Zscaler and PingOne Deployment Guide

Zscaler Business Development Solutions Architect Team

Sept 2020

Version 1.0
# Table of Contents

1 PingOne for Enterprise Authentication and Provisioning in use with Zscaler Services .................................................. 7  
   1.1 Overview .............................................................................. 7  

2 Configure PingOne and ZIA – SAML and SCIM ........................................... 9  
   2.1 Enable PingOne .................................................................. 9  
   2.2 Add the Zscaler ZIA Application .......................................... 10  
   2.3 Add the ZIA Application ...................................................... 11  
   2.4 Configure PingOne for ZIA (Part One) ................................. 13  
   2.5 Configure Zscaler ZIA for a PingOne IdP ............................. 14  
   2.6 Add PingOne as an IdP ...................................................... 15  
   2.7 Configure ZIA for PingOne ................................................. 16  
   2.8 Configure SCIM on ZIA ...................................................... 17  
   2.9 Configure PingOne for ZIA (Continued) .............................. 19  
   2.10 Configure PingOne for SCIM ........................................... 20  
   2.11 Provisioning Attribute Mapping ........................................ 22  
   2.12 Portal Settings .................................................................. 23  
   2.13 Configure Groups to use ZIA ........................................... 24  
   2.14 Finalize the PingOne Configuration .................................... 25  

3 Configure PingOne and ZPA – SAML and SCIM ........................................ 26  
   3.1 Add the Zscaler ZPA Application to PingOne .................... 26  
   3.2 Configure PingOne for ZPA (Part One) ............................... 29  
   3.3 Configure Zscaler ZPA for a PingOne IdP ............................ 30  
   3.4 Add the PingOne IdP on Private Access ............................. 31  
   3.5 IdP on Private Access – IdP Information ............................ 32  
   3.6 IdP on Private Access – SP Metadata ................................ 33  
   3.7 IdP on Private Access – Create IdP .................................... 34  
   3.8 Configure PingOne for ZPA (Continued) ............................ 35  
   3.9 Configure PingOne and SCIM ........................................... 37  
   3.10 PingOne Provisioning Attribute Mapping .......................... 38  
   3.11 PingOne Portal Settings ................................................... 39  
   3.12 Enable ZPA Users on PingOne ........................................ 40  
   3.13 Finalize the PingOne Configuration ................................... 41  
   3.14 Test the ZPA Authentication Configuration from the ZPA Portal .................. 42  
   3.15 Test the ZPA Authentication Configuration using the ZPA Test URL ........ 44  

4 Using PingOne for ZIA Admin Access ....................................................... 45  
   4.1 Add the PingOne SAML Application .................................. 45
4.2 PingOne SAML ZIA Admin Console Application ................................................. 46
4.3 Add the Application......................................................................................... 47
4.4 Configure the ZIA Administrator Application (Part 1)................................. 48
4.5 Configuring the ZIA Admin Portal for SAML Based Authentication .......... 49
4.6 Adding Administrators for SAML Based Authentication ............................. 50
4.7 Configure the ZIA Administrator Application (Continued) ....................... 51
4.8 Attribute Mapping ....................................................................................... 52
4.9 Changing the Portal Icon ............................................................................ 53
4.10 Adding the Administrator Group ................................................................. 54
4.11 Finalize the Configuration ........................................................................... 55
4.12 Test the Admin SSO Access ....................................................................... 56

5 Using PingOne for ZPA Admin Access............................................................ 57
  5.1 Add the PingOne Application for ZPA SAML Administrator Access ......... 57
  5.2 Configuring PingOne for SAML Authentication for ZPA Administrators .... 60
  5.3 Configure Zscaler ZPA for an Admin PingOne IdP ..................................... 61
  5.4 Add the ZPA IdP for Admin SSO on the ZPA UI ......................................... 62
  5.5 Configuring the ZPA IdP Information .......................................................... 63
  5.6 Copy the ZPA SP URLs .............................................................................. 64
  5.7 Finalize the PingOne IdP on the ZPA UI ..................................................... 65
  5.8 Define the Administrators for SAML Access .............................................. 66
  5.9 Create an Administrators for SAML Access ............................................. 67
  5.10 PingOne Configuration (Continued) .......................................................... 68
  5.11 Assign the Administrators or Groups to the Application ......................... 70
  5.12 Enable ZPA Admin Users on PingOne .................................................... 71
  5.13 Finalize the PingOne ZPA Admin Configuration ...................................... 72
  5.14 Test the ZPA Authentication Configuration ............................................ 73
  5.15 Administrator Sign-On Using SAML from the ZPA Admin Portal .......... 74

6 Transparent SSO using IWA with PingOne ..................................................... 75

7 PAC File and Zscaler Client Connector – Authentication Bypasses.............. 76

8 Testing and Troubleshooting - Capture the SAML Request for
Troubleshooting ................................................................................................. 77
  8.1 How to View a SAML Response in Your Browser for Troubleshooting .... 77
      Google Chrome ......................................................................................... 77
      Mozilla Firefox ......................................................................................... 77
      Apple Safari ............................................................................................... 78
      Microsoft Internet Explorer ................................................................. 78
  8.2 Configuring your Browser to Capture the ZIA SAML Response.............. 79

9 Appendix A: Capture the SAML Request for Troubleshooting .................... 86
  9.1 Zscaler Resources ..................................................................................... 86
  9.2 PingOne Resources .................................................................................... 87
## Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML</td>
<td>Security Assertion Markup Language</td>
</tr>
<tr>
<td>SCIM</td>
<td>System for Cross-domain Identity Management</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign On</td>
</tr>
<tr>
<td>AD</td>
<td>Microsoft Active Directory</td>
</tr>
<tr>
<td>ADFS</td>
<td>Microsoft Active Directory Federation Services</td>
</tr>
<tr>
<td>MFA</td>
<td>Multi-factor Authentication</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
<tr>
<td>ZEN</td>
<td>Zscaler Enforcement Node (Zscaler)</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access (Zscaler)</td>
</tr>
<tr>
<td>IWA</td>
<td>Integrated Windows Authentication</td>
</tr>
</tbody>
</table>
About This Document

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. Its flagship services, Zscaler Internet Access and Zscaler Private Access, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to 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. For more information on Zscaler, please visit www.zscaler.com or follow them on Twitter @zscaler.

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.[3] 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,[4] similar to identity management system tools developed by Microsoft and Okta (identity management).[5] 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.

For more information on Ping Identity, please visit www.pingidentity.com or follow them on Twitter @pingidentity.
Audience

This guide is written for Authentication Administrators, IT Administrators, and IT Analysts responsible for deploying, monitoring and managing authentication and provisioning services in an Enterprise environment. For additional product and company resources, please refer to the Appendix section.

Software Revisions

This document was authored using Zscaler Internet Access v6.0 and PingOne Production Release 2020.08.0.

Request for Comments

We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact us at partner-doc-support@zscaler.com.
1 PingOne for Enterprise Authentication and Provisioning in use with Zscaler Services

1.1 Overview

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 optionally other additional identity factors. SAML (Security Assertion Markup Language) is the preferred method for authentication for both Zscaler Internet Access and Zscaler Private Access and for this document PingOne will be configured as the SAML identity provider (IdP). SAML is an open protocol standard that allows PingOne to authenticate a user and pass the authorization credentials to Zscaler Services as a SAML service provider (SP).
Although beyond the scope of this document, SAML also provides Single-Sign On to any SAML SP. An example of this would be gaining access to both Zscaler Internet Access (ZIA) and Zscaler Private Access 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.

Provisioning as it relates to authentication is the automation of provisioning and deprovisioning of users and security groups to Zscaler services. SCIM (System for Cross-domain Identity Management) 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 will automatically provision the user and the associated security groups in the Zscaler database and likewise, when a user is deprovisioned, the user, associated groups, and credentials are also removed preventing access to resources. The primary use case would be for onboarding and offboarding users from an organization. When a user leaves an organization, the user is deprovisioned from the user directory and SCIM will make the associated changes in the Zscaler databases eliminating all ZIA and ZPA access. SCIM would then deprovision the user from all associated databases, preventing further access to company resources.

For more information, please see the resources in Appendix A: Zscaler Resources.
2 Configure PingOne and ZIA – SAML and SCIM

2.1 Enable PingOne

![PingOne Registration Page]

Figure 2: Creating a PingOne IdP

The scope of 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 / PingOne solution. However, a new, no cost PingOne developer instance was created from the PingOne website at https://admin.pingone.com/web-portal/register and used to create this document. Each step was validated for functionality in a live environment. The above figure shows to select the Classic UI and the shortcuts at the right give us an indication of what needs to be configured for SAML authentication to work.
2.2 Add the Zscaler ZIA Application

![Image of PingOne portal showing My Applications page]

**Figure 3: Adding an Application**

The first step is to add the Zscaler Applications to PingOne that will be used to enable authentication and provisioning to the Zscaler service. From the PingOne portal administrator account, select **Applications / My Applications** and then select **Add Application**.
2.3 Add the ZIA Application

Figure 4: Adding the Zscaler Applications

To add the appropriate Zscaler application, search for “zscaler” and then select the Zscaler application for Zscaler with SAML and Provisioning (API) for use with Zscaler Internet Access (ZIA) users.
Figure 5: Adding Zscaler 2.0 for Zscaler Internet Access (ZIA)

When you select the arrow on the right, it will bring up a description of the application. Click Setup to begin the installation process.
2.4 Configure PingOne for ZIA (Part One)

This will bring up the initial configuration screen. **Download the Signing Certificate**, and **copy the IdP ID, and the Example SAML Portal URL** listed in step 4. The IdP ID will be appended to the Example URL to create the SAML Portal URL that will be used in the Zscaler IdP setup process. **Select Continue to Next Step**.

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

```
https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=9e4858a9-65cf-44cd-a77a-619308ca5c58
```

We now need to bring up Zscaler Internet Access and start the process of adding a new IdP to our ZIA portal to get the additional information for the upcoming steps. Open a new browser Window and bring up the ZIA Admin UI. Leave the PingOne config as is for the moment.
2.5 Configure Zscaler ZIA for a PingOne IdP

To add PingOne as an IdP in your ZIA Portal, select **Administration / Authentication Settings**. This will bring up the Authentication settings screen.

Figure 7: Adding PingOne and the Zscaler Internet Access IdP
2.6 Add PingOne as an IdP

**Figure 8: Adding PingOne as an IdP**

Select **Add Identity Provider**. This will bring up the Edit Identity Provider screen.
2.7 Configure ZIA for PingOne

![Figure 9: The Edit Identity Provider Screen](image)

This is the IdP configuration screen. **Give the IdP a Name**, make sure the Status is enabled, and then **paste in the SAML Portal URL** we saved from Page 13. **Enter in NameID** (Case Sensitive) for the Login Name Attribute, **Upload the PingOne Public Certificate** from Figure 6, then **select PingOne as the Vendor** profile. For the Default IdP leave the Locations and Authentication Domains as None, however if this is for a specific Location or Domain, **select the pull down and select the specific Authentication Domain** the PingOne IdP will provide authentication for. **Select the saml_2022 signing certificate** and **download the SP Metadata and the SP SAML Certificate** and save for the next step. **Enable SAML Auto Provisioning**. Set the User Display Name Attribute to **displayName** (Case Sensitive), Set the Group Name Attribute to **memberOf** (Case Sensitive), and set the Department Name Attribute to **department** (Case Sensitive). **Save and Activate** the configuration. **Note**: To configure SCIM we must save the configuration first and then go back in and enable SCIM.
2.8 Configure SCIM on ZIA

To enable SCIM we now need to edit the IdP by clicking the pencil icon, which will re-open the Identity Provider configuration screen.

Figure 10: Edit the Identity Provider
To enable SCIM on the IdP we now need to select Enable SCIM Based Provisioning which will display the SCIM Base URL and Bearer Token. **Copy the SCIM Base URL and Bearer Token** for the next step in the PingOne Portal. **Save and Activate** the configuration.

We now need to finish the PingOne configuration. Go back to the PingOne configuration screen to finish the IdP setup.
2.9 Configure PingOne for ZIA (Continued)

To finish the PingOne configuration to use with ZIA. **Upload the Zscaler Metadata file and the Zscaler signing certificate** we downloaded on page 16 of this guide. **Select the Set Up Provisioning** check box and then select **Continue to Next Step**.
2.10 Configure PingOne for SCIM

![Table showing application name and type]

### 3. Provisioning Instructions

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

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Obtain Your Zscaler Base URL</td>
<td>The Base URL for Zscaler (for example, <a href="https://scim">https://scim</a>.&lt;cloud name&gt;&lt;org ID&gt;/scim).</td>
</tr>
<tr>
<td>2. Obtain Your Zscaler Bearer Token</td>
<td>The access token used to make authenticated API calls to Zscaler. For more information, see <a href="https://docs.pingidentity.com/bundle/integrations/page/hgh1563956073453.html">https://docs.pingidentity.com/bundle/integrations/page/hgh1563956073453.html</a></td>
</tr>
<tr>
<td>3. Application Configuration</td>
<td>On the Application Configuration screen enter the Base URL and Bearer Token obtained in the previous steps into the relevant fields.</td>
</tr>
<tr>
<td>4. Attribute Mapping</td>
<td>Map the user store attributes to Zscaler attributes that are to be managed during user provisioning. Note that the username attribute is required. For more information on Zscaler supported attributes, see <a href="https://docs.pingidentity.com/bundle/integrations/page/ewe15630507420.html">https://docs.pingidentity.com/bundle/integrations/page/ewe15630507420.html</a>.</td>
</tr>
<tr>
<td>5. Configure targeted group(s)</td>
<td>Once the application is configured, navigate to the Group Management page and select the group(s) to target for provisioning.</td>
</tr>
</tbody>
</table>

*Figure 13: Configure SCIM on the PingOne side*

This will display the setup steps for SCIM on PingOne select **Continue to Next Step** to proceed.
Enter the **Base URL** copied from the Identity Provider config on page 18 in the previous step into the **BASE_URL** field. Then enter the **Bearer Token** value into the **BEARER_TOKEN** Field and select **Continue to Next Step**.
2.11 Provisioning Attribute Mapping

<table>
<thead>
<tr>
<th>Application Attribute</th>
<th>Description</th>
<th>Identity Bridge Attribute or Literal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>memberOf (sso)</td>
<td>Groups user is a member of</td>
<td>memberOf</td>
</tr>
<tr>
<td>displayName (sso)</td>
<td>Users Display Name</td>
<td>displayName</td>
</tr>
<tr>
<td>department (sso)</td>
<td>Department user is in</td>
<td>department</td>
</tr>
<tr>
<td>SAML_SUBJECT (sso)</td>
<td>Map this to the username in Zscaler</td>
<td>SAML_SUBJECT</td>
</tr>
<tr>
<td>userName (provisioning) *</td>
<td>Zscaler’s unique identifier for the user. The expected format is user@domain (for example, &quot;<a href="mailto:bjensen@example.com">bjensen@example.com</a>&quot;). A username cannot be updated. This attribute is required.</td>
<td>Email</td>
</tr>
<tr>
<td>displayName (provisioning) *</td>
<td>The name of the user, suitable for display to end-users. This attribute is required.</td>
<td>UserName</td>
</tr>
<tr>
<td>department (provisioning)</td>
<td>The department for the user. If no department is specified, Zscaler sets a default value of 'Service Admin'.</td>
<td>department</td>
</tr>
<tr>
<td>email (provisioning)</td>
<td>The email for the user (for example, &quot;<a href="mailto:bjensen@example.com">bjensen@example.com</a>&quot;).</td>
<td>Email</td>
</tr>
<tr>
<td>externalID (provisioning)</td>
<td>A string that is an identifier for the resource as defined by the provisioning client.</td>
<td>externalID</td>
</tr>
<tr>
<td>firstName (provisioning)</td>
<td>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”).</td>
<td>First Name</td>
</tr>
<tr>
<td>lastName (provisioning)</td>
<td>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”).</td>
<td>Last Name</td>
</tr>
</tbody>
</table>

Figure 15: PingOne SCIM Synchronization Settings

For Self-Provisioning and SCIM to function properly we must map the Ping variables to match the expected ZIA variables. At a minimum, **set variables 1-3, memberOf, displayName, and department attributes** for Auto-provisioning. We also need to **set userName to Email and displayName to userName** for variables 5 and 6 for SCIM to push or delete the user. **select Continue to Next Step. Note:** SCIM will only push, delete or disable the user. SCIM will not push the Security Groups. The security groups are pulled over from auto-provisioning for use with ZIA policies.
2.12 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 select **Continue to Next Step**.
2.13 Configure Groups to use ZIA

The final step is to select the Security Groups that are allowed to use Zscaler Internet Access. Add any or all Groups specific to your installation and then select **Continue to Next Step**.

**Figure 17: PingOne SCIM Synchronization Settings**
2.14 Finalize the PingOne Configuration

Verify your configuration and select Finish. Your PingOne instance is now configured for authenticating ZIA users.
3 Configure PingOne and ZPA – SAML and SCIM

3.1 Add the Zscaler ZPA Application to PingOne

![Figure 19: Adding an Application](image)

The first step is to add the Zscaler Applications to PingOne that will used to enable authentication and provisioning to the Zscaler service. From the PingOne portal administrator account, select Application and then select Add Application.
To add the appropriate Zscaler application, search for “zscaler” and select Zscaler Private Access 2.0 SAML with Provisioning API for Zscaler Private Access (ZPA) with SCIM provisioning.
<table>
<thead>
<tr>
<th>Application Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zscaler</td>
<td>SAML with Provisioning (API)</td>
</tr>
<tr>
<td>Zscaler Private Access 2.0</td>
<td>SAML with Provisioning (API)</td>
</tr>
<tr>
<td>Zscaler Private Access Administrator 2.0</td>
<td>SAML</td>
</tr>
<tr>
<td>Zscaler Two</td>
<td>SAML</td>
</tr>
<tr>
<td>Zscaler Two Admin Console</td>
<td>SAML</td>
</tr>
<tr>
<td>Zscaler-Beta</td>
<td>SAML</td>
</tr>
</tbody>
</table>

**Figure 21: ZPA Private Access 2.0**

When you select the arrow on the right, it will bring up a description of the application. **Click Setup** to begin the installation process.
3.2 Configure PingOne for ZPA (Part One)

**Figure 22: PingOne Zscaler Private Access 2.0 Configuration**

This will bring up the initial configuration screen. **Download the Signing Certificate, copy the IdP ID, and the Issuer URL.** The IdP ID will be appended to the below URL Prefix to create the SAML Portal URL that will be used in the Zscaler Private Access IdP setup process. **Select Continue to Next Step.**

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 will be created by combining the Base SAML Portal URL and the IdP ID to become:

```
```

We now need to bring up Zscaler Private Access and start the process of adding a new IdP to our ZPA portal to get the additional information for the upcoming steps. Open a new browser Window and bring up the ZPA Admin UI. Leave the PingOne config as is for the moment.
3.3 Configure Zscaler ZPA for a PingOne IdP

Figure 23: Creating the PingOne IdP on ZPA

In the ZPA UI select **Administration** and then **select IdP Configuration**. This will bring up the IdP Configuration screen.
3.4 Add the PingOne IdP on Private Access

On the IdP configuration screen select **Add IdP Configuration** at the top right of the UI. This will bring up the IdP configuration wizard to walk you through the creation of the IdP. If the window is constrained only the circle with the white plus sign may be visible.
3.5 IdP on Private Access – IdP Information

**Figure 25: IdP Information**

Give the IdP an appropriate Name and leave the single Sign-on setting at User, select the authentication domains that will be services by this IdP, and then click Next.

**Note:** Multiple IdPs are supported in ZPA, and the IdP is bound to the domain in this step. ZPA only supports one domain for Client Connector deployments, additional IdPs are defined for Browser Access domains.
3.6 IdP on Private Access – SP Metadata

For our next step for the PingOne IdP we will need to download the Service Provider Metadata and the Service Provider Certificate. Download and Save both file’s and then select Next.
3.7 IdP on Private Access – Create IdP

In our final ZPA IdP configuration screen, upload the PingOne Certificate file, enter the Single Sign-On URL with the URL we created on page 29, and enter the Issuer URL as the IdP Entity ID. For SCIM select Enabled for SCIM Sync, then select Generate New Token. This will bring up our SCIM parameters we will need for the remaining PingOne configuration. Save both the SCIM Service Provider Endpoint URL and the Bearer Token for the PingOne configuration. Then select Save.
3.8 Configure PingOne for ZPA (Continued)

Figure 28: Add IdP Configuration

To finish the PingOne configuration to use with ZPA. **Upload the Zscaler Metadata file and the Zscaler signing certificate** we downloaded on page 33 of this guide. **Select the Set Up Provisioning** check box and then **select Continue to Next Step**.
Figure 29: Provisioning Instructions

Review the remaining configuration steps and then select Continue to Next Step.
3.9 Configure PingOne and SCIM

### Figure 30: PingOne SCIM Configuration

Enter the Base URL copied from the Identity Provider config on page 34 in the previous steps into the BASE_URL field. Then enter the Bearer Token value into the BEARER_TOKEN Field and select Continue to Next Step.
3.10 PingOne Provisioning Attribute Mapping

For Self-Provisioning and SCIM to function properly we must map the Ping attributes to match the expected ZPA attributes. **Set attributes 1-8 (Excluding Department name), set First Name, Last Name, Email and memberOf for Auto-provisioning.** We also need to **set userName to Email and displayName to userName** for variables 7 and 8 for SCIM to push or delete the user. **Select Continue to Next Step.** **Note:** SCIM will only push, delete or disable the user. SCIM will not push the Security Groups. The security groups are pulled over from auto-provisioning for use with ZPA policies.
3.11 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 select **Continue to Next Step**.
3.12 Enable ZPA Users on PingOne

The final step is to select the Security Groups that are allowed to use Zscaler Private Access. Add any or all Groups specific to your installation and then select **Continue to Next Step**.
3.13 Finalize the PingOne Configuration

![Image of SCIM Integration API Setup]

Figure 34: SCIM Integration API Setup

Select Enable API Integration This will bring up the API parameters. Enter the SCIM Service Provider Endpoint URL and the Bearer Token that were save from the ZPA IdP screen on page 29 and then select the Test API Credentials. If the credentials are valid and PingOne can communicate with the ZPA Cloud you should get the response highlighted in red above. If you receive an error, you will need to re-copy the URL and Token and possibly generate a new Bearer Token. Once you have verified your credentials select Save.
3.14 Test the ZPA Authentication Configuration from the ZPA Portal

We need to import the SAML variables in from PingOne. To do this from the ZPA UI, select Administration / IdP Configuration, then select the little blue arrow next to your IdP. This will show the PingOne configuration. Then select Import next to your domain under Import SAML Attributes. Once this is selected it will Authenticate to PingOne using your existing User if you are authenticated or will bring up the PingOne login screen. The SAML variables and the SAML assertion are then displayed in the screen on the next page.

Figure 35: SAML Variable Import
Review your mappings and then save the Attribute variables by selecting Save.
3.15 Test the ZPA Authentication Configuration using the ZPA Test URL

You can also test by using the below URL. Replace househarcourt.com with your domain in the URL and your SAML Assertion will be returned if you are an already authenticated user or you will be prompted to authenticate. Once you are authenticated your SAML assertion will be displayed.

Test URL:

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}
4 Using PingOne for ZIA Admin Access

4.1 Add the PingOne SAML Application

To use PingOne SAML authentication for ZIA Admin users we must install the SAML Service Provider Application. From the PingOne UI select the Applications tab at the top of the screen, and then select Add Application.
4.2 PingOne SAML ZIA Admin Console Application

Figure 38: The PingOne SAML for ZIA Administrators

Search for zscaler and then add the Zscaler Two Admin Console Application.
### 4.3 Add the Application

<table>
<thead>
<tr>
<th>Zscaler Two Admin Console</th>
<th>SAML</th>
</tr>
</thead>
</table>

**Icon**
![Zscaler Icon](image)

**Name** Zscaler Two Admin Console

**Description**
Zscaler Two Web Security leverages the world's largest global security cloud to deliver the industry's most comprehensive protection against advanced and emerging threats. And, because it relies on our patented, multi-tenant 100% cloud architecture, it delivers all the benefits of proactive, Real-time security without the need to deploy and manage appliances, software or agents.

**Category** Information Technology

![Setup Button](image)

**Figure 39: General Settings**

Verify the application description and select Setup.
4.4 Configure the ZIA Administrator Application (Part 1)

Figure 40: Configuration Settings

This will bring up the initial configuration screen. Download the Signing Certificate, and copy the IdP ID, and the Example SAML Portal URL listed in step 4. The IdP ID will be appended to the Example URL to create the SAML Portal URL that will be used in the Zscaler IdP setup process. Select Continue to Next Step.

We now need to bring up Zscaler Internet Access and start the process of adding a new IdP to our ZIA portal to get the additional information for the upcoming steps. Open a new browser Window and bring up the ZIA Admin UI. Leave the PingOne config as is for the moment.
4.5 Configuring the ZIA Admin Portal for SAML Based Authentication

To enable SAML based authentication for Administrators, bring up the ZIA console and select Administration / Administrator Management. This will bring up the Administrator Management screen. Select Enable SAML Authentication, and then Upload the IdP certificate we downloaded from page 48. The certificate file type will need to be changed to “.pem” for it to be uploaded. Download the XML Metadata and save the file for next steps. Add the Issuer URL from the previous step, then select Save.
4.6 Adding Administrators for SAML Based Authentication

![Administrator Management](image)

**Figure 42: Verify Administrators**

The Administrators must be added as a ZIA Administrator to use SAML Based Authentication. Select Administration / Administrators / + Add Administrators to add all of the Administrators that will using SAML SSO. Now let’s go back and finish the PingOne configuration.
4.7 Configure the ZIA Administrator Application (Continued)

To finish PingOne configuration **upload the Zscaler Metadata file** we saved from page 49 and select **Continue to Next Step**.
### 4.8 Attribute Mapping

#### 3. Attribute Mapping

Map your identity bridge attributes to the attributes required by the application.

<table>
<thead>
<tr>
<th>Application Attribute</th>
<th>Description</th>
<th>Identity Bridge Attribute or Literal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SAML_SUBJECT Map this to the username in Zscaler Two Admin Console</td>
<td>SAML_SUBJECT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>As Literal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advanced</td>
</tr>
<tr>
<td>2</td>
<td>department Map to the attribute that will contain the user’s department.</td>
<td>Name or Literal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>As Literal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advanced</td>
</tr>
<tr>
<td>3</td>
<td>displayName Map to the attribute that will contain the user’s display name.</td>
<td>Name or Literal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>As Literal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advanced</td>
</tr>
<tr>
<td>4</td>
<td>memberOf Map to the attribute that will contain a list of the user’s group membership.</td>
<td>Name or Literal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>As Literal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advanced</td>
</tr>
</tbody>
</table>

* Indicates a required attribute.

---

**Figure 44: Attribute Mapping**

Leave the attribute mapping as default and **Select Continue to Next Step**.
4.9 Changing the Portal Icon

Figure 45: Portal Icon and Description

Leave the portal icon and description as default and **Select Continue to Next Step**. However, you can customize the look and change the description if desired by your organization.
4.10 Adding the Administrator Group

We must add the groups that the Administrators are included in so they will be allowed to Authenticate using SAML. **Add the appropriate Security Groups** and **Select Continue to Next Step**.
4.11 Finalize the Configuration

Figure 47: Configuration Review

Verify the PingOne settings and **Select Finish** to save your configuration.
4.12 Test the Admin SSO Access

![PingOne Desktop](image)

**Figure 48: PingOne Desktop**

You are now ready to launch the ZIA UI from the PingOne portal and the SAML application. You should Authenticate to PingOne using SAML and the ZIA Administrator Portal should be launched.
5 Using PingOne for ZPA Admin Access

5.1 Add the PingOne Application for ZPA SAML Administrator Access

To use PingOne SAML authentication for ZPA Admin users we must install the SAML Service Provider Application. From the PingOne UI select the Applications tab at the top of the screen, and then select Add Application.
Figure 50: Select the ZPA Application

Search for Zscaler in the search bar and then select the Zscaler Private Access Administrator 2.0 Application by clicking on the arrow to the right of the application.
**Figure 51: General Description**

When you select the arrow on the right, it will bring up a description of the application. **Click Setup** to begin the installation process.
5.2 Configuring PingOne for SAML Authentication for ZPA Administrators

This will bring up the initial configuration screen. **Download the Signing Certificate, copy the IdP ID, and the Issuer URL.** The IdP ID will be appended to the below URL Prefix to create the SAML Portal URL that will be used in the Zscaler Private Access IdP setup process. **Select Continue to Next Step.**

**SAML Portal Base URL:** `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=+IdP ID`. In this configuration example the SAML Portal URL will be created by combining the Base SAML Portal URL and the IdP ID to become:

```
```

We now need to bring up Zscaler Private Access and start the process of adding a new IdP to our ZPA portal to get the additional information for the upcoming steps. Open a new browser Window and bring up the ZPA Admin UI. Leave the PingOne config as is for the moment.
5.3 Configure Zscaler ZPA for an Admin PingOne IdP

In the ZPA UI select Administration and then select IdP Configuration. This will bring up the IdP Configuration screen.
5.4 Add the ZPA IdP for Admin SSO on the ZPA UI

![ZPA UI - Add the PingOne IdP](image)

Figure 54: ZPA UI – Add the PingOne IdP

On the IdP configuration screen select **Add IdP Configuration** at the top right of the UI. This will bring up the IdP configuration wizard to walk you through the creation of the IdP. If the window is constrained only the circle with the white plus sign may be visible.
5.5 Configuring the ZPA IdP Information

![Add IdP Configuration Wizard]

When you click the Add IdP Configuration the IdP Configuration Wizard will be launch. **Give the IdP a unique name, select Admin under Single Sign-On, and select the organization’s domain/s that the Administrators will be signing in from. Then select Next.**
5.6 Copy the ZPA SP URLs

Figure 56: SP Metadata and SP Certificate

For our next step for the PingOne IdP we will need to download the Service Provider Metadata and the Service Provider Certificate. Download and Save both file’s and then select Next.
5.7 Finalize the PingOne IdP on the ZPA UI

![Add IdP Configuration](image)

In our final ZPA IdP configuration screen, upload the PingOne Certificate file, enter the Single Sign-On URL with the URL we created on page 60, and enter the Issuer URL as the IdP Entity ID. Then select Save.

Figure 57: ZPA IdP Completed Configuration
5.8 Define the Administrators for SAML Access

Administrators that will be using the SAML IdP for authentication must be defined as Administrators. To configure the administrators that will be authenticating, select Administration / Administrators. This will bring up the Add Administrator Screen. Select Add Administrator in the upper right corner of the UI. If the browser window is small the Add Administrator Configuration may show up as only a blue circle with a white plus sign in it.

Figure 58: Creating an Administrator
5.9 Create an Administrators for SAML Access

The Add Administrator window will now be displayed. Enter the Admin ID, the Password and Password Verification, Select ZPA Administration from the Role pulldown, and enter an Email Address and a Phone number (without formatting). Then select Save to complete the ZPA configuration. We are now ready to complete the PingOne configuration.
5.10 PingOne Configuration (Continued)

To finish the PingOne configuration to use with ZPA Administrators. **Upload the Zscaler Metadata file and the Zscaler signing certificate** we downloaded on page 64 of this guide then select **Continue to Next Step**.
### 3. Attribute Mapping

Map your identity bridge attributes to the attributes required by the application.

<table>
<thead>
<tr>
<th>Application Attribute</th>
<th>Description</th>
<th>Identity Bridge Attribute or Literal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. SUBJECT</td>
<td>Map this to the username in Zscaler Private Access Admin Console</td>
<td>SAML SUBJECT</td>
</tr>
<tr>
<td>2. Department</td>
<td>Map to the attribute that will contain the user’s department</td>
<td>Name or Literal</td>
</tr>
<tr>
<td>3. displayName</td>
<td>Map to the attribute that will contain the user’s display name</td>
<td>Name or Literal</td>
</tr>
<tr>
<td>4. memberOf</td>
<td>Map to the attribute that will contain a list of the user’s group membership</td>
<td>Name or Literal</td>
</tr>
<tr>
<td>5. First Name</td>
<td>Map to the attribute that contains the user’s First Name</td>
<td>Name or Literal</td>
</tr>
<tr>
<td>6. Last Name</td>
<td>Map to the attribute that contains the user’s Last Name</td>
<td>Name or Literal</td>
</tr>
<tr>
<td>7. Group</td>
<td>Map to the attribute that contains the user’s group membership for Zscaler</td>
<td>Name or Literal</td>
</tr>
<tr>
<td>8. Email Address</td>
<td>Map to the user’s email attribute</td>
<td>Name or Literal</td>
</tr>
</tbody>
</table>

Add new attribute

* Indicates a required attribute.

---

**Figure 61: Attribute Mapping**

Leave the Attributes as default and **select Continue to Next Step.**
5.11 Assign the Administrators or Groups to the Application

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 select **Continue to Next Step**.
5.12 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 select Continue to Next Step.
5.13 Finalize the PingOne ZPA Admin Configuration

Verify your configuration and select Finish. Your PingOne instance is now configured for authenticating ZPA Administrators using PingOne SAML SSO.
5.14 Test the ZPA Authentication Configuration

We can now see our applications from the PingOne portal for the Administrator. By clicking on the application, the app will launch the ZPA UI and Authenticate the user transparently. We can also login from the ZPA Admin Sign-on screen.

Figure 65: User PingOne Apps
5.15 Administrator Sign-On Using SAML from the ZPA Admin Portal

To sign in from the ZPA Admin Screen using the PingOne SAML IdP select the Single Sign-On Using IdP option and then select Sign In. This will launch the PingOne Authentication Screen.
6  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 clients AD infrastructure using the AD Connect server. Zscaler will take advantage of IWA if it is active and will automate the login process without the user having to enter credentials. However, it is important to note this is not a Zscaler configuration, Zscaler only utilizes 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.

See more details here https://docs.pingidentity.com/bundle/pingone/page/sxy1564020492140.html
7 PAC File and Zscaler Client Connector – Authentication Bypasses

When using Zscaler Internet Access you must bypass the IdP provider login URL’s for Authentication to succeed, or by entering the URLs in Authentication Bypass in the ZIA portal. For ZPA it is not a requirement and the destination URL’s can flow through ZIA but bypassing the URLs for ZIA is a requirement for both Browser PAC files and for the Zscaler Client Connector. The below entries need to be added to your Browser PAC and/or the Zscaler Client Connector Custom Pac File for the Application Profile. For more information see Appendix A in the back of this guide.

PAC File Bypasses:

// PingOne Authentication Bypass
if (dnsDomainIs(host, ".pingone.com") ||
    dnsDomainIs(host, ".pingidentity.com"))
    return "DIRECT";

Authentication Bypasses in the ZIA Portal:

In the Zcaler Internet Access Console go to Administration / Advanced Settings / Authentication Exemptions / Exempted URLS and Add .pingone.com and .pingidentity.com as exempted URLS.

![Figure 67: Administrator Sign-On using our SAML IdP](image)
8 Testing and Troubleshooting - Capture the SAML Request for Troubleshooting

Troubleshooting SAML can be challenging and the below procedures can be used to 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 Browsers Developer Tools and then decoding it using a base 64 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. Any browser can be used to capture the SAML Assertion and the procedures for the most common browsers are listed below.

8.1 How to View a SAML Response in Your Browser for Troubleshooting
To troubleshoot Single Sign On (SSO) login issues, it can be helpful to retrieve the SAML response from your service provider from in your browser.

Google Chrome - To view a SAML response in Chrome

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

- Press F12 to start the developer console.
- In the upper right of the developer tools window, click options (the small gear icon). Under Common Preferences select Enable persistent logs.
- Select the Network tab.
- Reproduce the issue.
- 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. **Note:** 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

- Enable Web Inspector in Safari. Open the Preferences window, select the Advanced tab, and then select Show Develop menu in the menu bar.
- Now you can open Web Inspector. Click Develop, then select Show Web Inspector.
- Select the Resources tab.
- Reproduce the issue.
- Look for a POST method with a samlconsumer file in the table.
- Scroll down to find Request Data with the name SAMLResponse. Note: The SAMLResponse attribute contains the encoded request; use a Base64 decoder to investigate the decoded response.

Microsoft Internet Explorer
To view a SAML response in Internet Explorer
The best way analyze network traffic in Internet Explorer is through the use of a third-party tool.

- Follow the steps at http://social.technet.microsoft.com/wiki/contents/articles/3286.ad-fs-2-0-how-to-use-fiddler-web-debugger-to-analyze-a-ws-federation-passive-sign-in.aspx to download and install Fiddler and capture the data.

What to do with the Base64-encoded SAML response
Once you find the Base64-encoded SAML response element in your browser, copy it and use your favorite Base-64 decoding tool to extract the XML tagged response.

Security Tip
Because the SAML response data that you are viewing might contain sensitive security data, we recommend that you do not use an online base64 decoder. Instead use a tool installed on your local system.
8.2 Configuring your Browser to Capture the ZIA SAML Response

Open the proxy configuration screen for the browser you are going to test with and enter in the Proxy IP address we just copied. You will also need to enter in the PingOne domains as bypasses so the request will make it to PingOne and not be blocked by ZIA. The three PingOne domains to bypass are .PingOne.com, and .PingOnecdn.com. Save the changes and you are now ready to test.

The first step is to configure Zscaler as a Proxy for your browser. You can configure the automatic FQDN that will select the fastest gateway response as the proxy. The FQDN is gateway.zscalerthree.net, where zscalerthree will be replaced by your cloud (i.e. gateway.zscloud.net, gateway.zscalertwo.net, etc…). However, for this exercise let’s manually select the proxy from our list of enforcement nodes. Enter your Clouds information center, in the above example the URL is ips.zscalerthree.net/cenr this will list all of the enforcement nodes for the Zscalerthree Cloud. The Dallas IP will then be used as the Proxy address we will define in our Browser.
Enter any URL in the browser and ZIA will now prompt you for authentication credentials. At this point we want to start our developer tools. Select the three dots at the top right of the browser. This will bring up a drop-down menu, then select More Tools, and then Developer Tools. This will start the developer screen.

**Figure 69: Selecting Developer Tools**
Figure 70: Select Network View

We now have our network trace which will show us the connection and packet information as we authenticate into Zscaler and PingOne. The initial authentication screen above is only looking for the user domain appended to the User ID so Zscaler knows which Zscaler instance to direct the request to. In this case testmypacket.com.
Figure 71: Authenticate to the PingOne IdP

Zscaler has redirected the authentication request to PingOne, and we now get the PingOne authentication screen. Log in with a valid User ID in the PingOne database associated with the Zscaler instance.
Once authentication has completed, select the packet called sfc_sso that is destined to login.zscaler.net. This is our SAML response from PingOne and contains our SAML Assertion. The Assertion is base64 encoded and we will need to use a decoder to get the clear text information. Select the SAML Response data excluding “SAMLResponse.” we want only the data.
Using a base64 decoder, paste the encoded text into the application and then copy the decoded SAML Assertion and let’s take a look. The Base64Anywhere app was used for this demonstration and was downloaded free from the Mac App store. There are also free decoders on the Windows store if you are a Microsoft user.
Figure 74: SAML Attributes in the Decoded Assertion

We can now see our clear text Assertion with the NameID of the user and our other attributes. In this example you see that the user is part of groups called Group1, Group2, Group3, Group4, and Users. All groups and attributes associated with the user can be seen in this response.
Appendix A: Capture the SAML Request for Troubleshooting

9.1 Zscaler Resources

Zscaler Internet Access (ZIA)
https://www.zscaler.com/products/zscaler-internet-access

ZIA Best Practices for Traffic Forwarding

ZIA – Configuring SAML
https://help.zscaler.com/zia/configuring-saml

ZIA – Configuring SCIM
https://help.zscaler.com/zia/configuring-scim

ZPA – Configuring SAML

IWA – Mark Ryan’s IWA / PingOne Demonstration
https://www.youtube.com/watch?v=CtRljdMDchc&list=PLLCE8u9uBMmugp00PC91GOpMz5kD_V1hn&index=59&t=0s

Zscaler Client Connector – App Profile
https://help.zscaler.com/z-app/configuring-zscaler-app-profiles

Tunnel-2 Bypasses

Zscaler Hosted PAC files
9.2 PingOne Resources

PingOne Documentation
https://docs.pingidentity.com/

PingOne How to Configure SAML for Zscaler Internet Access
https://docs.pingidentity.com(bundle/integrations/page/zhr1563995073160.html)

PingOne How to Configure SAML for Zscaler Private Access
https://docs.pingidentity.com(bundle/integrations/page/exl1587060854790.html)

Ping AD Connect
https://docs.pingidentity.com(bundle/pingone/page/sxy1564020492140.html)