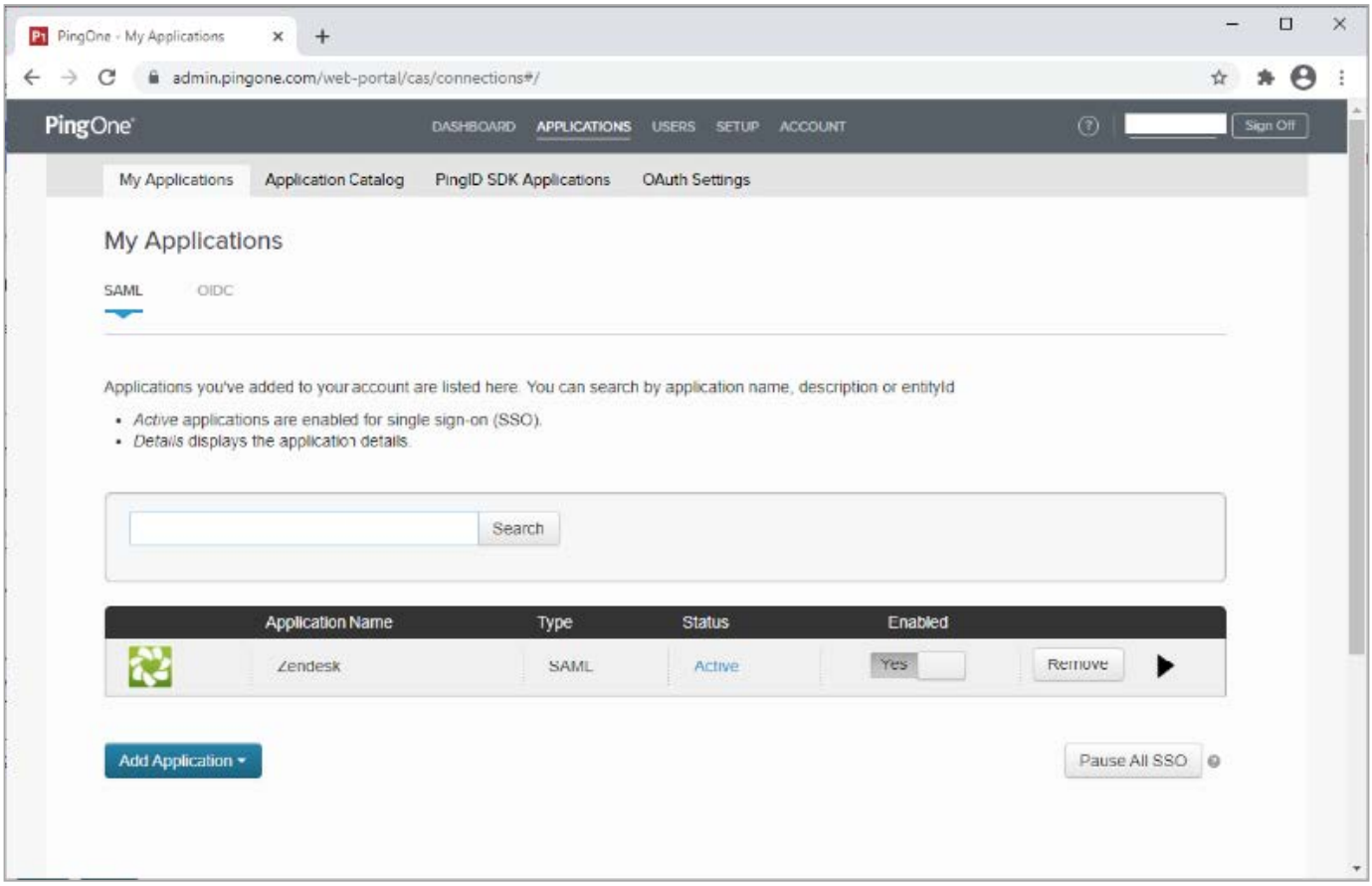
    1. On the **Signing Certificate** line, click **Download**.

       You'll use this in the Zendesk configuration.

20. On the **SAML Metadata** line, click **Download**.

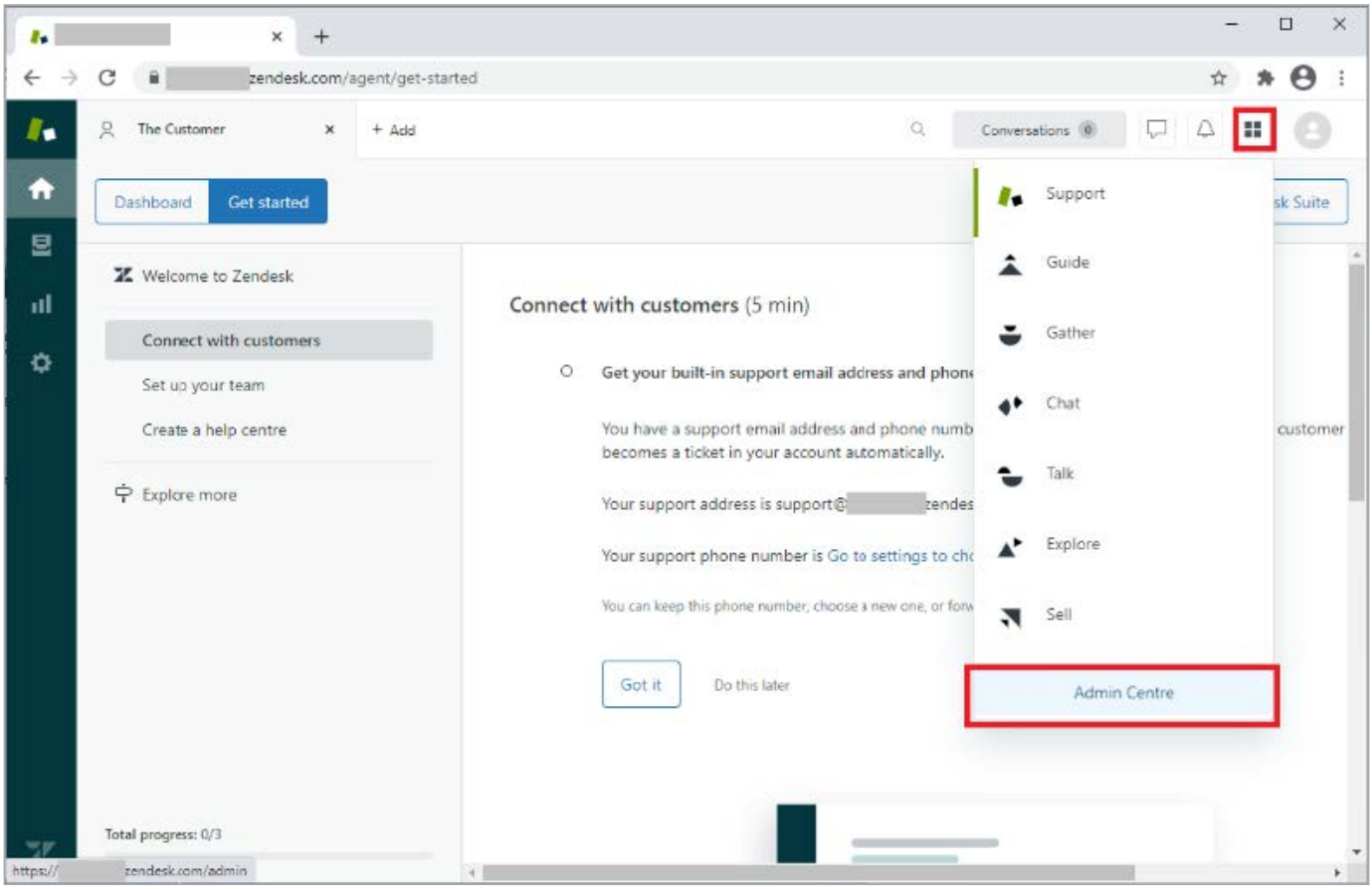
    You'll use this in the Zendesk configuration.

21. Click **Finish**.

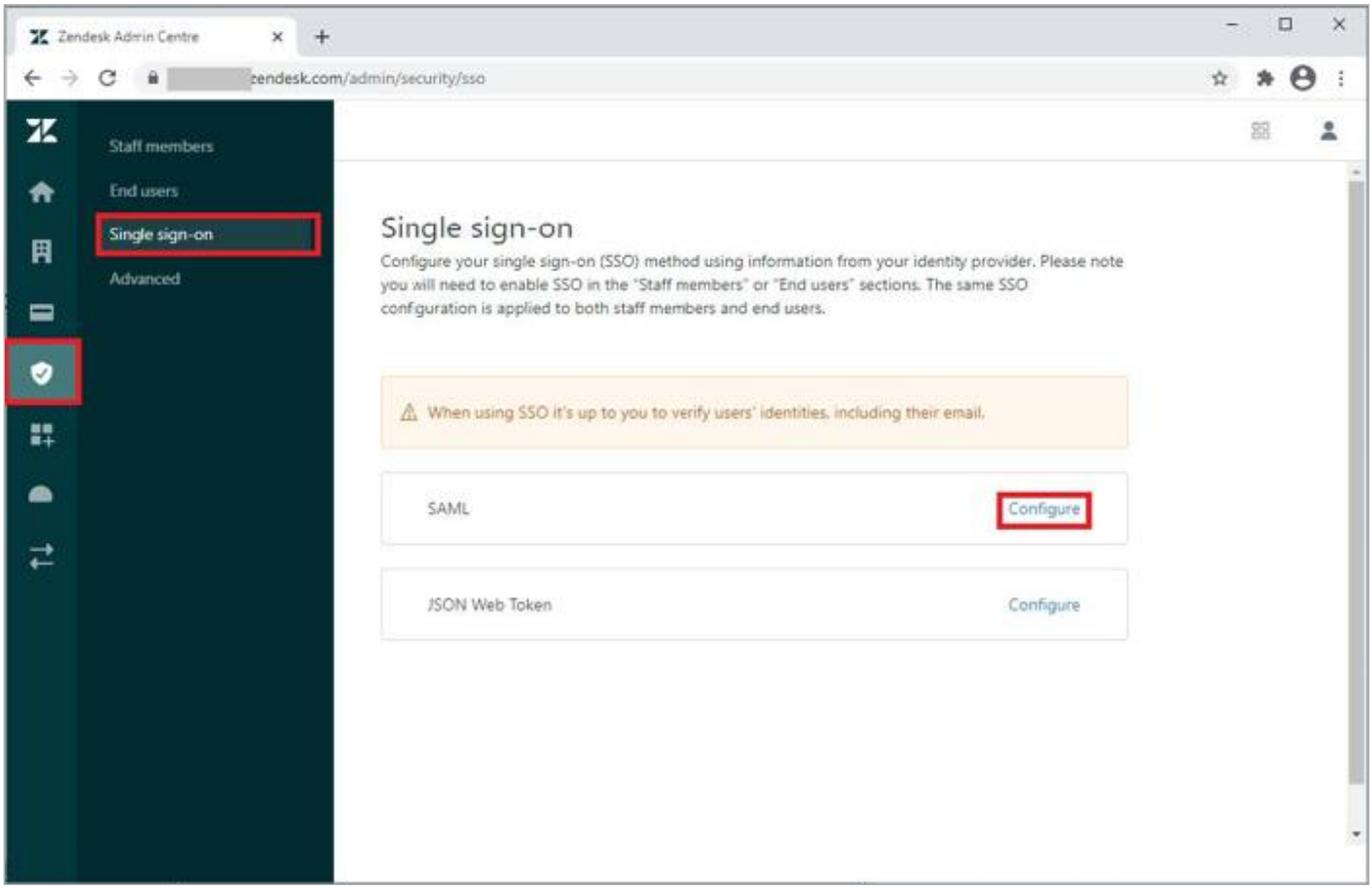


Configure the PingOne IdP connection for Zendesk

1. Sign on to Zendesk as an administrator.
2. Click the **Products** icon.
3. Click **Admin Centre**.



4. Click the **Security** icon.

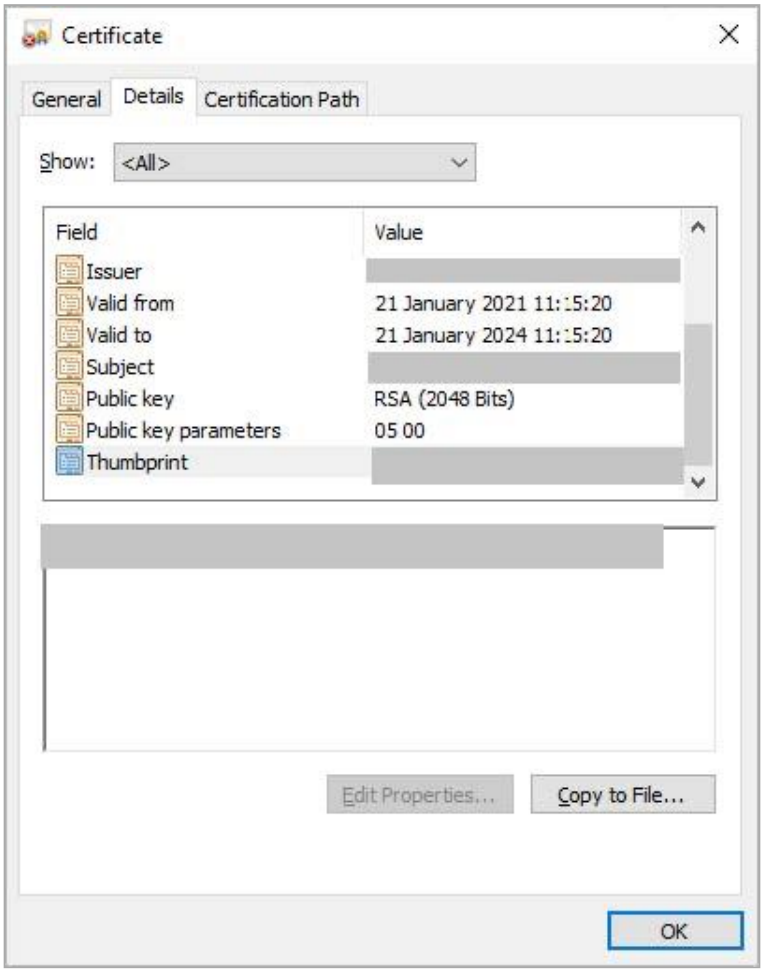


5. Click **Single sign-on**.
6. In the **SSO Login URL** field, enter the URL Location for the **SingleSignOnService Location** from the PingOne SP metadata that you downloaded from the Zendesk configuration.

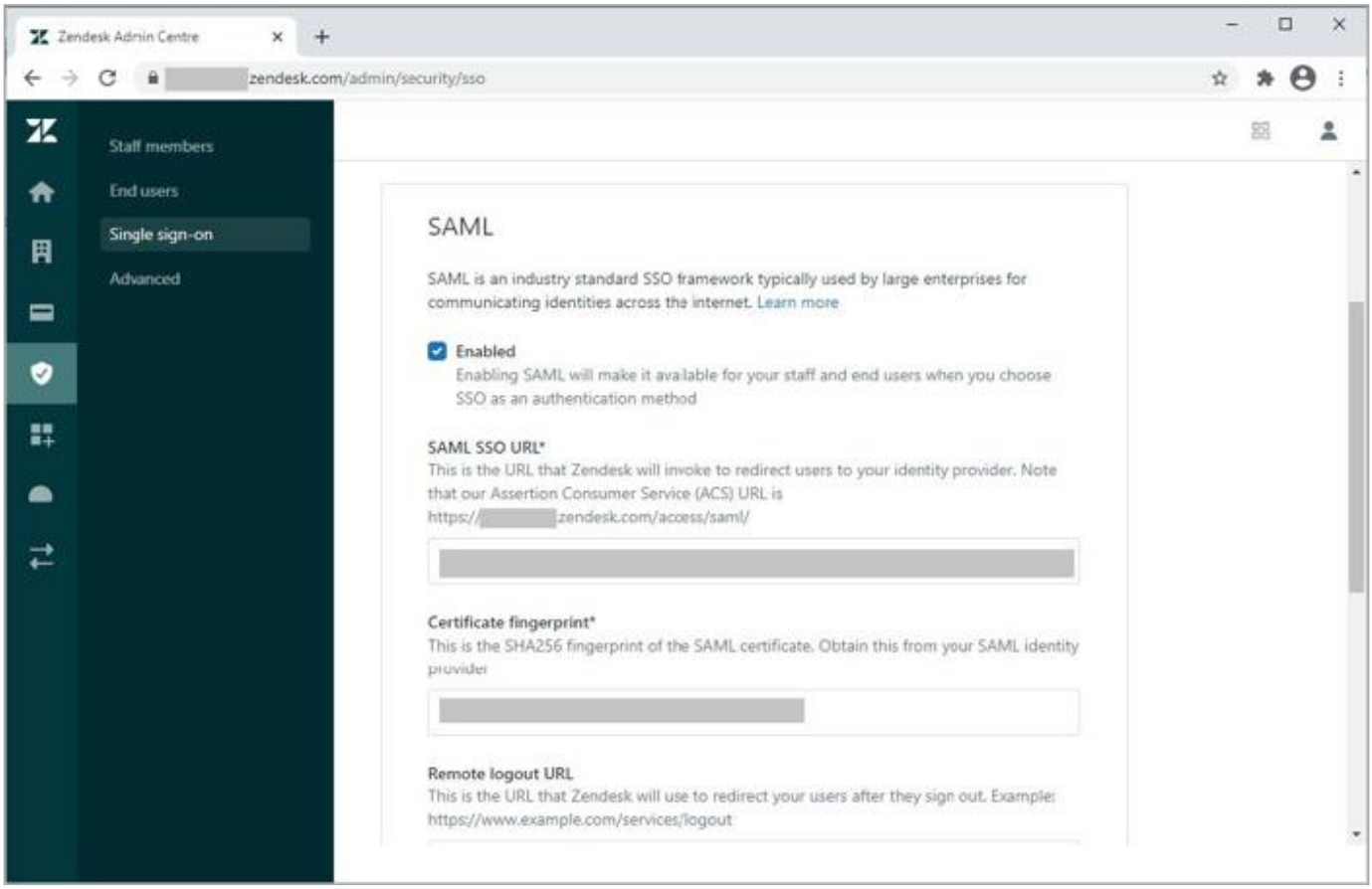
   For example:

   ```
   https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=idpid
   ```

7. Open the signing certificate that you downloaded in the PingOne SP configuration and paste the thumbprint into the **Certificate fingerprint** section.



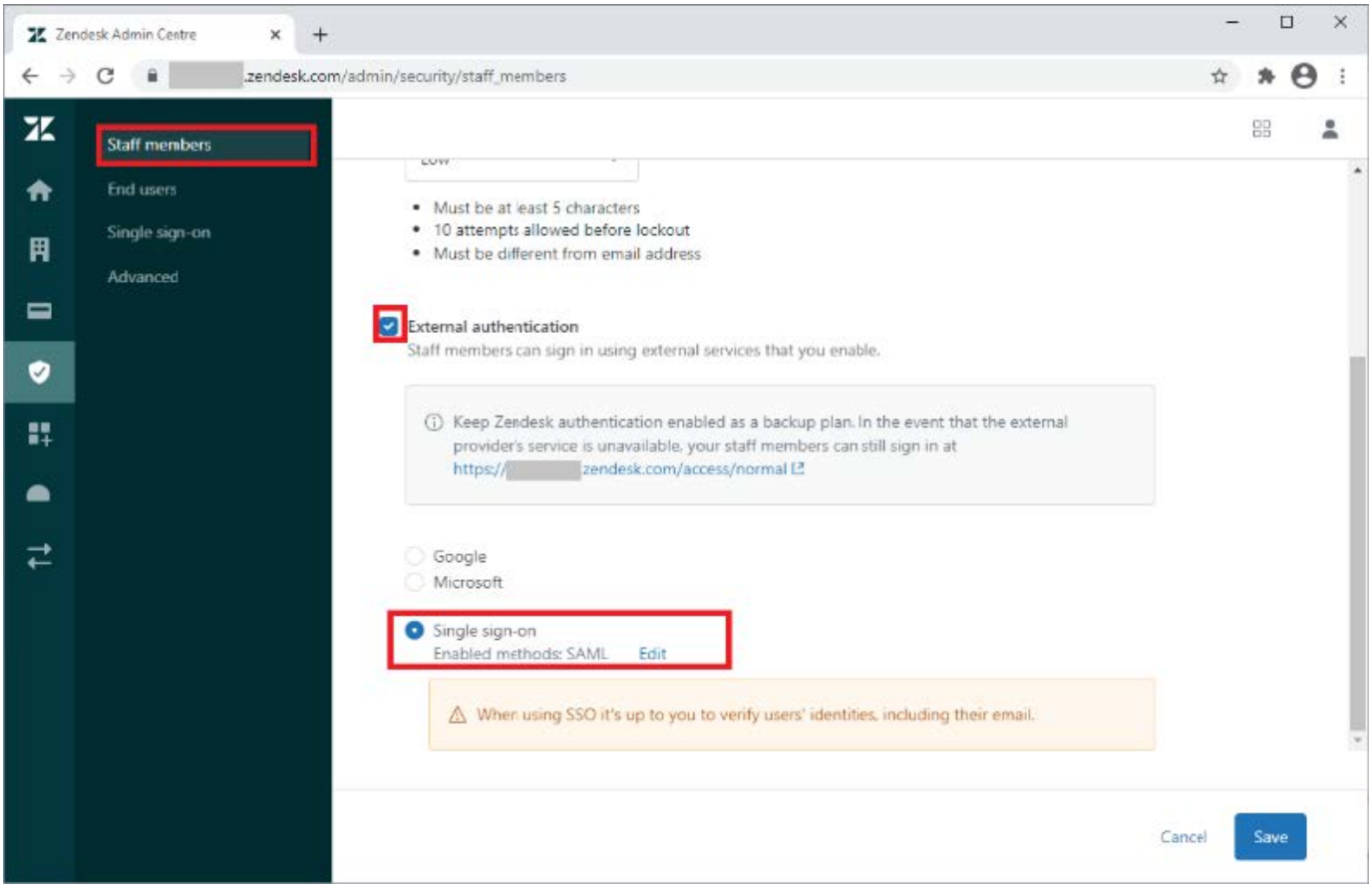
8. Click **Enabled**.



9. Click **Save**.
10. Enable external authentication for **Staff members** or **End users** as required.

> **Note**
>
> The following example enables it for **Staff members** only.

   - Click the **Security** icon.
   - Click **Staff members**.
   - Select the **External Authentication** check box.
   - Click **Single sign-on**. + Click **Save**.



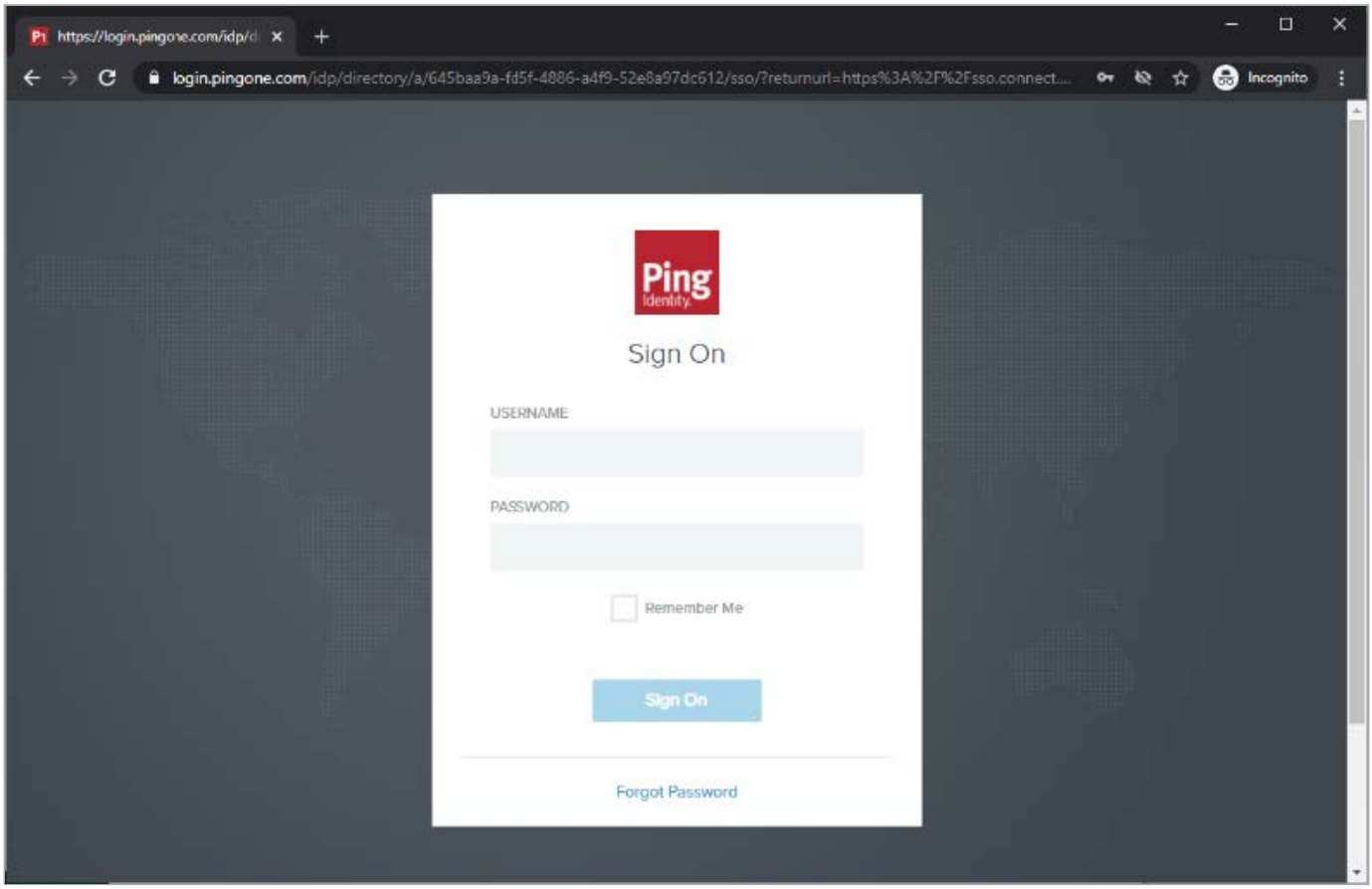
Test the integration

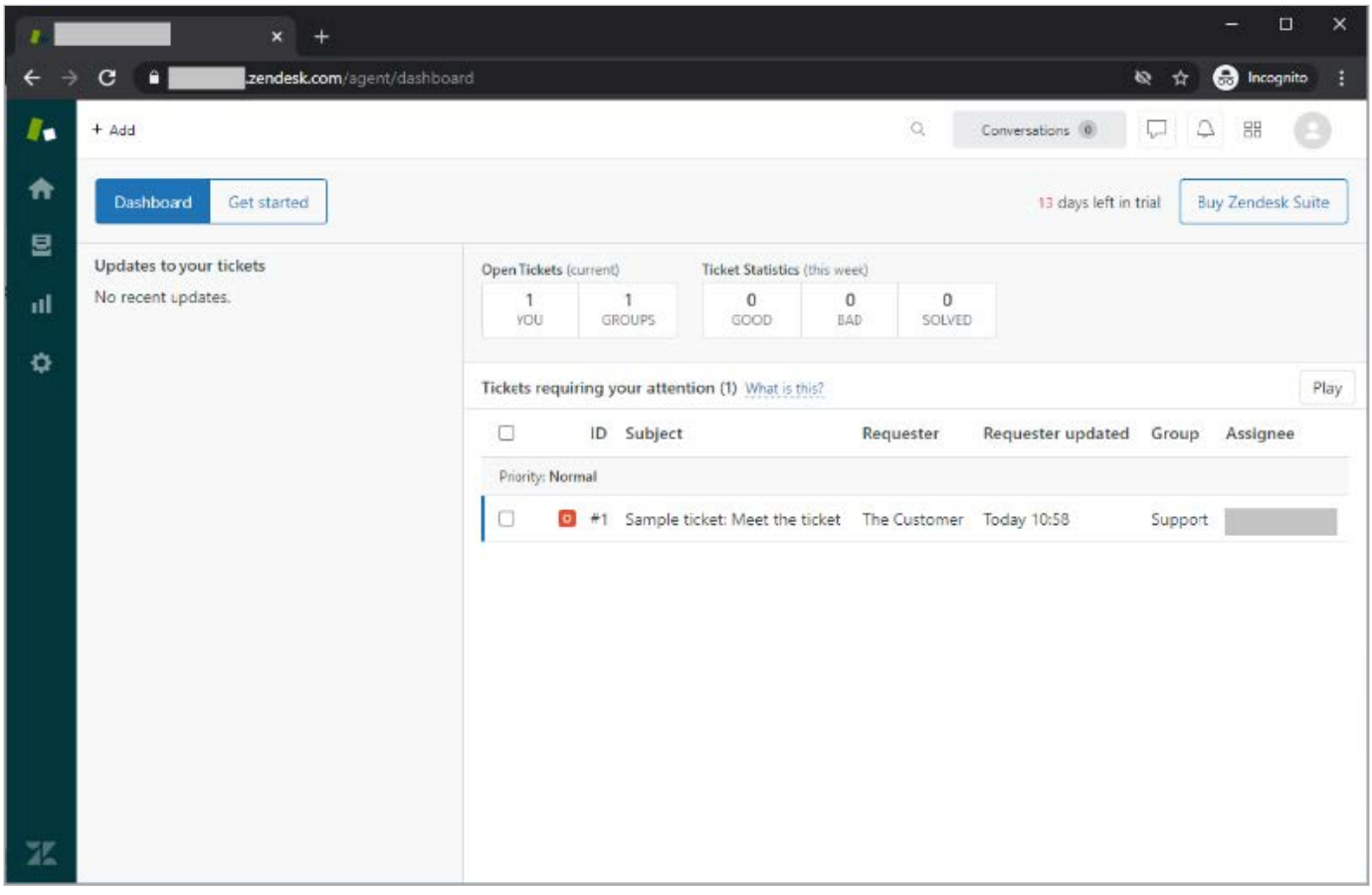
Choose from:

For PingFederate IdP-Initiated SSO

Go to the **Single Sign-On (SSO) URL** in the PingOne Application configuration to perform IdP initiated SSO.

For example, `https://PingFederateHostname:PingFederatePort__/idp/startSSO.ping?PartnerSpId=Zendesk`.



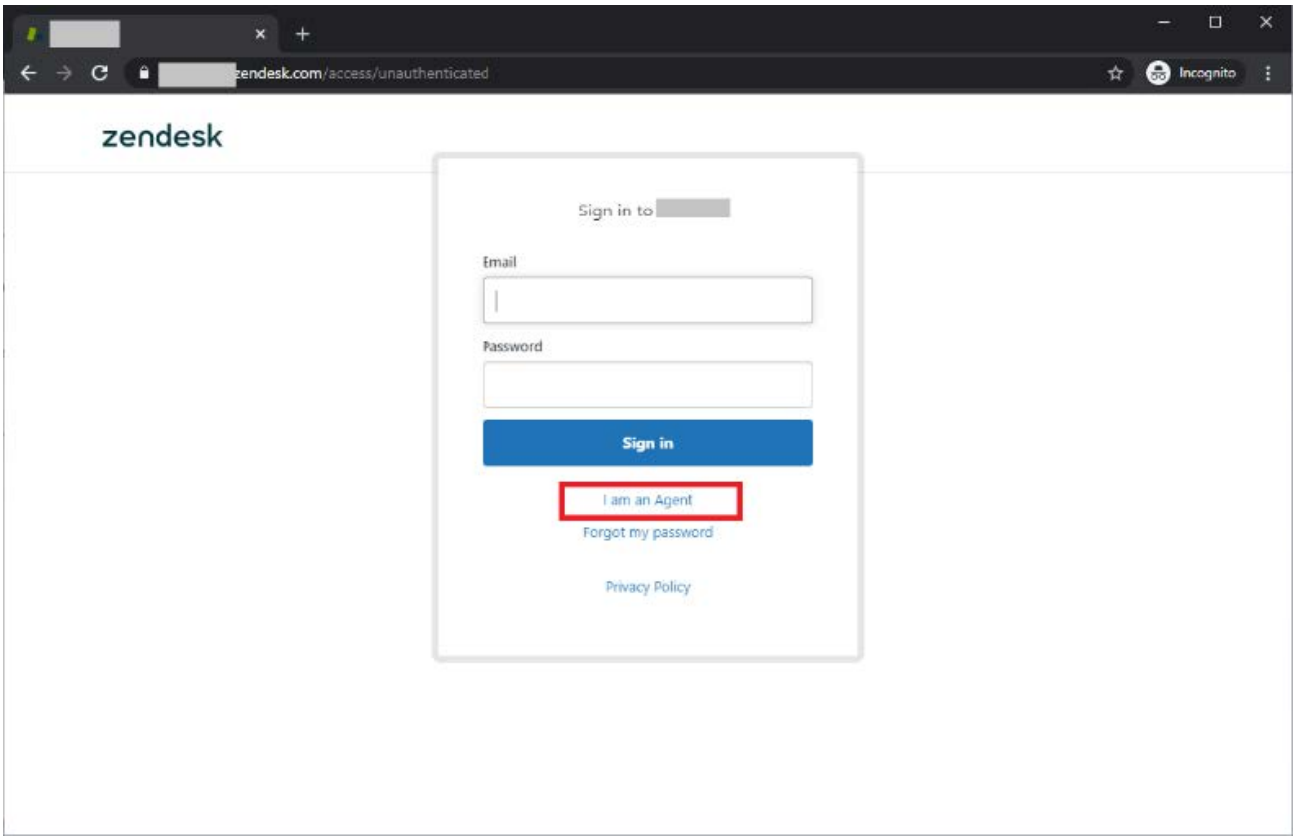


For PingOne SP Initiated SSO

1. Go to the URL for your Zendesk tenant. For example, `https://tenant.zendesk.com`.

> **Note**
>
> Because SSO is only enabled for Staff, you should see a sign on form.

2. Click **I am an Agent** to initiate SSO.



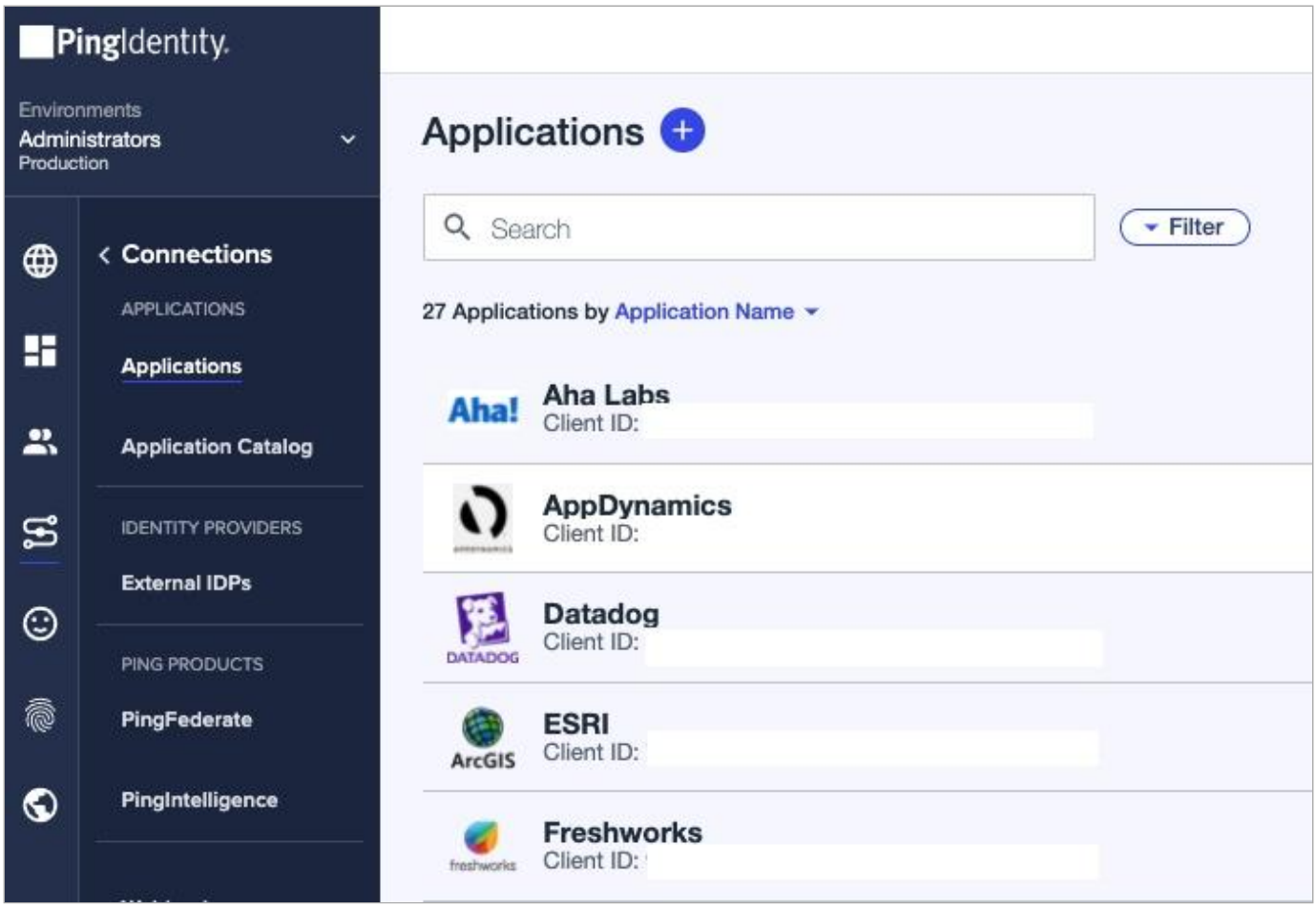
Zoho

Configuring SAML SSO with Zoho and PingOne

Learn how to configure SAML SSO using Zoho and PingOne.

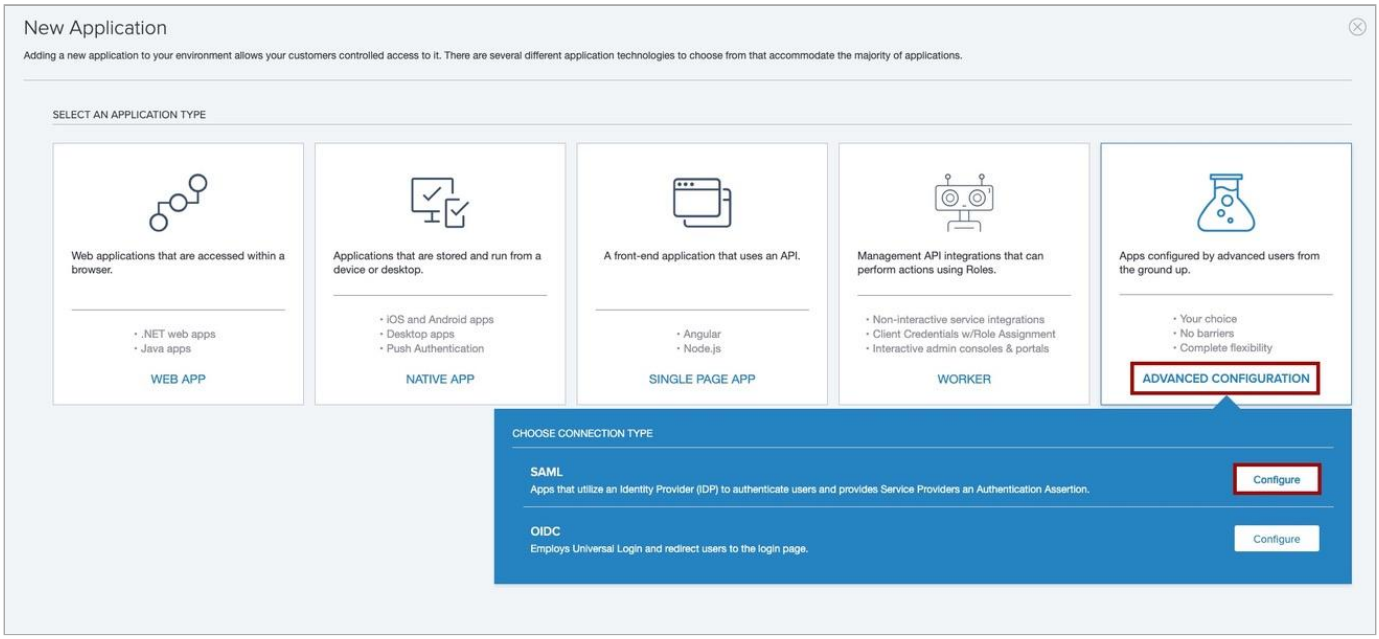
Configue SAML in PingOne

1. In PingOne, go to **Connections → Applications** and click the + icon.

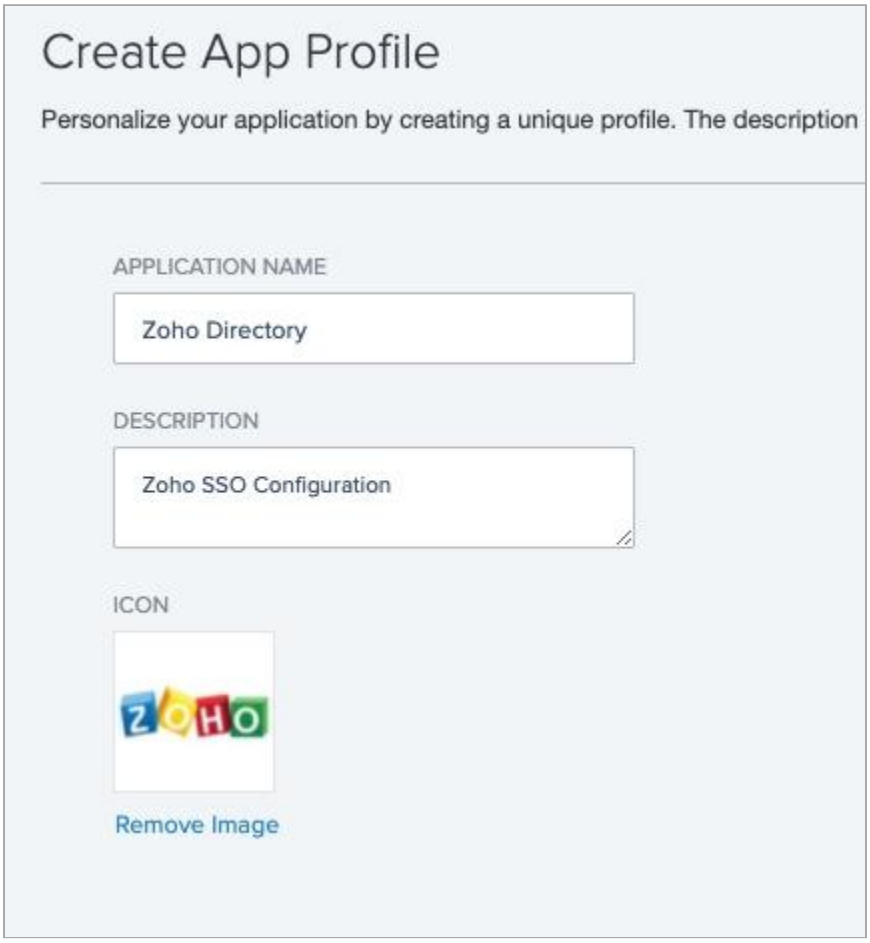


2. On the **New Application** page, click **Advanced Configuration**.

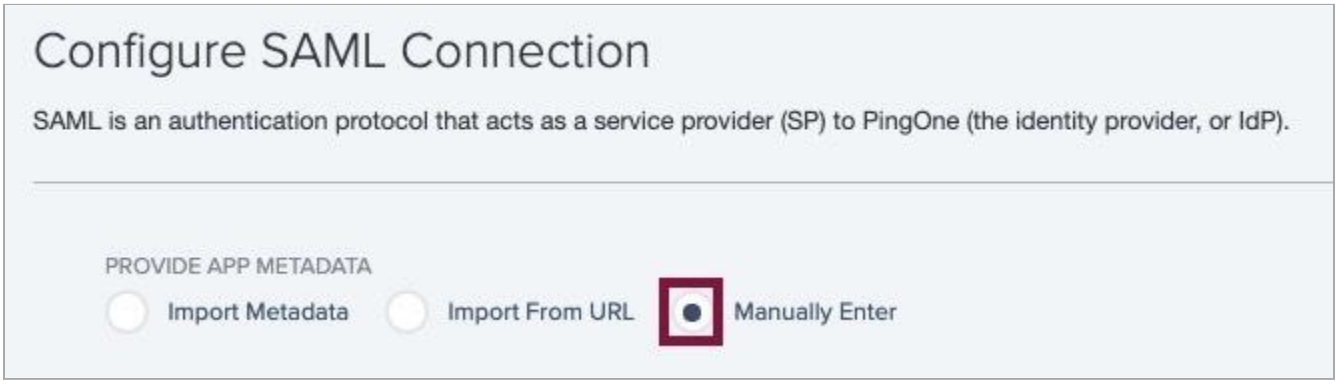
3. On the **SAML** line, click **Configure**.



4. On the **Create App Profile** page, enter the following details:
    - **Application Name** (Required)
    - **Description** (Optional)
    - **Icon** (Optional)

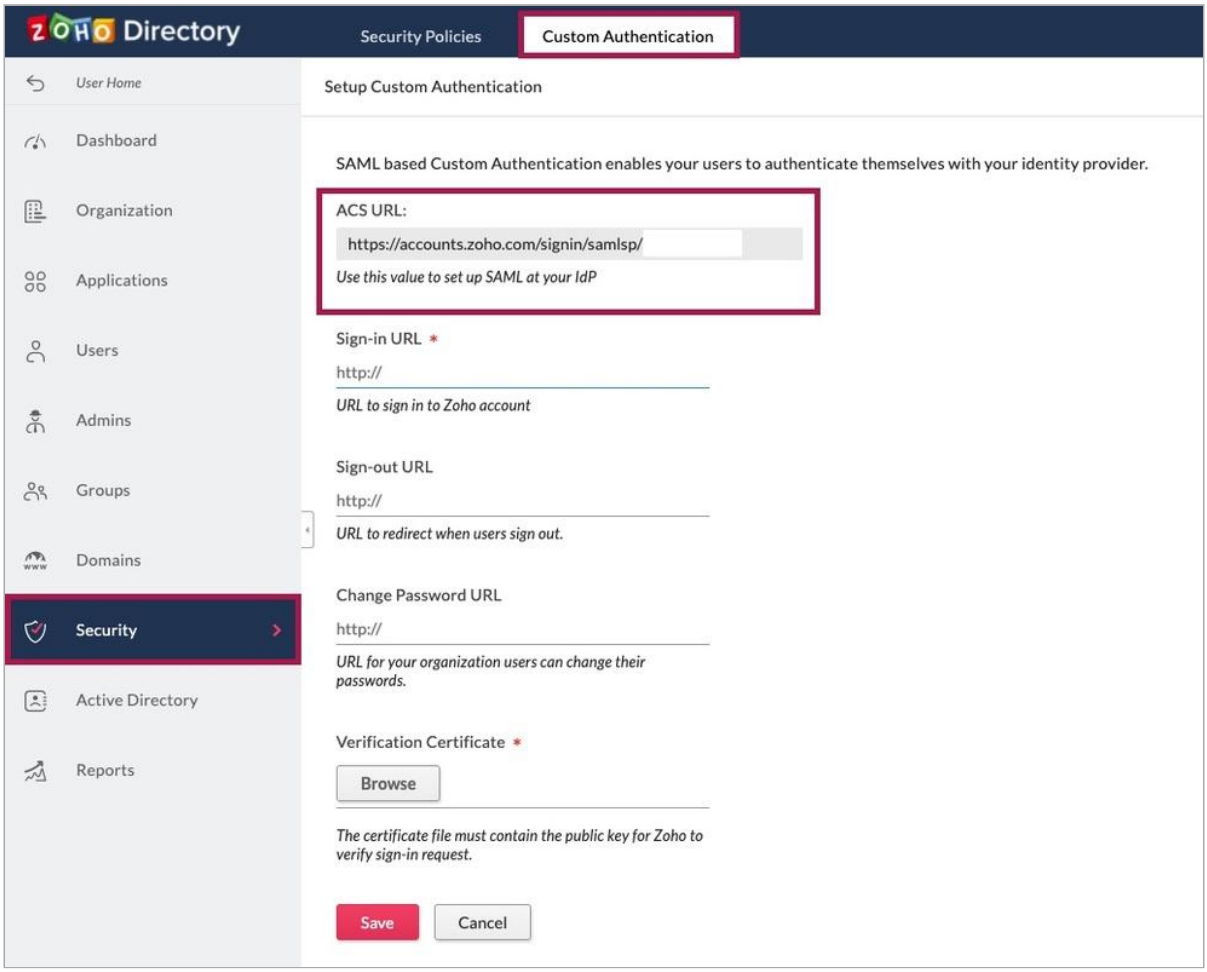


5. Click **Save and Continue**.
6. On the **Configure SAML Connection** page, in the **Provide App Metadata** section, select **Manually Enter**.



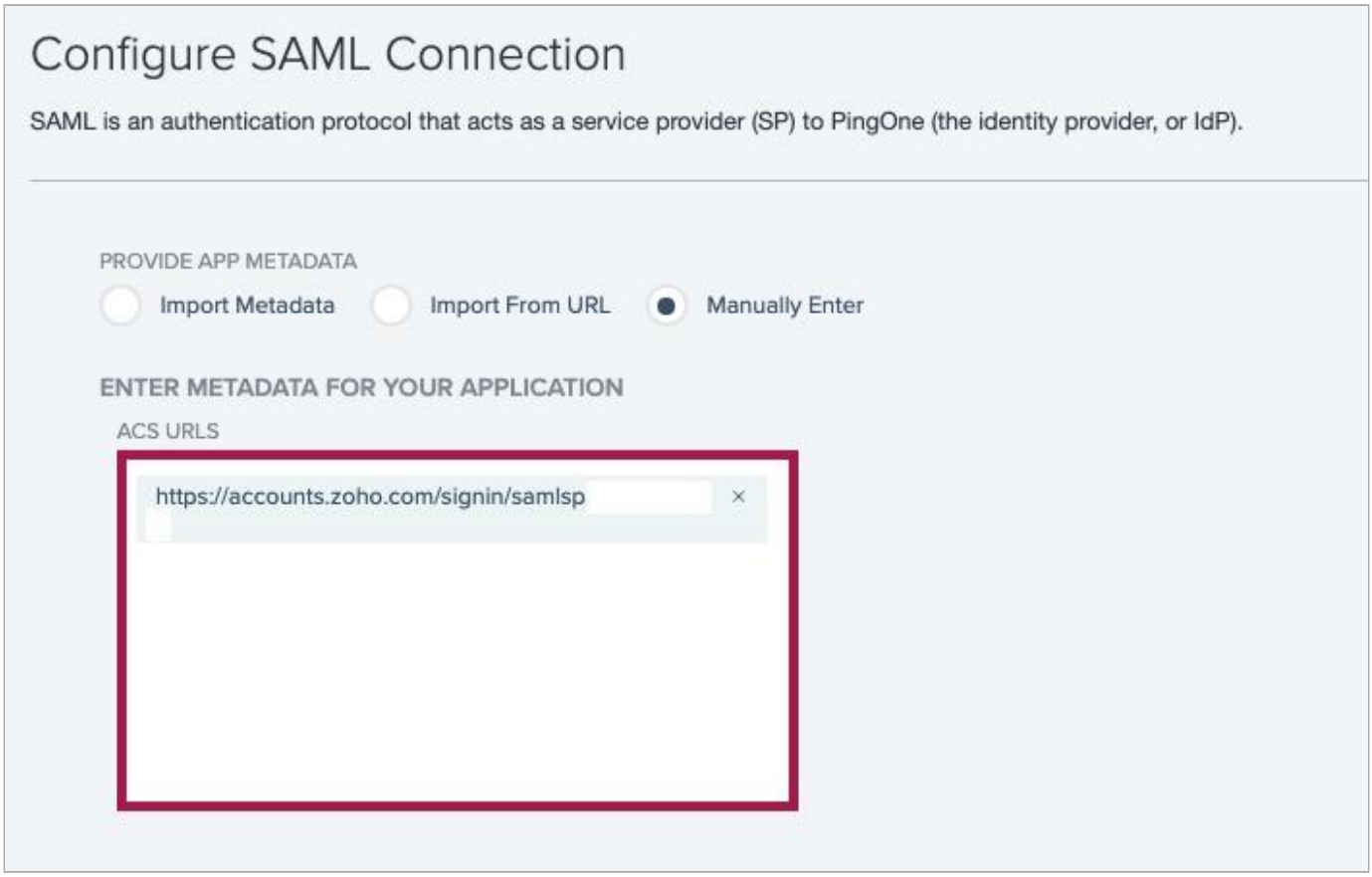
Set up SAML in Zoho

1. In a separate browser tab, sign on to your Zoho Directory admin account (directory.zoho.com).
2. Go to **Security → Custom Authentication**, select **Setup Now**, and note the **ACS URL** value.



3. Copy the **ACS URL** value from the previous step.

4. Go to your PingOne SSO browser tab and paste this value into the **ACS URLS** field.



Input the service provider (SP) data

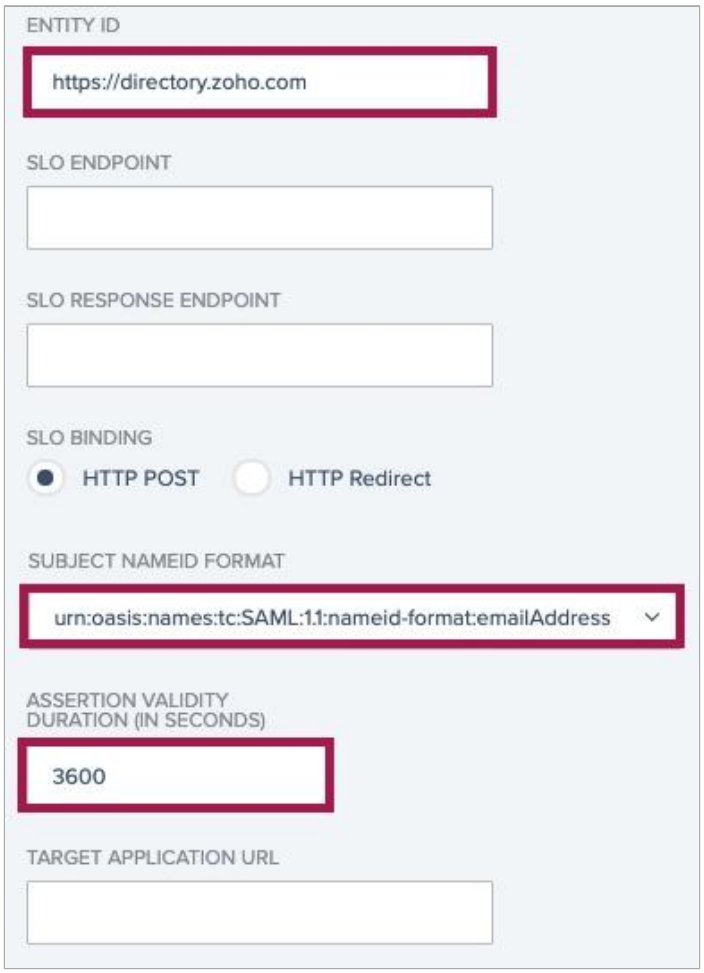
1. Enter the **ENTITY ID** in PingOne.

> **Note**
>
> This configuration example uses `https://directory.zoho.com`. Refer to the following table for instructions on which Entity ID to use, based on your location.

Zoho Directory account DC	Identifier (Entity ID)	Relay state
US	zoho.com	https://directory.zoho.com
EU	zoho.eu	https://directory.zoho.eu
IN	zoho.in	https://directory.zoho.in
AU	zoho.com.au	https://directory.zoho.com.au
CN	zoho.com.cn	https://directory.zoho.com.cn

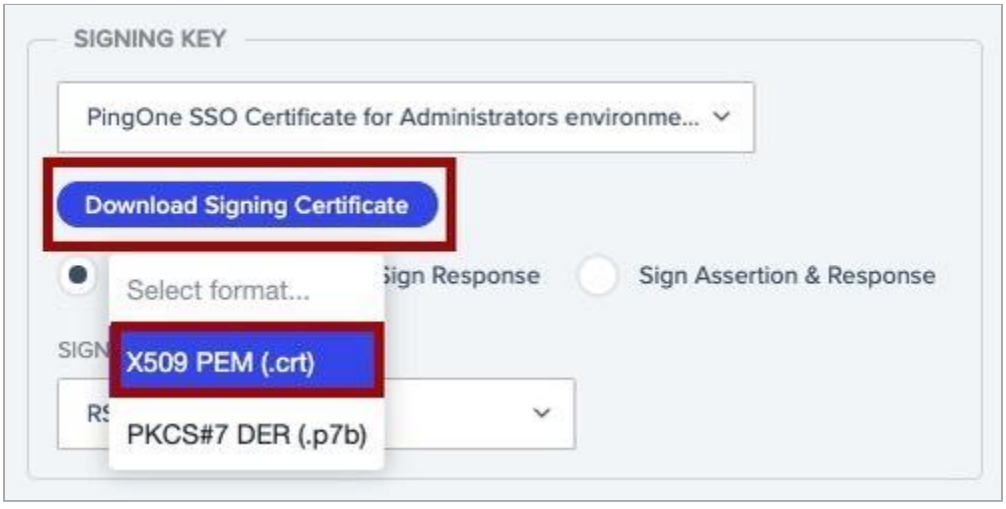
2. Update the **SUBJECT NAMEID FORMAT** to **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.

3. In the **Assertion Validity Duration (In Seconds)** field, enter a value, for example `3600`.



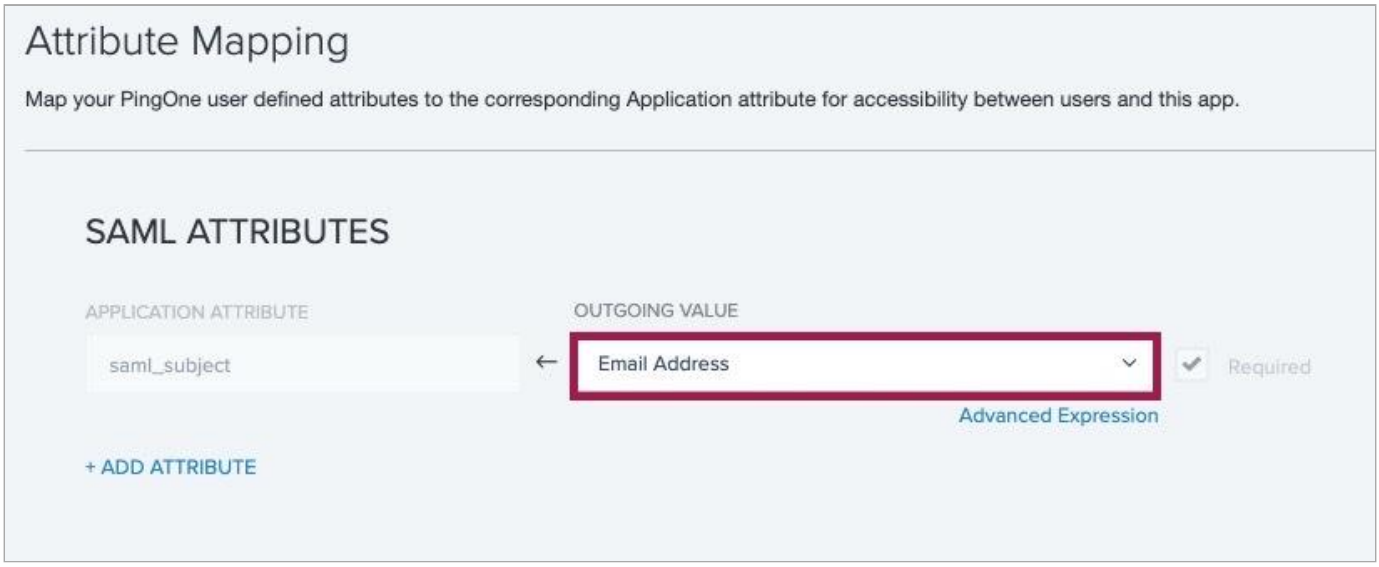
4. In the **Signing Key**, click **Download Signing Certificate** and select **X509 PEM (.crt)**for the format.

   You'll need the signing certificate later.

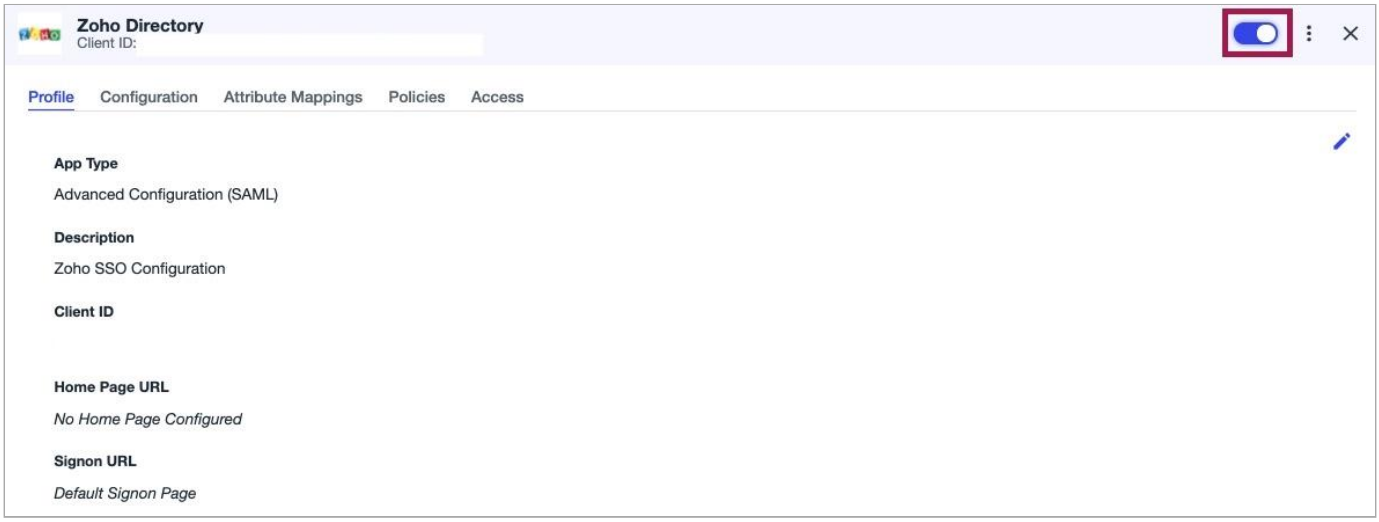


5. On the **Attribute Mapping** tab, in the **SAML Attributes** section, map the **Outgoing Value** for **saml_subject** to **Email Address**.

> **Note**
>
> This is the only required attribute for a successful connection.

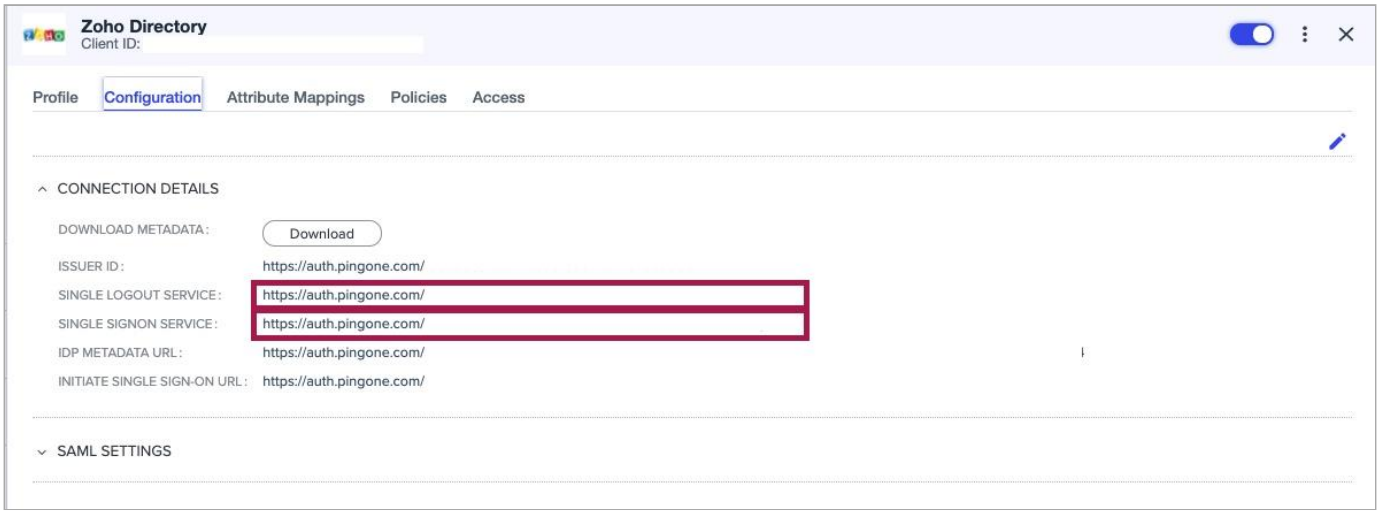


6. Click **Save and Close**.
7. On the **Applications** page, next to **Zoho Directory**, click the toggle to enable the connection.



8. On the **Configuration** tab, in the **Configuration Details** section, note the **Single Logout Service** and **Single SignOn Service** values.

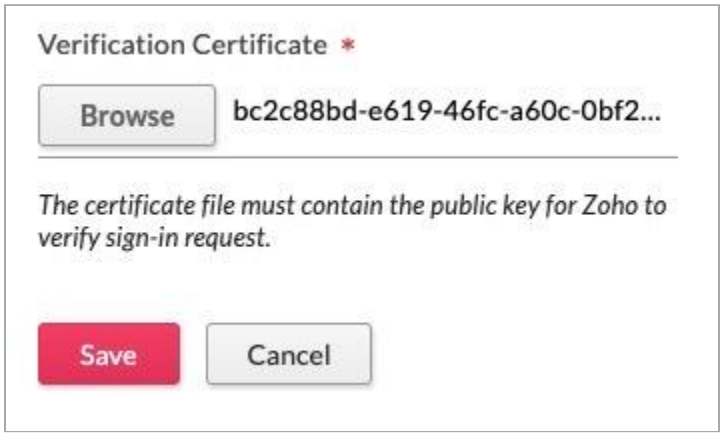
   You'll need these to complete the next procedure.



Configure Zoho for SSO

1. In Zoho, on the **Custom Authentication** page, paste the **Single SignOn Service** value from PingOne into the **Sign-in URL**.
2. **Optional:** Paste the **Single Logout Service** value from PingOne into the **Sign-out URL** field.

3. **Optional:** If required, enter your site's password change URL in the **Change Password URL** field.
4. In the **Verification Certificate** section, click **Browse** and upload the X509 certificate that you downloaded previously.

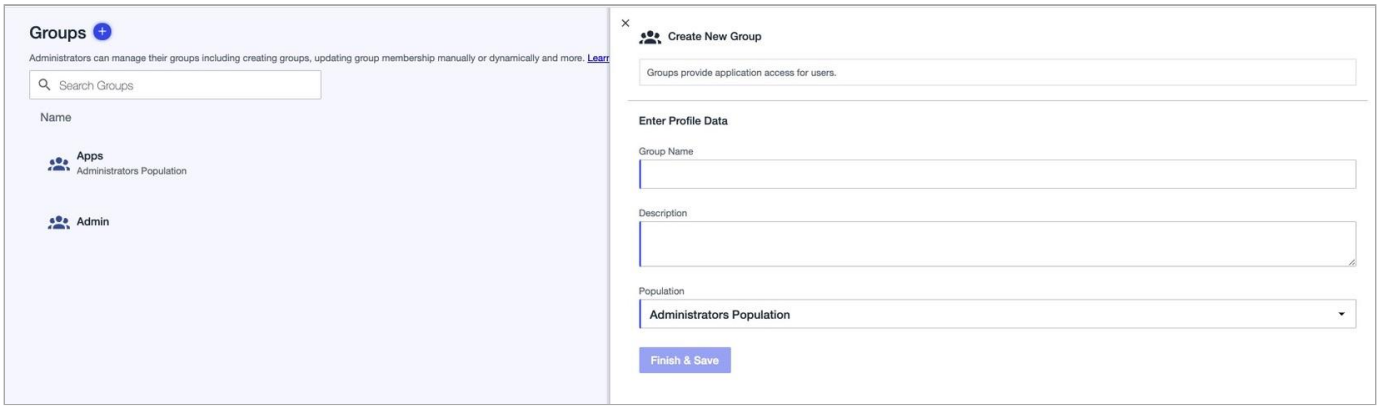


5. Click **Save** to save the connection and complete the setup.

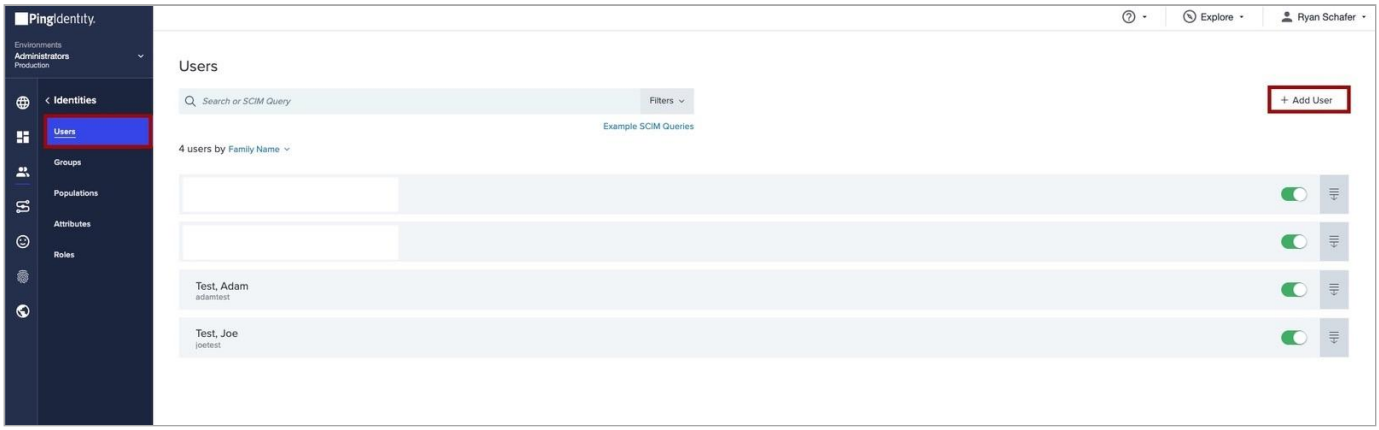
Create and assign identities in PingOne

If you've already assigned identities and groups in PingOne, move on to Test the integration.

1. In PingOne, go to **Identities Groups** and click the **+** icon next to **Groups**.
2. On the **Create New Group** page, enter values for the following:
    - **Group Name** (Required)
    - **Description** (Optional)
    - **Population** (Optional)
3. Click **Finish & Save**.



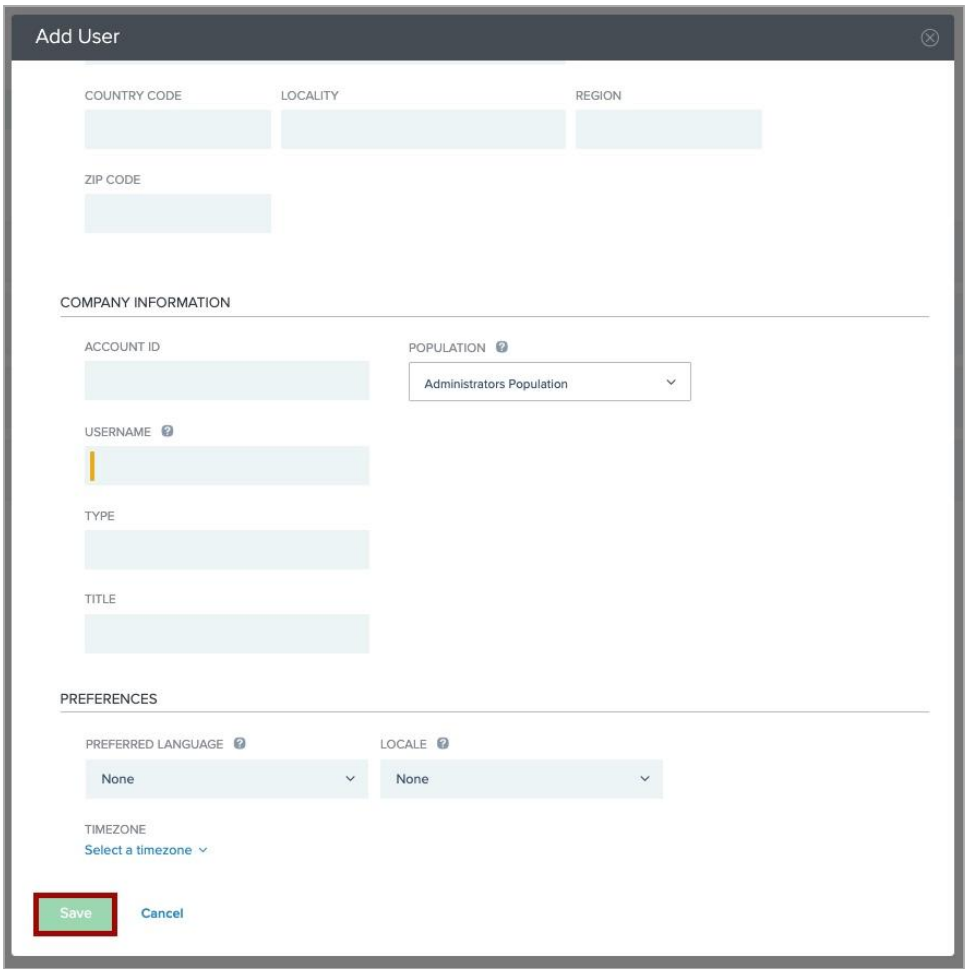
4. To add identities to the group, on the **Identities** tab, go to **Users → + Add User**.



5. On the **Add User** page, enter the required information for a user.

> **Important**
>
> Verify that the email address is correct, as this is the value passed in the SAML assertion.

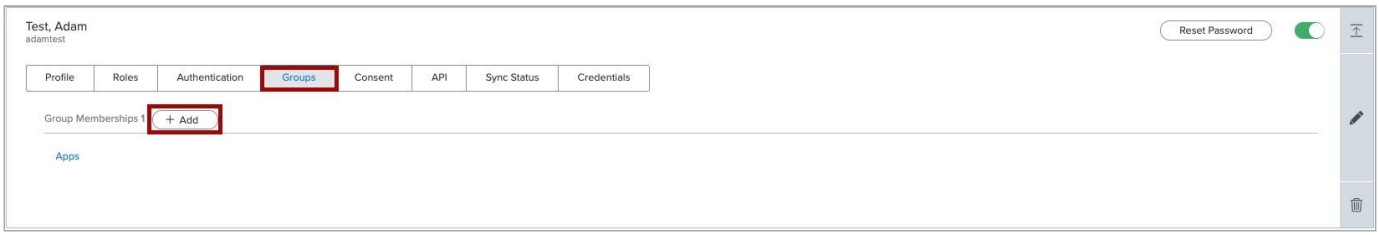
6. Click **Save**.



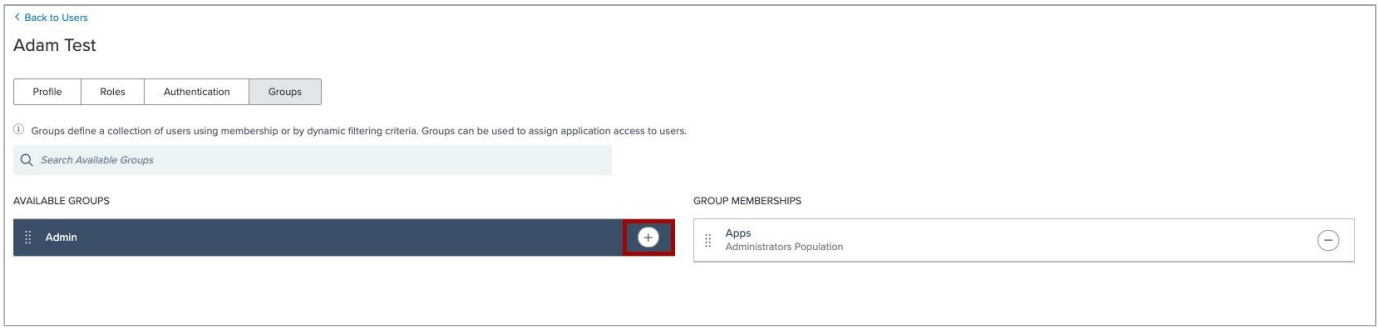
7. Assign the user that you created to the group that you created previously. Locate the user and do the following:

    1. Expand their section.

2. Select the **Groups** tab.
3. Click **+ Add**.

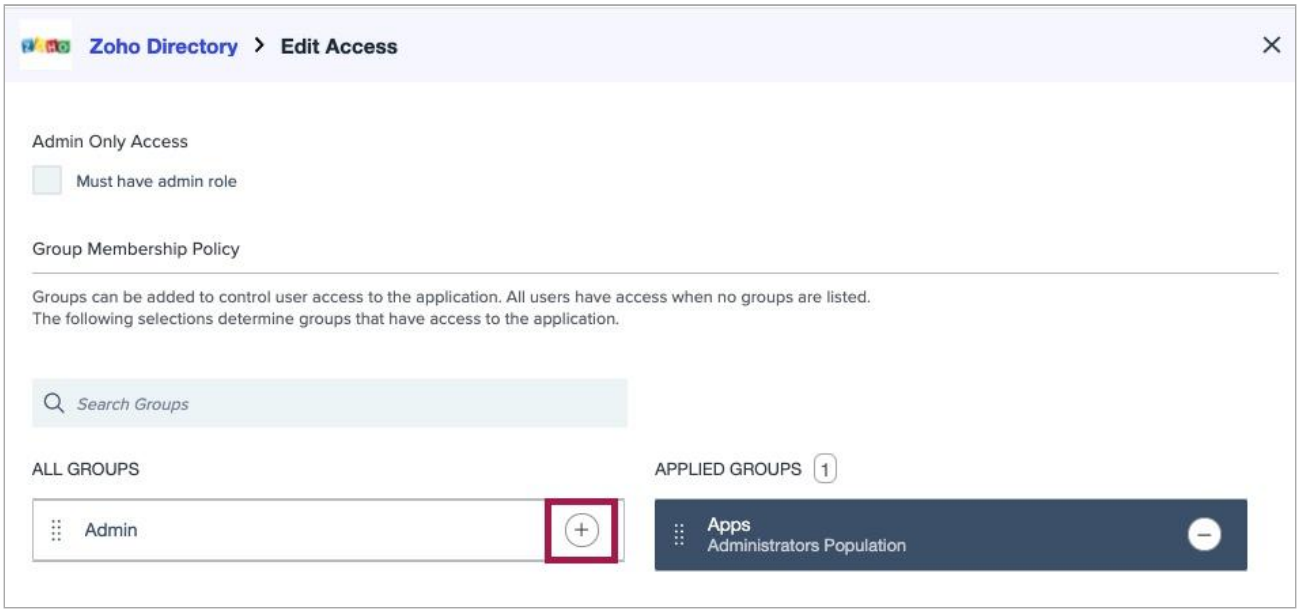


8. In the **Available Groups** section, select the group you created and click the **+** icon to add it to the user's group memberships. Click **Save**.



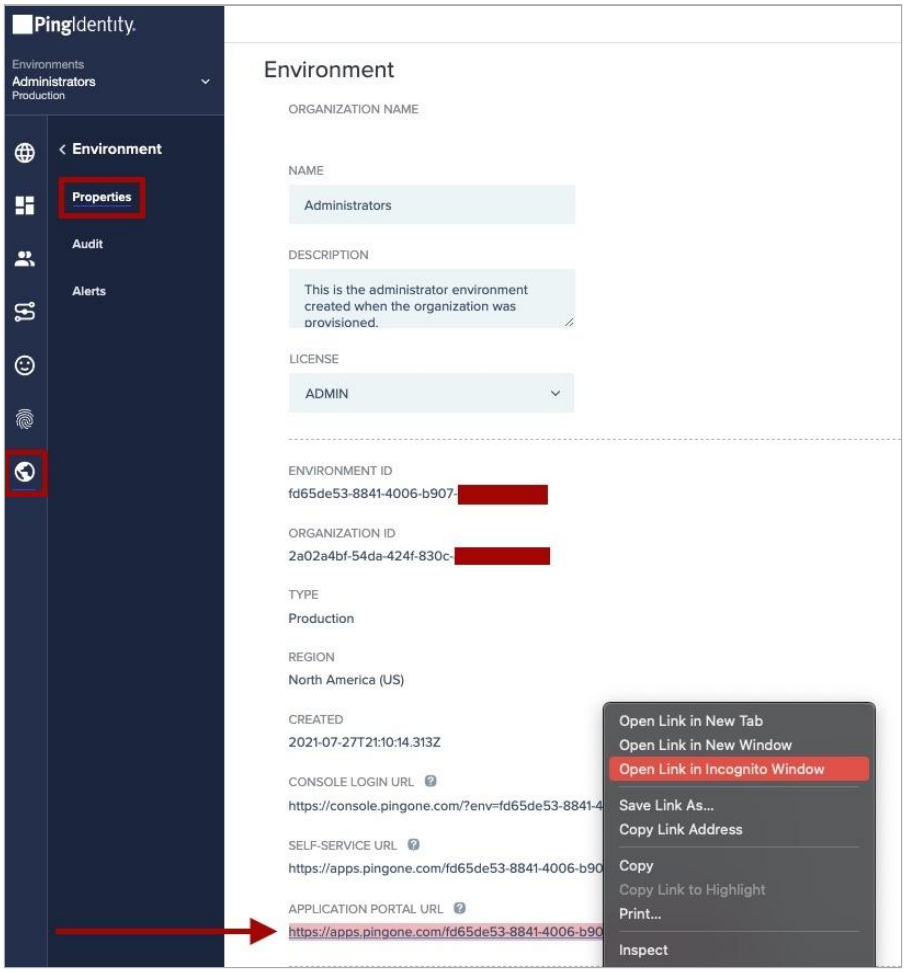
9. On the **Connections** tab, for the Zoho Directory application, do the following:
    1. Click the **Access** tab.
    2. Click the **Pencil** icon to edit the configuration.

    3. Select the group that you created and add it to the **Applied Groups** section. Click **Save**.

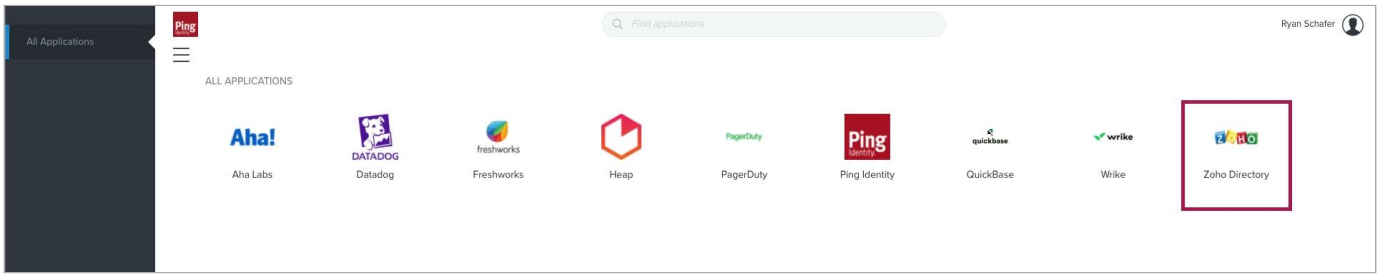


Test the integration

1. In the PingOne admin console, go to **Dashboard → Environment Properties**.
2. Right-click on the **Application Portal URL** and open it in a private browser session.



3. Sign on as the test user that you created and click the **Zoho Directory** tile.



You’re signed on to the user’s Zoho Directory account.