ZSCALER AND PING IDENTITY DEPLOYMENT GUIDE

SEPTEMBER 2022, VERSION 1.0

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

The following table defines acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
AD	Microsoft Active Directory
ADFS	Microsoft Active Directory Federation Services
CA	Central Authority (Zscaler)
CPU	Central Processing Unit
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
IWA	Integrated Windows Authentication
MFA	Multi-Factor Authentication
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SAML	Security Assertion Markup Language
SCIM	System for Cross-Domain Identity Management
SSL	Secure Socket Layer (RFC6101)
SSO	Single Sign-On
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZPC	Zscaler Posture Control (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

About This Document

The following sections describe the organizations and requirements of this deployment guide.

Zscaler Overview

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. To learn more, see Zscaler's website.

Ping Identity Overview

Ping Identity Corporation (NYSE: PING) is an American software company established in 2002 by Andre Durand and Bryan Field-Elliot. It is headquartered in Denver, Colorado; United States with development offices in Vancouver, British Columbia; Tel Aviv, Israel; Austin, Texas; Denver, Colorado; and Boston, Massachusetts. Ping also has European operations with offices in London, Paris, and Switzerland as well as offices in Bangalore, Melbourne, and Tokyo, serving Asia-Pacific.

The company's software provides federated identity management and self-hosted identity access management to web identities via attribute-based access controls, similar to identity management system tools developed by Microsoft and Okta (identity management). This single sign-on (SSO) gives users a single set of credentials to access applications (web applications, apps on mobile devices, VPN, etc.) that have company data. This is primarily done with identity providers such as Ping, Okta (identity management), and Microsoft Azure by leveraging open standards such as SAML and OAuth.

Ping Identity products include PingID, PingFederate, PingOne, PingAccess, PingDirectory, PingDataGovernance, and PingIntelligence. This guide is specifically written for deploying Zscaler using PingOne which is the Ping SaaS.

To learn more, refer to the Ping Identity website.

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, refer to:

- Zscaler Resources
- Ping Identity Resources
- Appendix A: Requesting Zscaler Support

Software Versions

This document was authored using the latest version of the Zscaler software.

Request for Comments

- **For prospects and customers**: Zscaler values reader opinions and experiences. Contact partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- **For Zscaler employees**: Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

Zscaler and Ping Identity Introduction

The following are overviews of the Zscaler and Ping Identity applications described in this deployment guide.

If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of it as a secure internet on-ramp—all you do is make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via the lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, CASB, and Isolation, allowing you to start with the services you need now and activate others as your needs grow.

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on a cloud or data center using a Zero Trust framework. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity rather than extending the network to them.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT administrator within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, Zscaler Client Connector is installed. Zscaler Client Connector ensures the user's device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal application.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name and Link	Description
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA
Best Practices for Traffic Forwarding	(ZIA) List of and help for the ZIA-supported traffic forwarding methods.
Configuring SAML	(ZIA) Help for configuring SAML in ZIA.
Configuring SCIM	(ZIA) Help for configuring SCIM in ZIA.
About Hosted PAC Files	(ZIA) Help for ZIA and hosted PAC files.
Configuration Guide for Ping Identity PingOne	(ZPA) Help for configuring SAML in ZPA.
Configuring Zscaler Client Connector Profiles	(Zscaler Client Connector) List of and help for policy rules for supported platforms.
Best Practices for Adding Bypasses for Z-Tunnel 2.0	(Zscaler Client Connector) Help for adding tunnel bypasses.
IWA – Mark Ryan's IWA / PingOne Demonstration	A video demonstrating how to configure Okta Integrated Windows Authentication (IWA) and PingOne.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name and Link	Description
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA
Best Practices for Traffic Forwarding	(ZIA) List of and help for the ZIA-supported traffic forwarding methods.
Configuring SAML	(ZIA) Help for configuring SAML in ZIA.
Configuring SCIM	(ZIA) Help for configuring SCIM in ZIA.
About Hosted PAC Files	(ZIA) Help for ZIA and hosted PAC files.
Configuration Guide for Ping Identity PingOne	(ZPA) Help for configuring SAML in ZPA.
Configuring Zscaler Client Connector Profiles	(Zscaler Client Connector) List of and help for policy rules for supported platforms.
Best Practices for Adding Bypasses for Z-Tunnel 2.0	(Zscaler Client Connector) Help for adding tunnel bypasses.
IWA – Mark Ryan's IWA / PingOne Demonstration	A video demonstrating how to configure Okta Integrated Windows Authentication (IWA) and PingOne.

Name and Link	Description
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

PingOne Overview

PingOne for Workforce is a cloud identity solution for helping organizations secure employees' access to resources so they can get work done—anytime, anywhere. Available in three solution packages to meet a variety of common business requirements, PingOne for Workforce can help increase productivity with no-code orchestration, SSO, multi-factor authentication and centralized risk-aware access to the right resources.

- Deliver seamless experiences: Reduce friction with identity orchestration to weave together the Ping, AWS, and other authentication vendor services your employees need to be secure.
- Rapid deployment: Supports over 1,700 out-of-the box integrations to popular apps, providing rapid time to value for your workforce.
- Deploy rapidly with AWS integrations: The PingOne Cloud Platform works seamlessly alongside AWS Identity and Access Management (IAM), AWS Organizations, AWS SSO, AWS Session Tags, and Amazon Control Tower.

Ping Identity Resources

The following table contains links to Ping Identity support resources.

Name and Link	Description
Ping Identity Documentation	Online help for Ping Identity.
How to Configure SAML for ZIA	Online help for configuring SAML for ZIA in PingOne.
How to Configure SAML for ZPA	Online help for configuring SAML for ZPA in PingOne.
Ping AD Connect	Online help for Ping AD Connect.

PingOne for Enterprise Authentication and Provisioning in Use with Zscaler Services

Identity, authentication, and provisioning is an inherent part of the Zscaler solution and allows Zscaler to provide granular user visibility, logging, and security to an organization, down to the individual user level.

Authentication is the process of verifying a user's identity through the use of credentials (and other identity factors). Security Assertion Markup Language (SAML) is the preferred method for authentication for both ZIA and ZPA.

For this document PingOne is the SAML identity provider (IdP). SAML is an open protocol standard that allows PingOne to authenticate a user and pass the authorization credentials to the Zscaler service as a SAML service provider. Although beyond the scope of this document, SAML also provides SSO to any SAML service provider. An example of this would be gaining access to both ZIA and ZPA by entering your credentials a single time instead of having to enter it for both ZIA and ZPA. SSO greatly enhances the user experience by providing a cohesive solution to a modern Cloud and SaaS environment. SAML and SSO are the catalyst to make a unified solution possible.

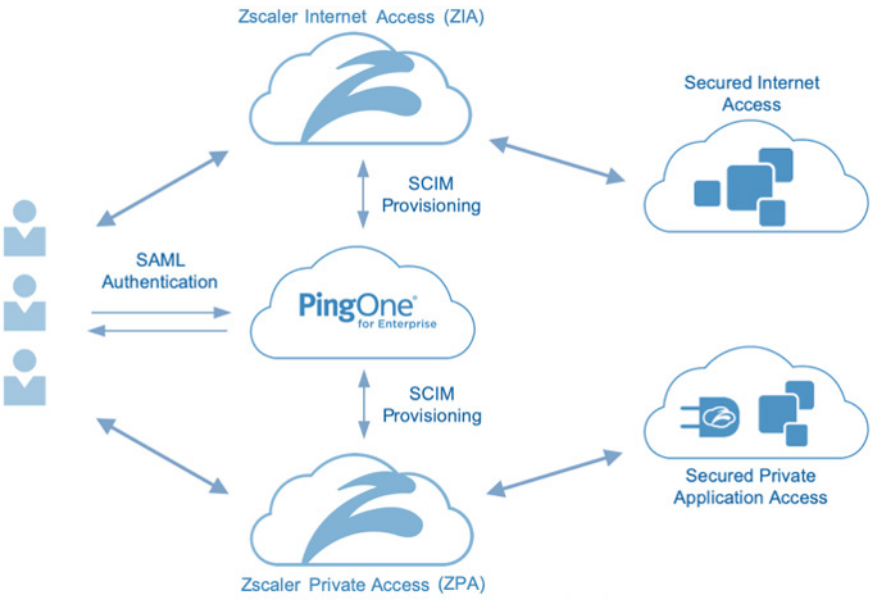


Figure 1. ZIA and ZPA in a PingOne authentication environment

Authentication provisioning is the automation of provisioning and deprovisioning of users and security groups to Zscaler services. System for Cross-Domain Identity Management (SCIM) is a standards-based protocol used for signaling and automating the changes in an environment. When a user is added to the user database, SCIM automatically provisions the user and the associated security groups in the Zscaler database. When a user is deprovisioned, the associated groups, and credentials are also removed, which prevents access to resources. The primary use case is onboarding and offboarding users from an organization. When a user leaves an organization, the user is deprovisioned from the user directory and SCIM changes the Zscaler databases to eliminate all ZIA and ZPA access. SCIM then deprovisions the user from all associated databases, preventing further access to company resources.

To learn more, see Zscaler Resources.

Configure PingFederate and ZIA

For current documentation on PingFederate and ZIA, refer to the Ping Identity documentation.

PingFederate is an enterprise federation server that enables user authentication and SSO. It serves as a global authentication authority that allows employees, customers, and partners to securely access all the applications they need from any device.

PingFederate easily integrates with applications across the enterprise, third-party authentication sources, diverse user directories, and existing IAM systems, all while supporting current and past versions of identity standards like OAuth, OpenID Connect, SAML, and WS-Federation. It can be deployed on-premises or in the cloud.

The following sections describe how to integrate PingFederate and ZIA.

Creating an SSO Connection

To allow PingFederate to handle SSO to ZIA, create a service provider (SP) connection.

Follow these steps to create a new connection, or you can modify your provisioning connection.

1. In the PingFederate administrative console, create a new service provider connection:
   - For PingFederate 10.1 or later, go to **Applications** > **Integration** > **SP Connections**. Click **Create Connection**.
   - For PingFederate 10.0 or earlier, go to **Identity Provider** > **SP Connections**. Click **Create Connection**.
2. Configure the basic connection details with the ZIA quick-connection template:
   a. On the **Connection Template** tab, select **Use a template for this connection**.
   b. In the **Connection Template** list, select **Zscaler ZIA Provisioner**.
   c. In the **Metadata File** row, upload the `zscaler-metadata.xml` file.
   d. Click **Next**.
   e. On the **Connection Type** tab, select **Browser SSO Profiles**.
   f. Click **Next**.
   g. On the **General Info** tab, in the **Connection Name** field, enter a name for the connection.
   h. Click **Next**.
3. On the **Browser SSO** tab, configure SSO as shown in the PingFederate documentation, with the following details:
   a. On the **Browser SSO** > **SAML Profiles** tab, select **IdP-Initiated SSO** and **SP-Initiated SSO**.

Zscaler recommends that you leverage SP-initiated SSO because IdP-initiated SSO is not commonly used.

For more information, see IdP-Initiated SAML and refer to the Ping Identity documentation.

If you want to use both IdP-initiated SSO and SP-initiated SSO, both endpoints are accessible using the ACSIdx parameter.

To learn more, refer to the Ping Identity documenation.

   b. On the **Browser SSO** > **Protocol Settings** > **Allowable SAML Bindings** tab, select **POST**.
   c. On the **Browser SSO** > **Protocol Settings** > **Signature Policy** tab, select **Always sign assertion**.

4. On the **Credentials** tab, configure the connection credentials as shown in the PingFederate documentation.
5. Click **Next**.
6. On the **Activation and Summary** tab, above the **Summary** section, click the toggle to turn on the connection.
7. Click **Save**.

Registering PingFederate as an IdP in Zscaler

Export your PingFederate signing certificate and use it to configure SAML in ZIA.

For more information on setting up SSO, see Configuring SAML.

1. In PingFederate, export your signing certificate:
   a. Go to **Security** > **Signing & Decryption Keys & Certificates**.
   b. For the certificate that you want to use, in the **Action** column, click **Export**.
   c. On the **Export Certificate** tab, click **Next**.
   d. On the **Export & Summary** tab, click **Export**.
   e. Open the .crt file in a text editor and copy the contents.
   f. Rename the file extension to .pem.
2. In ZIA, go to **Administration** > **Authentication** > **Authentication Settings**.
3. On the **Authentication Profile** tab, in the **Authentication Type** section, select **SAML**.
4. Click **Configure SAML**.

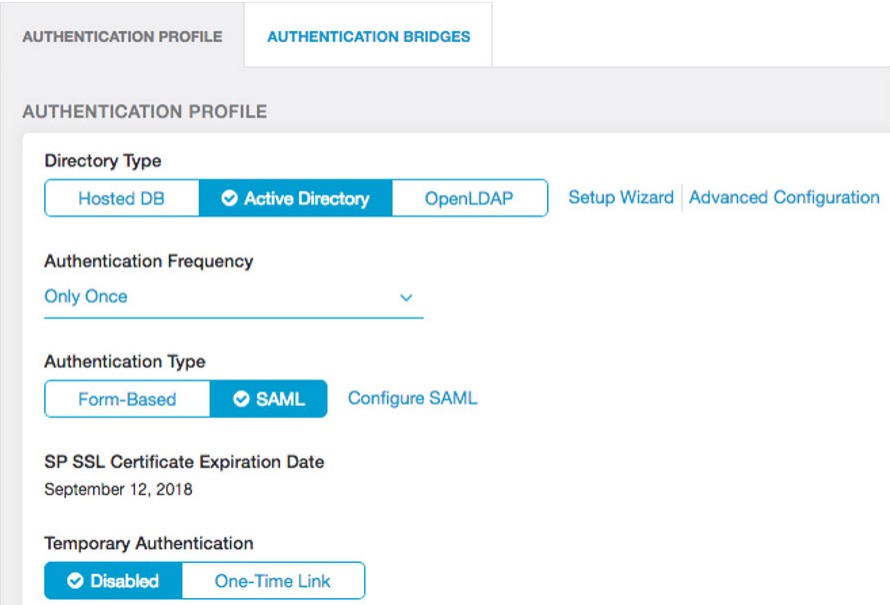


Figure 2. Authentication settings

5. In the **SAML Portal URL** field, enter your PingFederate SSO endpoint (e.g., `https://<pf_host>:<pf_port>/idp/SSO.saml2`).
6. In the **Login Name Attribute** field, enter the LDAP attribute that maps to the login name that users enter when they authenticate with ZIA, such as `NameID`.

7. In the **Public SSL Certificate** section, click **Upload**.
8. Click **Choose File**.
9. Select the .pem file that you exported from PingFederate, and then click **Upload**.
10. Click **Save**.
11. Click **Save** again, then activate the change as shown in Saving and Activating Changes in the ZIA Admin Portal.

Configure PingOne and ZIA—SAML and SCIM

The following sections describe how to configure PingOne to work with ZIA using SAML and SCIM.

Enable PingOne

This document assumes that the user has a working PingOne environment, and only the Zscaler applications need to be installed and configured to provide a working Zscaler and PingOne solution.

However, a new no-cost PingOne Account Type was created from the PingOne website and used to create this document. Each step was validated for functionality in a live environment.

The following image shows how to select the Classic UI.

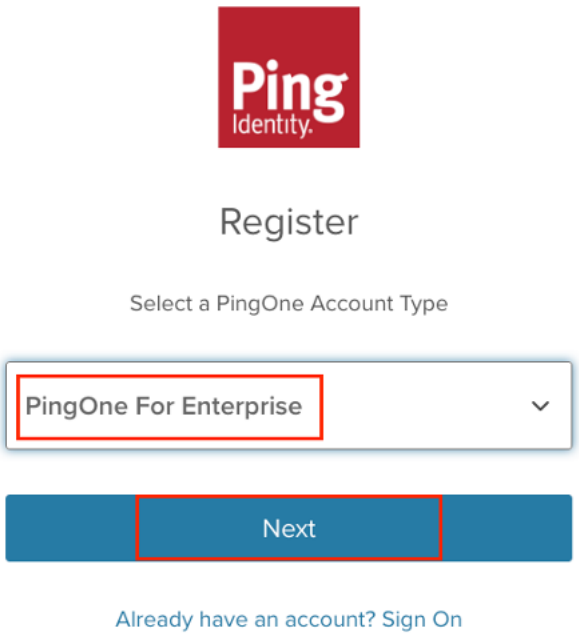


Figure 3. Creating a PingOne IdP

Add the Zscaler ZIA Application

First, add the Zscaler applications that enable authentication and provisioning to PingOne.

From the PingOne portal administrator account:

1. Go to **Applications** > **My Applications**.
2. Click **Add Application**.

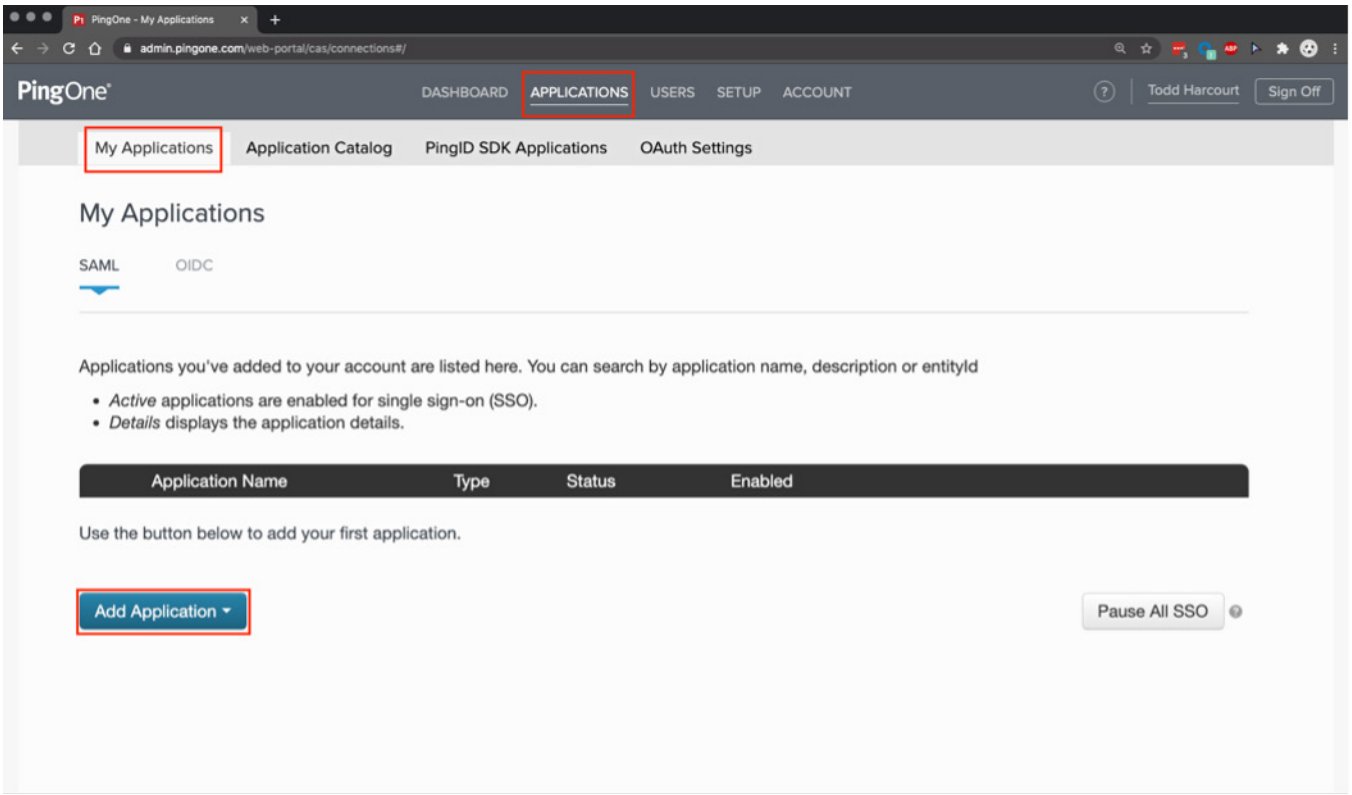


Figure 4. Adding an application

Add the ZIA Application

To add the appropriate Zscaler application:

1. Search for `zscaler`.
2. Select the Zscaler application for **Zscaler** with **SAML with Provisioning (API)** for use with ZIA users.

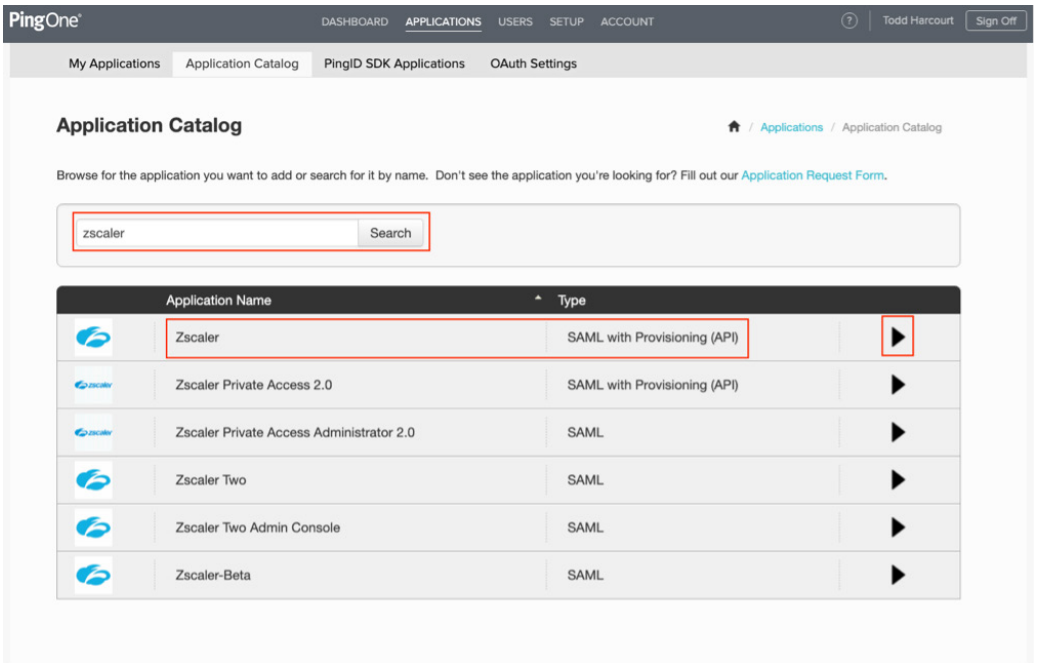


Figure 5. Adding the Zscaler applications

3. Click the arrow on the right to display a description of the application.
4. Click **Setup** to begin the installation process.

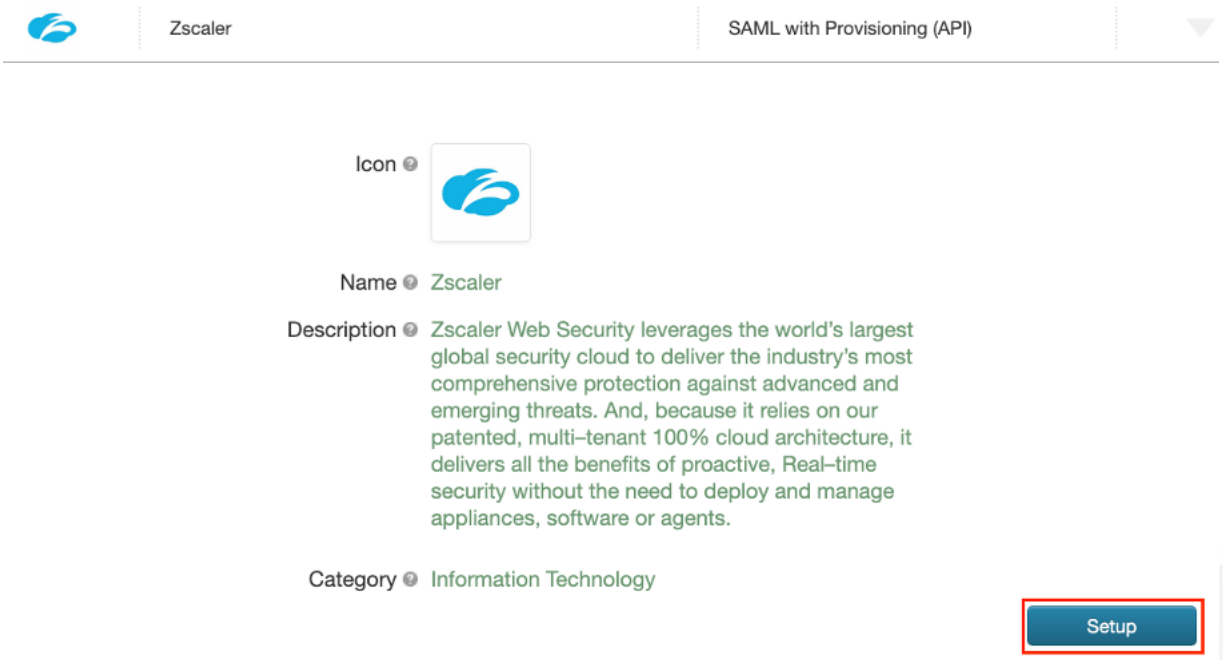


Figure 6. Adding Zscaler 2.0 for ZIA

Configure PingOne for ZIA

In the initial configuration window:

1. Click **Download** next to the Signing Certificate, and copy the IdP ID and the **URL of the SAML Portal**. The IdP ID is appended to the example URL to create the SAML Portal URL that is used in the Zscaler IdP setup process.
2. Click **Continue to Next Step**.

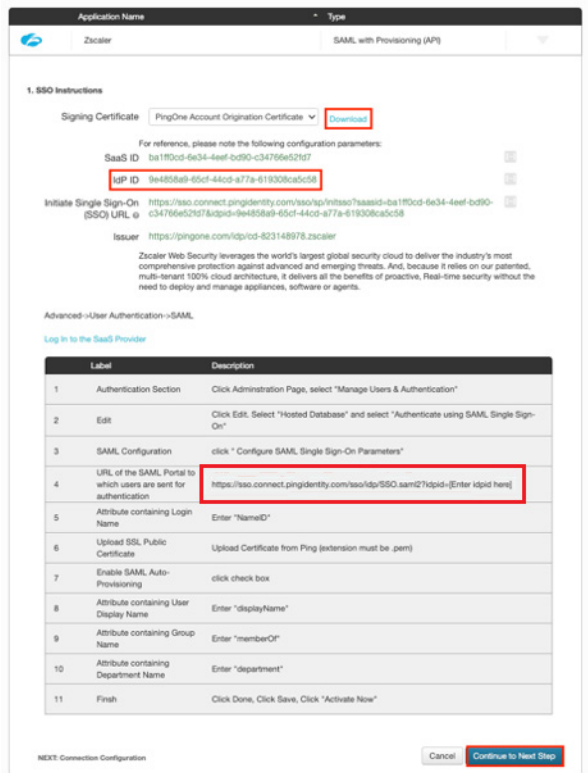


Figure 7. PingOne configuration

The SAML Portal URL is created by combining the Base SAML Portal URL and the IdP ID:

In a new browser window, open the ZIA Admin Portal.

Configure Zscaler ZIA for a PingOne IdP

To add PingOne as an IdP in your ZIA Admin Portal, go to **Administration** > **Authentication Settings**. The **Authentication Settings** window is displayed.

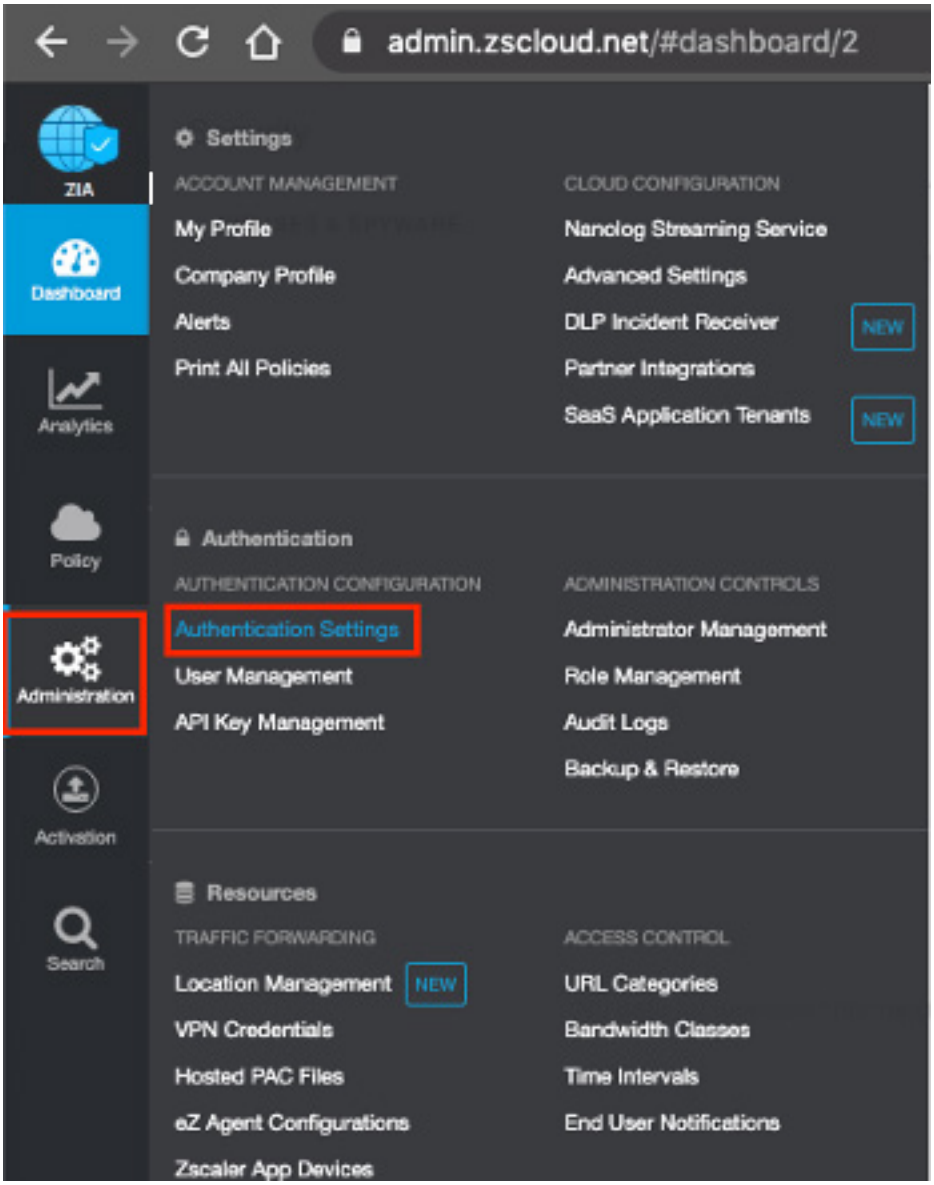


Figure 8. Adding PingOne and the ZIA IdP

Add PingOne as an IdP

Click **Add Identity Provider**. The **Add Identity Provider** page is displayed.

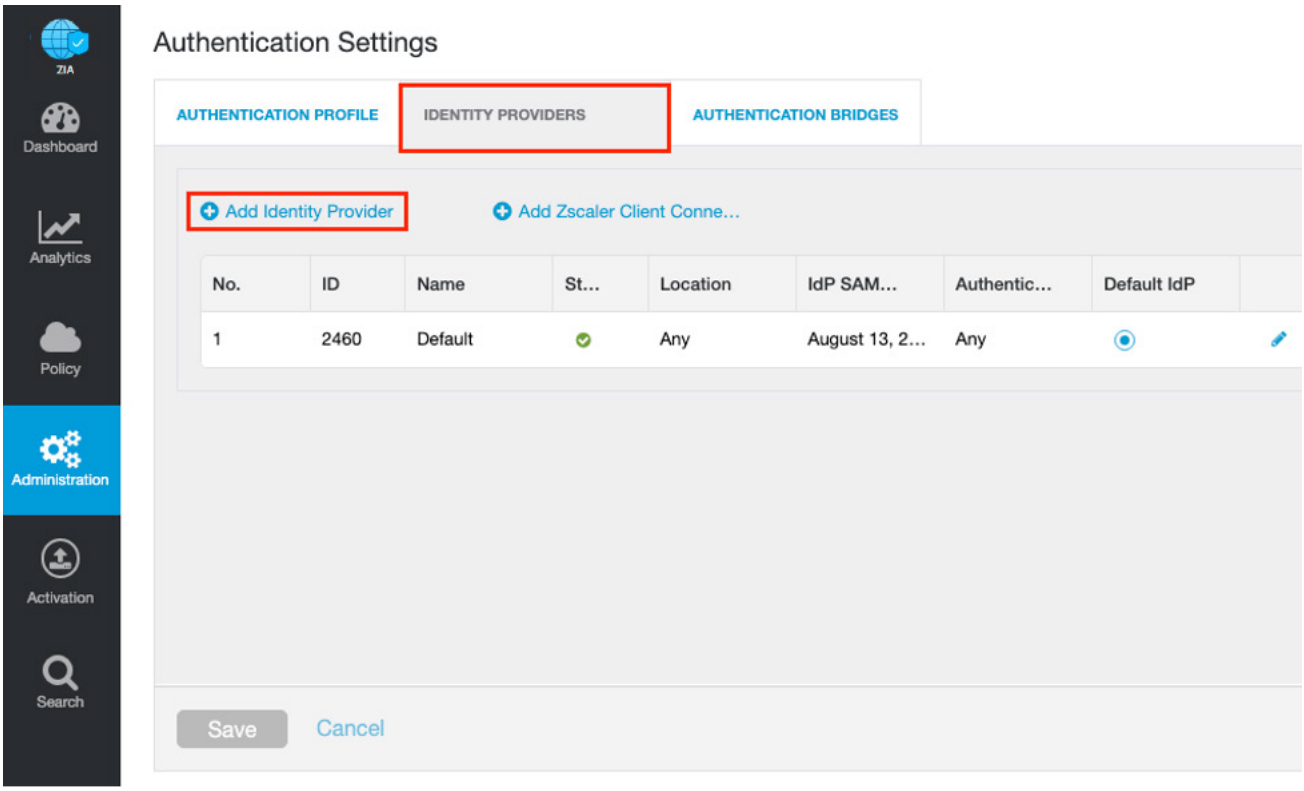


Figure 9. Adding PingOne as an IdP

Configure ZIA for PingOne

In the **Add Identity Provider** window:

1. Enter a **Name** for the PingOne IdP.
2. Set the **Status** to **Enabled**.
3. Paste in the **SAML Portal URL**.
4. Enter `NameID` (case sensitive) for the **Login Name Attribute**.
5. Upload the **IdP SAML Certificate**.
6. Select **PingOne** as the **Vendor**.
7. For the **Criteria**, leave the **Locations** and **Authentication Domains** as **None**, unless this is for a specific location or domain. In that case, select the specific **Authentication Domain** from the drop-down menu for which the PingOne IdP provides authentication.
8. Select **saml_2022** for the **Request Signing SAML Certificate**, then download the **SP Metadata** and the **SP SAML Certificate** and save for the next step.
9. Set **Enable SAML Auto-Provisioning** to **Enabled**.
10. Enter the **User Display Name Attribute** as `displayName` (case sensitive).
11. Enter the **Group Name Attribute** as `memberOf` (case sensitive).
12. Enter the **Department Name Attribute** as `department` (case sensitive).
13. Click **Save** and activate the configuration.

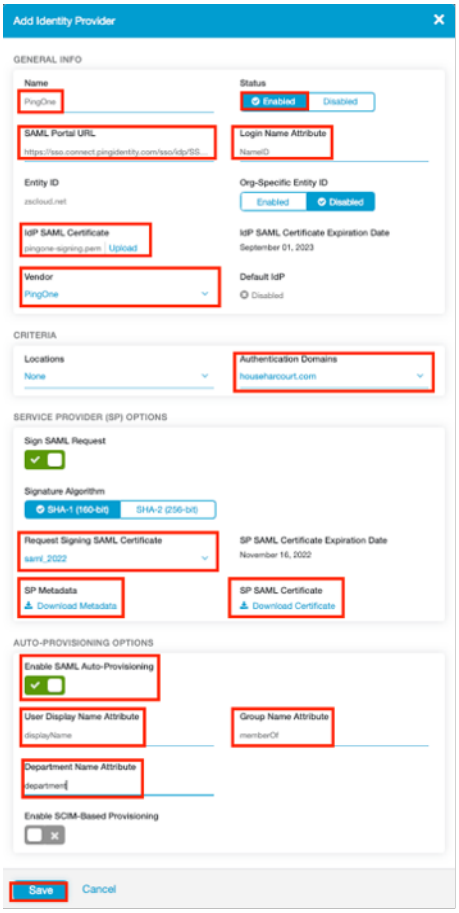


Figure 10. The Add Identity Provider dialog window

To configure SCIM, you must save the configuration first and then enable SCIM.

Configure SCIM on ZIA

To enable SCIM, edit the IdP by clicking the **Edit** icon, which re-opens the **Identity Provider** window.

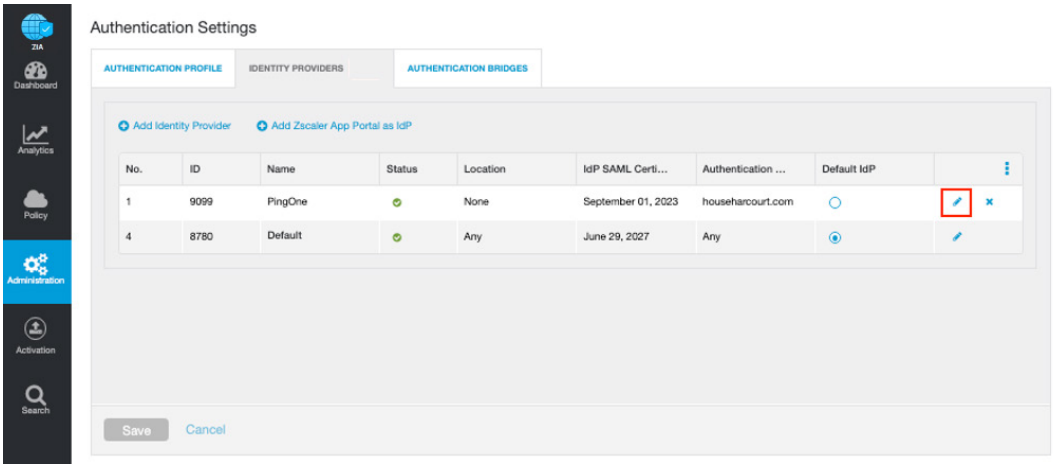


Figure 11. Edit the Identity Provider

To enable SCIM on the IdP:

1. Select **Enable SCIM-Based Provisioning**, which displays the **Base URL** and **Bearer Token**.
2. Copy the **Base URL** and **Bearer Token** for the next step in the PingOne portal.
3. Click **Save** and activate the configuration.

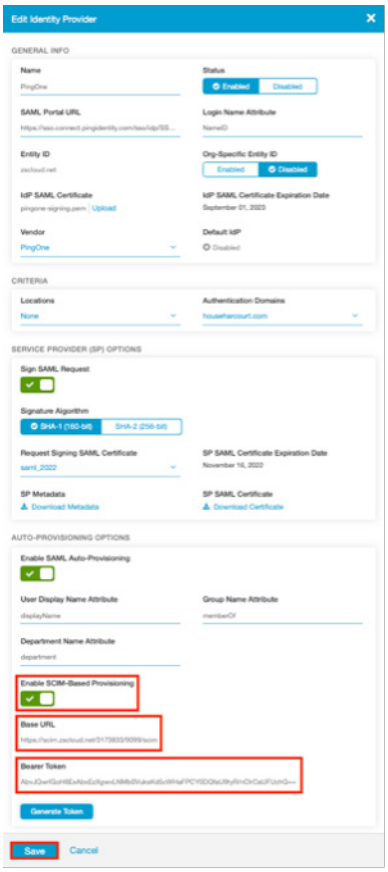


Figure 12. Enable SCIM

To finish the PingOne configuration, return to the PingOne configuration window to finish the IdP setup.

Finish Configuring PingOne for ZIA

To finish the PingOne configuration to use with ZIA:

1. Upload the Zscaler metadata file and the Zscaler signing certificate.
2. Select the **Set Up Provisioning** checkbox.
3. Click **Continue to Next Step**.

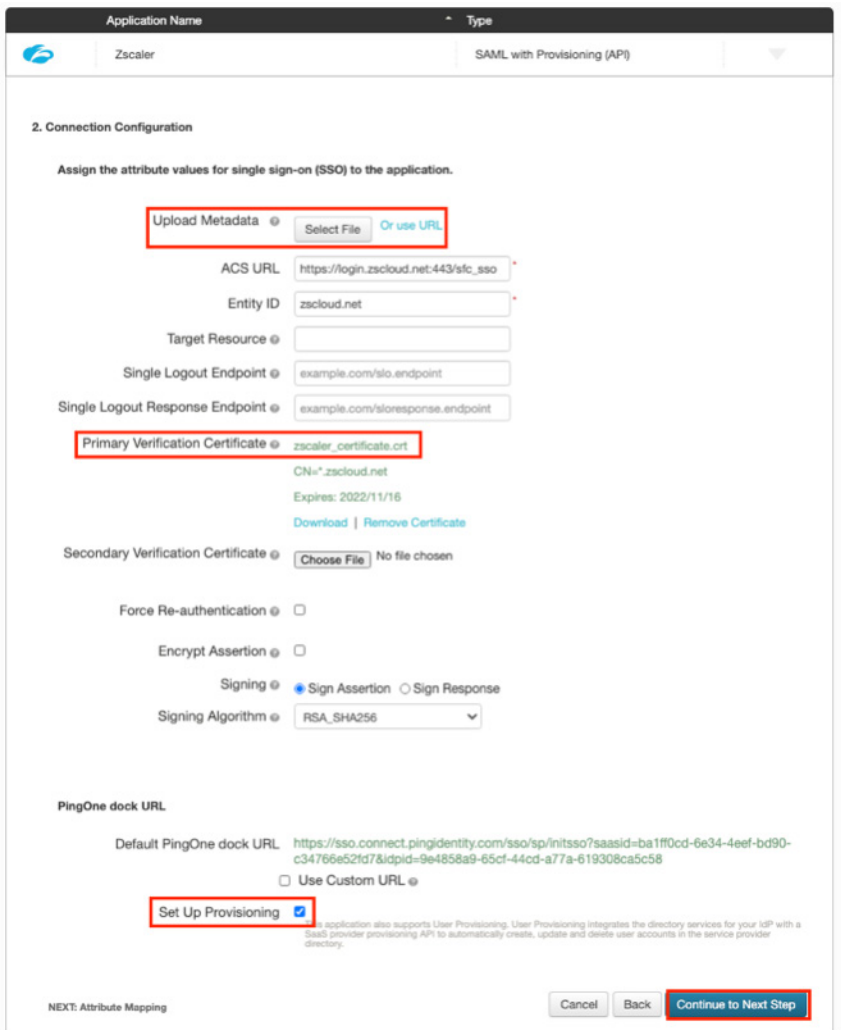


Figure 13. Assigning the ZIA application

The setup steps for SCIM on PingOne are displayed.

Configure PingOne for SCIM

Click **Continue to Next Step** to proceed.

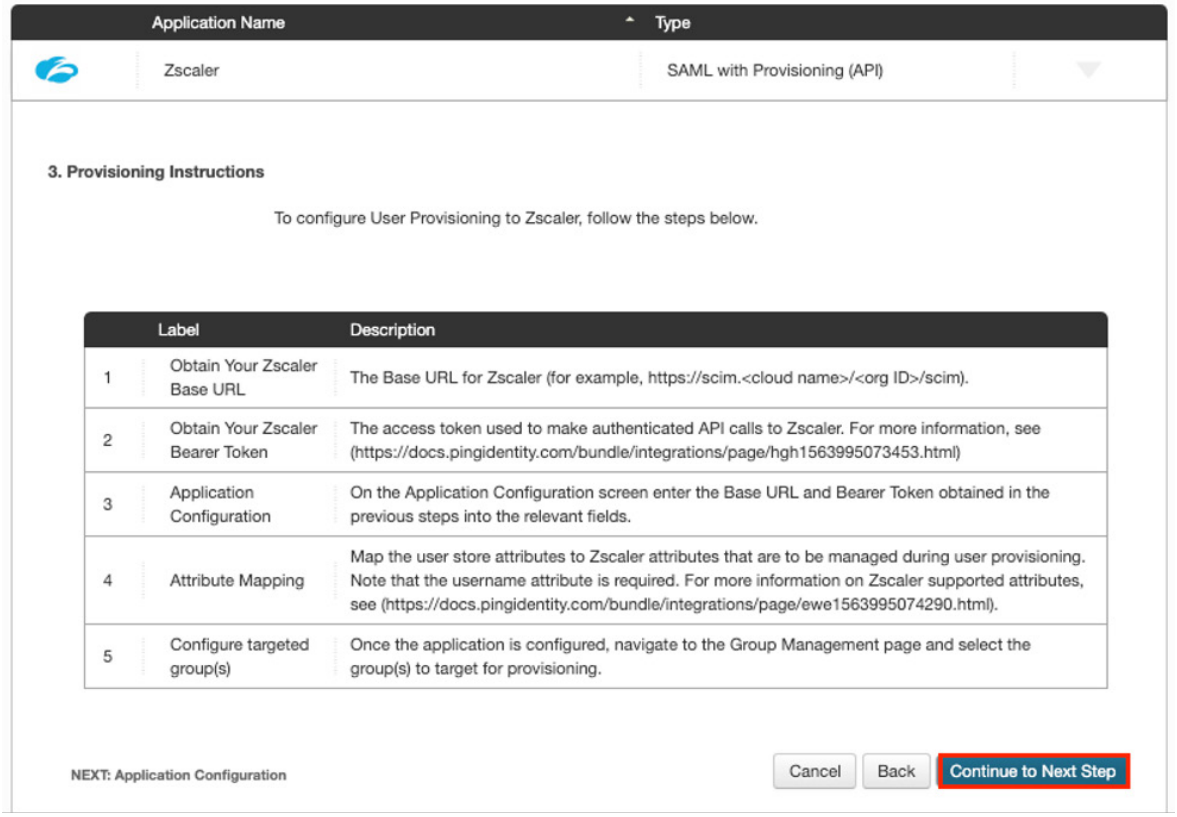


Figure 14. Configure SCIM on the PingOne side

1. Enter the base URL into the **BASE_URL** field.
2. Enter the Bearer Token value into the **BEARER_TOKEN** field.
3. Click **Continue to Next Step**.

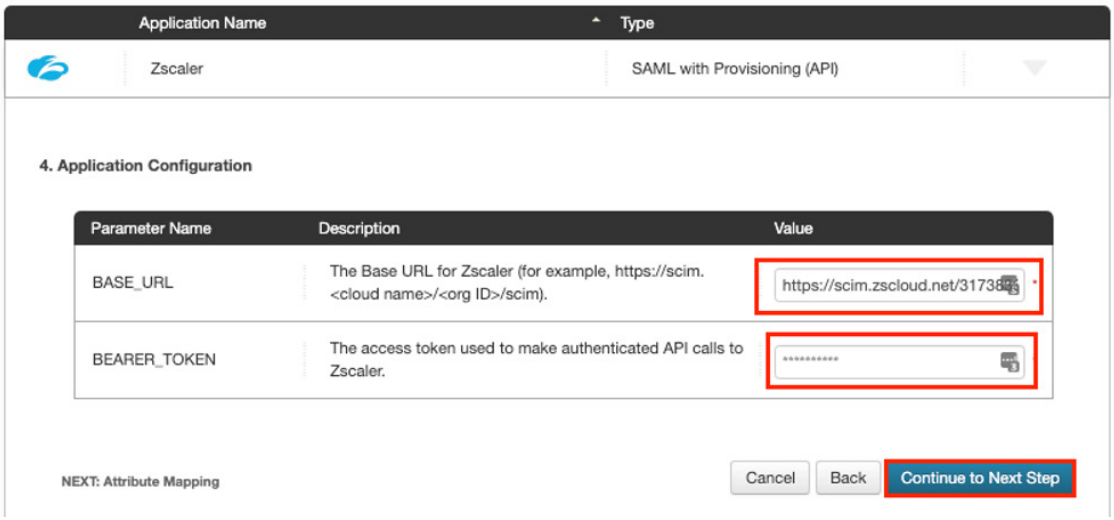


Figure 15. PingOne SCIM provisioning

Provisioning Attribute Mapping

You must map the PingOne variables to the expected ZIA variables for Self-Provisioning and SCIM to function properly. At a minimum:

1. Set variables **memberOf**, **displayName**, and **department** attributes for auto-provisioning.
2. Set **userName** to **Email** and **displayName** to **userName** for SCIM to push or delete the user.
3. Click **Continue to Next Step**.

	Application Attribute	Description	Identity Bridge Attribute or Literal Value
1	memberOf (sso)	Groups user is a member of	memberOf As Literal Advanced
2	displayName (sso)	Users DisplayName	displayName As Literal Advanced
3	department (sso)	Department user is in	department As Literal Advanced
4	SAML_SUBJECT (sso)	Map this to the username in Zscaler	SAML_SUBJECT As Literal Advanced
5	userName (provisioning) *	Zscaler's unique identifier for the user. The expected format is user@domain (for example, 'bjensen@example.com'). A username cannot be updated. This attribute is required.	Email As Literal Advanced
6	displayName (provisioning) *	The name of the user, suitable for display to end-users. This attribute is required.	userName As Literal Advanced
7	department (provisioning)	The department for the user. If no department is specified, Zscaler sets a default value of 'Service Admin'.	department As Literal Advanced
8	email (provisioning)	The email for the user (for example, 'bjensen@example.com').	Email As Literal Advanced
9	externalID (provisioning)	A String that is an identifier for the resource as defined by the provisioning client.	externalID As Literal Advanced
10	firstName (provisioning)	The given name of the User, or first name in most Western languages (e.g., 'Barbara' given the full name 'Ms. Barbara Jane Jensen, III').	First Name As Literal Advanced
11	lastName (provisioning)	The family name of the User, or last name in most Western languages (e.g., 'Jensen' given the full name 'Ms. Barbara Jane Jensen, III').	Last Name As Literal Advanced

Figure 16. PingOne SCIM synchronization settings

SCIM only pushes, deletes, or disables the user. SCIM doesn't push the Security Groups. The security groups are pulled from auto-provisioning for use with ZIA policies.

Portal Settings

Next, customize how the application is going to look on the PingOne portal.

Make any changes specific to your installation, and then click **Continue to Next Step**.

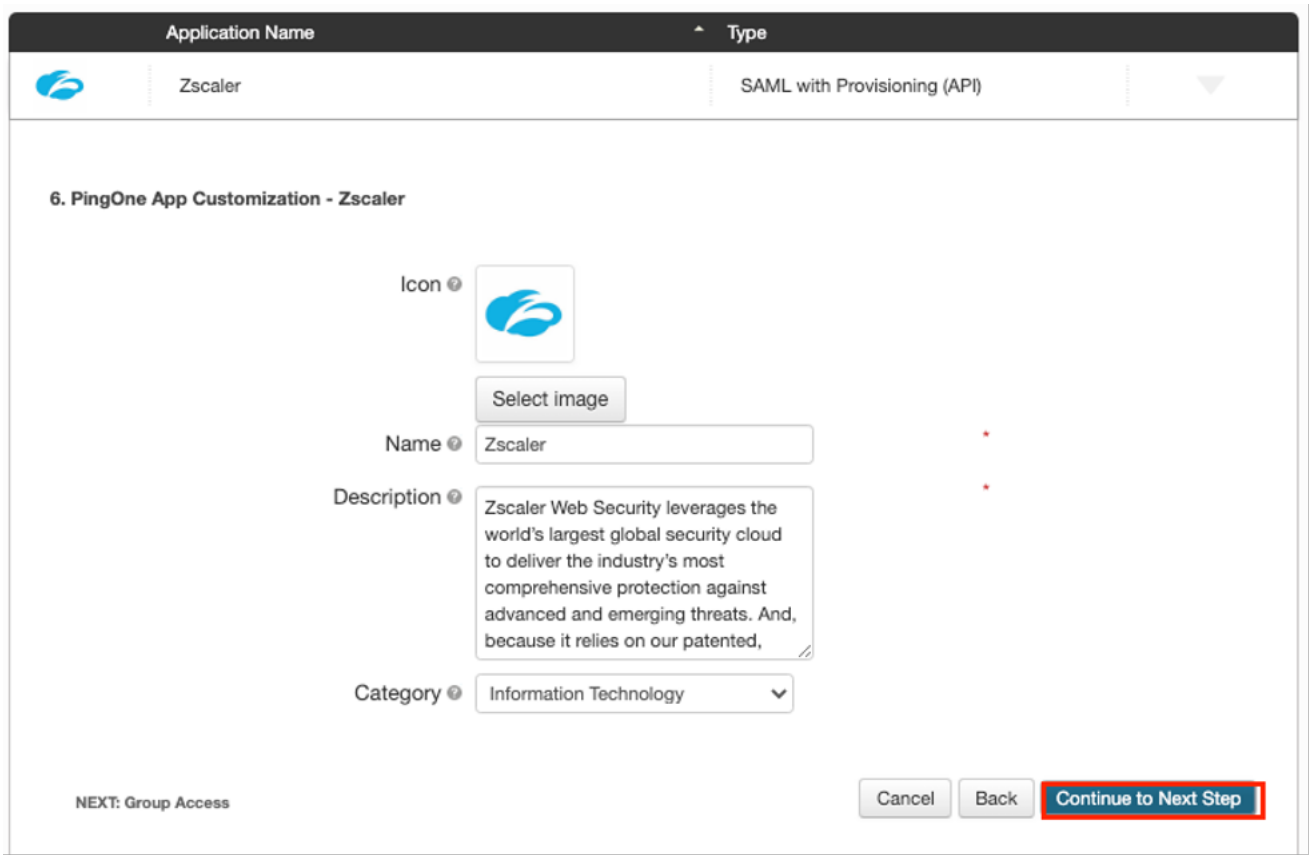


Figure 17. PingOne portal settings

Configure Groups to Use ZIA

Select the **Security Groups** that are allowed to use ZIA.

Add any or all groups specific to your installation, and then click **Continue to Next Step**.

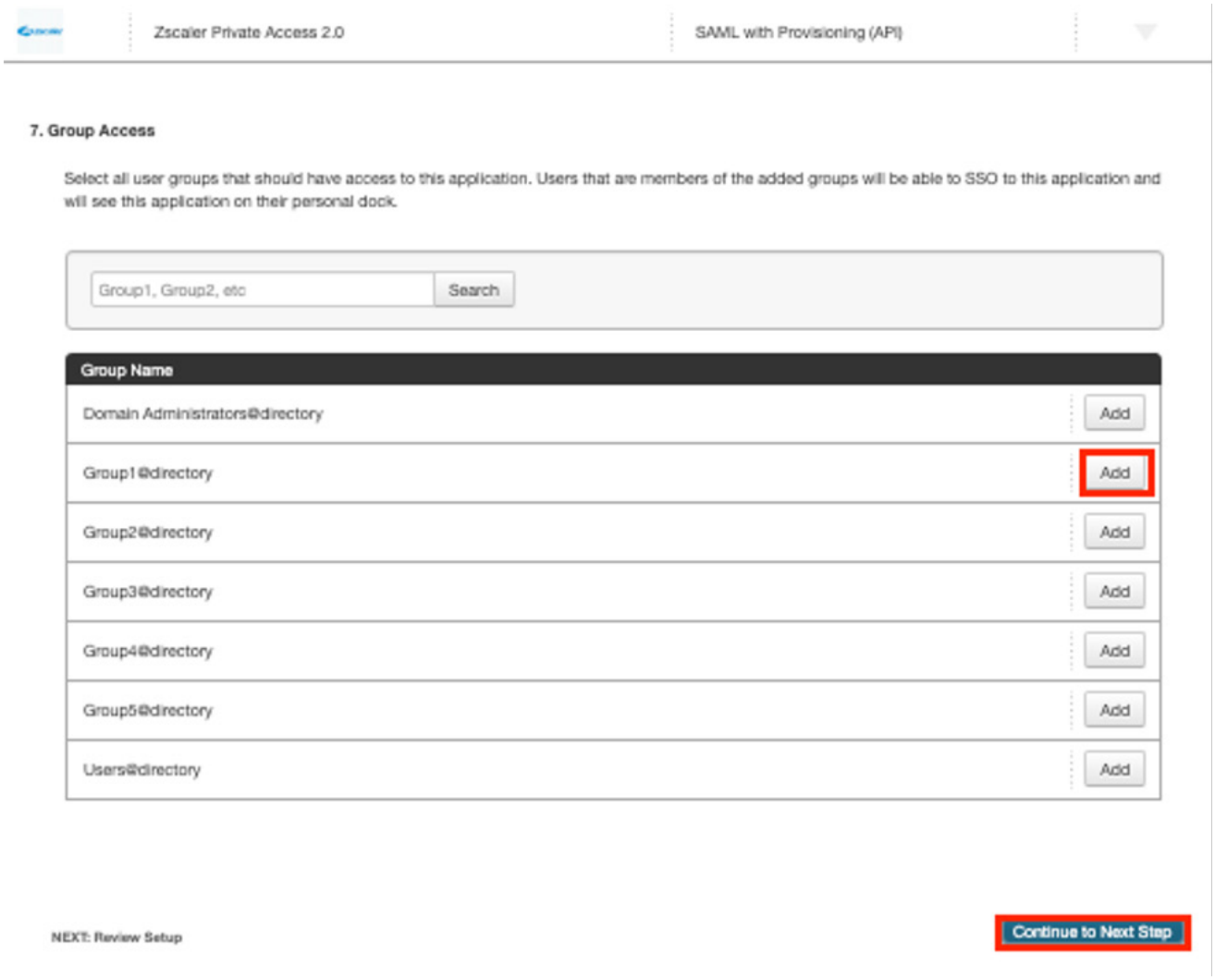


Figure 18. PingOne SCIM synchronization settings

Finalize the PingOne Configuration

Verify your configuration and click **Finish**.

Figure 19. PingOne configuration

Your PingOne instance is now configured for authenticating ZIA users.

Configure PingFederate and ZPA

For documentation to configure PingFederate with ZPA, refer to the PingOne documentation.

Upgrading an Existing Deployment

If you're upgrading from a previous version of the Zscaler Private Access Provisioner, note your existing SP connection configuration and create a new connection.

PingFederate 10.1 or Later

1. To back up your current PingFederate configuration, refer to the PingFederate documentation.
2. In the PingFederate administrative console, go to **Applications** > **Integration** > **SP Connections** and select your connection.
3. Note the attribute mappings for your existing SP connection. To learn more, refer to the PingFederate documentation.
4. Delete your existing SP connection:
    a. Go to **Applications** > **Integration** > **SP Connections**.
    b. For your existing connection, click **Select action**.
    c. Click **Delete**.
    d. Click **Confirm**.
5. Complete the steps in the PingFederate documentation.
6. Complete the steps in the PingFederate documentation. From **Outbound Provisioning** > **Manage Channels** > **Channel on the Attribute Mapping** tab, configure the attribute mappings based on your notes.
7. (Optional) Complete the steps in the PingFederate documenationon.

PingFederate 10.0 or Earlier

1. To back up your current PingFederate configuration, refer to the PingFederate documentation.
2. In the PingFederate administrative console, go to **Identity Provider** > **SP Connections** and select your connection.
3. Note the attribute mappings for your existing SP connection. To learn more, refer to the PingFederate documentation.
4. Delete your existing SP connection.
    a. Go to **Identity Provider** > **SP Connections** > **Manage All**.
    b. For your existing connection, click Select action, and then click **Delete**.
    c. Click **Save**.
5. Complete the steps in the PingFederate documentation.
6. Complete the steps in the PingFederate documentation. From **Outbound Provisioning** > **Manage Channels** > **Channel**, on the **Attribute Mapping** tab, configure the attribute mappings based on your notes.
7. (Optional) Complete the steps in the PingFederate documentation.

Deploying the Integration Files

To get started with the integration, deploy the Zscaler Private Access Provisioner files to your PingFederate directory.

1. Download the Zscaler Private Access Provisioner.zip archive from the Ping Identity Integration Directory.
2. Stop PingFederate.
3. If you're upgrading an existing deployment, delete the `pf-zscaler-zpa-quickconnection-<version>.jar` file from your `<pf_install>/pingfederate/server/default/deploy` directory.
4. Extract the .zip archive and merge the contents of the `dist` directory with your `<pf_install>/pingfederate/server/default/deploy` directory.
5. Enable the PingFederate provisioning engine:
   a. Open your `<pf_install>/pingfederate/bin/run.properties` file.
   b. Change `pf.provisioner.mode` to `STANDALONE`.
   c. Save the file.

To configure the FAILOVER mode instead, refer to the PingFederate documentation.

6. Start PingFederate.
7. If you operate PingFederate in a cluster, repeat steps 2–4 and step 6 for each engine node.

Enabling SSO in PingFederate

Before you can configure SSO in ZPA, you must set a SAML entity ID in PingFederate.

1. In the PingFederate administrative console, go to **System** > **Protocol Settings** > **Federation Info**.
2. In the **SAML 2.0 Entity ID** field, enter a name for PingFederate to use to identify itself to SAML partners.
3. Click **Save**.

Exporting SAML Metadata from PingFederate

Export a metadata file that describes your PingFederate identity provider configuration. For general information about these steps, refer to the PingFederate documentation.

1. In the PingFederate administrative console, go to the **Metadata Export** window.
   - For PingFederate 10.1 or later, go to **System** > **Protocol Metadata** > **Metadata Export**.
   - For PingFederate 10.0 or earlier, go to **System** > **Metadata Export**.
2. On the **Metadata Role** tab, select **I am the identity provider (IdP)**.
3. Click **Next**.
4. On the **Metadata Mode** tab, select **Select information to include in metadata manually**.
5. Click **Next**.
6. On the **Protocol** tab, click **Next**.
7. On the **Attribute Contract** tab, click **Next**.
8. On the **Signing Key** tab, select a signing certificate.
9. Click **Next**.

10. (Optional) On the **Metadata Signing** tab, select a certificate to sign the metadata XML file.
11. Click **Next**.
12. On the **XML Encryption Certificate** tab, select the certificate that you want to use to encrypt the XML content.
13. Click **Next**.
14. On the **Export & Summary** tab, click **Export**.
15. Save `metadata.xml`.
16. Click **Done**.

Enabling Provisioning and SSO in Zscaler

Register PingFederate as an identity provider in Zscaler and download the SAML metadata information. For more information about configuring Zscaler, see Configuring an IdP for Single Sign-On and Enabling SCIM for Identity Management.

1. Sign in to the ZIA Admin Portal as an administrator.
2. On the **Administration** > **Authentication** > **Settings** page, click **Add IdP Configuration**.
3. On the **Add IdP Configuration** page, on the **IdP Information** tab, complete the basic information.
4. Click **Next**.

If you cannot select an authentication domain, contact Zscaler Support. For more information, see Configuring Authentication Settings.

5. On the **SP Metadata** tab, click **Download Metadata**. Save the file as `sp_metadata.xml`.
6. Click **Download Certificate**.
7. Click **Next**.
8. On the **Create IdP** tab, complete the information from PingFederate.
    a. For the **IdP Metadata File**, upload the `metadata.xml file`.
    b. For the **IdP Certificate**, upload your PingFederate signing certificate. For instructions, refer to the PingFederate documentation.
    c. In the **Single Sign-On URL** field, enter your PingFederate single sign-on endpoint based on `https://pf_host:pf_port/idp/SSO.saml2`.
9. In the **IdP Entity ID** field, enter the **SAML 2.0 Entity ID**.
10. In the **SCIM** section, configure **SCIM provisioning**. Click **Save**.
    a. For **SCIM Sync**, click **Enable**.
    b. Note the **SCIM Service Provider Endpoint** and **Bearer Token**.

Creating a Provisioning Connection

To allow PingFederate to manage users in ZPA, create a service provider (SP) connection.

You can follow these steps to create a new SP connection, or you can modify your provisioning connection.

1. In the PingFederate administrator console, configure the data store that PingFederate uses as the source of user data. For instructions, refer to the PingFederate documentation.

   When targeting users and groups for provisioning, exclude the user account that you use to administer users in your connection to ZPA. This prevents the PingFederate provisioning engine from interfering with the account that provisions users and groups.

2. Enable provisioning:
   a. On the **System** > **Protocol Settings** > **Roles & Protocols** window, select **Enable Identity Provider IdP Role** and **Support the Following.**
   b. Select **Outbound Provisioning**.
   c. Click **Save**.

3. In the **Identity Provider** window, in the **SP Connections** section, open an existing connection or create a new one as follows:
   a. Click **Create new**.
   b. In the **Connection Template** window, select **Use a template for this connection**.
   c. In the **Connection Template** list, select **Zscaler ZPA Connector**.
   d. Click **Choose File**, select the `sp_metadata.xml` file, and then click **Open**.
   e. Click **Next**.

4. In the **Connection Type** window, select **Outbound Provisioning** and clear any unwanted types.
5. Click **Next**.
6. In the **General Info** window, the basic connection information is populated by the metadata XML file. Click **Next**.
7. In the **Outbound Provisioning** window, configure the provisioning target and channel as shown in the PingFedreate documentation.
   a. Click **Configure Provisioning**.
   b. In the **Target** window, in the **Base URL** field, enter the **SCIM Service Provider Endpoint**.
   c. In the **Target** window, enter the **Bearer Token**.

PingFederate verifies the access token when you activate the channel and SP connection.

   d. Under **Provisioning Options**, customize the provisioning connector actions as shown in the PingFederate documentation.
   e. Click **Next**.

f. In the **Manage Channels** window, create a channel as shown in the PingFederate documentation.

g. Click **Done**.

For more information about the attributes available in your channel configuration, refer to the PingFederate documentation.

h. In the **Outbound Provisioning** window, click **Next**.

8. In the **Activation and Summary** window, above the **Summary** section, turn on the connection.
9. Click **Save**.

Provisioning Options Reference

The following table lists the main provisioning capabilities available in the Zscaler connection configuration.

Field Name	Description
User Create	Selected (default) – PingFederate creates users in Zscaler. Cleared – PingFederate does not create users in Zscaler.
User Update	Selected (default) – PingFederate updates existing users in Zscaler. Cleared – PingFederate does not update existing users in Zscaler.
User Disable / User Delete	Selected (default) – PingFederate disables or deletes users in Zscaler according to the Remove User Action setting. Cleared – PingFederate does not disable or delete users in Zscaler.
Note: If any of the previous options are cleared, PingFederate logs a warning in the user workflow section of the provisioner.log when the related action fails.	
Remove User Action	This option applies when: • User Disable / User Delete is selected, and a previously provisioned user no longer meets the condition set on the Source Location tab, or a user has been disabled or deleted from the data store. • Disable (default) – PingFederate disables the user in ZPA. • Delete – PingFederate deletes the user from ZPA.

Supported Attributes Reference

The following table lists the attributes that can be mapped for user provisioning to Zscaler.

Attribute	Description
Username	The user's unique identifier in Zscaler. The expected format is user@domain. This attribute is required.
Email	The user's email address.
Display Name	The user's display name (e.g., "Barb Jensen").
Nickname	The user's nickname.(e.g., "Barb" instead of "Barbara").
First Name	The user's first name (e.g., "Barbara" in "Ms. Barbara Jane Jensen, III").
Last Name	The user's last name (e.g., "Jensen" in "Ms. Barbara Jane Jensen, III").
Formatted Name	The user's complete name, including all middle names, titles, and suffises (e.g., "Ms. Barbara Jane Jenson, III").
Department	The user's department or work group, such as "Sales." If no department is specified, Zscaler sets a default value of Service Admin.
Organization	The user's organization.
Cost Center	The user's cost center location.
User type	The type of user in the organization (e.g., "Employee," "Contractor," "Intern," or "Temp").
External ID	A string identifier assigned to a person by the provisioning client.

Creating an SSO Connection

To allow PingFederate to handle SSO to ZPA and create a SP connection:

You can follow these steps to create a new SP connection, or you can modify your provisioning connection.

1. In the PingFederate administrator console, configure the data store that PingFederate uses as the source of user data. For instructions, refer to the PingFederate documentation.
2. On the **Identity Provider** tab, in the **SP Connections** section, open an existing connection or create a new one as follows:
    a. Click **Create new**.
    b. On the **Connection Template** tab, select **Use a template for this connection**.
    c. In the **Connection Template** list, select **Zscaler ZPA Connector**.
    d. Click **Choose File**.
    e. Select the `sp_metadata.xml` file.
    f. Click **Open**.
    g. Click **Next**.
3. On the **Connection Type** tab, select **Browser SSO Profiles** and clear any unwanted types.
4. Click **Next**.
5. On the **General Info** tab, the basic connection information is populated by the metadata XML file.
6. Click **Next**.

7. On the **Browser SSO** tab, configure the browser SSO. For a complete guide, refer to the PingFederate documentation.
    a. On the **Browser SSO** > **SAML Profiles** tab, select **IdP-Initiated SSO** and **SP-Initiated SSO**.
    b. On the **Browser SSO** > **Protocol Settings** > **Allowable SAML Bindings** tab, select **POST**.
    c. On the **Browser SSO** > **Protocol Settings** > **Signature Policy** tab, select **Always sign assertion**.
8. On the **Credentials** tab, configure the connection credentials.
9. Click **Next**. For a complete guide, refer to the PingFederate documentation.
10. On the **Credentials** > **Signature Verification Settings** > **Signature Verification Certificate** tab, click **Manage Certificates** and import the certificate.
11. On the **Activation and Summary** tab, above the **Summary** section, turn on the connection.
12. Click **Save**.

Configure PingOne and ZPA—SAML and SCIM

The following sections describe how to configure PingOne and ZPA to use SAML and SCIM.

Add the Zscaler ZPA Application to PingOne

The first step is to add the Zscaler applications used to enable authentication and provisioning to PingOne. From the PingOne portal administrator account:

1. Go to **Applications** > **My Applications** > **Add Application**.

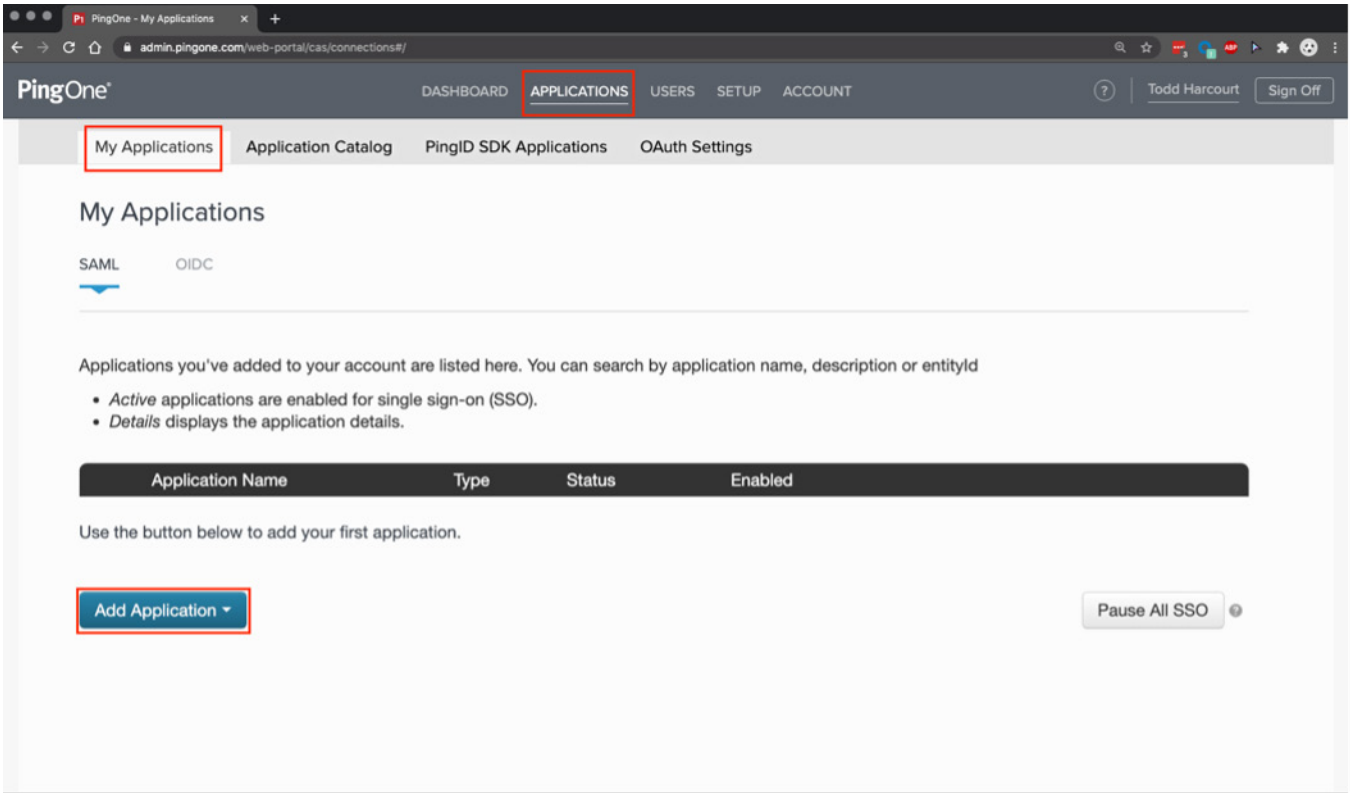


Figure 20. Adding an application

2. Search for `zscaler` and select **Zscaler Private Access 2.0 SAML** with provisioning API for ZPA and SCIM provisioning.

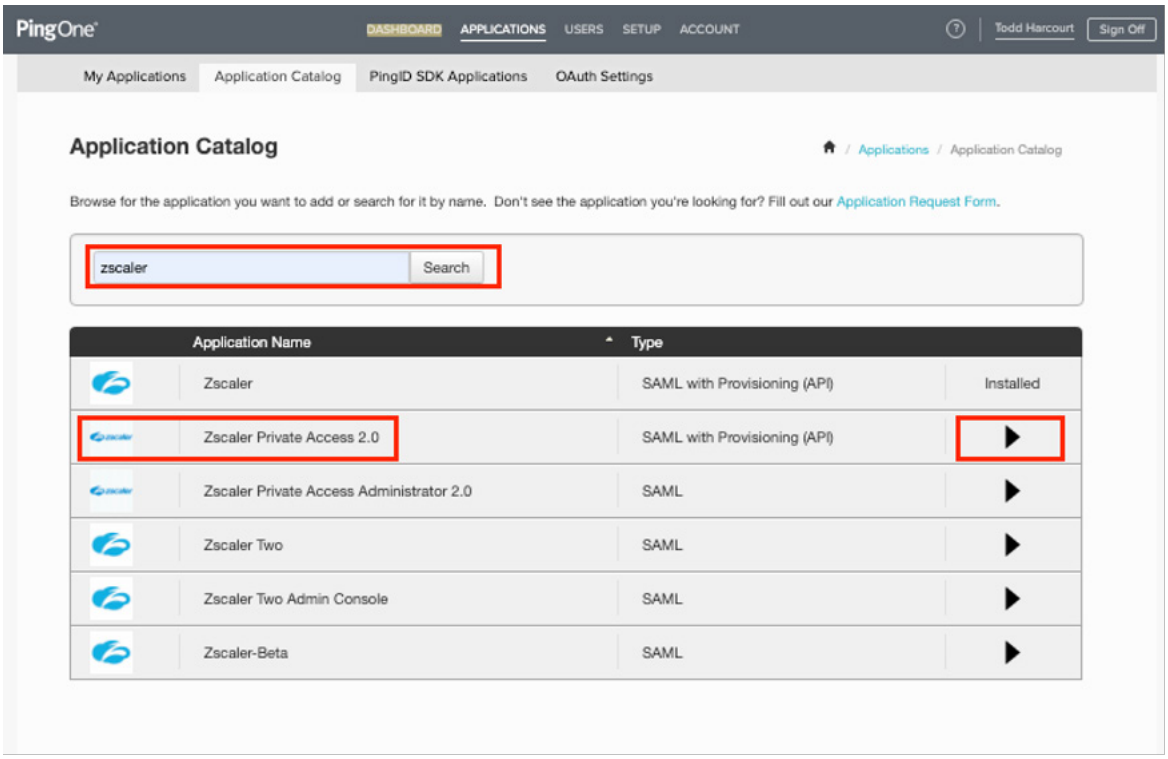


Figure 21. Adding the Zscaler ZPA application

3. Click the arrow on the right to display a description of the application.
4. Click **Setup** to begin the installation process.

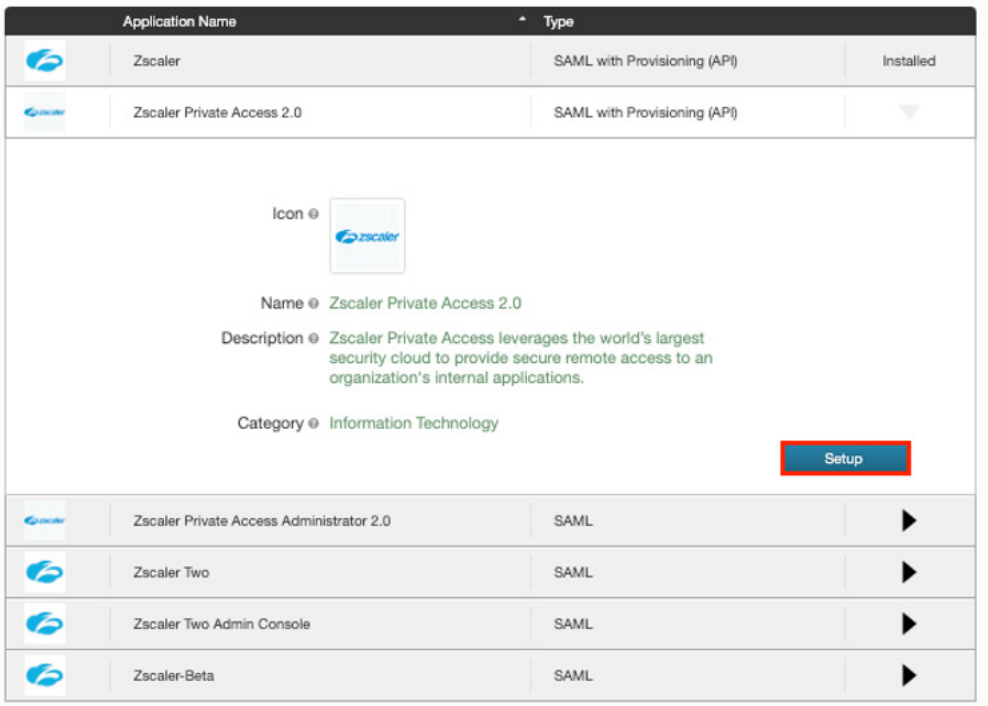


Figure 22. ZPA 2.0

The initial configuration window is displayed.

Configure PingOne for ZPA

To configure PingOne and ZPA:

1. Click **Download** next to the Signing Certificate.
2. Copy the **IdP ID** and the **Issuer** URL. The IdP ID is appended to the **URL Prefix** to create the **SAML Portal URL** used in the ZPA IdP setup process.
3. Click **Continue to Next Step**.

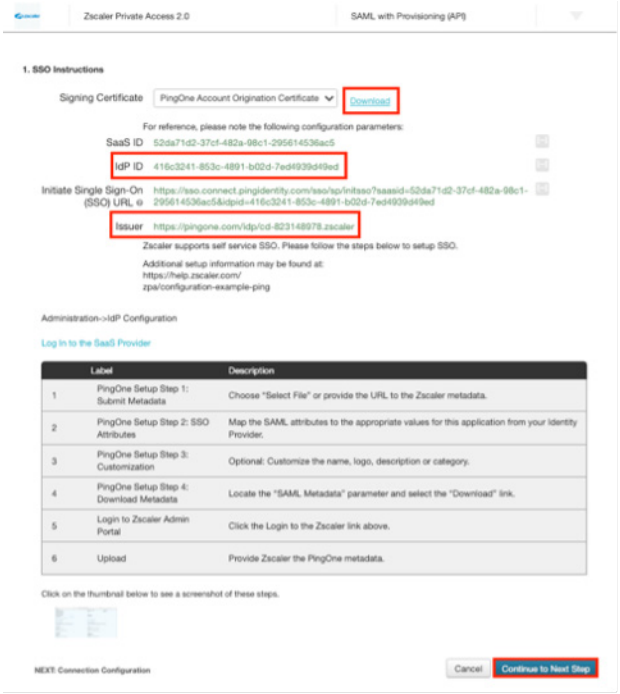


Figure 23. PingOne Zscaler Private Access 2.0 configuration

You can find the SAML base URL in the PingIdentity documentation.

In this configuration example, the SAML Portal URL is created by combining the Base SAML Portal URL and the IdP ID to become:

Open a new browser and log in the ZPA Admin Portal.

Configure ZPA for a PingOne IdP

In the ZPA Admin Portal, go to **Administration** > **Authetication** > **User Authenticantion** > **IdP Configuration**. The **IdP Configuration** page appears.

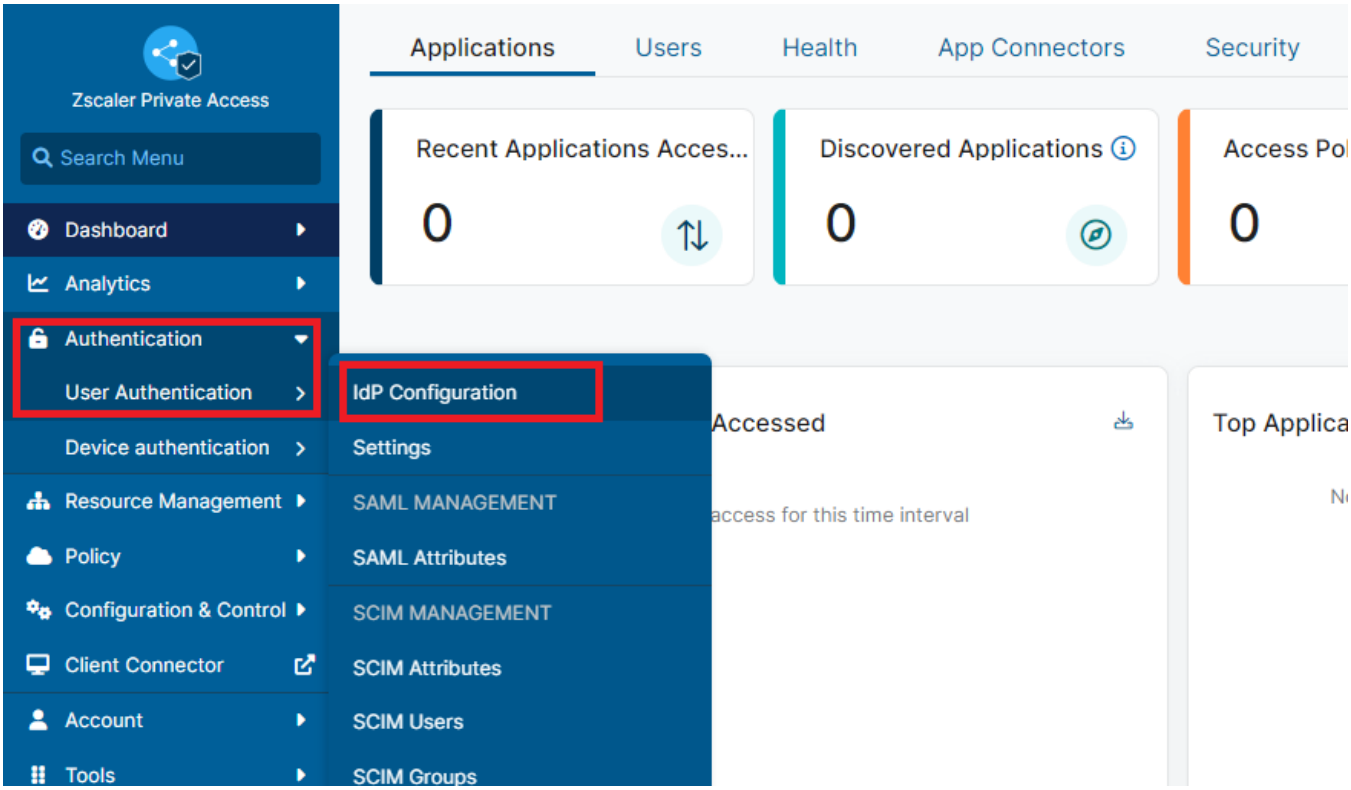


Figure 24. Creating the PingOne IdP on ZPA

Add the PingOne IdP on ZPA

On the **IdP Configuration** page, select **Add IdP Configuration**. The IdP Configuration wizard appears, which walks you through the creation of the IdP.

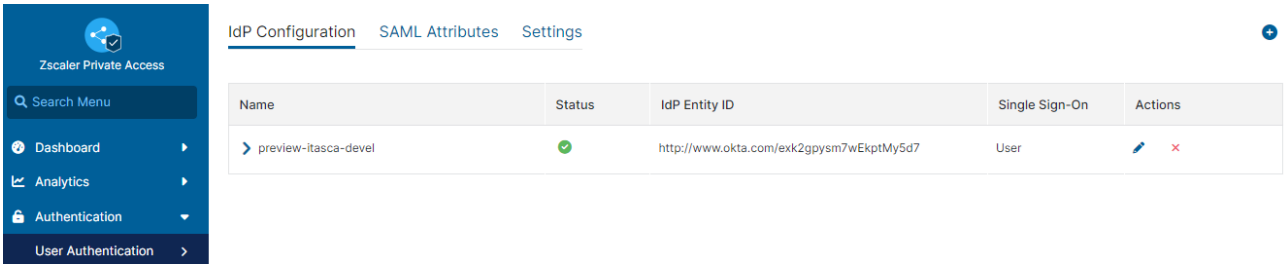


Figure 25. Add a new IdP

If the window is constrained, only the circle with the white plus sign is visible.

IdP on ZPA—IdP Information

In the **Add IdP Configuration** window:

1. Enter a **Name** for the IdP.
2. Make sure **User** is selected for **Single Sign-On**.
3. Select the authentication domains that are serviced by this IdP.
4. Click **Next**.

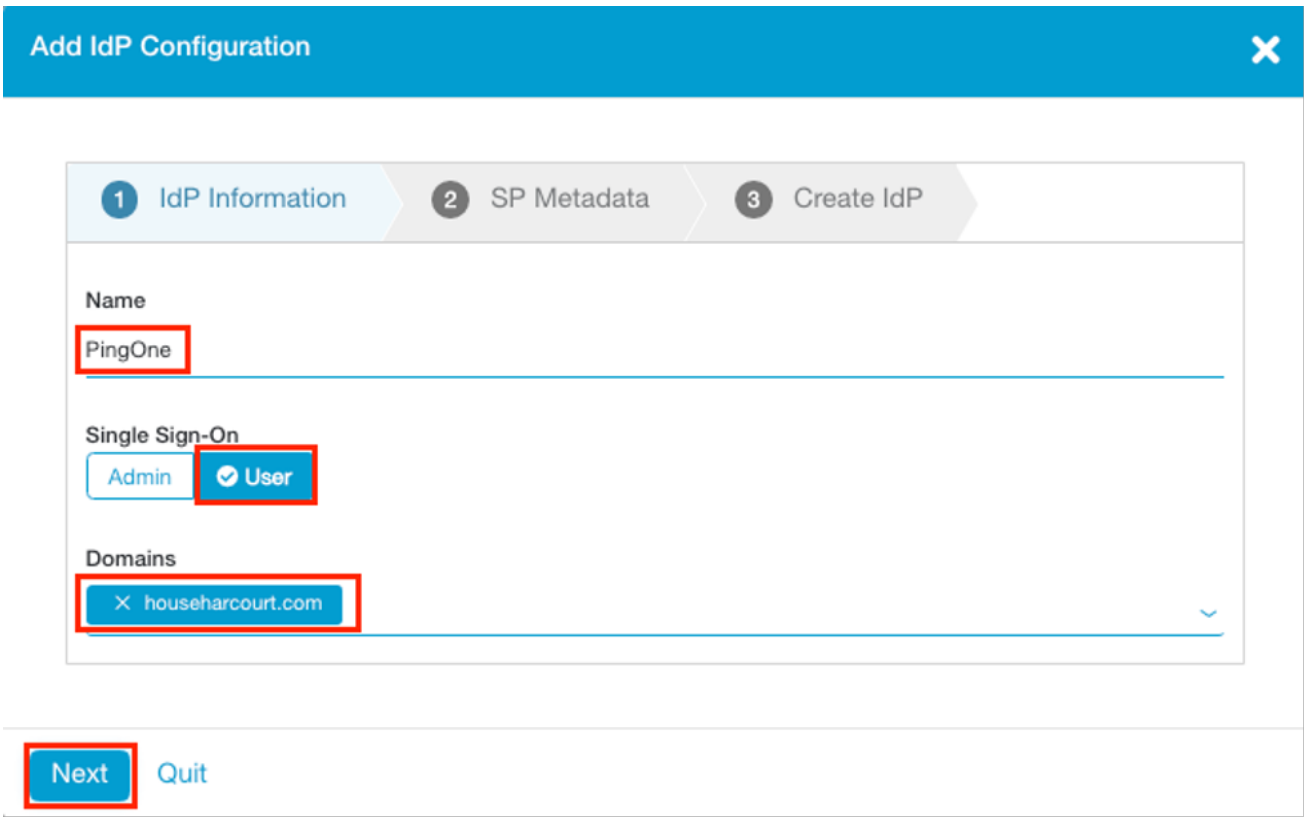


Figure 26. IdP information

Multiple IdPs are supported in ZPA, and the IdP is bound to the domain in this step. ZPA only supports one domain for Zscaler Client Connector deployments. Additional IdPs are defined for Browser Access domains.

IdP on ZPA—SP Metadata

You must download the Service Provider Metadata and the Service Provider Certificate.

On the **SP Metadata** tab, download and save both files, and then click **Next**.

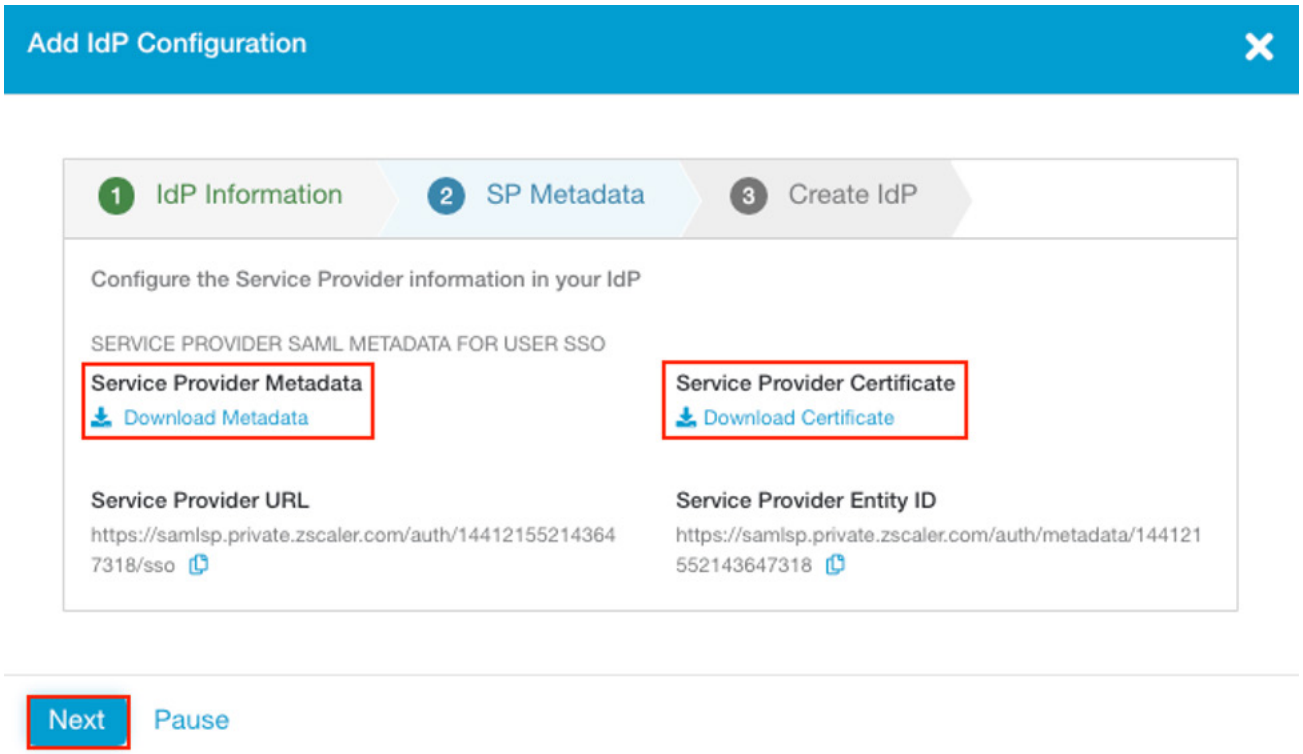


Figure 27. Service Provider Metadata

IdP on ZPA—Create IdP

On the **Create IdP** tab:

1. Upload the PingOne certificate file (downloaded in the previous step).
2. Enter the **Single Sign-On URL**.
3. Enter the **Issuer** URL as the **IdP Entity ID**.
4. Select **Enabled** for **SCIM Sync**.
5. Click **Generate New Token**. This displays the SCIM parameters needed for the remaining PingOne configuration.
6. Save both the **SCIM Service Provider Endpoint** URL and the **Bearer Token** for the PingOne configuration.
7. Click **Save**.

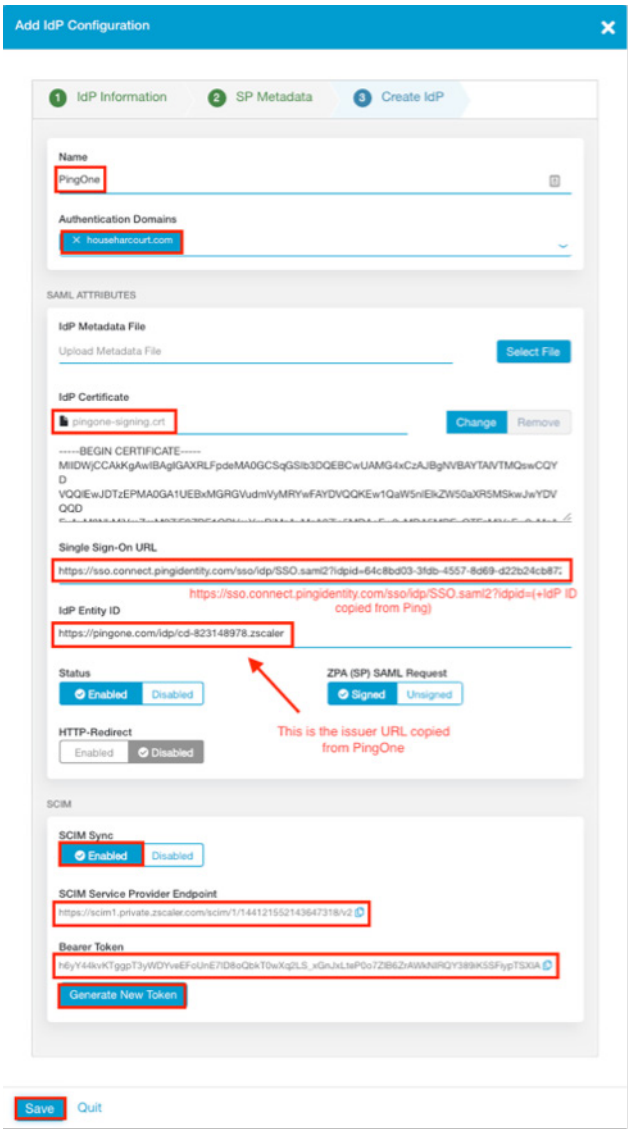


Figure 28. Add IdP configuration

Finish Configuring PingOne for ZPA

To finish the PingOne configuration to use with ZPA:

1. Upload the Zscaler metadata file and the Zscaler signing certificate.
2. Select **Set Up Provisioning**.
3. Click **Continue to Next Step**.

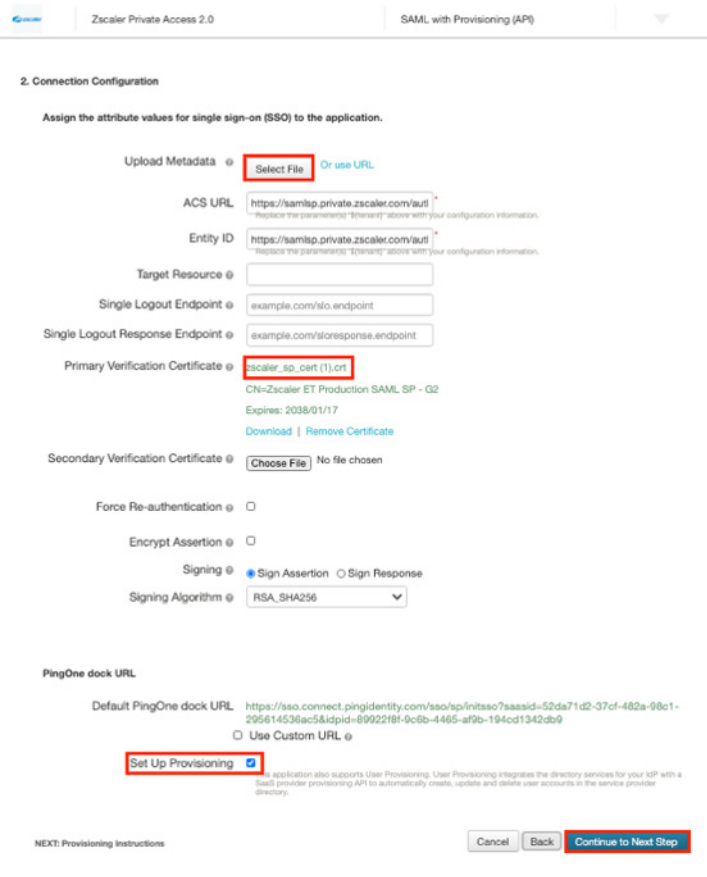


Figure 29. Add IdP configuration

4. Review the remaining configuration steps, and then click **Continue to Next Step**.

Zscaler Private Access 2.0 | SAML with Provisioning (API)

3. Provisioning Instructions

To configure User Provisioning to Zscaler Private Access, follow the steps below.

	Label	Description
1	ZPA Provisioning Setup	For more information on the required ZPA configuration, see https://help.zscaler.com/zpa/enabling-scim-identity-management. Note the Base URL and Bearer Token required for the next steps.
2	Obtain Your Zscaler Base URL	The Base URL for Zscaler. For example, https://scim1.private.zscaler.com/scim/1/<directoryId>/v2.
3	Obtain Your Zscaler Bearer Token	The access token used to make authenticated API calls to Zscaler.
4	Application Configuration	On the Application Configuration screen enter the Base URL and Bearer Token obtained in the previous steps into the relevant fields.
5	Attribute Mapping	Map the user store attributes to Zscaler attributes that are to be managed during user provisioning.
6	Configure targeted group(s)	Once the application is configured, navigate to the Group Management page and select the group(s) to target for provisioning.

NEXT: Application Configuration

Cancel | Back | Continue to Next Step

Figure 30. Provisioning instructions

Configure PingOne and SCIM

To configure SCIM:

1. Enter the base URL into the **BASE_URL** field.
2. Enter the Bearer Token value into the **BEARER_TOKEN** field.
3. Click **Continue to Next Step**.

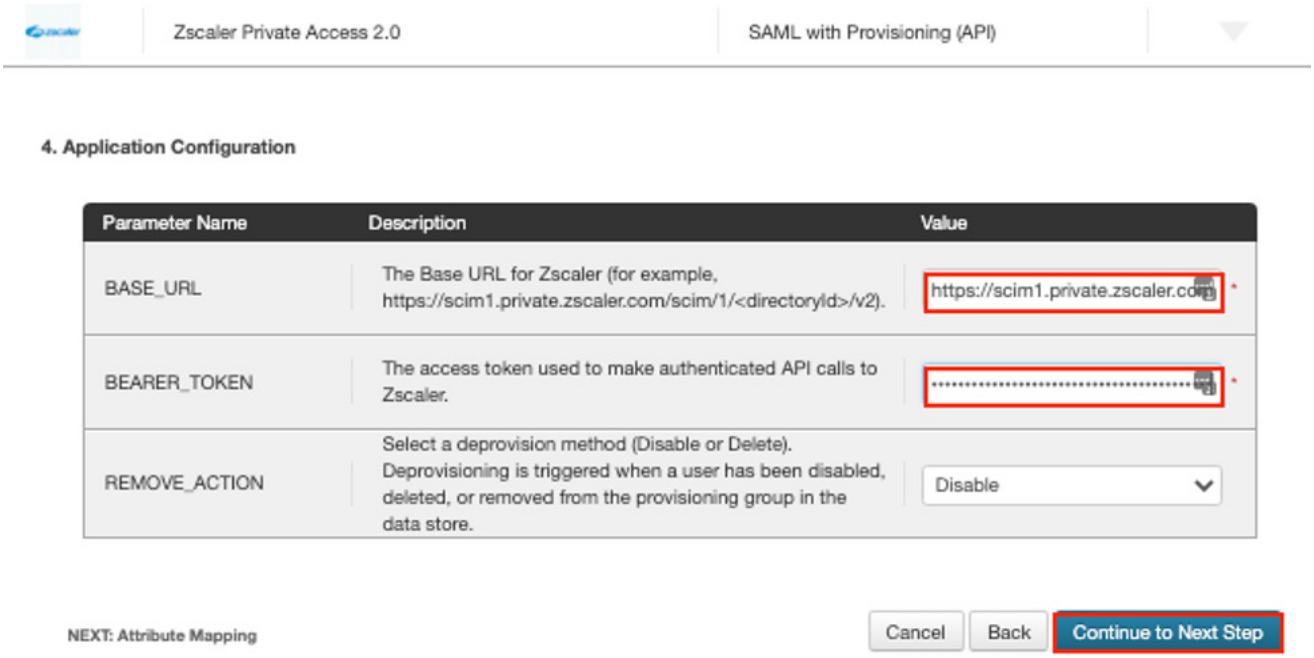


Figure 31. PingOne SCIM configuration

PingOne Provisioning Attribute Mapping

For Self-Provisioning and SCIM to function properly, you must map the Ping attributes to match the expected ZPA attributes. Set the following attributes:

1. **SAML_SUBJECT (sso)**: `SAML_SUBJECT`
2. **First Name (sso)**: `First Name`
3. **Last Name (sso)**: `Last Name`
4. **Email Address (sso)**: `Email`
5. **Group (sso)**: `memberOf`
6. **userName (provisioning)**: `Email`
7. **displayName (provisioning)**: `userName`
8. **externalID (provisioning)**: `externalID`
9. **firstName (provisioning)**: `First Name`
10. **lastName (provisioning)**: `Last Name`

	Application Attribute	Description	Identity Bridge Attribute or Literal Value
1	SAML_SUBJECT (sso) *	Map this to the username in Zscaler	SAML_SUBJECT
2	First Name (sso)	Map appropriate source attribute for user's first name	First Name
3	Last Name (sso)	Map appropriate source attribute for user's last name	Last Name
4	Email Address (sso)	Map appropriate source attribute for user's email address	Email
5	Department (sso)	Map appropriate source attribute for user's department	
6	Group (sso)	Map appropriate source attribute for user's group memberships	memberOf
7	userName (provisioning) *	Zscaler's unique identifier for the user. The expected format is user@domain (for example, 'bjensen@example.com'). A username cannot be updated. This attribute is required.	Email
8	displayName (provisioning) *	The name of the user, suitable for display to end-users. This attribute is required.	userName
9	costCenter (provisioning)	The cost center for the user.	
10	department (provisioning)	The department for the user. If no department is specified, Zscaler sets a default value of 'Service Admin'.	
11	division (provisioning)	The division for the user.	
12	email (provisioning)	The email for the user (for example, 'bjensen@example.com').	Email
13	externalID (provisioning)	A String that is an identifier for the resource as defined by the provisioning client.	externalID
14	firstName (provisioning)	The given name of the User, or first name in most Western languages (e.g., 'Barbara' given the full name 'Ms. Barbara Jane Jensen, III').	First Name
15	formattedName (provisioning)	The user's formatted name.	
16	lastName (provisioning)	The family name of the User, or last name in most Western languages (e.g., 'Jensen' given the full name 'Ms. Barbara Jane Jensen, III').	Last Name
17	nickName (provisioning)	The user's nickname.	
18	organization (provisioning)	The organization for the user.	
19	userType (provisioning)	The user type for the user. (E.g. 'Contractor', 'Employee', or 'Intern')	

Figure 32. Assigning the ZPA application

SCIM only pushes, deletes, or disables the user. SCIM doesn't push the security groups. The security groups are pulled over from auto-provisioning for use with ZPA policies.

PingOne Portal Settings

The next step is to customize how the application is going to look on the PingOne portal. Make any changes specific to your installation, and then click **Continue to Next Step**.

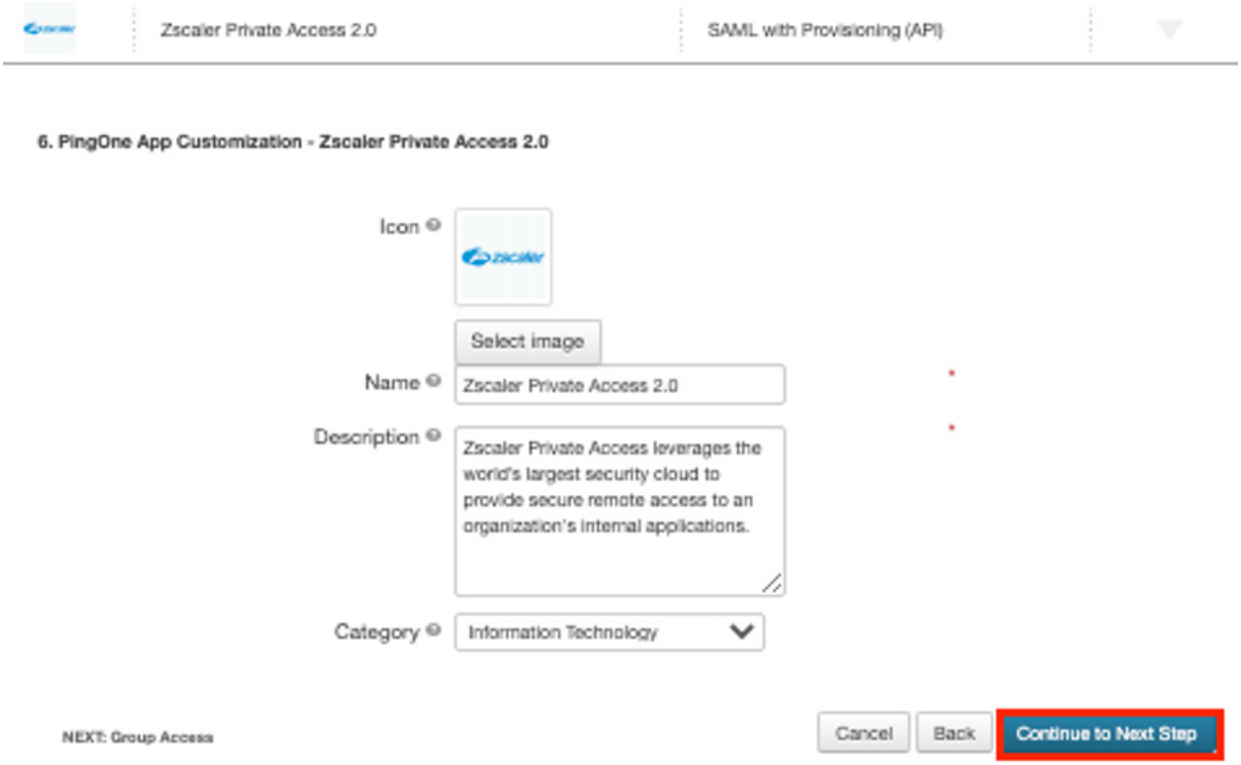


Figure 33. PingOne portal settings

Enable ZPA Users on PingOne

The last step is to select the security groups that can use ZPA. Add any or all groups specific to your installation, and then click **Continue to Next Step**.

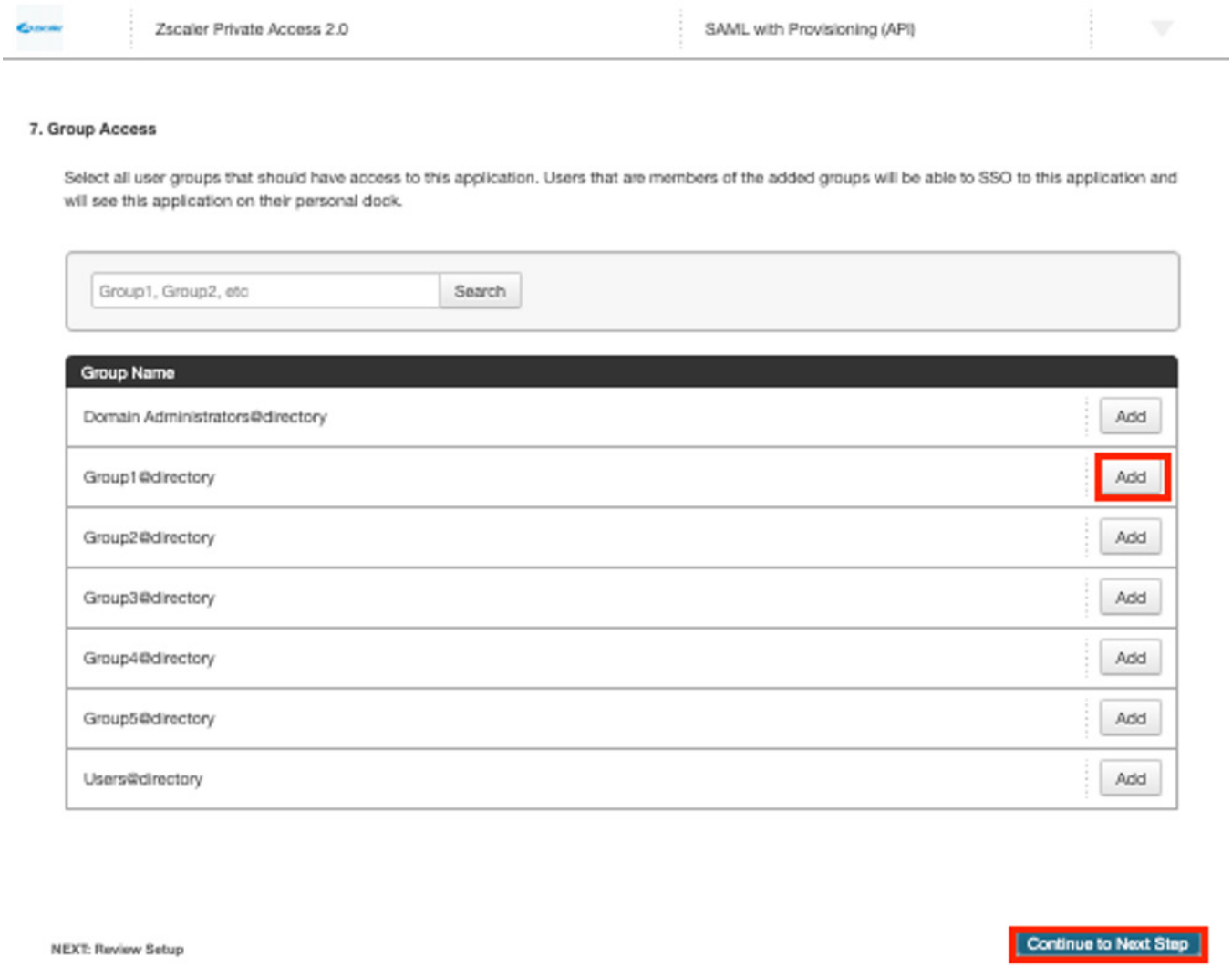


Figure 34. PingOne provisioning

Finalize the PingOne Configuration

Select **Enable API Integration**, which displays the API parameters:

1. Enter the **SCIM Service Provider Endpoint URL** and the **Bearer Token**.
2. Click **Test API Credentials**. If the credentials are valid and PingOne can communicate with the Zscaler cloud, the response is highlighted in red. If you receive an error, you need to re-copy the URL and token and possibly generate a new Bearer Token.
3. After you have verified your credentials, click **Finish**.

Figure 35. SCIM integration API setup

Test the ZPA Authentication Configuration from the ZPA Admin Portal

Import the SAML variables from PingOne. In the ZPA Admin Portal:

1. Select **Authentication** > **User Authentication** > **IdP Configuration**.
2. Click the **Expand** icon next to your IdP. This shows the PingOne configuration.
3. Click **Import** under **Import SAML Attributes**. After this is selected, ZPA authenticates to PingOne using your existing user if you are authenticated, or the PingOne login window is displayed. The SAML variables and the SAML assertion are displayed in the window on the next page.

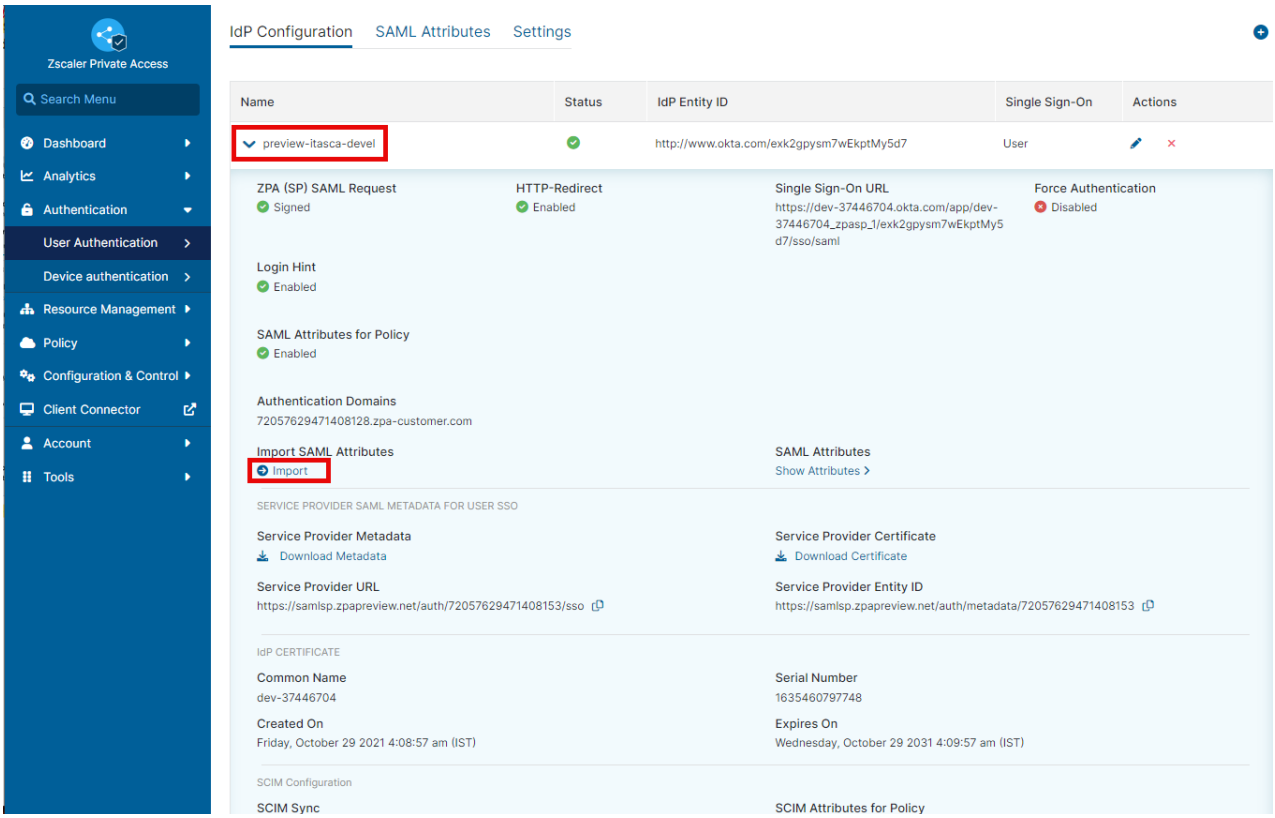


Figure 36. SAML variable import

4. Review your mappings and click **Save** to save the Attribute variables.

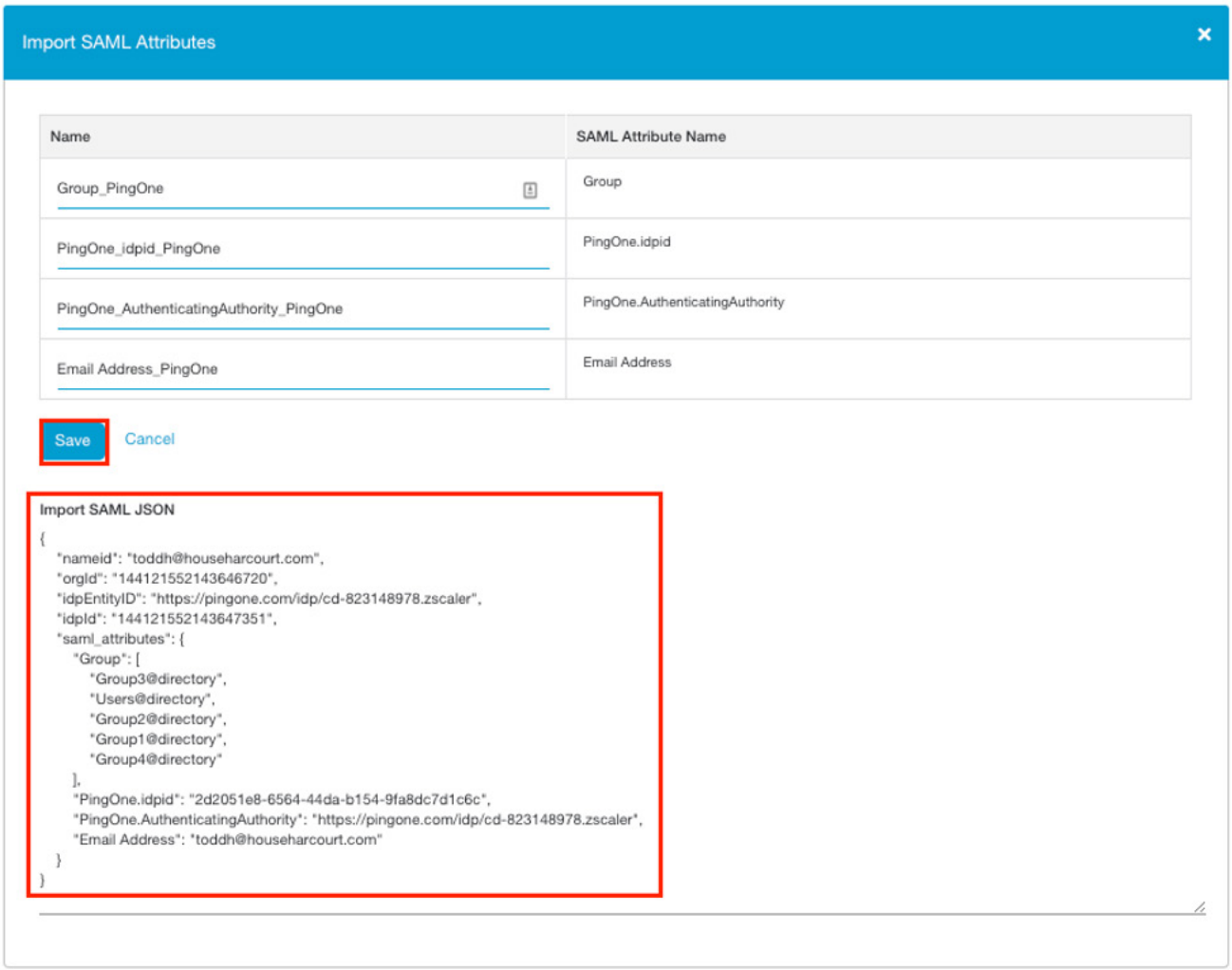


Figure 37. SAML Assertion and SAML Attributes

Test the ZPA Authentication Configuration Using the ZPA Test URL

You can test the configuration using the following URL. Replace <domain> with your domain in the URL, and your SAML Assertion is returned if you are an already authenticated user. Otherwise, you are prompted to authenticate.

After you are authenticated, your SAML assertion is displayed.

Test URL:

```
https://samlsp.private.zscaler.com/auth/v2/login?domain=<domain>&ssotype=test
```

SAML Assertion


```
{"nameid":"toddh@househarcourt.com","orgId":null,"idpEntityID":null,"idpId":null,"saml_
attributes":{"Group":["Group3@directory","Users@directory","Group2@directory","Group1@
directory","Group4@directory"],"PingOne.idpid":"2d2051e8-6564-44da-b154-
9fa8dc7d1c6c","PingOne.AuthenticatingAuthority":"https://pingone.com/idp/cd-823148978.
zscaler","Email Address":"toddh@househarcourt.com"},"samlassertion":null}
```


Using PingOne for ZIA Admin Access

The following sections describe how to configure PingOne and ZIA access.

Add the PingOne SAML Application

To use PingOne SAML authentication for the ZIA Admin Portal, install the **SAML Service Provider Application**.

From the PingOne portal:

1. Go to **Applications** > **My Applications**.
2. Click **Add Application**.

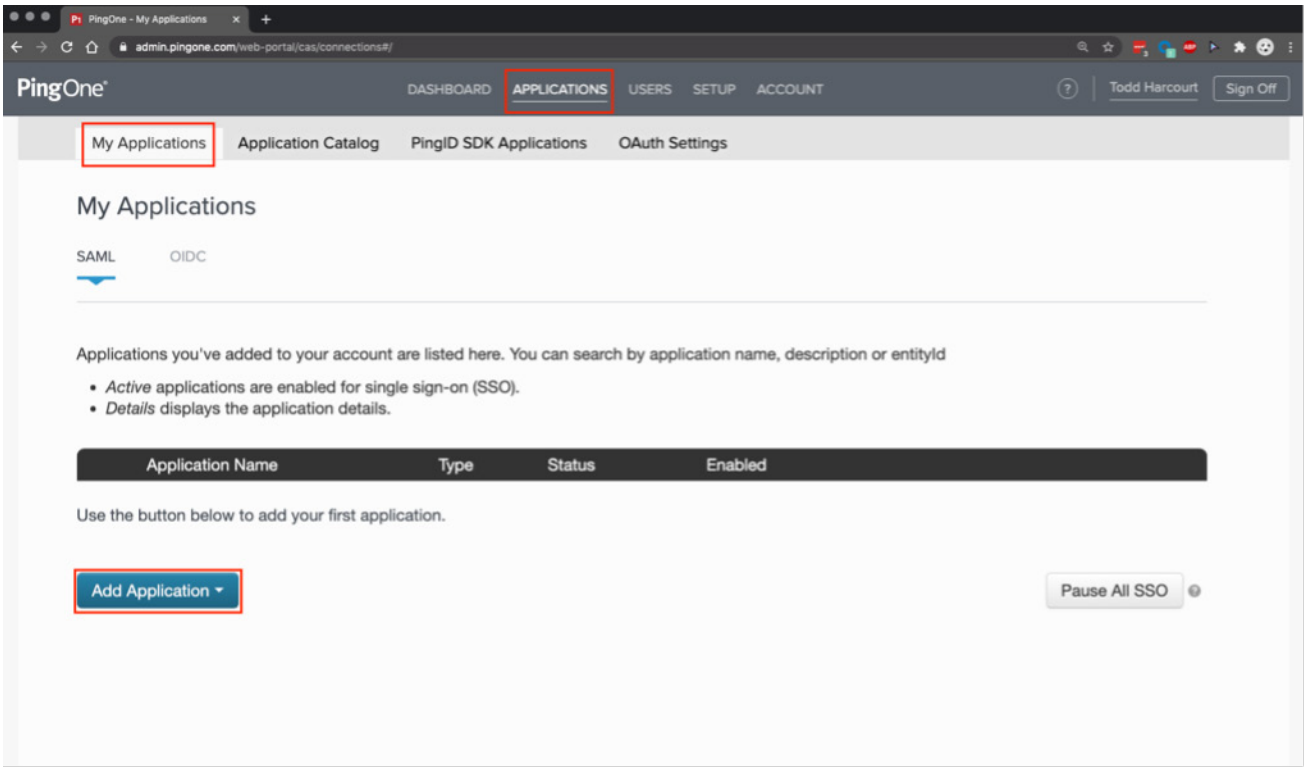


Figure 38. Adding the PingOne SAML application for ZIA admin authentication

PingOne SAML ZIA Admin Console Application

To add the application:

1. Search for `zscaler`.
2. Select **Zscaler Two Admin Console Application**.
3. Select the arrow on the right to display a description of the application.

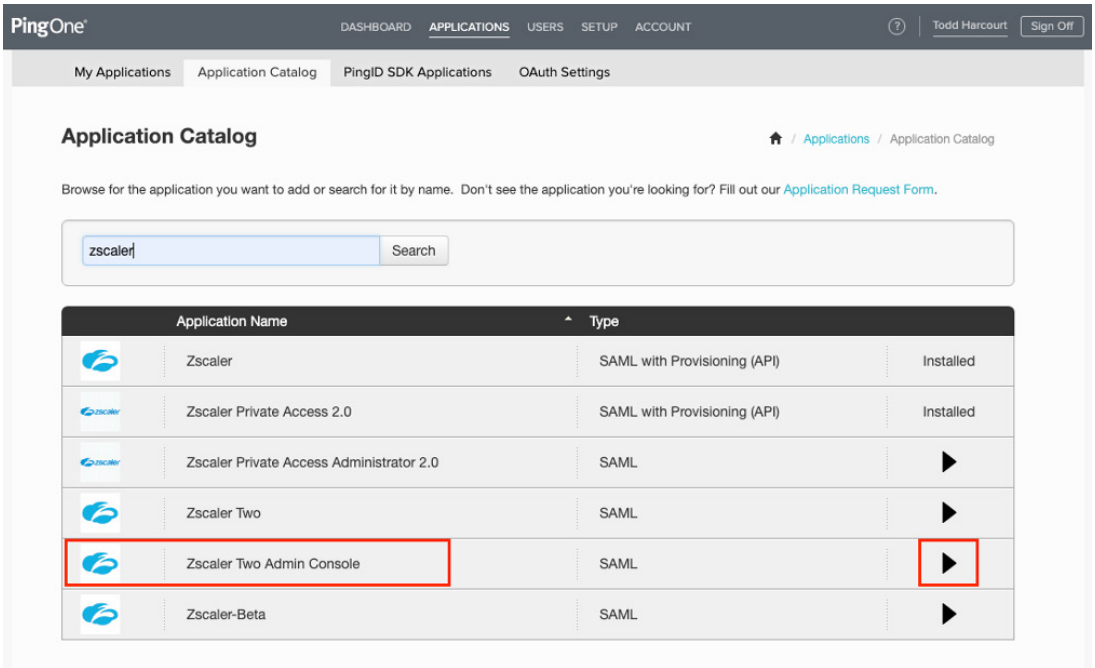


Figure 39. The PingOne SAML for ZIA administrators

Add the Application

Verify the application description and click **Setup**.

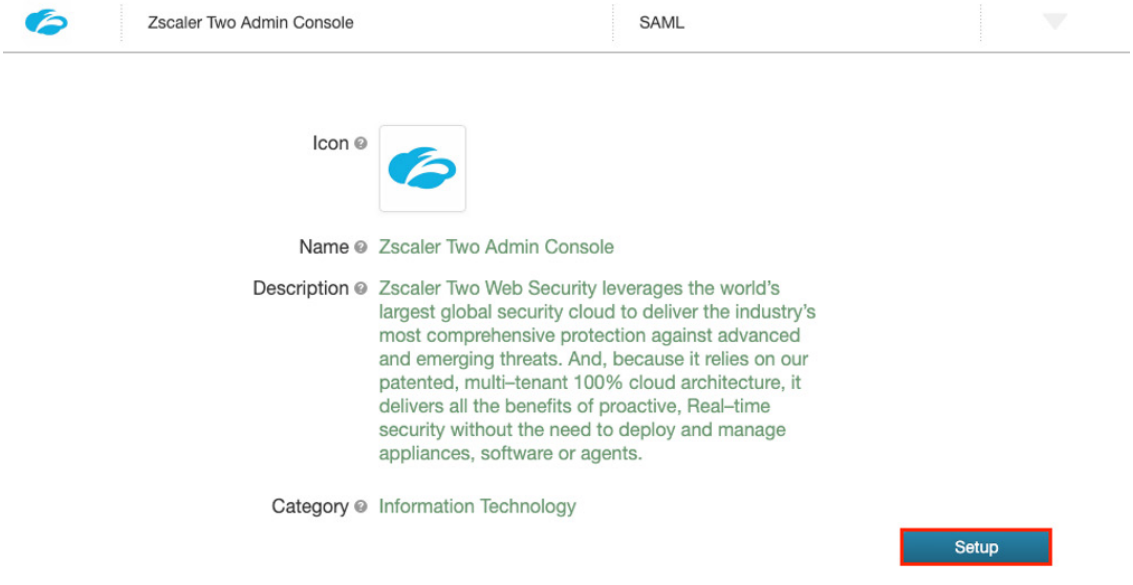


Figure 40. General settings

Configure the ZIA Administrator Application

To display the initial configuration window:

1. Click **Download** to download the signing certificate.
2. Copy the **IdP ID** and the **URL of the SAML Portal**. The IdP ID is appended to the Example URL to create the **SAML Portal URL** that is used in the Zscaler IdP setup process.
3. Click **Continue to Next Step**.

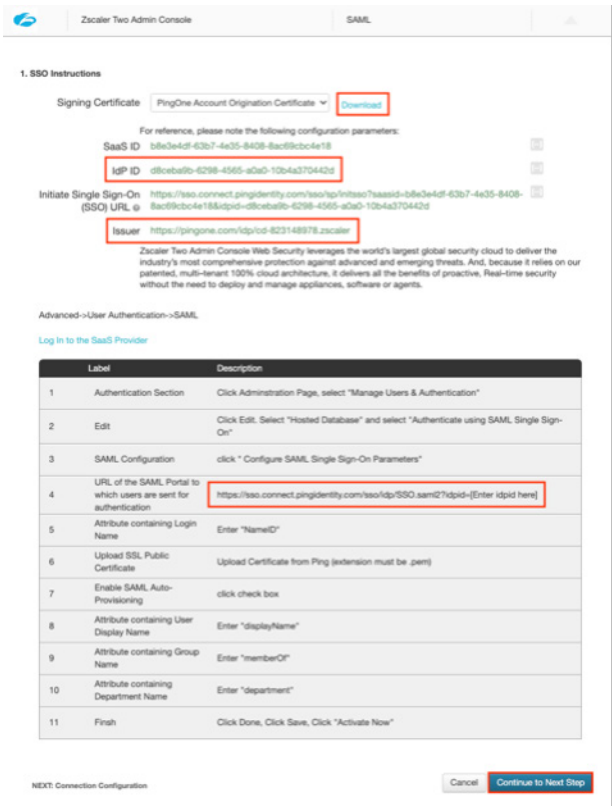


Figure 41. Configuration settings

Configuring the ZIA Admin Portal for SAML-Based Authentication

In the ZIA Admin Portal:

1. Go to **Administration** > **Administrator Management**.
2. Select **Enable SAML Authentication**.
3. Verify the certificate file type is .pem.
4. Upload the IdP certificate.
5. Download and save the **XML Metadata**.
6. Add the **Issuer** URL by clicking **Add Items**.
7. Click **Save**.

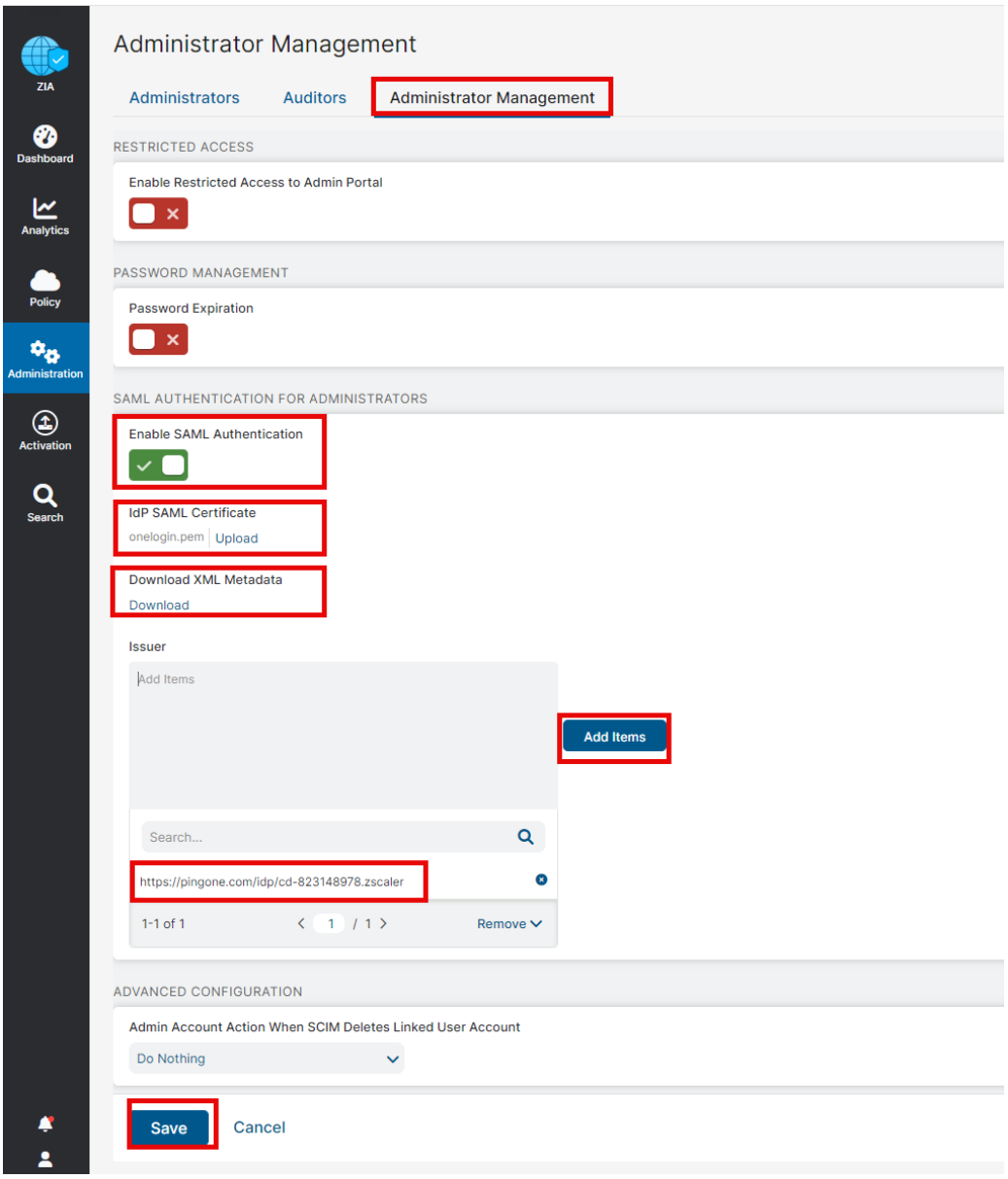


Figure 42. Configure SAML-based authentication for administrators

Adding Administrators for SAML-Based Authentication

Each administrator must be added as a ZIA administrator to use SAML-Based Authentication.

1. Go to **Administration** > **Administrators**.
2. Click **Add Administrators** to add the administrators.

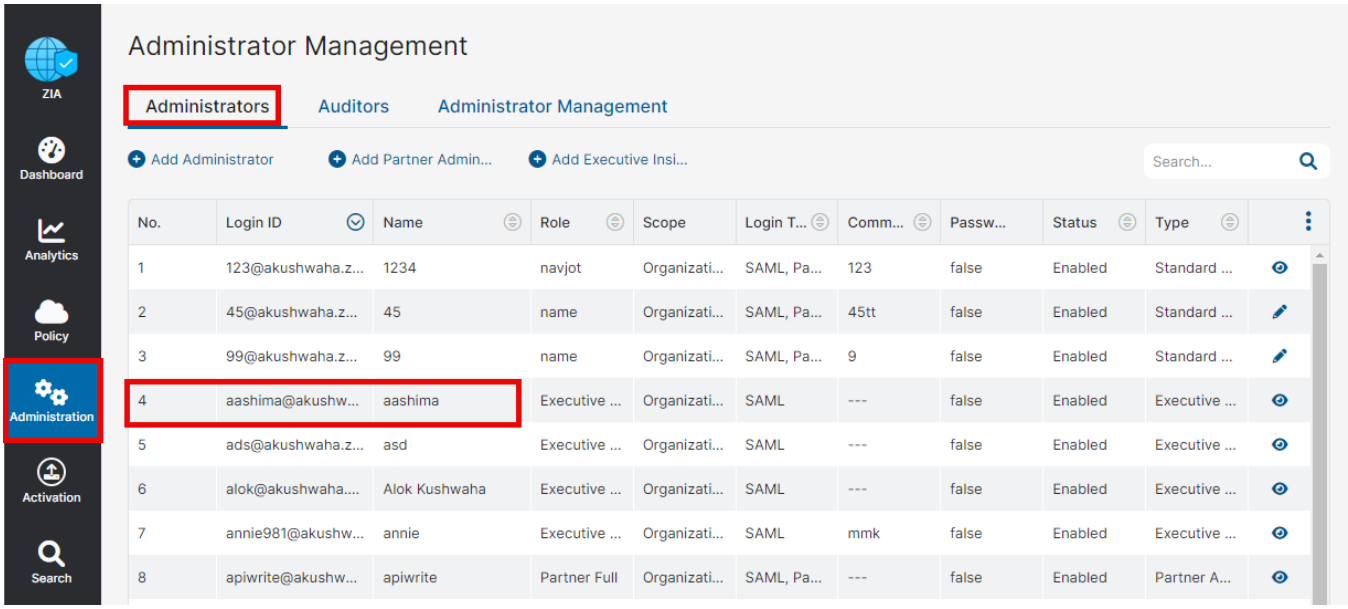


Figure 43. Verify administrators

Finish Configuring the ZIA Administrator Application

In the PingOne configuration, upload the Zscaler metadata file and click **Continue to Next Step**.

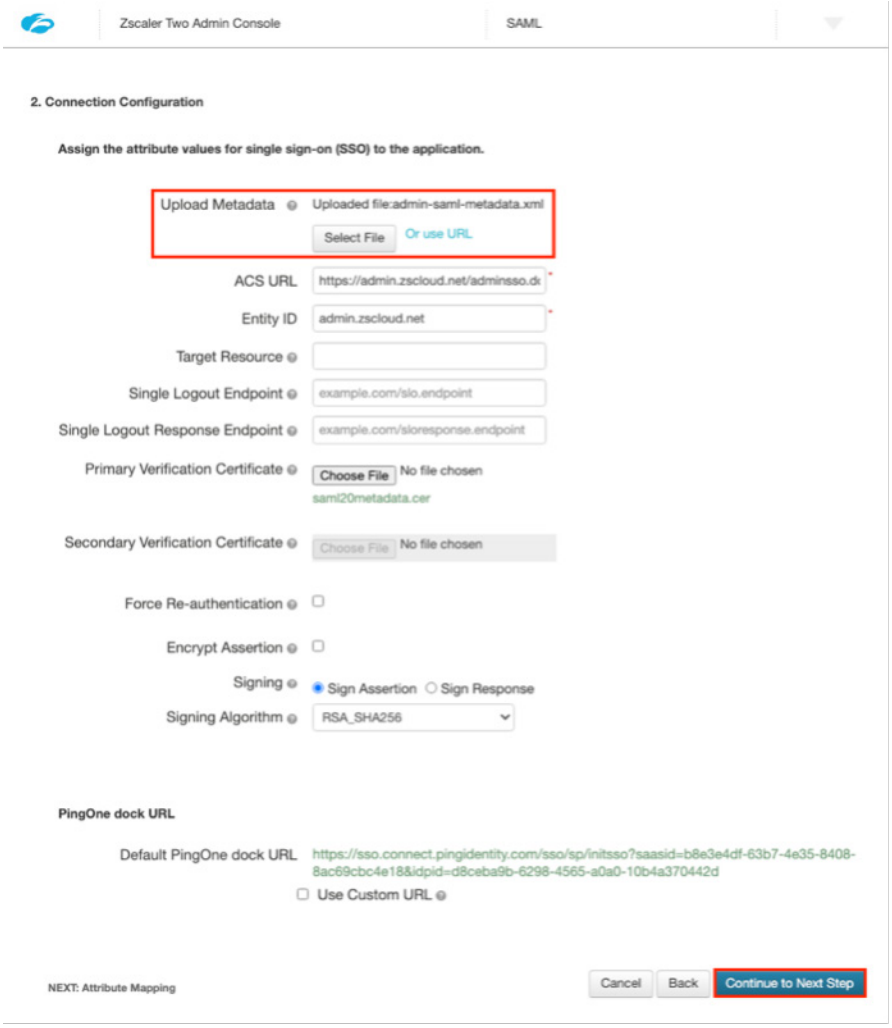


Figure 44. PingOne configuration

Attribute Mapping

Leave the attribute mapping as default, and click **Continue to Next Step**.

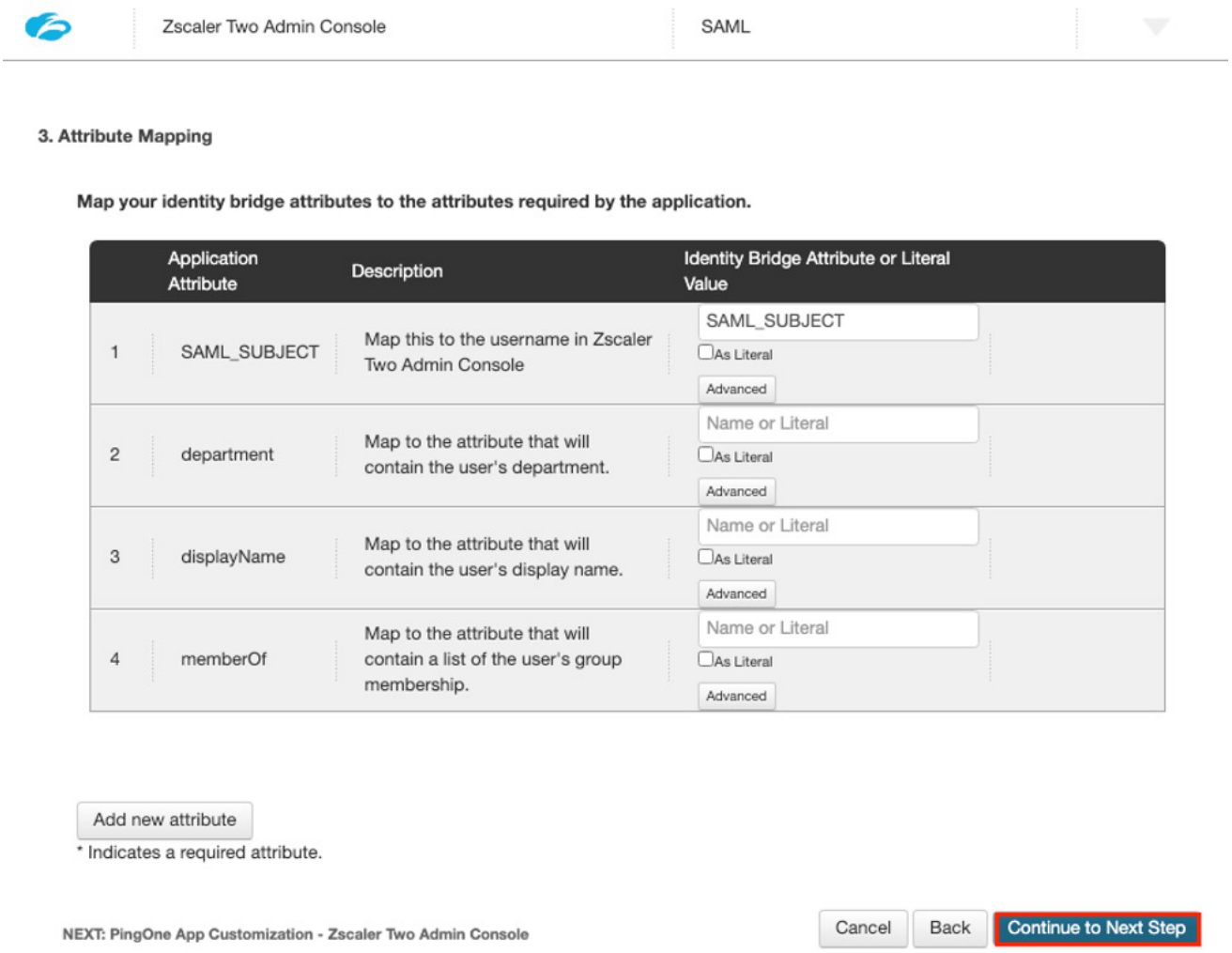


Figure 45. Attribute mapping

Changing the Portal Icon

Leave the **Icon** and **Description** as default, and click **Continue to Next Step**.

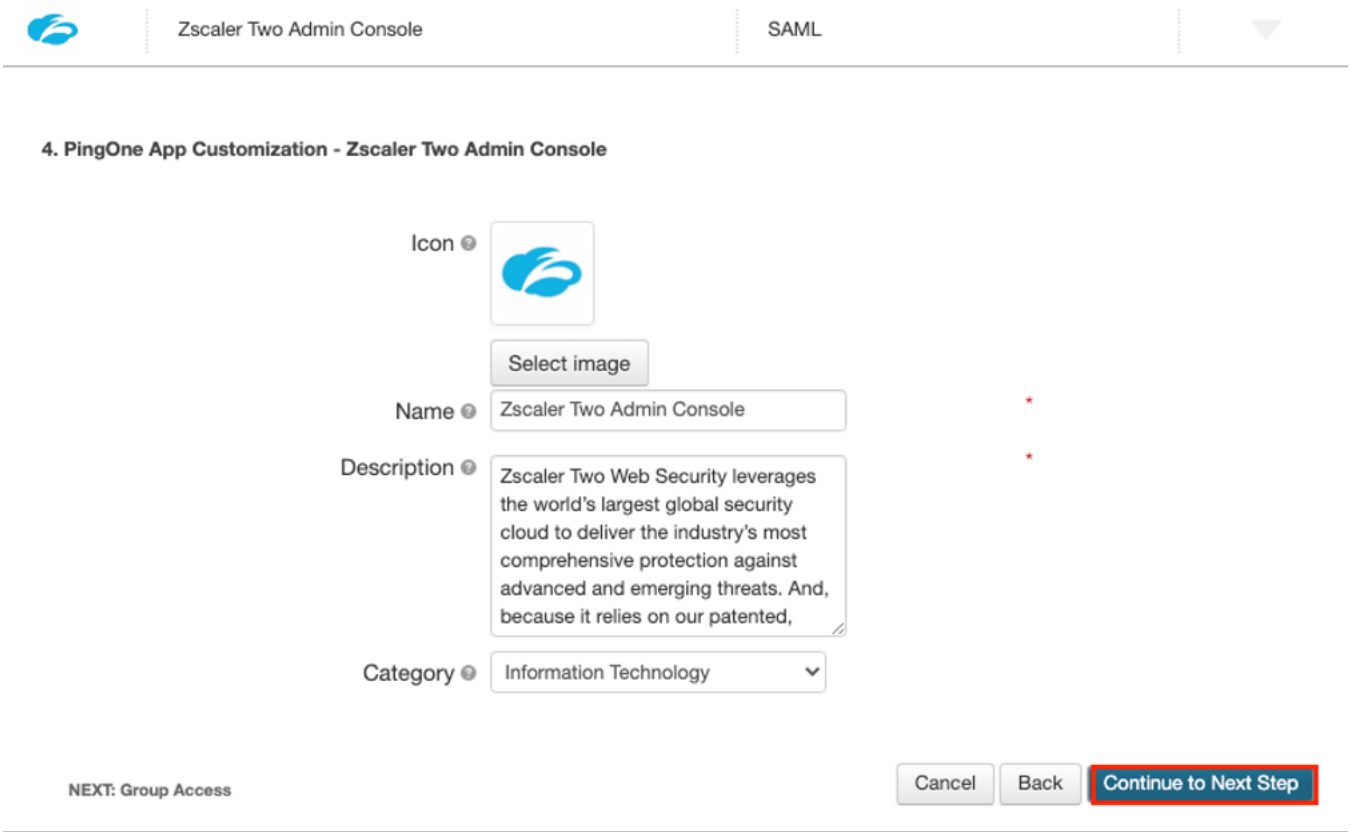


Figure 46. Portal icon and description

You can customize the look and change the description as desired by your organization.

Adding the Administrator Group

Add the groups included in the Administrators so they are allowed to authenticate using SAML.

Add the appropriate groups, and click **Continue to Next Step**.

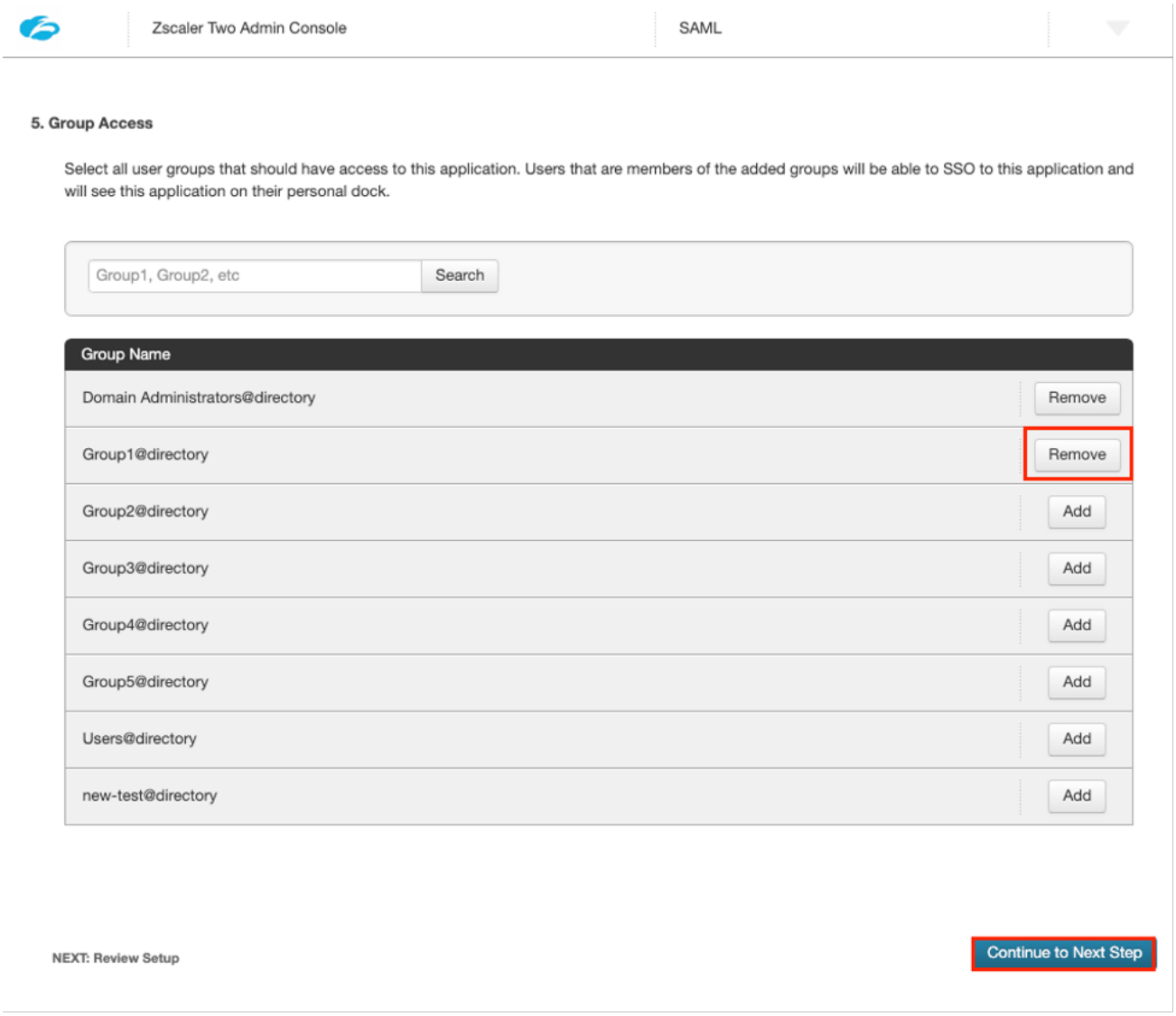


Figure 47. Add administrator groups

Finalize the Configuration

Verify the PingOne settings, and click **Finish** to save your configuration.

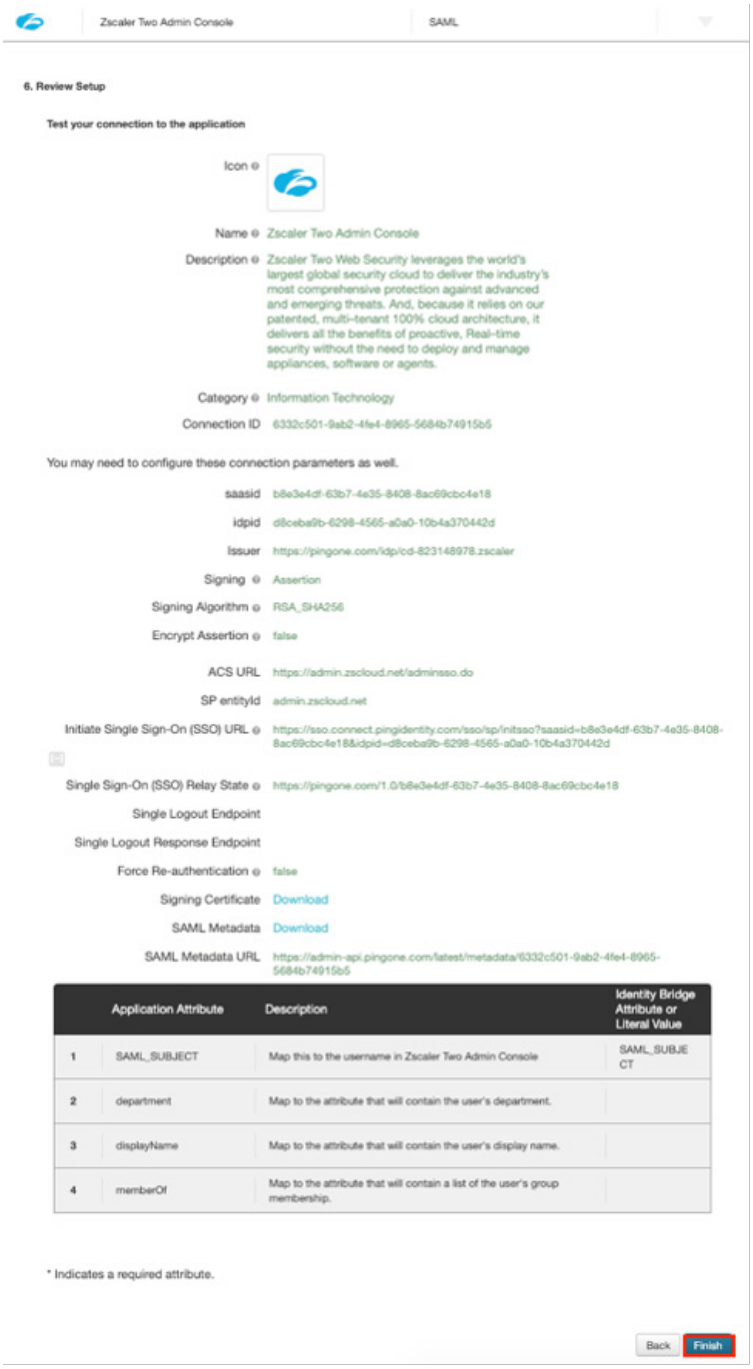


Figure 48. Configuration review

Test the Admin SSO Access

You are now ready to launch the ZIA Admin Portal from the PingOne portal and the SAML application. Authenticate to PingOne using SAML and log in to the ZIA Admin Portal.

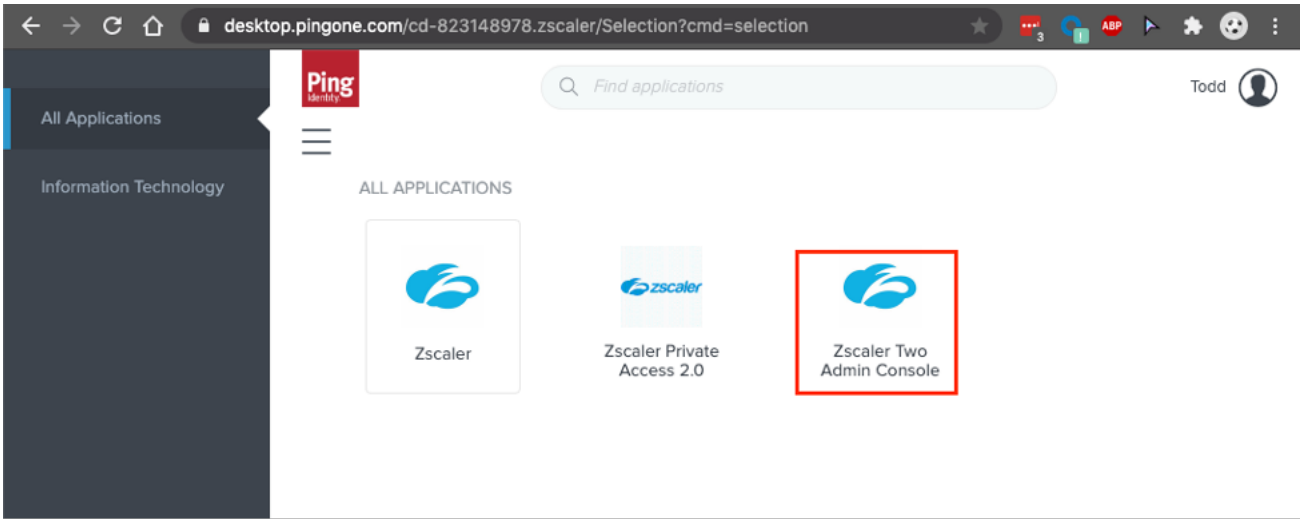


Figure 49. PingOne desktop

Using PingOne for ZPA Admin Access

The following sections describe using PingOne with ZPA.

Add the PingOne Application for ZPA SAML Administrator Access

To use PingOne SAML authentication for ZPA admin users, you must install the SAML Service Provider Application.

1. From the PingOne portal, go to the **Applications** > **Add Application**.

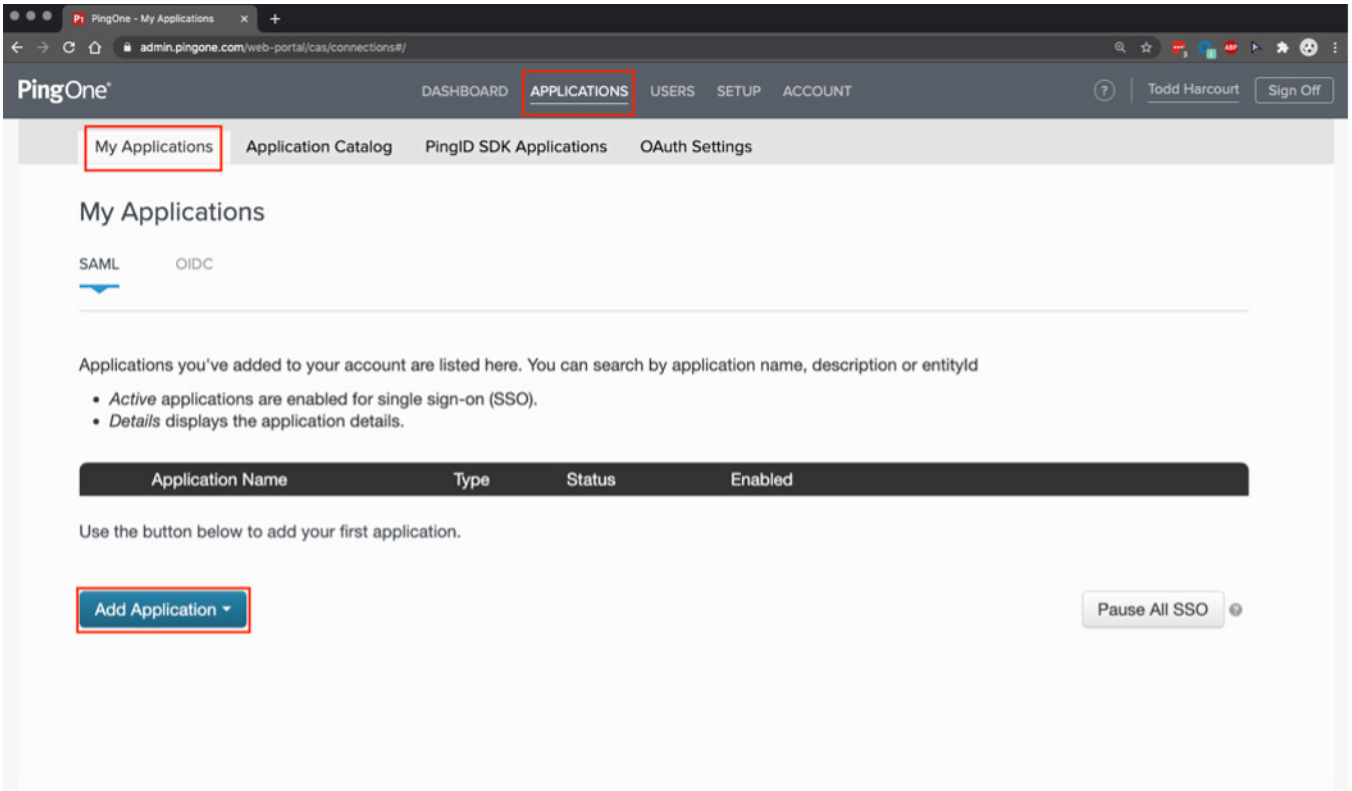


Figure 50. Add the ZPA PingOne application

2. Search for `zscaler`.
3. Select **Zscaler Private Access Administrator 2.0** and click the arrow to display a description of the application.

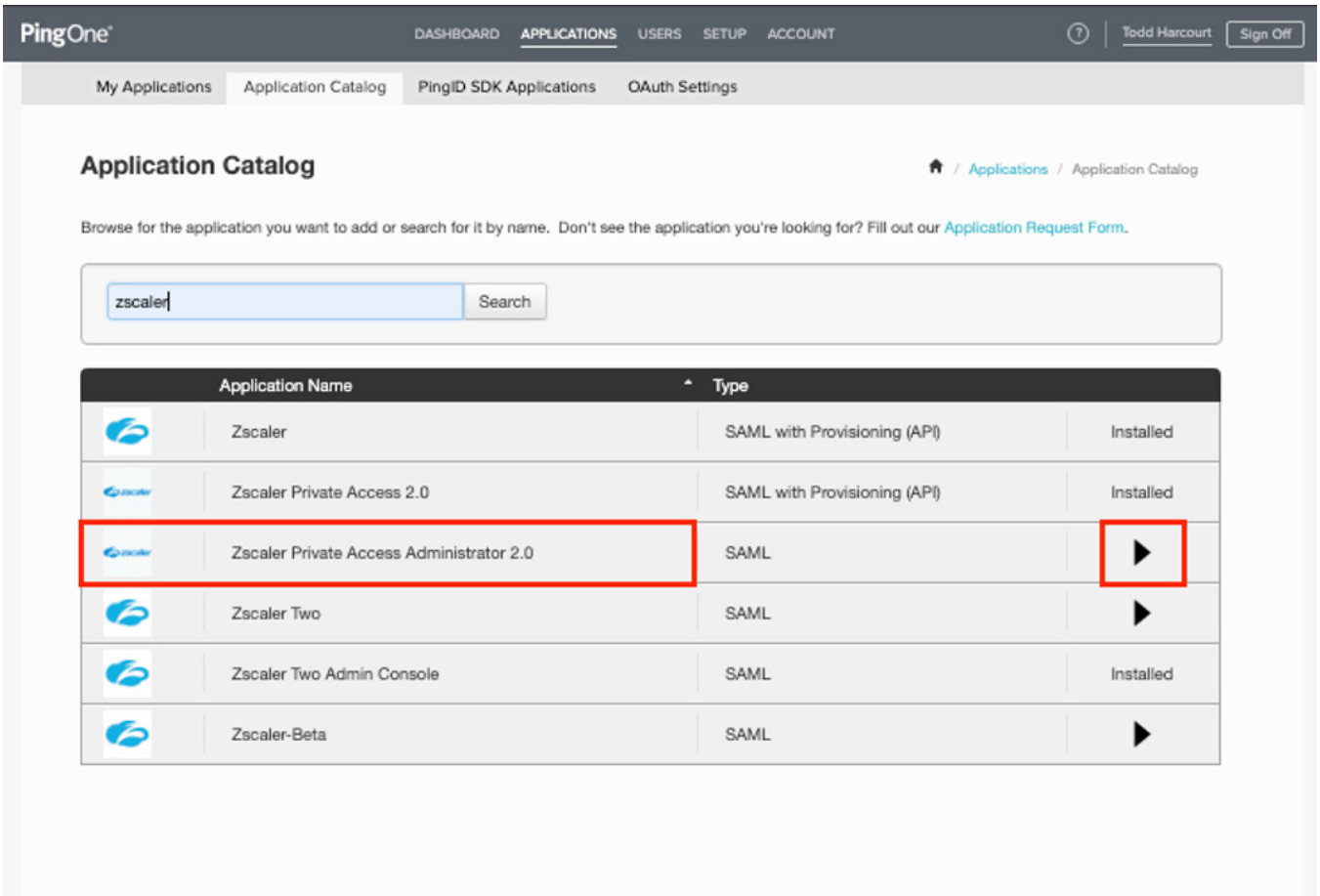


Figure 51. Select the ZPA application

A description of the application is displayed. Click **Setup** to begin the installation process.

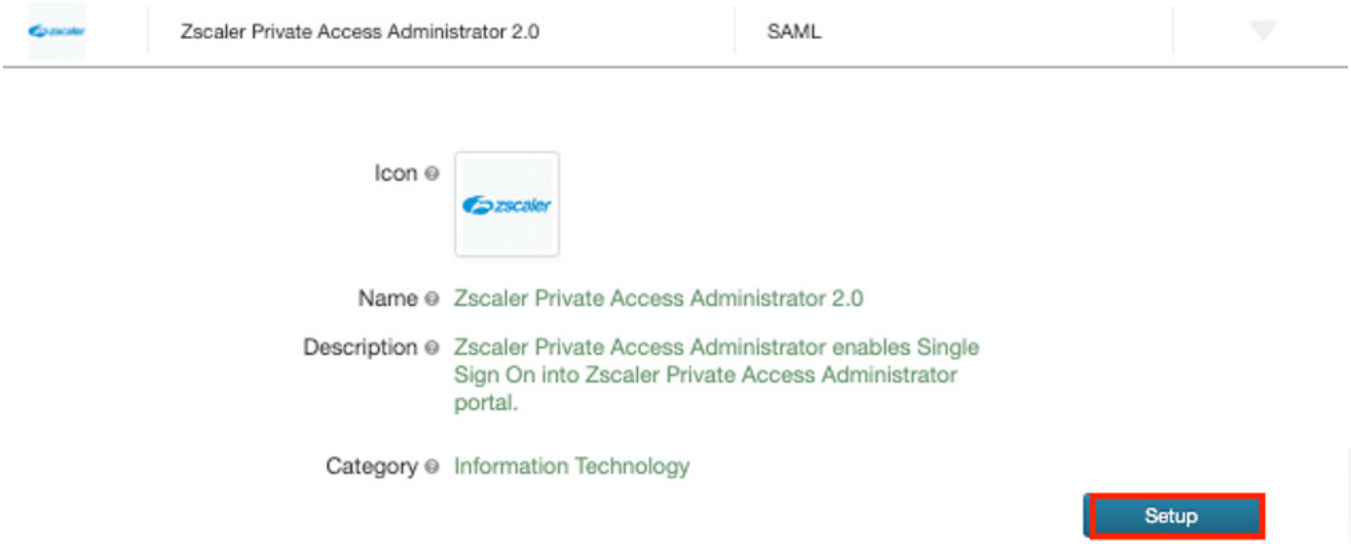


Figure 52. General description

Configuring PingOne for SAML Authentication for ZPA Administrators

To display the initial configuration window:

1. Download the Signing Certificate.
2. Copy the **IdP ID** and the **Issuer** URL. The IdP ID is appended to the URL Prefix to create the **SAML Portal URL** that is used in the ZPA IdP setup process.
3. Click **Continue to Next Step**.

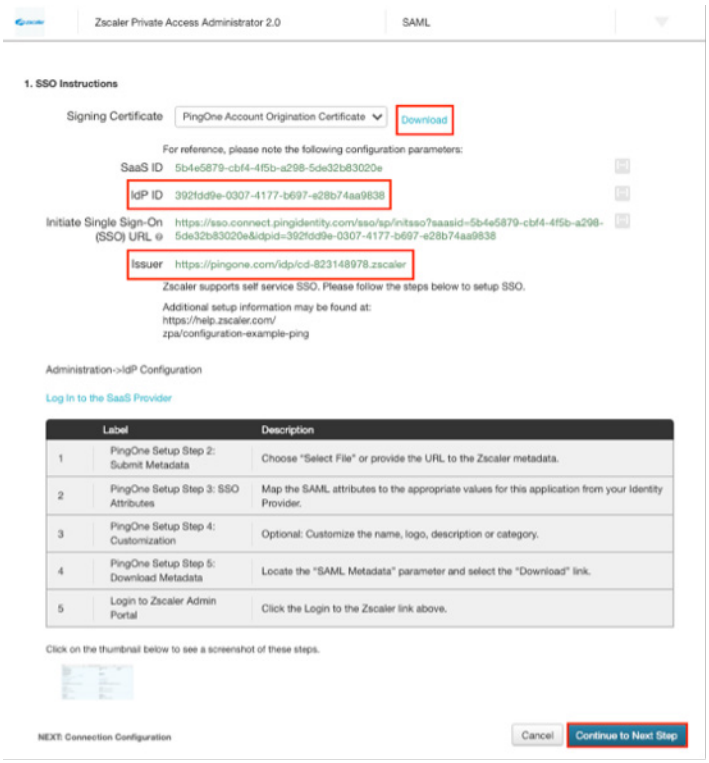
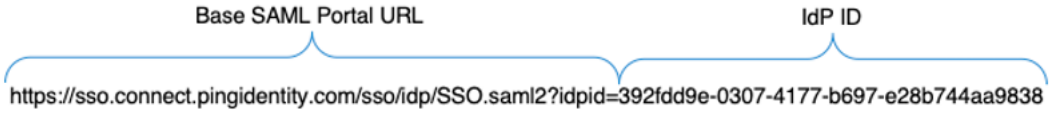


Figure 53. Application configuration

SAML Portal Base URL:

```
https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=(plus IdP ID).
```

In this configuration example, the SAML Portal URL is created by combining the **Base SAML Portal URL** and the **IdP ID**:



Configure Zscaler ZPA for an Admin PingOne IdP

Log in to the ZPA Admin Portal.

In the ZPA Admin Portal, go to **Authentication** > **User Authentication** > **IdP Configuration**.

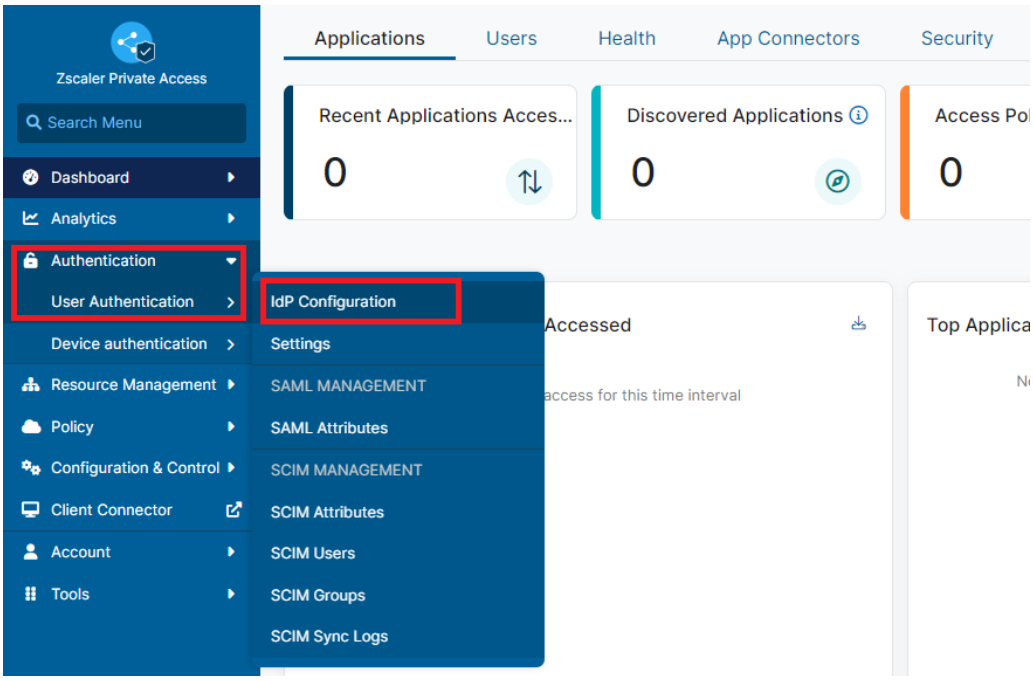


Figure 54. ZPA Admin Portal—Add the PingOne IdP

Add the ZPA IdP for Admin SSO to ZPA

On the IdP configuration window, click **Add IdP Configuration**.

The IdP Configuration wizard appears, which walks you through the creation of the IdP.

If the window is constrained, only the circle with the white plus sign is visible.

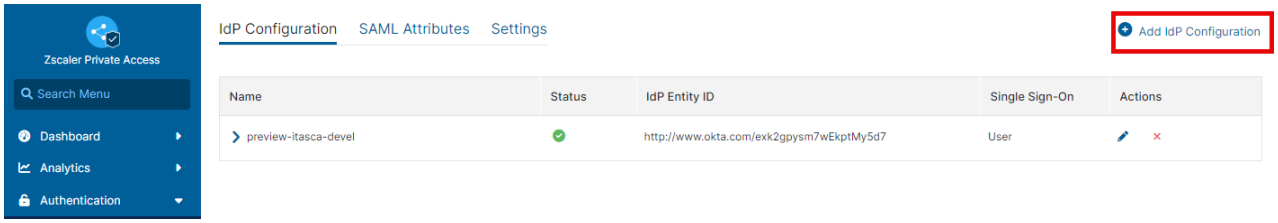


Figure 55. ZPA Admin Portal—Add the PingOne IdP

Configuring the ZPA IdP Information

In the IdP Configuration wizard:

1. Give the IdP a unique name.
2. Select **Admin** under **Single Sign-On**.
3. Select the **Domains** from which the administrators sign in.
4. Click **Next**.

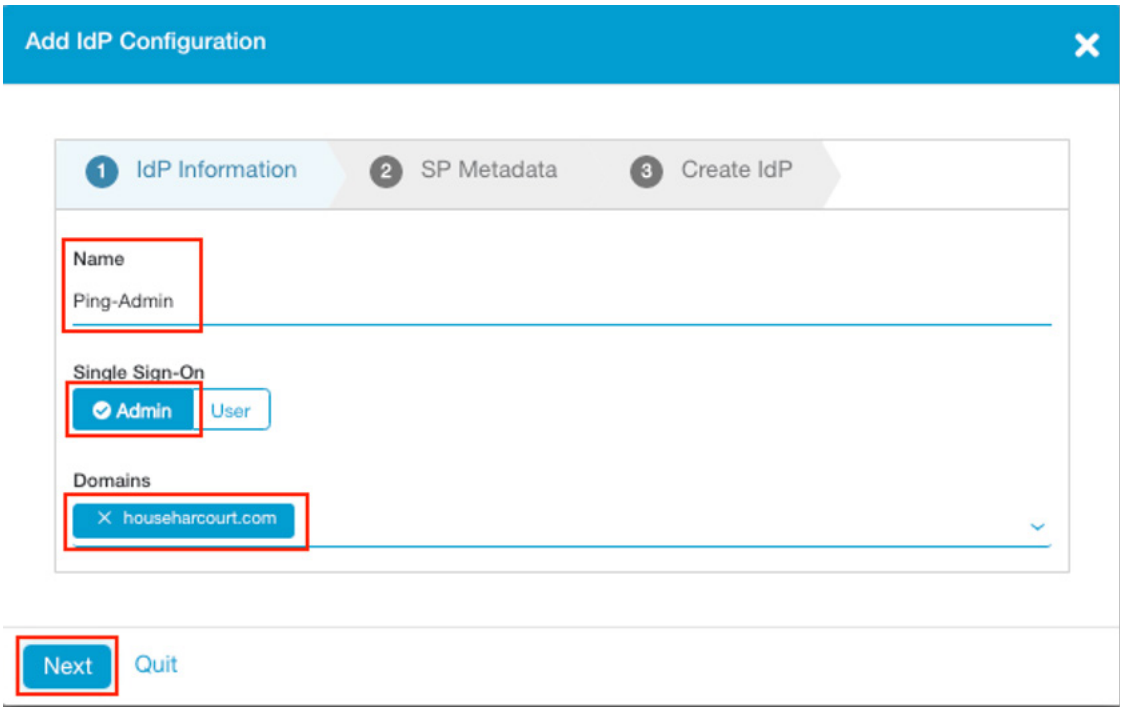


Figure 56. Add IdP Configuration wizard

Copy the ZPA SP URLs

On the **SP Metadata** tab, download and save the **Service Provider Metadata** and the **Service Provider Certificate**. Then click **Next**.

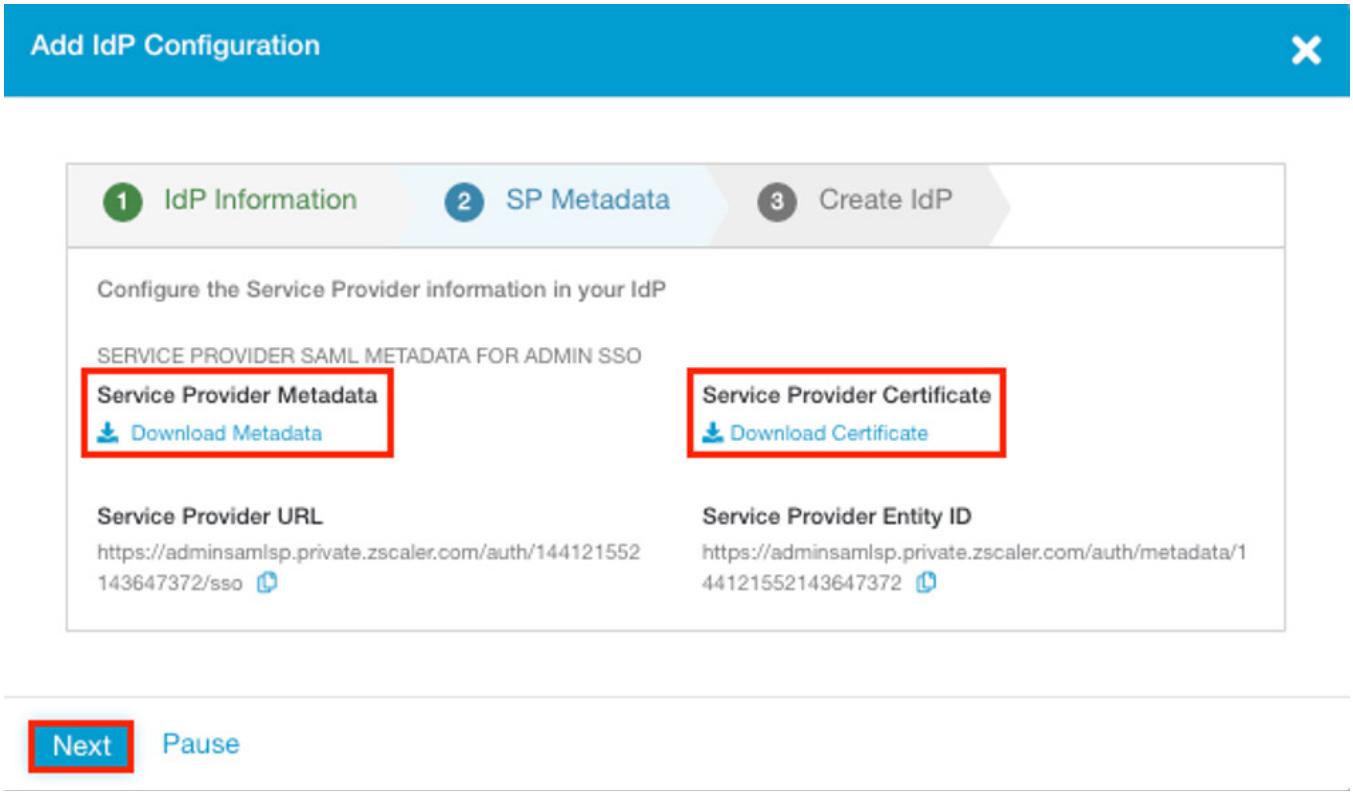


Figure 57. Service Provider Metadata and Service Provider Certificate

Finalize the PingOne IdP to ZPA

On the **Create IdP** tab:

1. Upload the PingOne Certificate file.
2. Enter the **Single Sign-On URL**.
3. Enter the **Issuer** URL as the **IdP Entity ID**.
4. Click **Save**.

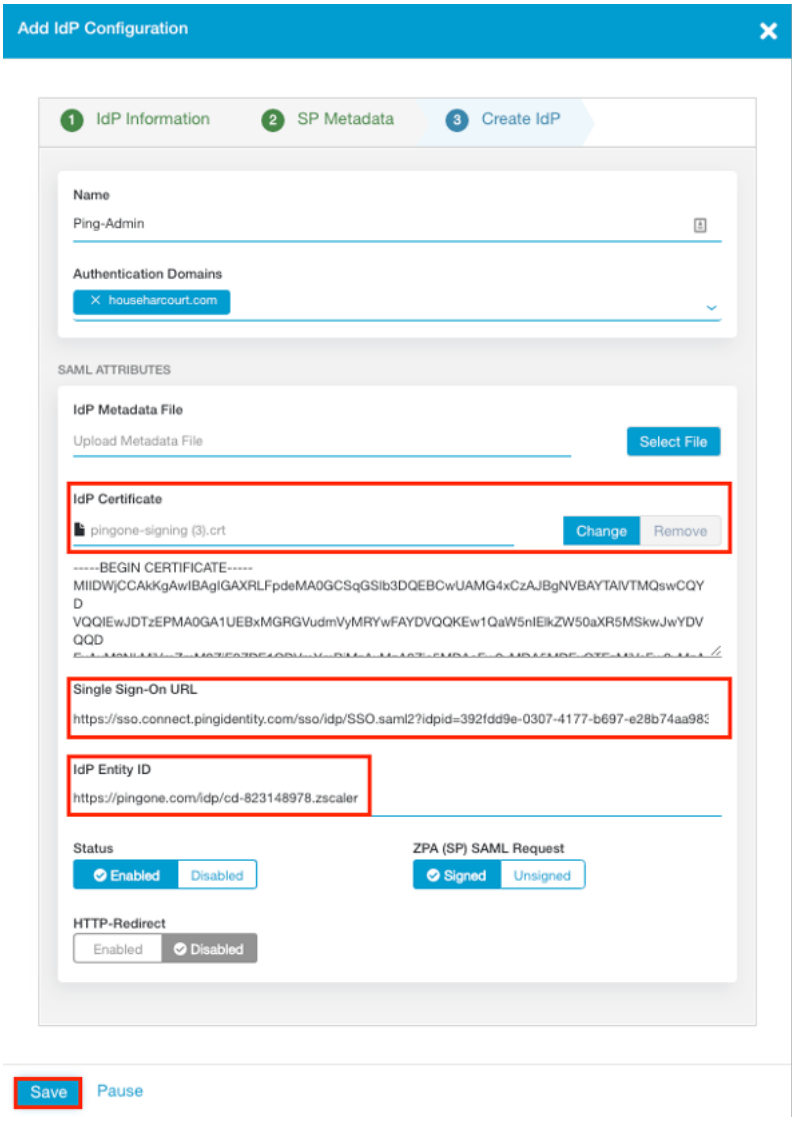


Figure 58. ZPA IdP completed configuration

Define the Administrators for SAML Access

Administrators using the SAML IdP for authentication must be defined as administrators.

1. To configure the authenticating administrators, in the ZPA Admin Portal, go to **Administration** > **Administrators**.
2. Click **Add Administrator**.

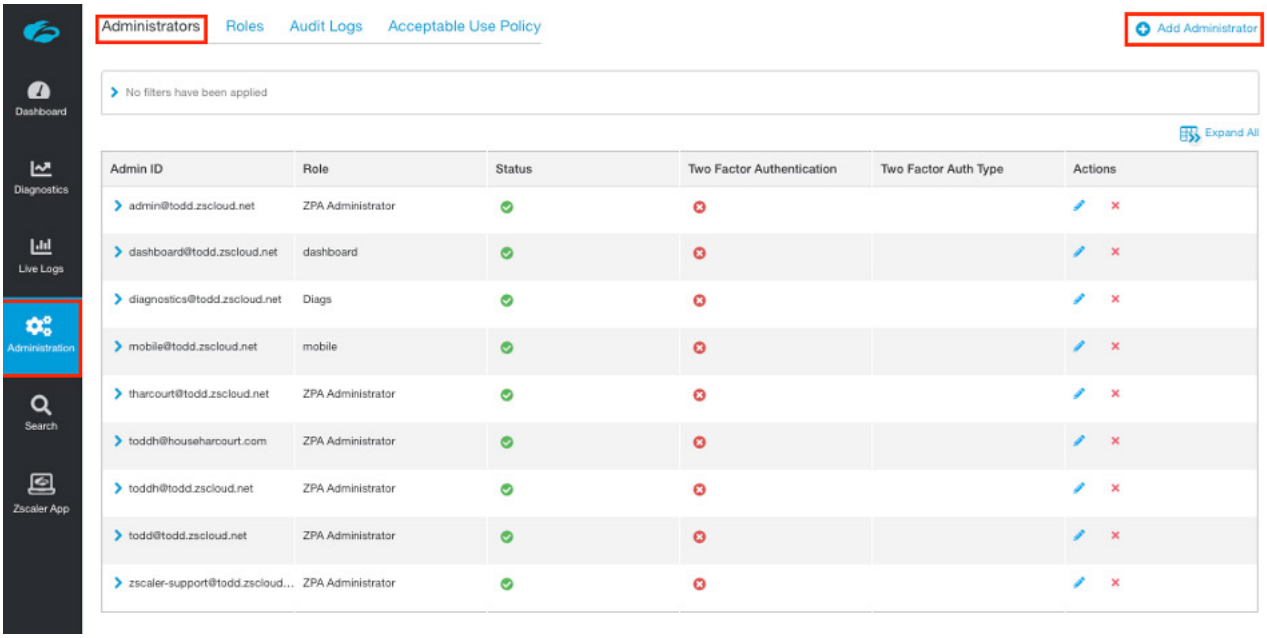


Figure 59. Creating an administrator

If the browser window is small, the **Add Administrator** configuration displays as only a blue circle with a white plus sign in it.

Create an Administrator for SAML Access

In the **Add Administrator** window:

1. Enter the **Admin ID** and the **Password**.
2. Select **ZPA Administrator** from the **Role** drop-down menu.
3. Enter an email address and a phone number.
4. Click **Save**.

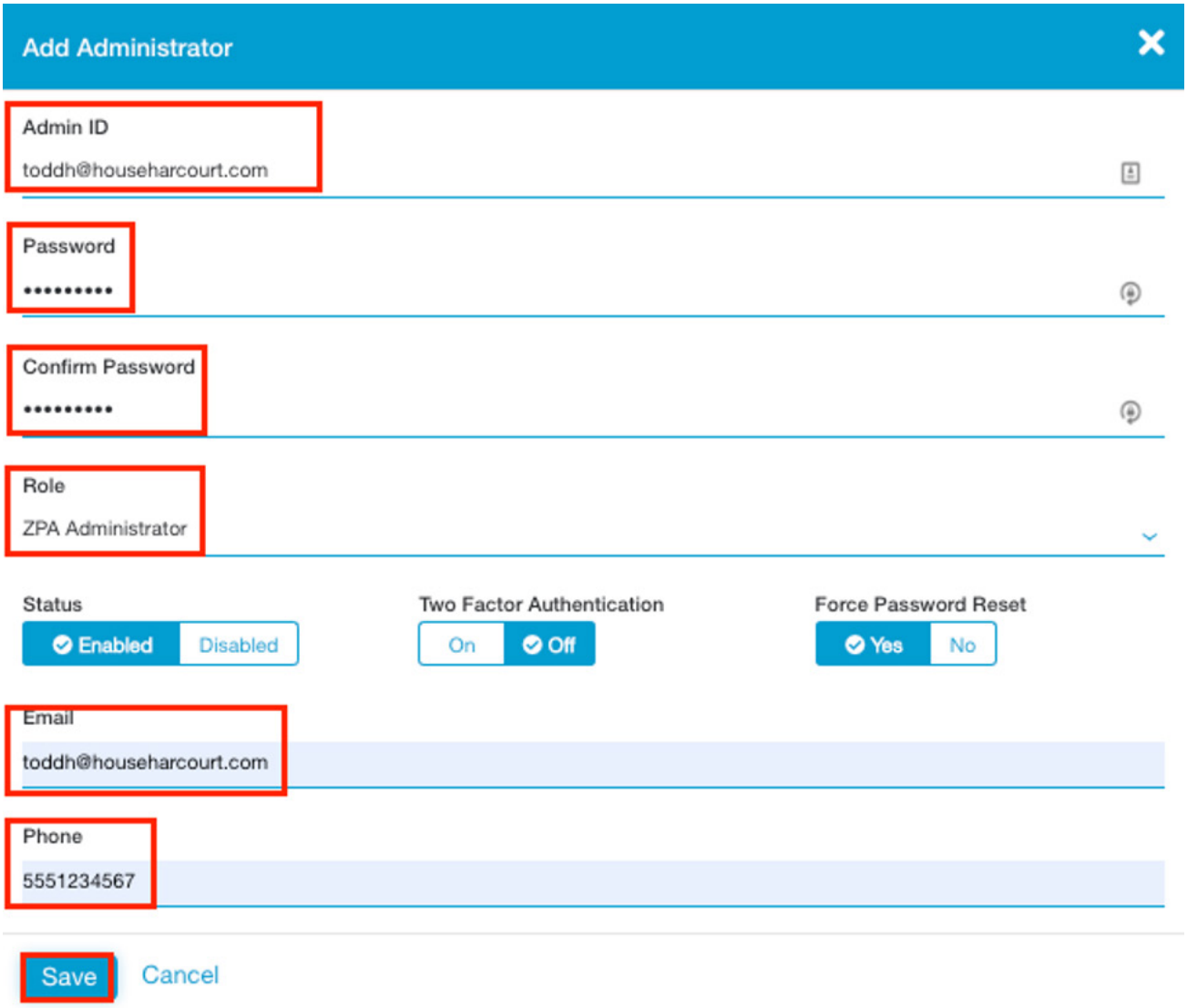


Figure 60. Create an administrator

Finish Configuring PingOne

To finish the PingOne configuration:

1. Upload the Zscaler metadata file and the Zscaler signing certificate, and click **Continue to Next Step**.

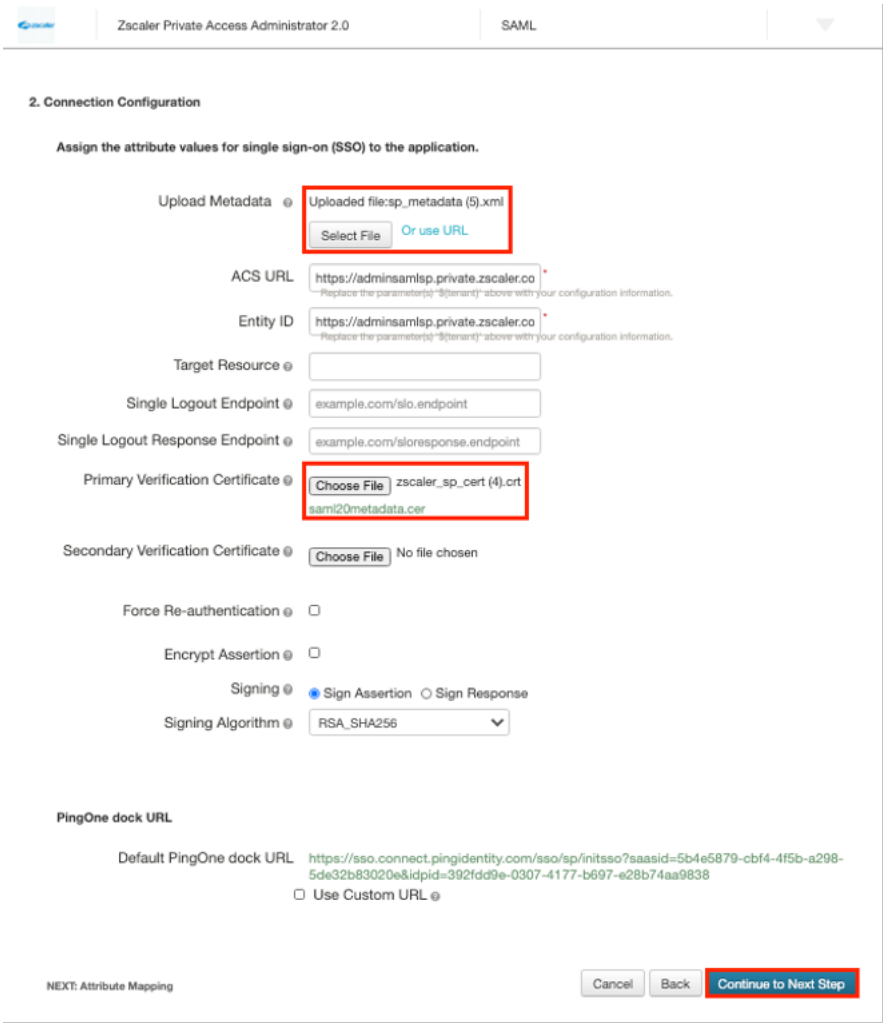


Figure 61. PingOne configuration

2. Leave the **Attributes** as default.
3. Click **Continue to Next Step**.

Figure 62. Attribute mapping

Assign the Administrators or Groups to the Application

The next step is to customize how the application is going to look in the PingOne portal. Make any changes specific to your installation, and then click **Continue to Next Step**.

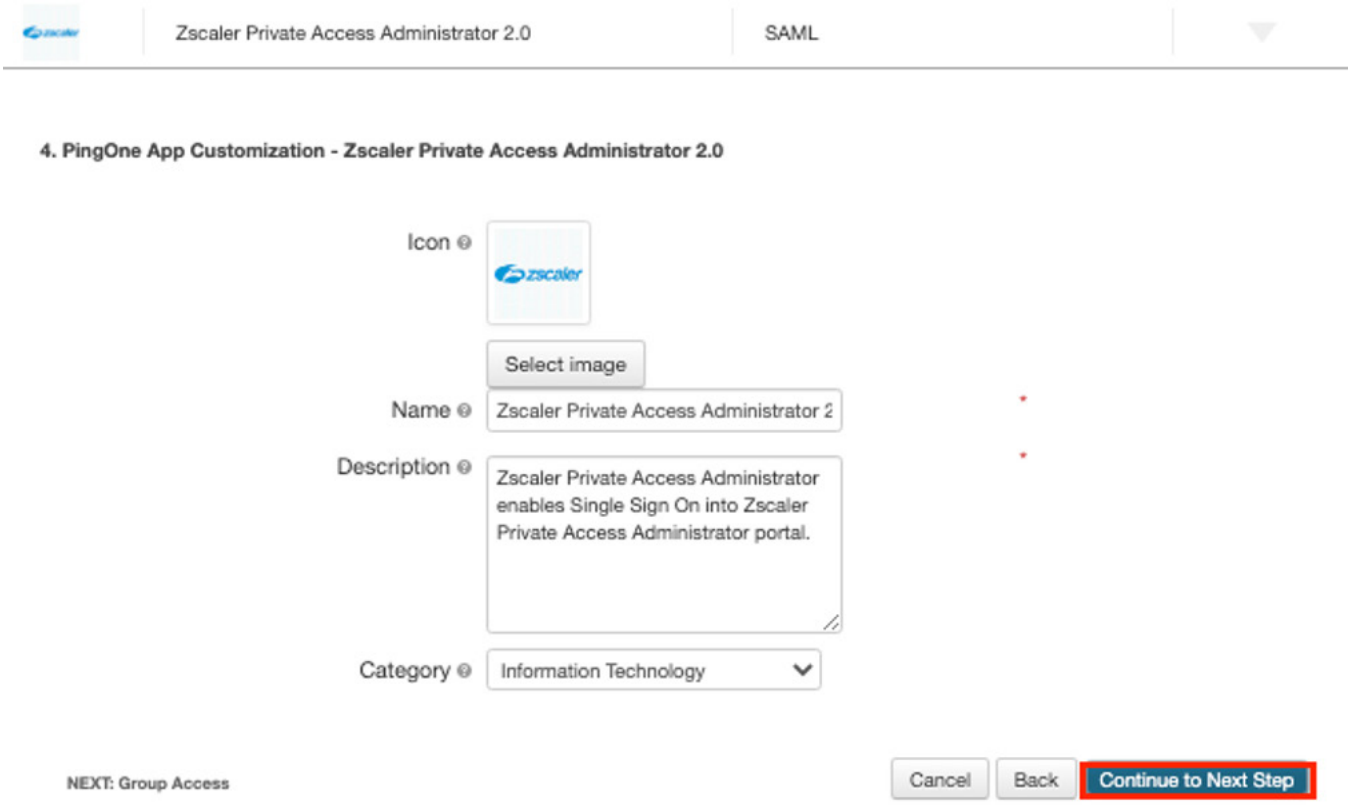


Figure 63. PingOne portal settings

Enable ZPA Admin Users on PingOne

The final step is to select the Security Groups that include the Administrators. Add any or all groups specific to your installation, and then click **Continue to Next Step**.

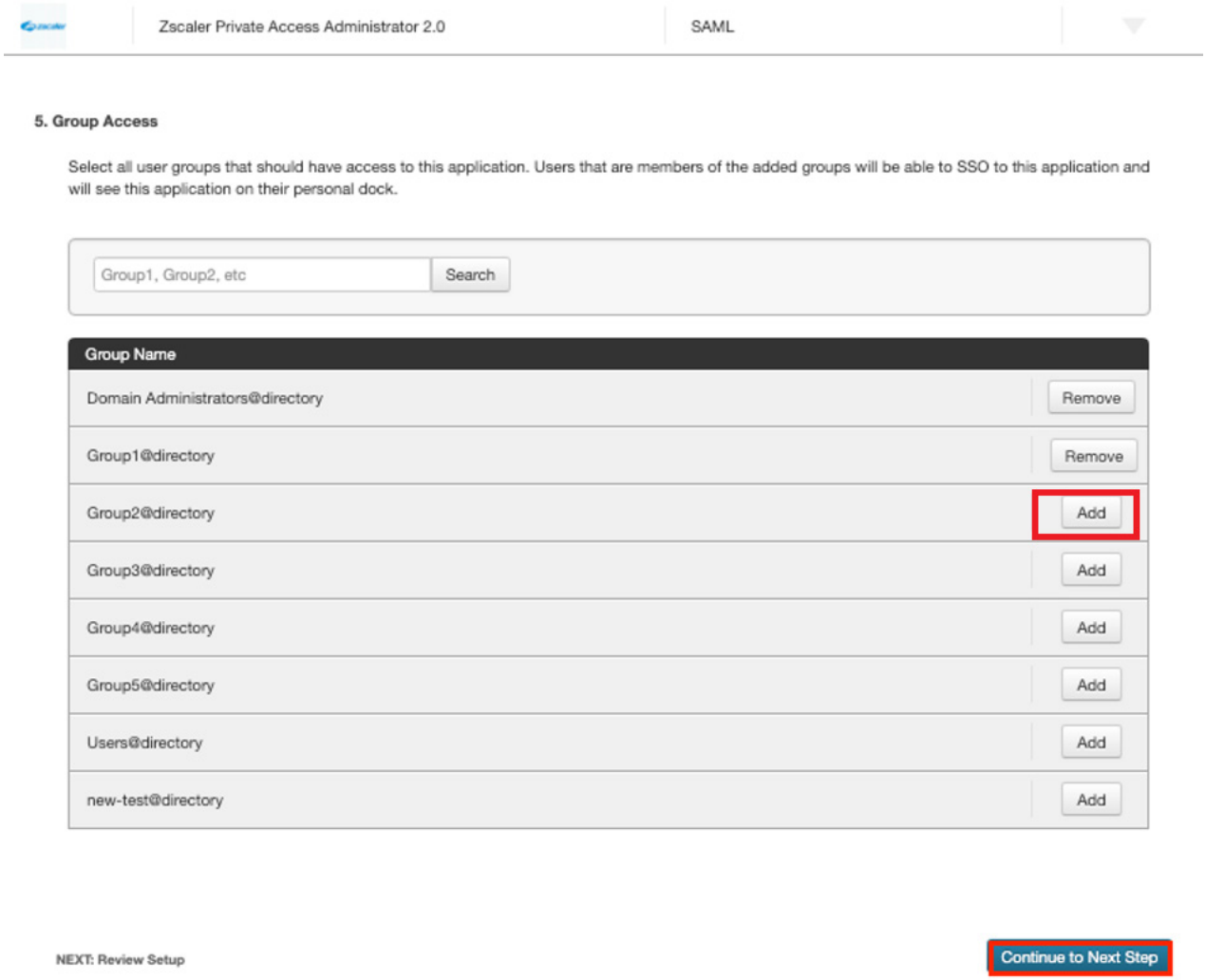


Figure 64. PingOne provisioning

Finalize the PingOne ZPA Admin Configuration

Verify your configuration, and click **Finish**.

Your PingOne instance is now configured for authenticating ZPA Administrators using PingOne SAML SSO.

Figure 65. PingOne configuration

Test the ZPA Authentication Configuration

You can now see your applications from the PingOne portal for the Administrator. By clicking the application, the app launches the ZPA Admin Portal, and authenticates the user transparently.

You can also log in from the **ZPA Admin Sign-on** window.

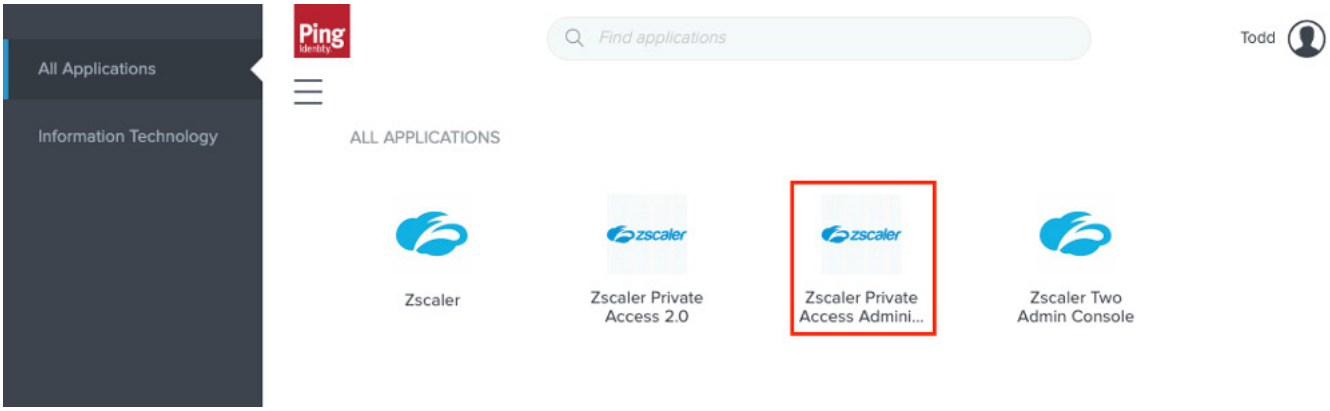


Figure 66. PingOne User apps

Administrator Sign-On Using SAML from the ZPA Admin Portal

To sign in from the ZPA Admin Portal, use the PingOne SAML IdP, select **Single Sign-On Using IdP** checkbox, and then click **Sign In**.

This launches the **PingOne Authentication** window.

Figure 67. Administrator sign-on using SAML IdP

Transparent SSO Using IWA with PingOne

For complete transparent authentication when using Zscaler with Ping Identity, Ping supports Integrated Windows Authentication (IWA) with PingOne via the Ping AD Connect component. IWA is only supported when PingOne is connected to the client's AD infrastructure using the AD Connect server.

Zscaler takes advantage of IWA if it is active and automates the login process without the user having to enter credentials. However, it is important to note this is not a Zscaler configuration, and that Zscaler only uses it if it is configured and working. IWA is configured between the Windows Client, the Ping AD Connect component, and the Windows AD server.

IWA is not applicable when using the PingOne User Database.

To learn more, refer to the Ping Identity documentation.

PAC File and Zscaler Client Connector—Authentication Bypasses

When using ZIA, you must bypass the IdP provider login URLs for authentication to succeed, or you can enter the URLs in Authentication Bypass in the ZIA Admin Portal. It is not a requirement for ZPA, and the destination URLs can flow through ZIA. However, bypassing the URLs for ZIA is a requirement for both Browser PAC files and for Zscaler Client Connector.

The following entries must be added to your Browser PAC or the Zscaler Client Connector Custom PAC File for the Application Profile. For more information, see Zscaler Resources.

PAC File Bypasses

```
// PingOne Authentication Bypass

if (

dnsDomainIs(host, ".pingone.com") ||

dnsDomainIs(host, ".pingidentity.com"))

return "DIRECT";
```

Authentication Bypasses in the ZIA Admin Portal

In the ZIA Admin Portal, go to **Administration** > **Advanced Settings** > **Authentication Exemptions** > **Exempted URLs**. Add `.pingone.com` and `.pingidentity.com` as exempted URLs.

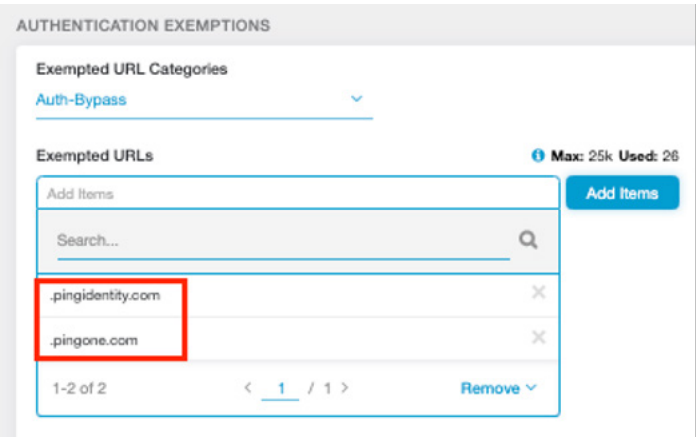


Figure 68. Exempted URLs

Capture the SAML Request for Troubleshooting

Troubleshooting SAML can be challenging. The following procedures help find and decode the SAML assertion to look at the attributes returned by the IdP. These steps were written to capture the assertion by using the Chrome Browser developer tools and then decoding the assertion using a Base64 decoder on the desktop. This was selected as the most secure method.

You can use browser extensions and/or cloud-based Base64 decoders, but when clear text passwords are present in the data, keeping things in house are always more secure. You can use any browser to capture the SAML assertion. The procedures for the most common browsers are described in the following sections.

How to View a SAML Response in Your Browser for Troubleshooting

To troubleshoot SSO login issues, it can be helpful to retrieve the SAML response from your service provider in your browser.

Google Chrome—To view a SAML Response in Chrome

1. Press **F12** to start the developer console.
2. Select the **Network** tab, and then select **Preserve log**.
3. Reproduce the issue.
4. Look for a **SAML Post** in the developer console pane. Select that row, and then select the **Headers** tab at the bottom. Look for the **SAMLResponse** attribute that contains the encoded request.

The SAMLResponse attribute contains the encoded request. Use a Base64 decoder to investigate the decoded response.

Mozilla Firefox—To view a SAML Response in Firefox

1. Press **F12** to start the developer console.
2. In the upper-right of the developer tools window, click **Options** (the gear icon). Under **Common Preferences**, select **Enable persistent logs**.
3. Select the **Network** tab.
4. Reproduce the issue.
5. Look for a POST SAML in the table. Select that row. In the **Form Data** window on the right, select the **Params** tab and find the **SAMLResponse** element.

The SAMLResponse attribute contains the encoded request. Use a Base64 decoder to investigate the decoded response.

Apple Safari—To view a SAML Response in Safari

1. Enable Web Inspector in Safari. Open the **Preferences** window, select the **Advanced** tab, and then select **Show Develop menu** in the menu bar.
2. Open Web Inspector. Click **Develop**, then select **Show Web Inspector**.
3. Select the **Resources** tab.
4. Reproduce the issue.
5. Look for a POST method with a samlconsumer file in the table.
6. Scroll down to find Request Data with the name **SAMLResponse**.

The SAMLResponse attribute contains the encoded request. Use a Base64 decoder to investigate the decoded response.

Microsoft Edge—To view a SAML Response in Microsoft Edge

The best way to analyze network traffic in Microsoft Edge is through the use of a third-party tool. Refer to the Microsoft documentation to download and install Fiddler and capture the data.

After you find the Base64-encoded SAML response element in your browser, copy it and use a Base64 decoding tool to extract the XML-tagged response.

Because the SAML response data that you are viewing might contain sensitive security data, Zscaler recommends that you do not use an online Base64 decoder. Instead use a tool installed on your local system.

Configuring Your Browser to Capture the ZIA SAML Response

Open the proxy configuration window for the browser you are going to test, and enter the Proxy IP address. You must also enter the PingOne domains as bypasses so the request makes it to PingOne and isn't blocked by ZIA. The two PingOne domains to bypass are .PingOne.com and .PingOnecdn.com.

Click **OK** to save the changes. You are now ready to test.

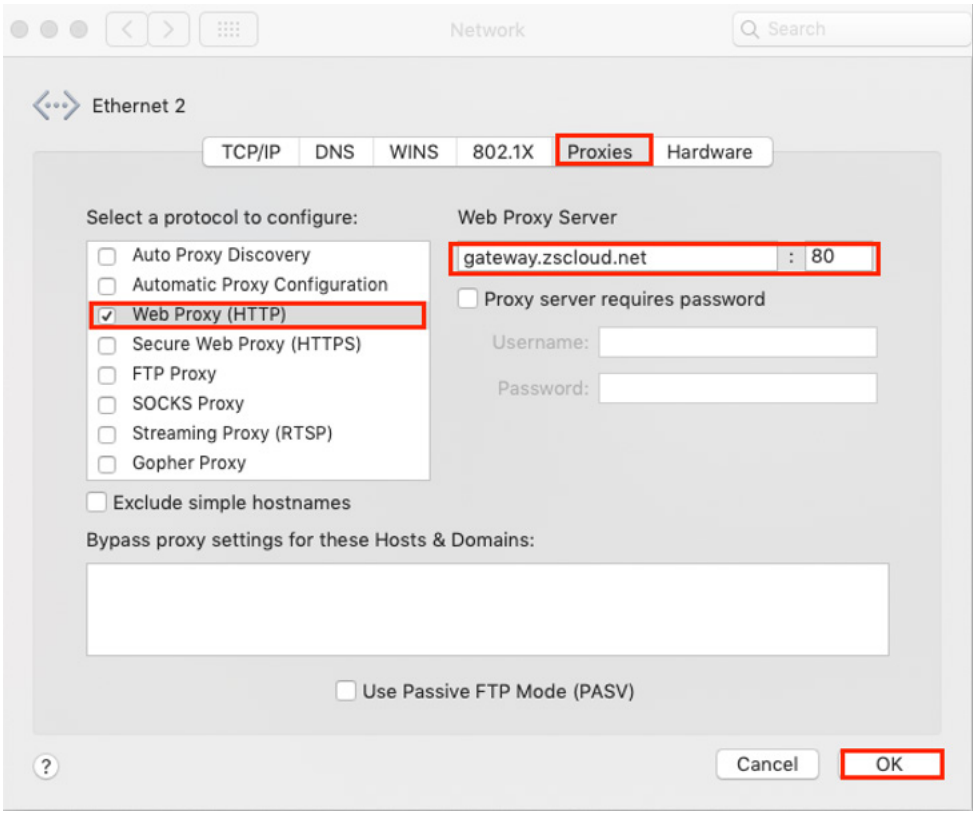


Figure 69. Configure proxy settings on your browser

1. Configure Zscaler as a proxy for your browser.
2. Configure the automatic FQDN that selects the fastest gateway response as the proxy. The FQDN is gateway.zscalerthree.net, where zscalerthree replaces your cloud (i.e., gateway.zscloud.net, gateway.zscalertwo.net, etc.).
3. Select the proxy from the list of Public Service Edges.
4. Enter your cloud's information center (e.g., the URL is ips.zscalerthree.net/cenr). This lists all of the Public Service Edges for the Zscalerthree cloud. The Dallas IP address is then used as the proxy address defined in the browser.
5. Enter any URL in the browser and ZIA prompts you for authentication credentials.
6. Start the developer tools by clicking the **Meatball** icon at the top right of the browser.
7. Select **More Tools**.
8. Select **Developer Tools**. This opens the developer window.

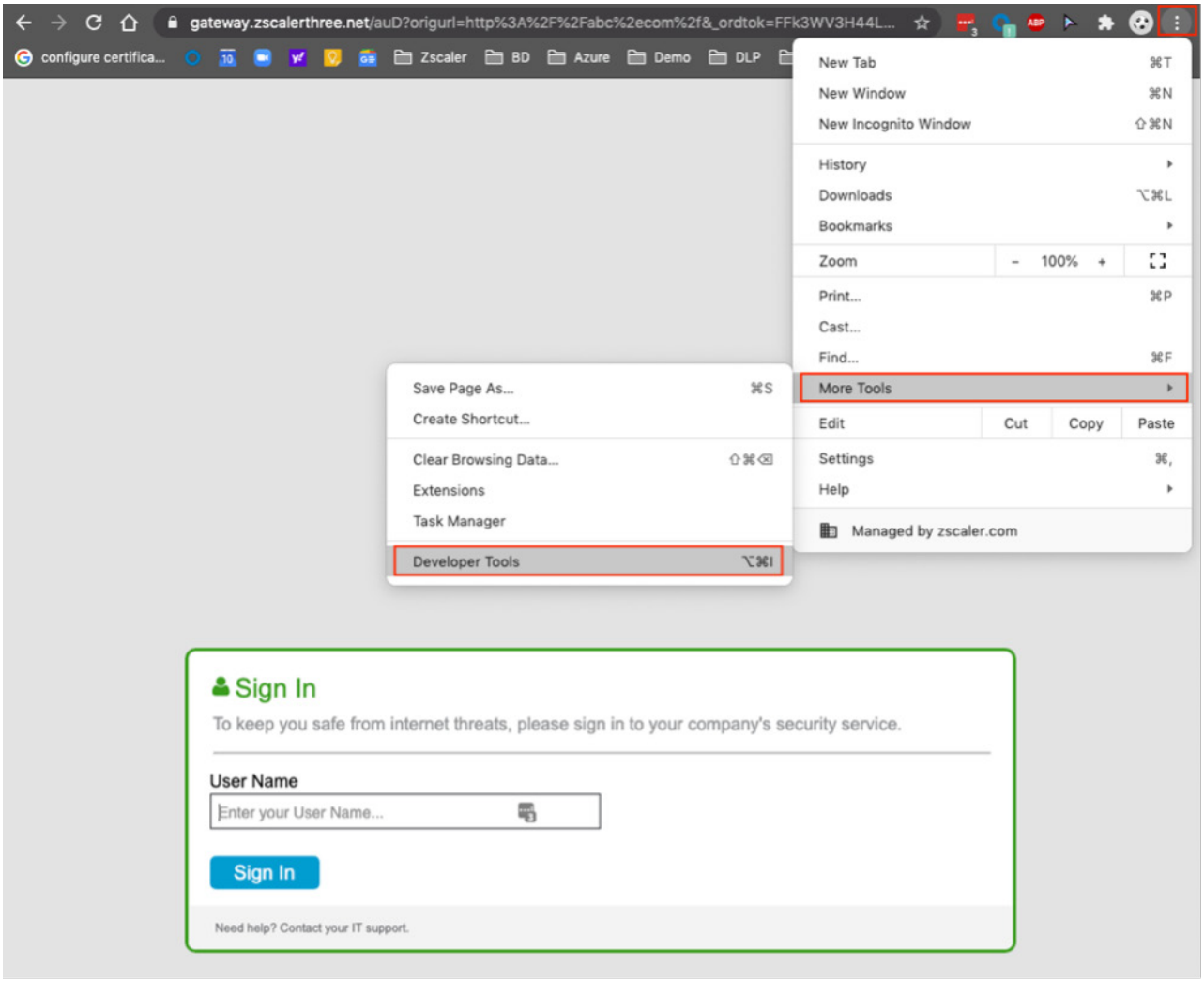


Figure 70. Selecting developer tools

Your network trace shows you the connection and packet information as you authenticate into Zscaler and PingOne. The initial authentication window is only looking for the user domain appended to the User ID, so Zscaler knows which Zscaler instance to direct the request to.

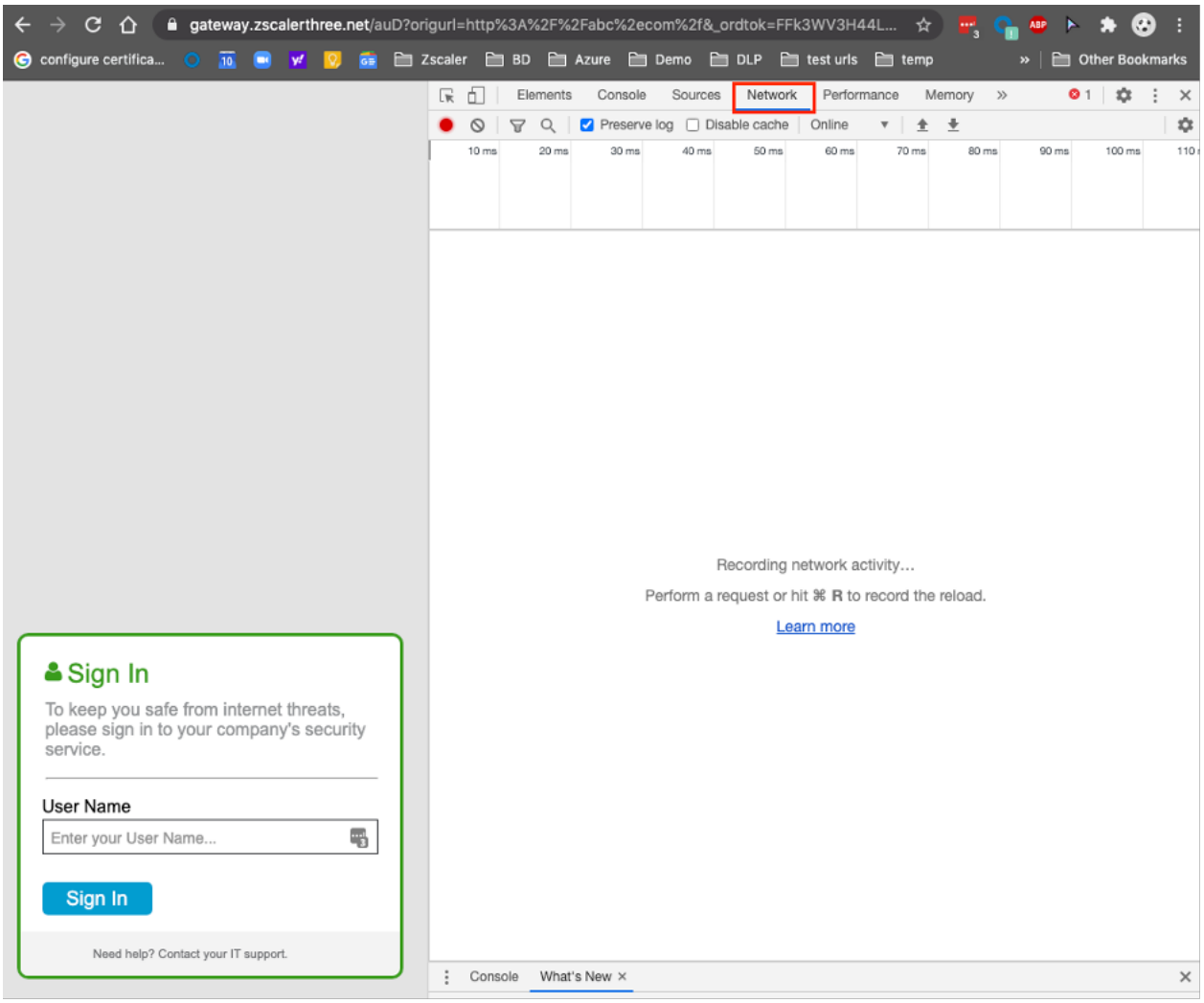


Figure 71. Select Network view

Zscaler redirects the authentication request to PingOne and opens the **PingOne authentication** window.

Log in with a valid User ID in the PingOne database associated with the Zscaler instance.

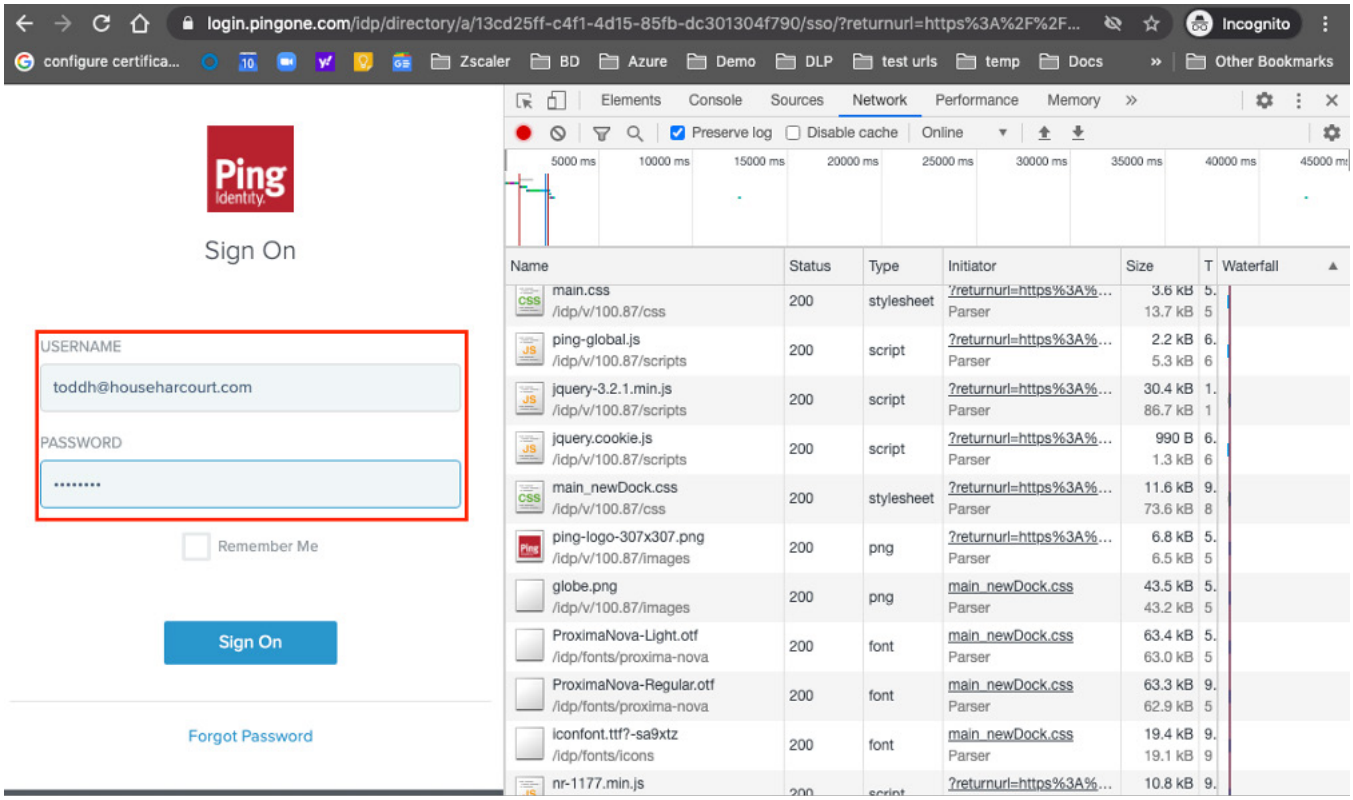


Figure 72. Authenticate to the PingOne IdP

After authentication is complete, select the packet called sfc_sso that is destined to login.zscloud.net. This is the SAML response from PingOne and contains the SAML assertion. The assertion is Base64-encoded, and you must use a decoder to get the clear text information.

Copy the **SAML Response** data, excluding the bolded **SAMLResponse** text (you want only the data).

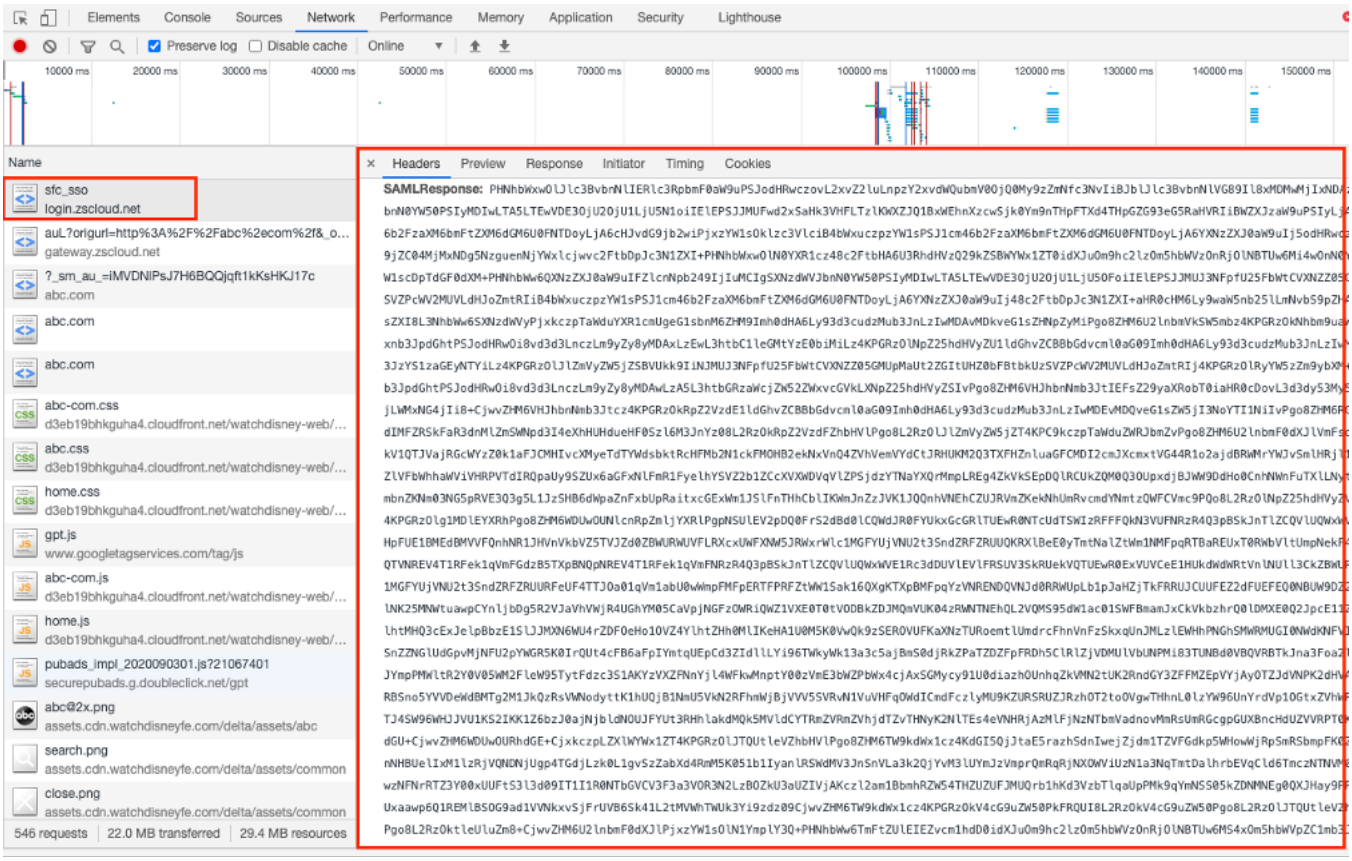


Figure 73. SAML response containing the Assertion

Using a Base64 decoder, paste the encoded text into the application and then copy the decoded SAML Assertion.

The Base64Anywhere app used for this demonstration was downloaded for free from the Apple store. There are also free decoders from the Microsoft store if you are a Windows user.

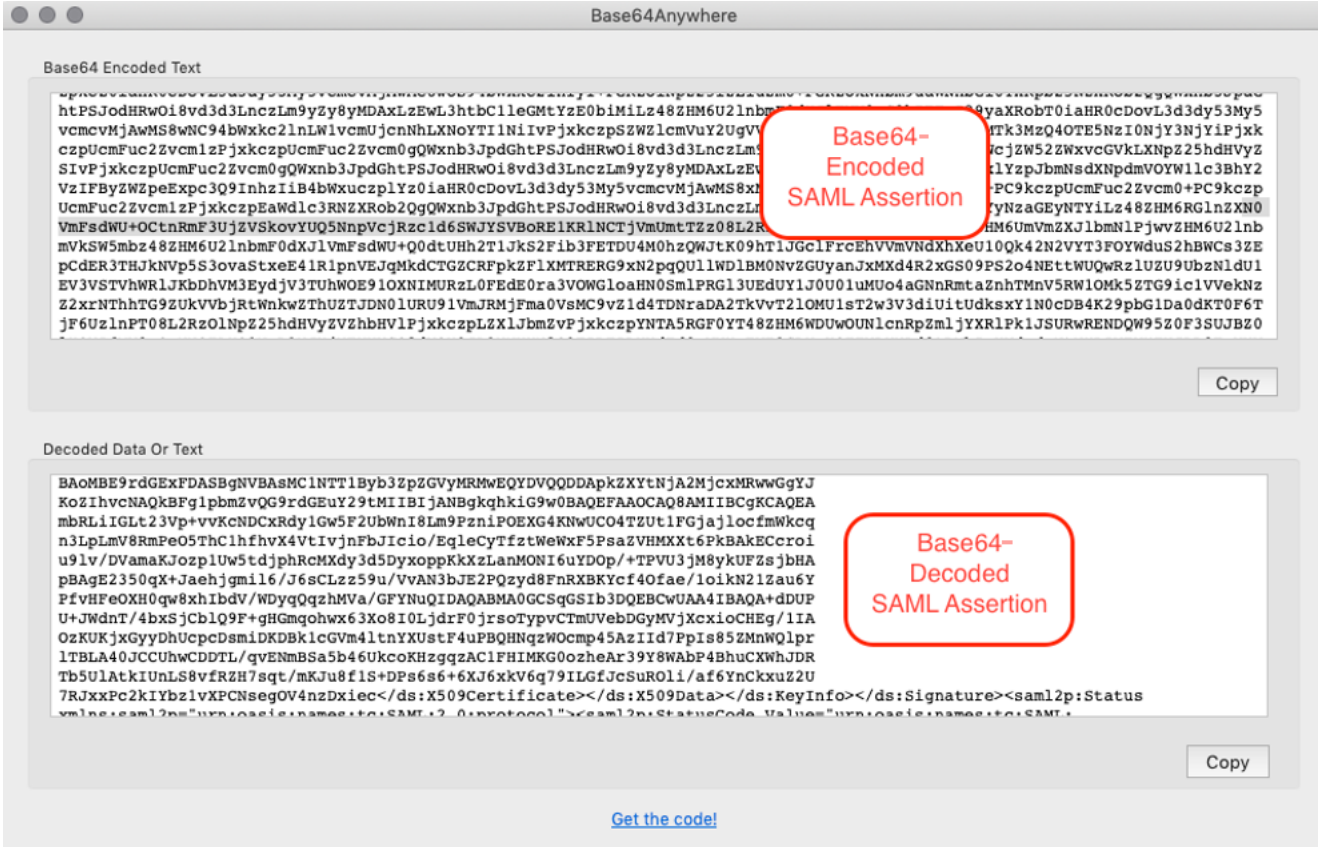


Figure 74. Decoding the Base64-Encoded Assertion

You can see the clear text assertion with the **NameID** of the user and the other attributes. In this example, you see that the user is part of groups called Group1, Group2, Group3, Group4, and Users. You can see all groups and attributes associated with the user.


```
<samlp:Response Destination="https://login.zscloud.net:443/sfc_sso" InResponseTo="_10302214039120527080" IssueInstant="2020-09-
10T17:56:55.597Z" ID="I1ApwlRhy7TqKO9JYvICPqXHg_70J94bogLzEMwxLzFdowxnQhuQ" Version="2.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://pingone.com/idp/cd-823148978.zscaler</saml:Issuer><samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></samlp:Status><saml:Assertion Version="2.0" IssueInstant="2020-
09-10T17:56:55.598Z" ID="I1Bw4Z_SnEmkBUsYgNF1JLiKvdb-PvtlPmnE3IVOqevlEKtrhfkQ" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
<saml:Issuer>https://pingone.com/idp/cd-823148978.zscaler</saml:Issuer><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
<ds:Reference URI="#I1Bw4Z_SnEmkBUsYgNF1JLiKvdb-PvtlPmnE3IVOqevlEKtrhfkQ">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>x4Z43LV7H0VQJAZGwg2VfIciwr8yxGPwnxqtK9z3rgc=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
pqnKj/SZ2qOMbOnEuA2Uj4Fqf3gI5hRB0r/qs2y7SaglnKQpqLocurAL8pvzCqVt8eXUzeXt+IDu
3d7MqGfynhaB026rbWrlmTn8GZ6j7AEc+aboJiGF9u79J/Gjhg59rCy98BvGfUEmhaiebTtOU7HE
ZS/ReLzhaq6QfGQrzXXIVvoVBquWX5jVVOJ7sa3Zat+2jKDH8fEdHJCBTBRFP3D79Jqv0IYoCtz4
xMZqnMyK7+FR1fz4x2JGXtqlAg92fnvJ6m74niEQ7Cx9/RsHpzujZfqqmJQj+qpalZmIJQgLxBnR
Zbgg2U+RPBxU4HBeBQVfJzCaRdorgX6ksAaBVg==
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIIDWjCCAkKgAwIBAgIGAXRLFpdeMA0GCSqGSIb3DQEBCwUAMG4xCzAJBgNVBAYTAlVTMQswCQYD
VQQIEwJDTzEPMA0GAlUEBxMGRGVudmVyMRYwFAYDVQQKEwlQaW5nIElkZW50aXR5MSkwJwYDVQQD
EyAxM2NkMjVmZmM0ZjE0ZDE1ODVmYmRjMzAxMzA0Zjc5MDAeFw0yMDA5MDExOTEzMjVaFw0yMzA5
MDExOTEzMjVaMG4xCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDTzEPMA0GAlUEBxMGRGVudmVyMRYw
FAYDVQQKEwlQaW5nIElkZW50aXR5MSkwJwYDVQQDEyAxM2NkMjVmZmM0ZjE0ZDE1ODVmYmRjMzAx
MzA0Zjc5MDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALW/QdpoTZJPEb69M+nL5knk
Bbycl89GeIiXUZ4xPhX3NBiZc4as9dbAfuUq4OKU80dd2LBeT+N3EcS4HP/ePl/yumZsMRXPfjbq
Edo8kCIC1q4CbipMugev98k227FY5AXYxdlvXm0t7pLIzZAol5JRIlszYN+dlNxz59VxbXmdxt2R
xp5SC9+EpBOsHDNUAJissMDhzkeRgkpXgVqsJLjRrL/9DXxO4hRldLPb45gJ4UHp8S703gCNQ/qF
ycLrJvY4iTtjo2JESjXXdy+B+AKxpPzhZHbkjPJBwvHvYKb/zMi2ZMwkw9j0fKGcFFOi6CdZED8y
Tef5ClIUmCO2/7MCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAgIbjOlimGf4WNV3aeyoyO+Ew77KP
c5WdSgb9xXY02zmcM3Va7mfOmlxr01Hc2s/uSGbk8NRxjfEL7kT+dgtf7dQLdJUb0296IuSO+gGT
mv9ekWSznuteTVj4rDAJz9aUCygA1863RdC4lUchw+m+XTB0u6e9VCvDXfZ0cUUyITo7UnTqj9gH
gEs9r1OJeDREFIG8NOkh9X0Lxg/IsaozRv+uZu8kqeXVGwac6QNGScm86NpggZM2xIozXrIUMJKb
+Vzo2tj3cnWM9BEaKwDxejGLBNLVWBa4feTfeXcu6oLsr+ceLK8ySGF032Qc73SneZvz/2dlRdFr
FQpgpwTeUQ==
</ds:X509Certificate>
</ds:X509Data>
<ds:KeyValue>
<ds:RSAKeyValue>
<ds:Modulus>
tb9B2mhNkk8Rvr0z6cvmSeQFvJyXz0Z4iJdRnjE+Ffc0GJlzhqzllsB+5Srg4pTzRl3YsF5P43cR
xLgc/94/X/K6ZmwxFc9+NuoR2jyQIgLWrgJuKky6B6/3yTbbsVjkBdjF3W9ebS3uksjNkCjXklEj
WzNg353U3HPnlXFteZ3G3EHGnlIL34SkE6wcMlQAmKywwOHOR5GCSleBWqwkuNGsv/0NfE7iFHV0
s9vjmAnhQenxLvTeAI1D+oXJwusm9jiJO2OjbcRKNdd3L4H4ArGk/OFkduSM8kHC8e9gpv/MyLZk
zCTD2PR8oZwUU6LoJ1kQPzJN5/kLUhSYI7b/sw==
</ds:Modulus>
<ds:Exponent>AQAB</ds:Exponent>
</ds:RSAKeyValue>
</ds:KeyValue>
</ds:KeyInfo>
</ds:Signature><saml:Subject><saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">toddh@househarcourt.com</saml:NameID><saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData InResponseTo="_10302214039120527080" NotOnOrAfter="2020-09-10T18:11:55.598Z"
Recipient="https://login.zscloud.net:443/sfc_sso"/></saml:SubjectConfirmation></saml:Subject><saml:Conditions NotOnOrAfter="2020-09-
10T18:11:55.598Z" NotBefore="2020-09-10T17:51:55.598Z"><saml:AudienceRestriction><saml:Audience>zscloud.net</saml:Audience>
</saml:AudienceRestriction></saml:Conditions><saml:AuthnStatement AuthnInstant="2020-09-10T17:56:55.598Z"
SessionIndex="IlusuUKnjMxnAZ6mHa5Ei2jHpQ8CtN1RnU4NoOsr569Ui8t2e0zg"><saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnContextClassRef>
<saml:AuthenticatingAuthority>https://pingone.com/idp/cd-823148978.zscaler</saml:AuthenticatingAuthority></saml:AuthnContext>
</saml:AuthnStatement><saml:AttributeStatement xmlns:xs="http://www.w3.org/2001/XMLSchema"><saml:Attribute
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="Groups"><saml:AttributeValue xsi:type="xs:string"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">Group3@directory</saml:AttributeValue><saml:AttributeValue xsi:type="xs:string"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">Users@directory</saml:AttributeValue><saml:AttributeValue xsi:type="xs:string"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">Group2@directory</saml:AttributeValue><saml:AttributeValue xsi:type="xs:string"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">Group1@directory</saml:AttributeValue><saml:AttributeValue xsi:type="xs:string"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">Group4@directory</saml:AttributeValue></saml:Attribute><saml:Attribute
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="PingOne.idpid"><saml:AttributeValue xsi:type="xs:string"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">9e4858a9-65cf-44cd-a77a-619308ca5c58</saml:AttributeValue></saml:Attribute>
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="PingOne.AuthenticatingAuthority">
<saml:AttributeValue xsi:type="xs:string" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">https://pingone.com/idp/cd-
823148978.zscaler</saml:AttributeValue></saml:Attribute></saml:AttributeStatement></saml:Assertion></samlp:Response>
```


Our UseID and the Groups associated with the User

Figure 75. SAML Attributes in the Decoded Assertion

Appendix A: Requesting Zscaler Support

You might need Zscaler Support to provision certain services, or to help troubleshoot configuration and service issues. Zscaler Support is available 24/7/365.

To contact Zscaler Support:

1. Go to **Administration** > **Settings** and click **Company Profile**.

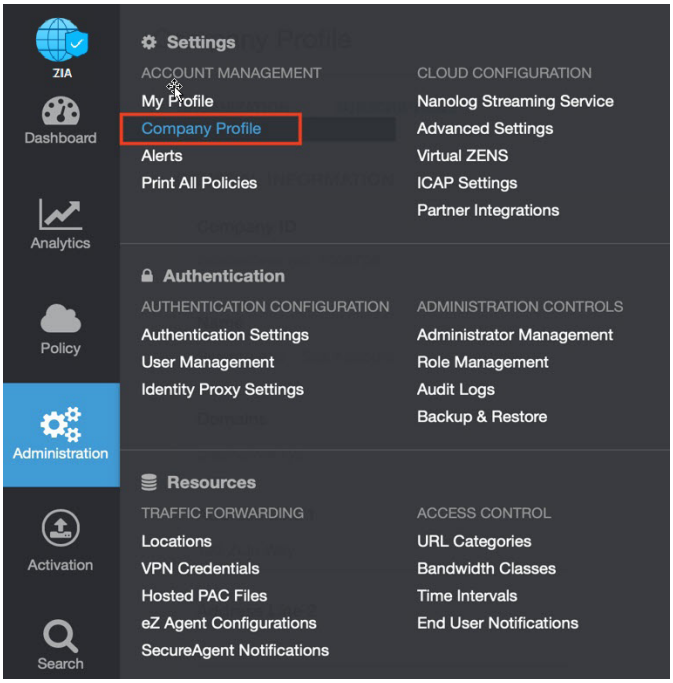


Figure 76. Collecting details to open support case with Zscaler TAC

2. Copy the Company ID.

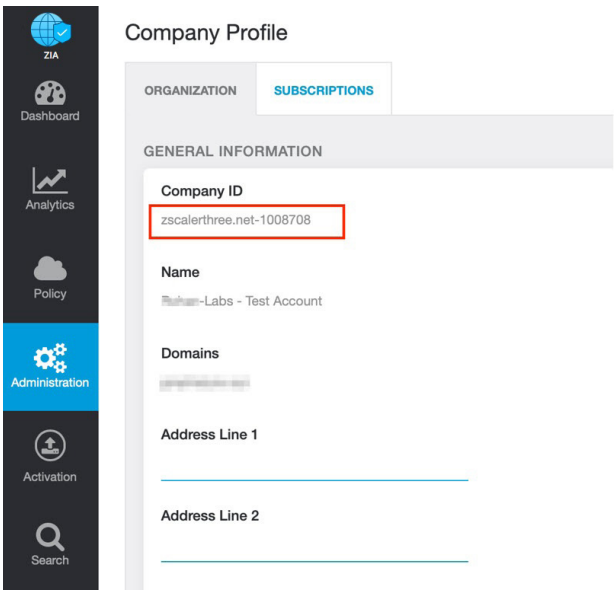


Figure 77. Company ID

3. With your company ID, you can open a support ticket. Go to **Dashboard** > **Support** > **Submit a Ticket**.

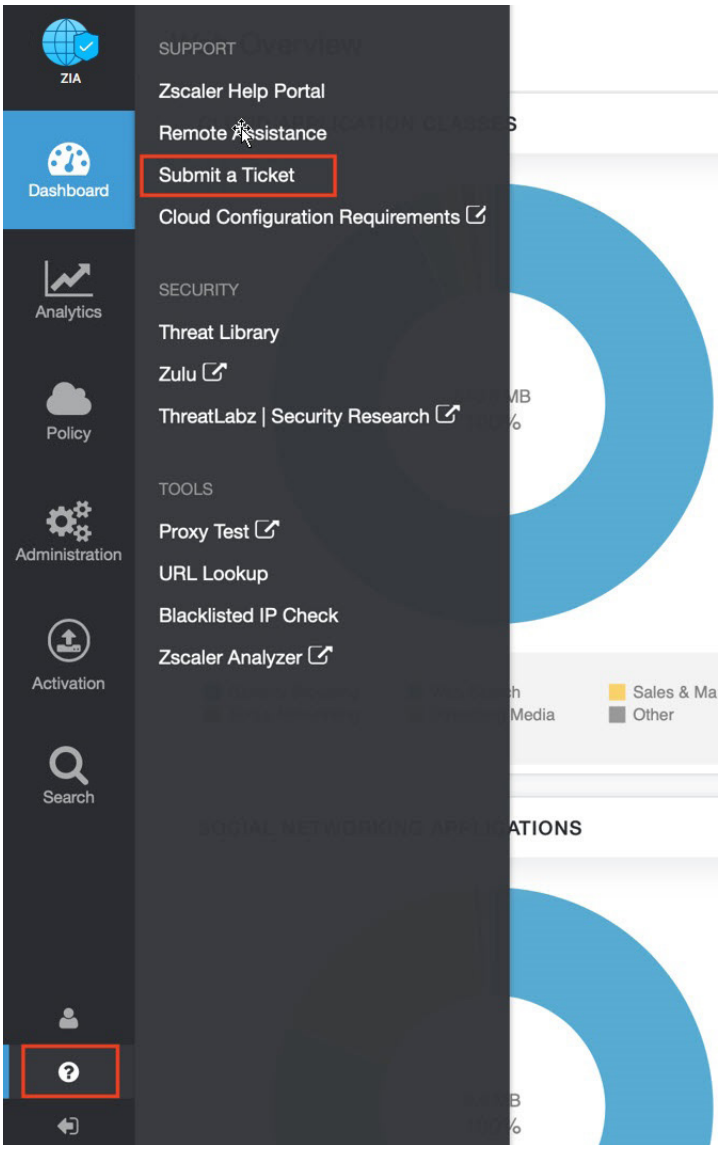


Figure 78. Submit a ticket

