ZSCALER AND AZURE IDENTITY DEPLOYMENT GUIDE

OCTOBER 2021, VERSION 1.2

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

This 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
SAML	Security Assertion Markup Language
SCIM	System for Cross-domain Identity Management
SSO	Single Sign On
Microsoft Entra ID	Microsoft Active Directory
MFA	Multi-factor Authentication
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)
IWA	Integrated Windows Authentication

About This Document

The following sections describe the organizations and requirements for the integration covered by 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) 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. For more information go to **Zscaler's website**, or follow Zscaler on Twitter @zscaler.

Microsoft Overview

Microsoft (Nasdaq: **MSFT**), Microsoft develops and licenses consumer and enterprise software. It is known for its Windows operating systems and Office productivity suite. The company is organized into three equally sized broad segments: productivity and business processes (legacy Microsoft Office, cloud-based Office 365, Exchange, SharePoint, Skype, LinkedIn, Dynamics), intelligence cloud (infrastructure- and platform-as-a-service offerings Azure, Windows Server OS, SQL Server), and more personal computing (Windows Client, Xbox, Bing search, display advertising, and Surface laptops, tablets, and desktops). To learn more, refer to **Microsoft's 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 the Zscaler Resources and Microsoft Entra ID Identity Resources.

Software Versions

This document was authored using Zscaler Internet Access (ZIA) v6.0 and Microsoft Entra ID Production Release December 2020.

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 Microsoft Introduction

Overviews of the Zscaler and Microsoft applications are described in this section.

⚠ 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, please contact your Zscaler Account Representative.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—just 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 our 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, and Browser 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 a 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, software called 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	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA
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.

Name	Definition
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	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
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.

Microsoft Entra ID Identity Overview

Microsoft Entra ID, part of Microsoft.com (NASDAQ: MSFT) is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers. Microsoft Entra ID is Microsoft's cloud-based identity and access management service. Microsoft Entra ID is an integral part of the Azure solution that provides:

- Authentication
- Conditional access
- Device Management
- Domain Services
- Identity Governance
- Identity Protection
- Privileged Identity Management

For more information go to Azure's website.

Microsoft Entra ID Identity Resources

The following table contains links to Microsoft Entra ID support resources.

Name	Definition
Microsoft Entra ID Help Center	Help articles on Microsoft Entra ID.
Microsoft Entra ID How to Configure SAML for Zscaler	Help article on configuring SAML for Microsoft Entra ID and Zscaler.
Microsoft Entra ID IWA	Quick Start guide for Microsoft Entra ID Seamless Single Sign-On.
Enable IWA on Browsers	Configure user browsers for Integrated Windows Authentication (IWA).

Microsoft Entra ID for Authentication and Provisioning

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

Authentication is the process of verifying a user's identity through credentials and other optional identity factors. Security Assertion Markup Language (SAML) is the preferred authentication method for both ZIA and Zscaler Private Access (ZPA). The procedures in this document describe how Microsoft Entra ID uses SAML identity provider (IdP).

SAML is an open protocol standard that Microsoft Entra ID uses to authenticate users and pass the authorization credentials to Zscaler Services. Although beyond the scope of this document, SAML also provides single sign-on (SSO) to any SAML service provider (SP). SSO enhances the user experience by providing a cohesive solution to modern cloud and SaaS environments. SAML and SSO are the catalyst to make a unified solution possible.

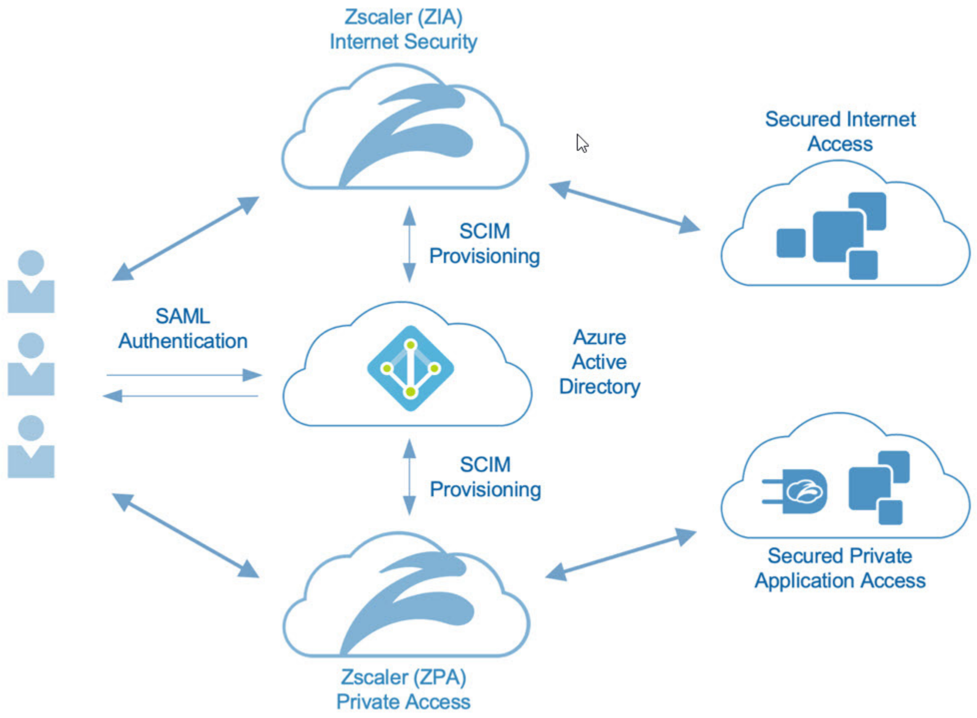


Figure 1. Zscaler Internet Access, Zscaler Private Access in an Microsoft Entra ID authentication environment

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 user, associated groups, and credentials are removed to prevent access to resources. The primary use case for authentication provisioning is onboarding and offboarding users from an organization. When a user leaves an organization, the user is deprovisioned from the user directory and SCIM makes the associated changes in the Zscaler databases by eliminating all ZIA and ZPA access. SCIM then deprovisions the user from all associated databases, preventing further access to company resources.

This guide covers seven Zscaler services or components in this document to build a complete Zscaler authentication infrastructure. Not all services need to be configured. A complete greenfield installation is typically configured in the manner this document flows.

- ZIA SAML Authentication
- ZIA SCIM Provisioning or SAML Auto-Provisioning
- ZIA Configuration for ZPA Entitlement
- ZPA SAML Configuration
- ZPA SCIM Provisioning or SAML Auto-Provisioning

Optionally, you can also set up:

- ZIA SAML Authentication for ZIA Administrators
- ZPA SAML Authentication for ZPA Administrators

A ZIA and ZPA best practice is to install SAML authentication, with SCIM provisioning of users and groups. You might need to configure SAML provisioning instead of, or alongside of, SCIM provisioning. There are caveats when both provisioning methods are used together, which are not covered in this document. Both methods can work together, if needed.

Using SCIM provisioning requires scoping only the users and groups that use Zscaler or policies. Procedures for precisely controlling and selecting the appropriate users and groups are provided in the **ZIA SCIM Provisioning** section. The procedures apply to (and required for) both ZIA and ZPA SCIM installations.

The procedure for Microsoft Entra ID Role to Microsoft Entra ID Security Group creation and mapping is included, even though the procedure is not a best practice. The procedure was a ZPA requirement until the December 2020 release of SCIM.

For administrators of Zscaler, this guide includes SAML provisioning procedures for accessing the Zscaler portal for Administrators Accounts by Zscaler admins. It is an optional feature and is placed after the information about the service configurations.

The document also covers an overview of Integrated Windows Authentication, which Zscaler leverages to automate the Zscaler authentication process. When configuring Zscaler in an Microsoft Entra ID hybrid installation using IWA, Zscaler provides a transparent user authentication experience and should be evaluated in every installation.

Required authentication bypasses are also provided, and basic troubleshooting steps if you run into issues.

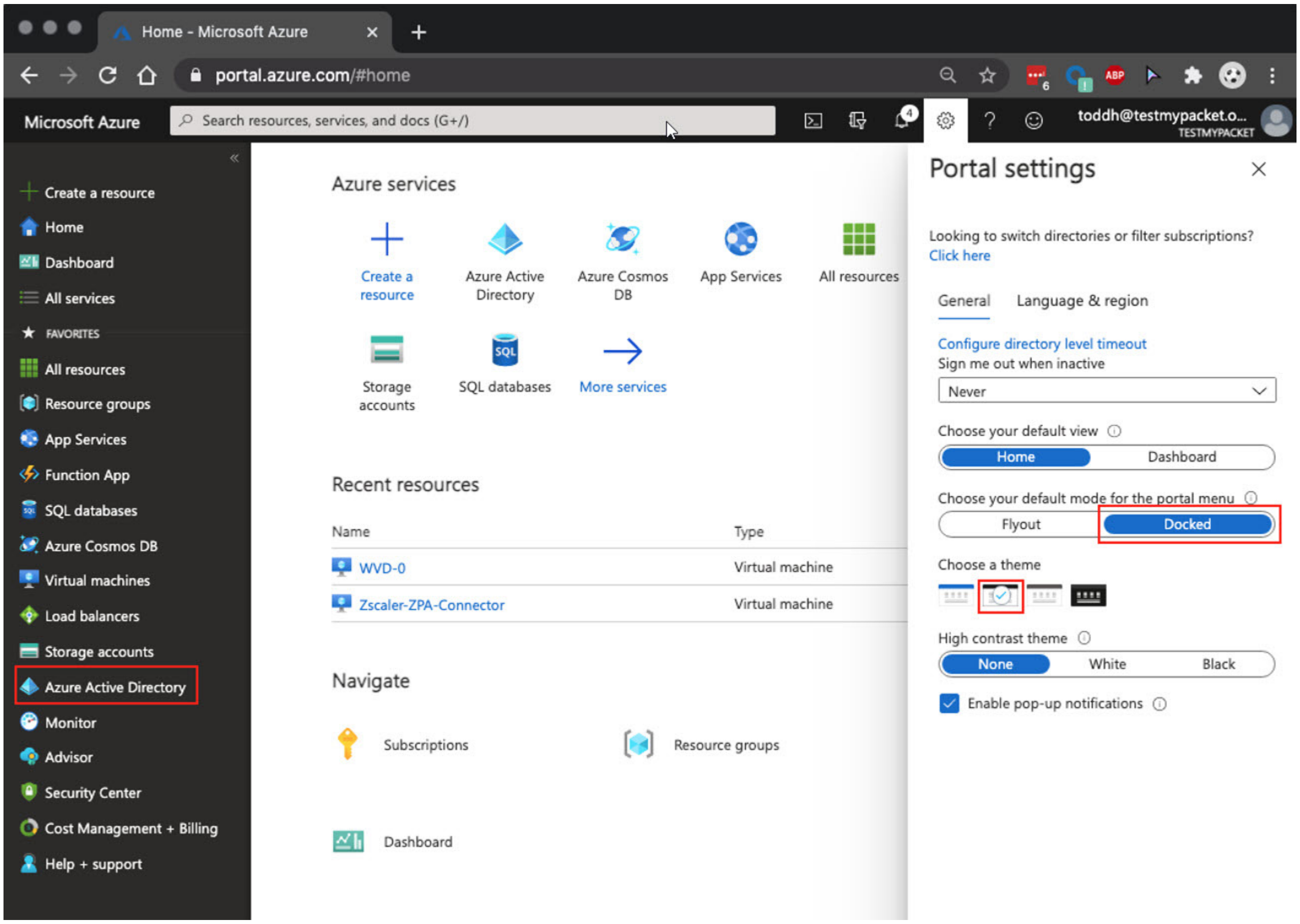
For more information, see the resources in **Zscaler Resources**.

ZIA Authentication

The following sections cover configuring ZIA Authentication to Azure ID.

The Azure Portal Settings

This document assumes that the user has a working Microsoft Entra ID environment, and covers only the installation and configuration of Zscaler applications. However, as a reference, you can view a no cost Microsoft Entra ID developer instance that was created from the [Microsoft Entra ID website]() and used to create this document.



Portal settings

Looking to switch directories or filter subscriptions? Click here

Configure directory level timeout

Sign me out when inactive: Never

Choose your default view: Home

Choose your default mode for the portal menu: Docked

High contrast theme: None

☑ Enable pop-up notifications

Figure 2. Azure Portal settings

Each step was validated for functionality in a live environment. The portal settings shown in the preceding image make Microsoft Entra ID available from a sidebar.

Add the Azure Zscaler Internet Access AAD Application

To add support for the Zscaler services, you must add the Microsoft Entra ID Enterprise application to your individual Zscaler service. The ZIA cloud that was used to create this document was named Zscaler Three. Zscaler added the Zscaler Three ZIA application to AAD to start the IdP installation.

From the Azure Portal:

1. Select **Microsoft Entra ID**.
2. Select **Enterprise applications**.
3. Select **New application**.

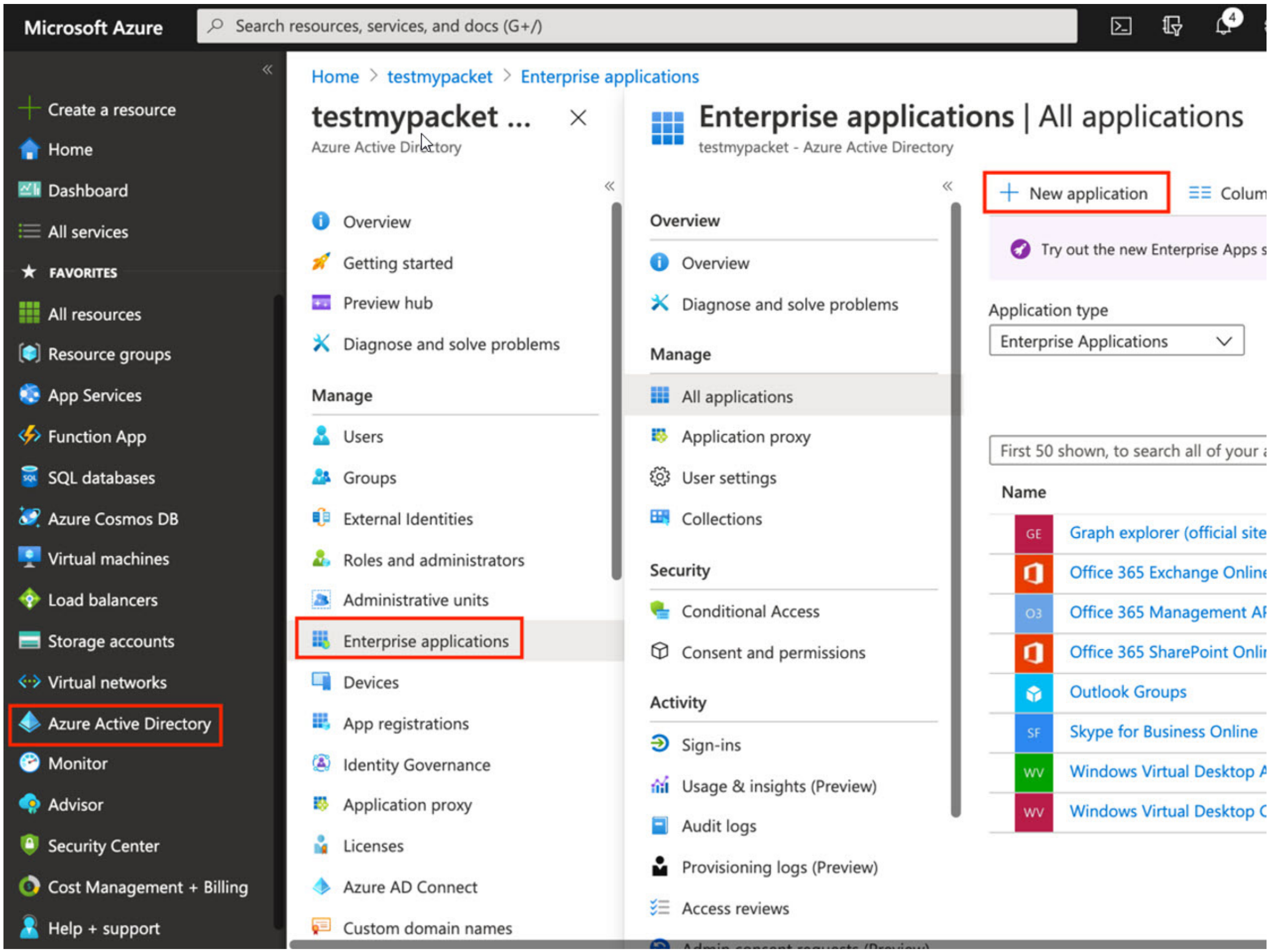


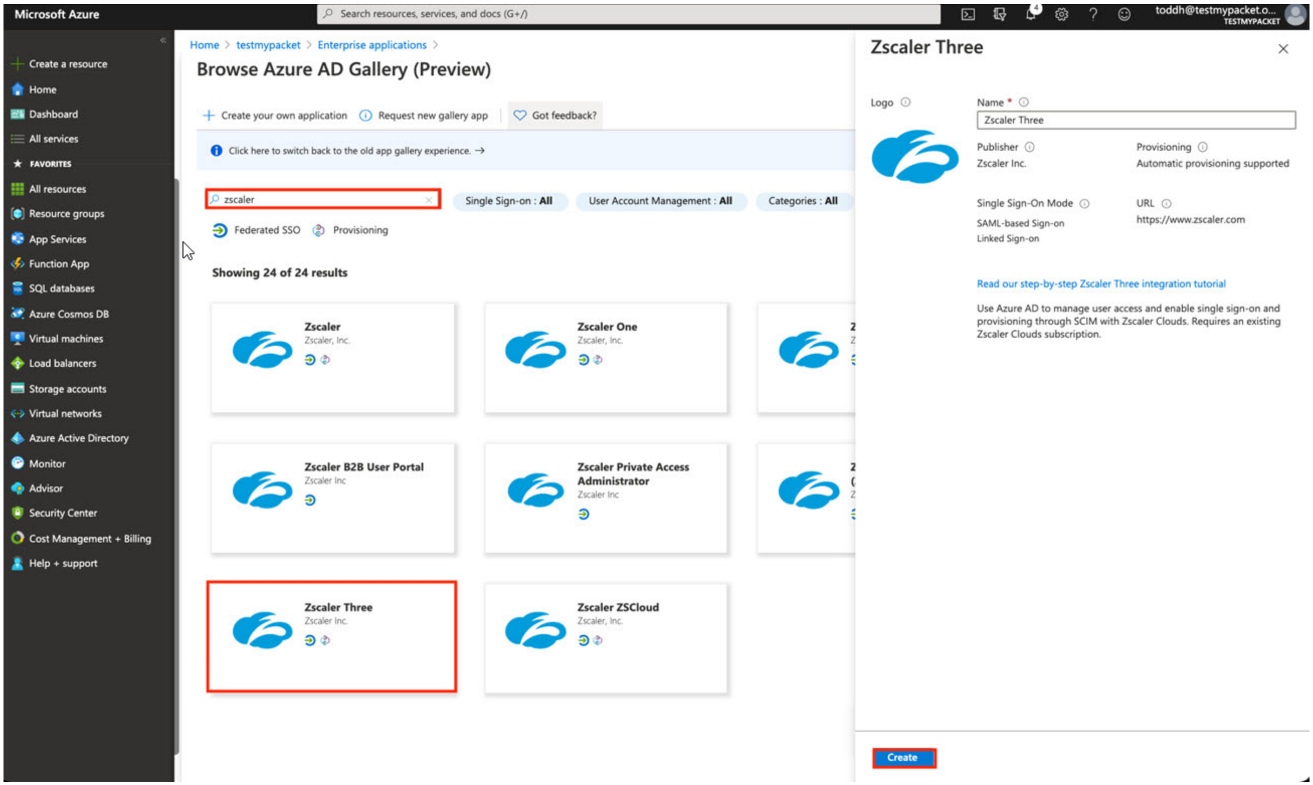
Figure 3. Adding a New AAD enterprise application

Each ZIA cloud embeds specific cloud variables into a configuration by using its own AAD application, which simplifies the configuration. This document adds the Zscaler Three application, but you must match to the appropriate Zscaler ZIA cloud that your organization's tenant is associated with.

The Zscaler cloud continues to expand but currently is one of the following cloud domains: zscaler.net, zscalerone.net, zscalertwo.net, zscalerthree.net, or zscloud.net. Information about the cloud domain you are using for your application can be found in your ZIA Admin Portal under **Administration** > **Company Profile** > **Company ID**. In the following Company ID example (zscloud.net-3173833), "zscloud.net" is your Zscaler Cloud.

To add the application:

1. In AAD, search for **Zscaler**. All Zscaler services appear.
2. Select the **Appropriate Cloud Application**.
3. Click **Create**.



Zscaler Three

Logo

Name * Zscaler Three

Publisher: Zscaler Inc.

Provisioning: Automatic provisioning supported

Single Sign-On Mode: SAML-based Sign-on, Linked Sign-on

URL: https://www.zscaler.com

Read our step-by-step Zscaler Three integration tutorial

Use Azure AD to manage user access and enable single sign-on and provisioning through SCIM with Zscaler Clouds. Requires an existing Zscaler Clouds subscription.

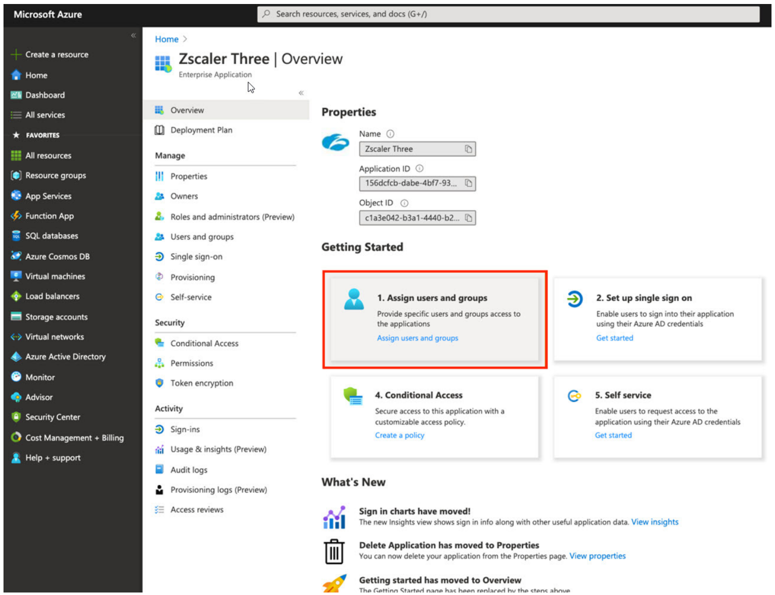
Figure 4. Add the Zscaler ZIA Application

Assign Users to the ZIA Application

First, assign the users and groups that encompass the ZIA Users that use Microsoft Entra ID for authentication. If any user is not assigned to the app, you receive error from Microsoft Entra ID during the login process stating that.

To assign users and groups, do one of the following:

1. Select the **Assign users and groups** tile.
2. Select **Users and groups** from the **Manage** section under the application.



Name: Zscaler Three

Application ID: 156dcfcb-dabe-4bf7-93...

Object ID: c1a3e042-b3a1-4440-b2...

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

Sign in charts have moved!
The new Insights view shows sign in info along with other useful application data. View insights

Delete Application has moved to Properties
You can now delete your application from the Properties page. View properties

Getting started has moved to Overview
The Getting Started page has been replaced by the steps above

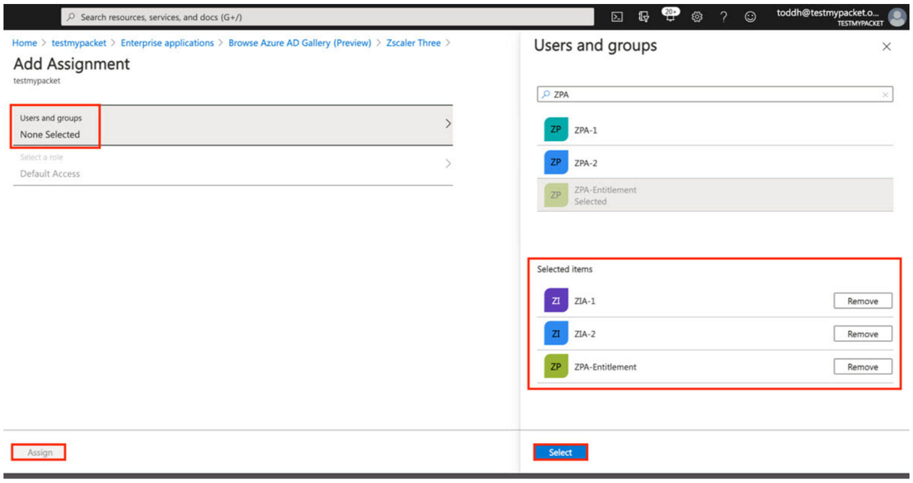
Figure 5. Assign users to the application

Assign Users to the Azure ZIA IdP

In this example, you see two ZIA security groups (ZIA-1 and ZIA-2) for policies, and a ZPA-Entitlement group that enables ZPA for set of ZPA users referred to later in this document.

To add the groups:

1. Select the **Users and groups** under the **Add Assignment** section.
2. Search and select the desired users and groups.
3. Click **Select**.
4. Click **Assign**.



Users and groups
None Selected

Select a role
Default Access

ZPA

Selected items
ZIA-1
ZIA-2
ZPA-Entitlement

Search resources, services, and docs (G+/)
20+
toddh@testmypacket.o...
TESTMYPACKET
Home > testmypacket > Enterprise applications > Browse Azure AD Gallery (Preview) > Zscaler Three >
Add Assignment
testmypacket
Users and groups
ZP ZPA-1
ZP ZPA-2
ZP ZPA-Entitlement Selected
ZI
ZI
ZP
Remove
Remove
Remove
Assign
Select

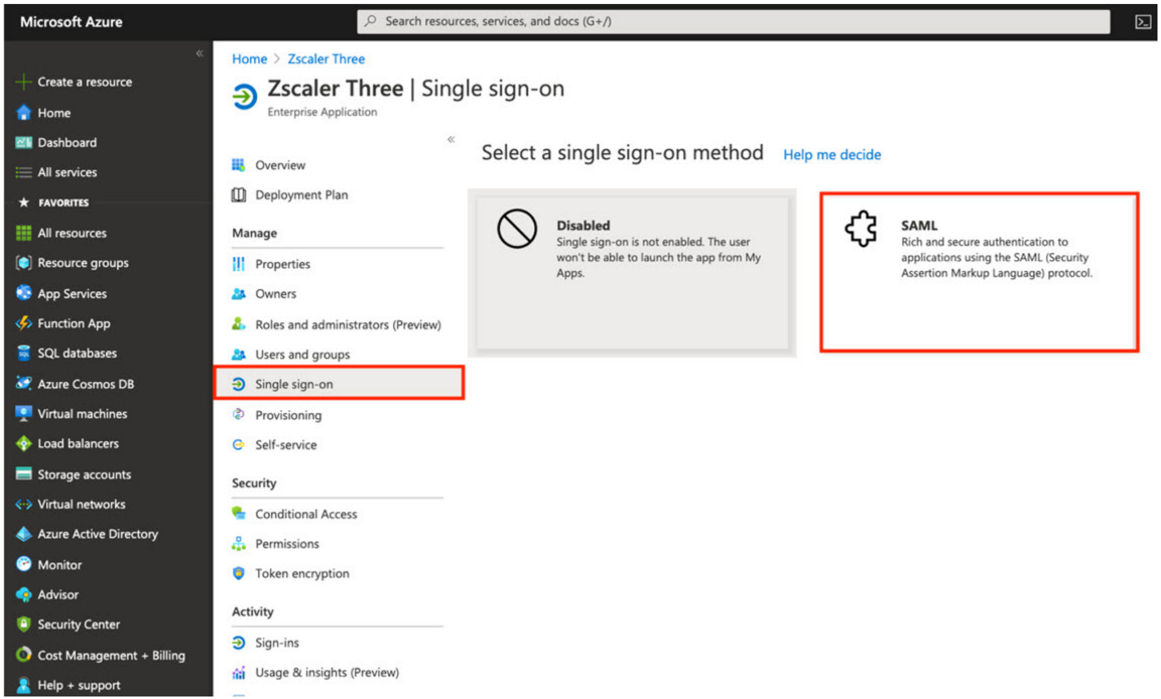
Figure 6. Assign Users and Groups to the Zscaler application

Configure SAML for the Azure IdP

To configure the authentication method used for the client and the exchange between Azure and Zscaler, you need to configure SAML. Parameters and certificates are exchanged between the two different portals. It is easier to move information between the Azure and ZIA portals if you open a second browser or tab so that you can see both portals at the same time.

To start the configuration process in Azure:

1. Click **Single sign-on**.
2. Select **SAML**, on the right side of the window.



Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

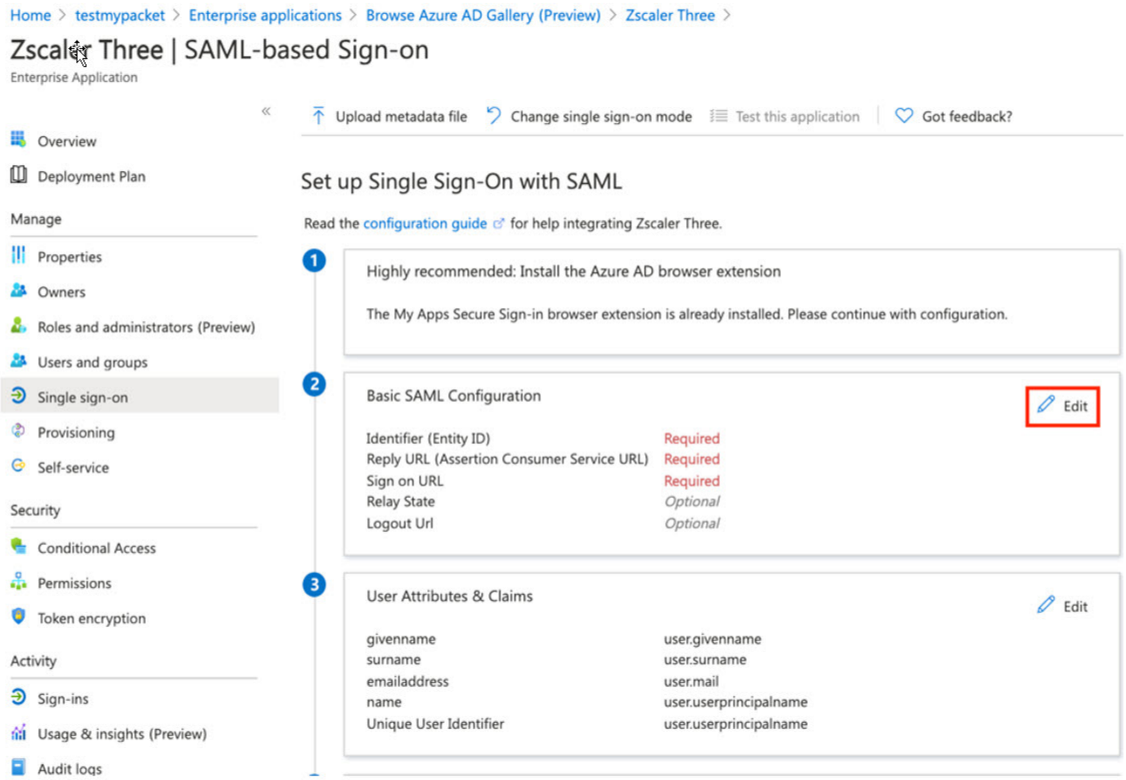
Figure 7. Configuring SAML for Single Sign-On

Configure the Basic SAML Settings for the Azure IdP

The configuration page, Step 1, facilitates installing **My Apps Secure Sign-in browser extension**. If you select to install the app, some of the processes are automatically configured.

This document walks through the manual configuration steps, which don't take that much longer and show the configuration details.

To configure the SAML parameters, click **Edit** under the **Basic SAML Configuration**.



Set up Single Sign-On with SAML

Read the configuration guide for help integrating Zscaler Three.

1 Highly recommended: Install the Azure AD browser extension

The My Apps Secure Sign-in browser extension is already installed. Please continue with configuration.

2 Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Required
Relay State	Optional
Logout Url	Optional

3 User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

Figure 8. Configuring the SAML parameters

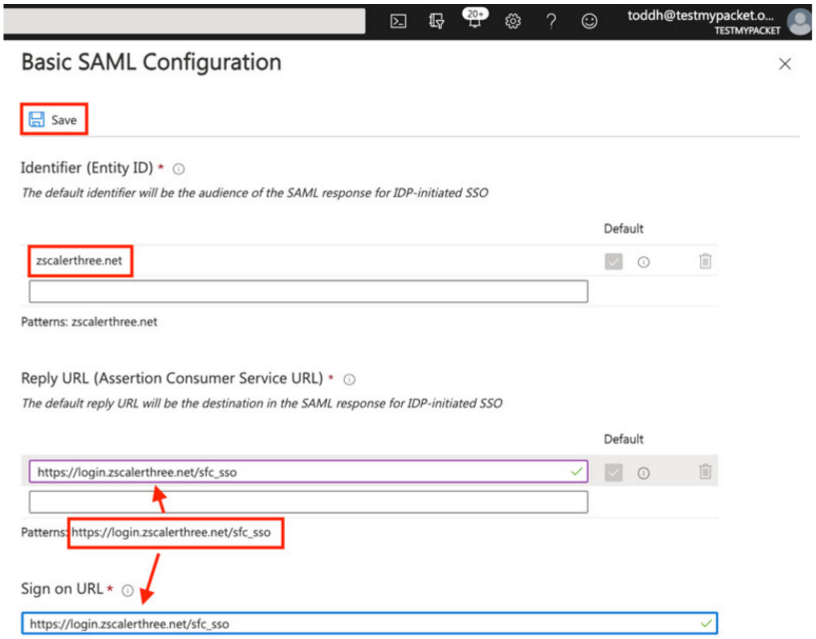
The **Basic SAML configuration** page enables you to enter the **Entity ID**, the **Reply URL**, and the **Sign on URL**. These values should already be populated with the name of the application that was selected at the beginning of this process. However, you can change the values if they are not correct.

The **Entity ID** is the ZIA cloud for your organization's tenant. It should be one of the following cloud domains: zscaler.net, zscalerone.net, zscalertwo.net, zscalerthree.net, or zscloud.net. Your company's domain information can be found in your ZIA Admin Portal under **Administration** > **Company Profile** > **Company ID**. In the following Company ID example (zscalerthree.net-3173833), "zscalerthree.net" is the Zscaler Cloud that would be entered as the Entity ID for the Microsoft Entra ID setup.

⚠ Replace zscalerthree.net with your ZIA cloud.

Configure the Basic SAML parameters:

1. Enter zscalerthree.net as the **Entity ID**.
2. Enter `https://login.zscalerthree.net/sfc_sso` for both the **Reply URL** and **Sign on URL**.
3. Make sure the checkmarks are selected on the new entries.
4. Click **Save**.



Basic SAML Configuration

Save

Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

zscalerthree.net

Patterns: zscalerthree.net

Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

https://login.zscalerthree.net/sfc_sso

Patterns: https://login.zscalerthree.net/sfc_sso

Sign on URL *

https://login.zscalerthree.net/sfc_sso

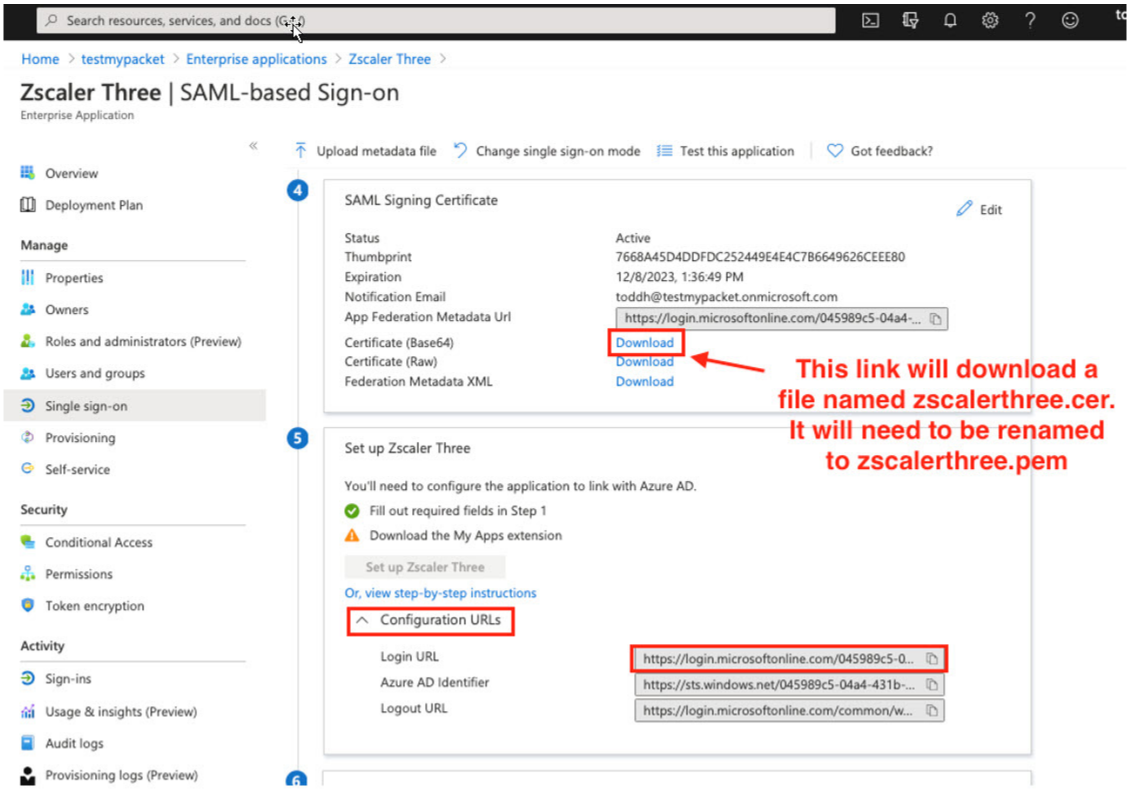
Figure 9. Configure the SAML URLs

After you save the basic SAML parameters, the **SAML Signing Certificate** and the **Configuration URLs** are created and displayed.

Download the Certificate and Prepare to Configure Access

Complete the following steps:

1. Download the SAML signing certificate.
2. Copy the Microsoft Entra ID **Login URL** for the Zscaler configuration.
3. Rename the certificate from a .cer file to a .pem file.
4. Open a browser and log into the ZIA Admin Portal.



Zscaler Three | SAML-based Sign-on

Enterprise Application

SAML Signing Certificate

Status: Active
Thumbprint: 7668A45D4DDFDC252449E4E4C7B6649626CEEE80
Expiration: 12/8/2023, 1:36:49 PM
Notification Email: toddh@testmypacket.onmicrosoft.com
App Federation Metadata Url: https://login.microsoftonline.com/045989c5-04a4-...
Certificate (Base64): Download
Certificate (Raw): Download
Federation Metadata XML: Download

This link will download a file named zscalerthree.cer. It will need to be renamed to zscalerthree.pem

Set up Zscaler Three

You'll need to configure the application to link with Azure AD.

✓ Fill out required fields in Step 1
⚠ Download the My Apps extension

Or, view step-by-step instructions

Configuration URLs

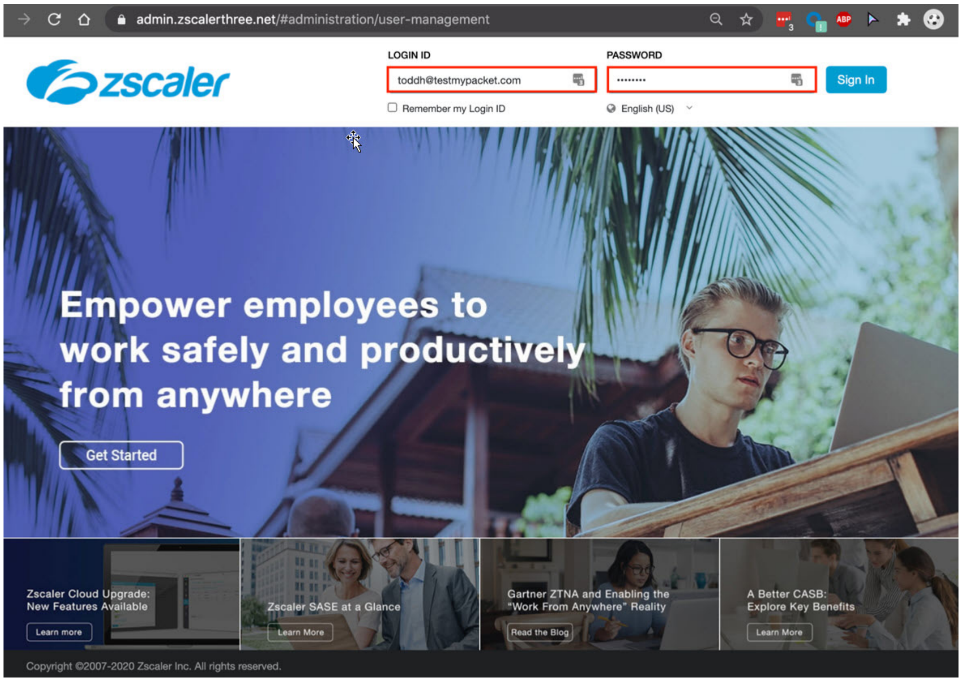
Login URL: https://login.microsoftonline.com/045989c5-0...
Azure AD Identifier: https://sts.windows.net/045989c5-04a4-431b-...
Logout URL: https://login.microsoftonline.com/common/w...

Figure 10. Certificate and URL for the ZIA configuration

In this example, the URL to open the ZIA Admin Portal is https://admin.zscalerthree.net. Login with your admin credentials. The certificate file "zscalerthree.cer" was renamed to "zscalerthree.pem".

Configuring the Azure IdP on ZIA

Log into the ZIA Admin Portal using your admin credentials to start the Azure IdP configuration.



admin.zscalerthree.net/#administration/user-management

LOGIN ID: toddh@testmypacket.com

PASSWORD: ••••••••

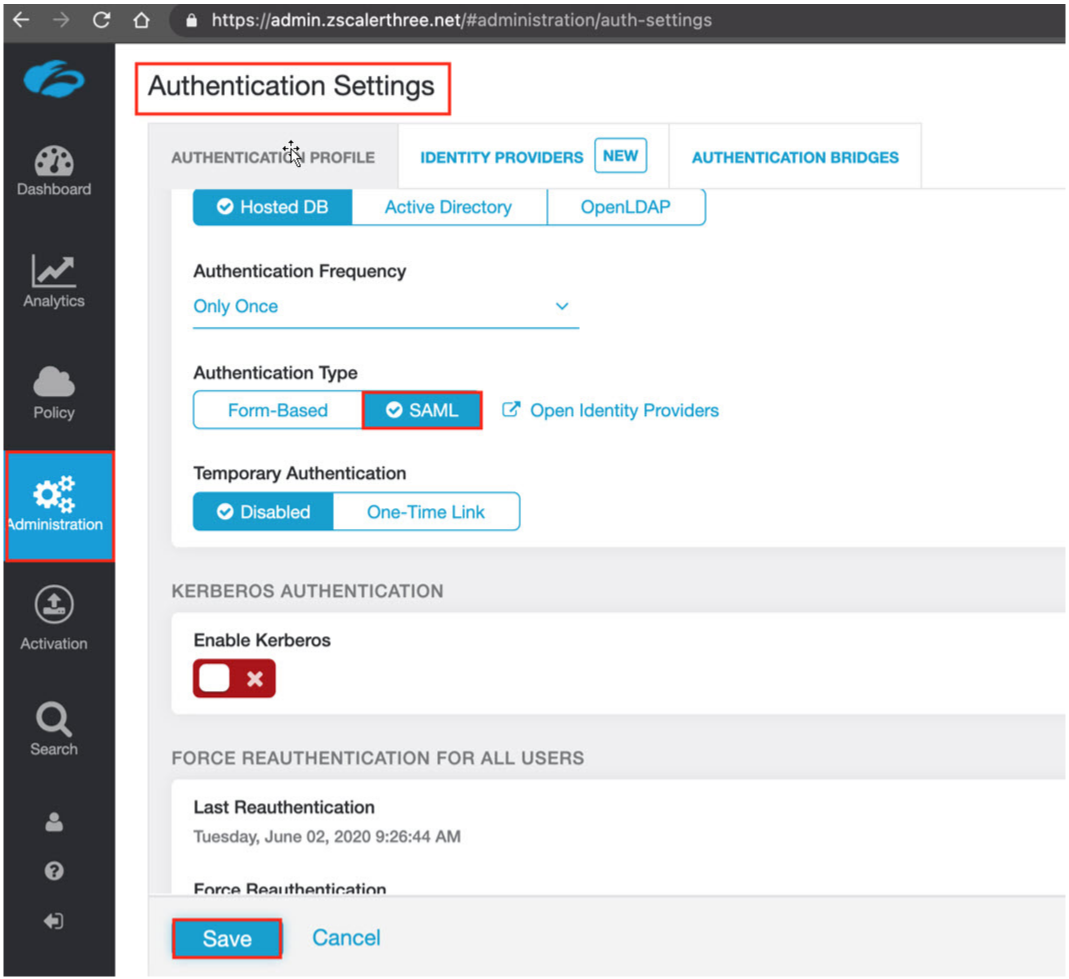
zscaler
Sign In
Remember my Login ID
English (US)
Empower employees to work safely and productively from anywhere
Get Started
Zscaler Cloud Upgrade: New Features Available
Learn more
Zscaler SASE at a Glance
Learn More
Gartner ZTNA and Enabling the "Work From Anywhere" Reality
Read the Blog
A Better CASB: Explore Key Benefits
Learn More
Copyright ©2007-2020 Zscaler Inc. All rights reserved.

Figure 11. ZIA Admin Portal

Enable SAML Authentication on ZIA

To enable SAML Authentication in the ZIA Admin Portal:

1. Go to **Administration** > **Authentication Settings**.
2. Select **SAML**.
3. Click **Save**.



Authentication Frequency: Only Once

Authentication Type: Form-Based / ✓ SAML

Temporary Authentication: ✓ Disabled / One-Time Link

Enable Kerberos: ✗

Last Reauthentication: Tuesday, June 02, 2020 9:26:44 AM

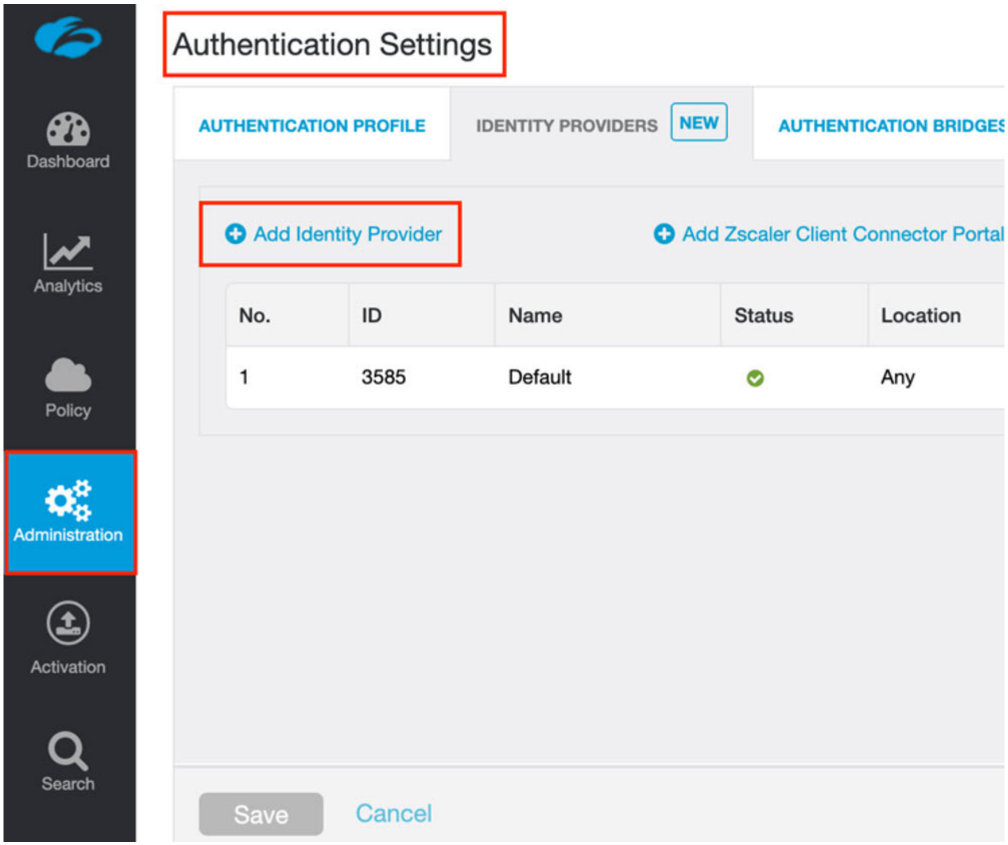
Figure 12. Enable SAML

Adding the Azure IdP on ZIA

To enable Microsoft Entra ID Authentication, you must add Azure as a new IdP for ZIA.

In the ZIA Admin Portal:

1. Select the **Identity Providers** tab.
2. Select **Add Identity Provider**.



No.	ID	Name	Status	Location
1	3585	Default	✓	Any

Figure 13. Adding an Identity Provider

This launches the **Edit Identity Provider** wizard.

Detailed Settings for the Azure IdP on ZIA

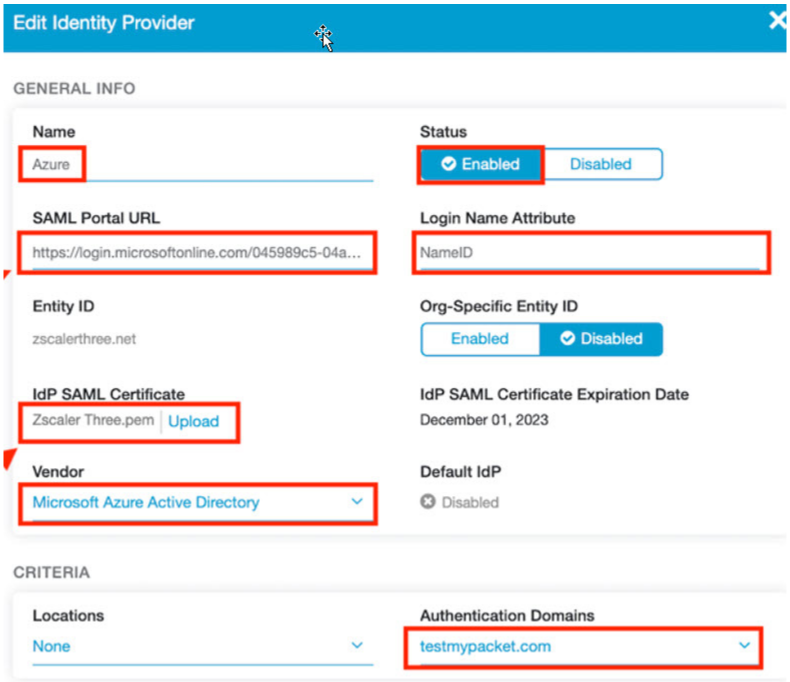
In the **Identity Provider** wizard:

1. Provide a name for the IdP.
2. Select **Enabled**.
3. Paste the Login URL copied for Azure into the **SAML Portal URL** field.
4. Verify that the **Login Name Attribute** is set to `NameID`.
5. Upload the zscalerthree.pem certificate file downloaded from the Azure Portal.
6. Select **Microsoft Microsoft Entra ID** as the **Vendor**.
7. Choose to either specify an IdP or select a specific authentication domain:
   - **Specify an IdP:**
     1. Set **Default IdP** to **Enabled**.
     2. Select **Authentication Domains** > **Any**.

- **Select a specific authentication domain:**
  1. Leave **Default IdP** as **disabled**.
  2. Select the authentication domain that authenticates to Azure.
  3. Select the saml_2022 Request Signing SAML Certificate.

8. Click **Save**.
9. **Activate** your changes.

Next you must configure provisioning to sync users and groups from the Azure IdP to Zscaler. Proceed to the next section to configure auto-provisioning or SCIM provisioning.


Edit Identity Provider

GENERAL INFO

Name: Azure

Status: ● Enabled | Disabled

SAML Portal URL: https://login.microsoftonline.com/045989c5-04a...

Login Name Attribute: NameID

Entity ID: zscalerthree.net

Org-Specific Entity ID: Enabled | ● Disabled

IdP SAML Certificate: Zscaler Three.pem | Upload

IdP SAML Certificate Expiration Date: December 01, 2023

Vendor: Microsoft Azure Active Directory

Default IdP: Disabled

CRITERIA

Locations: None

Authentication Domains: testmypacket.com

Figure 14. Creating the Azure IdP in the Identity Provider wizard

ZIA Provisioning

Provisioning is the way that the Zscaler user database gets populated with the users and groups configured in Microsoft Entra ID. You can provision by using either of two methods: SCIM or SAML auto-provisioning.

SCIM provisioning is an open standard that allows for the automation of user provisioning. User data is more secure and the user experience is simplified when you automate the user identity lifecycle management process. All requests to add and delete users and groups happen in Microsoft Entra ID, and then Azure syncs those changes to Zscaler. Microsoft Entra ID currently updates changes automatically, every 40 minutes.

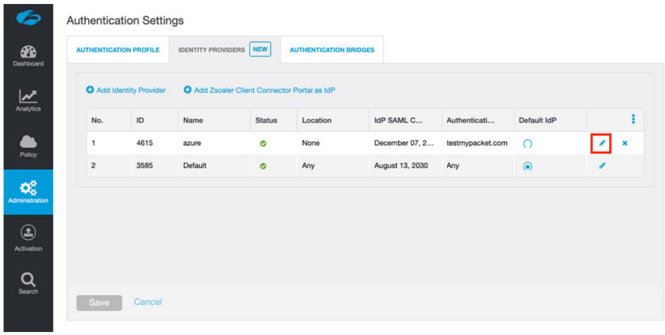
SAML auto-provisioning populates the Zscaler user database with users, groups, and departments when the SAML response is successful. The Zscaler user database is populated with the data from the users SAML Assertion.

Removing users and groups from Zscaler is a manual process. So even if a user is removed in Microsoft Entra ID, the user must be kept in the Zscaler user database. No passwords are kept in Zscaler for either SCIM or SAML auto-provisioning, so a user cannot authenticate if removed from Microsoft Entra ID.

ZIA SAML Self-Provisioning

To enable SAML auto-provisioning, go back into the Azure IdP configuration.

1. Select **Authentication** > **Identity Providers** tab.
2. Click the blue pencil to start the editor or advance to the SCIM section.



Authentication Settings

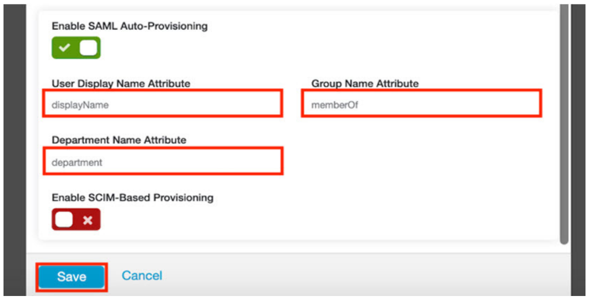
No.	ID	Name	Status	Location	IdP SAML C...	Authenticati...	Default IdP
1	4615	azure	✓	None	December 07, 2...	testmypacket.com	○
2	3585	Default	✓	Any	August 13, 2030	Any	●

Figure 15. Edit the IdP to enable Auto-Provisioning

ZIA SAML Auto-Provisioning

To enable SAML auto-provisioning complete the following steps. All fields are prepopulated with the default attribute and the value is case-sensitive.

1. Select **SAML Auto-Provisioning**.
2. Verify that the **User Display Name Attribute** is set to `displayName`.
3. Verify that the **Group Name Attribute** is set to `memberOf`.
4. Verify that the **Department Name Attribute** is set to `department`.
5. Click **Save**.
6. Activate your changes.



Enable SAML Auto-Provisioning: ☑

User Display Name Attribute: displayName

Group Name Attribute: memberOf

Department Name Attribute: department

Enable SCIM-Based Provisioning: ☒

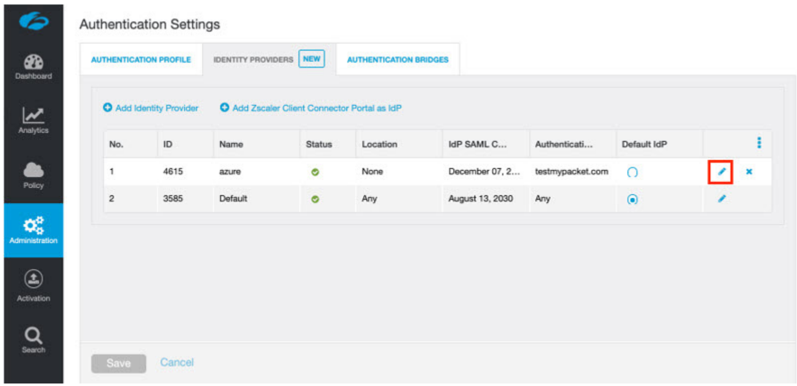
Figure 16. Enable SAML Auto-Provisioning

ZIA SCIM Provisioning

The System for Cross-Domain Identity Management (SCIM) specification is designed to make managing user identities in cloud-based applications and services easier and is used as best practice for user and group management between Zscaler and the Zscaler identity partners.

To enable SCIM:

1. Select **Authentication** > **Identity Providers** tab.
2. Click the blue pencil to start the editor.



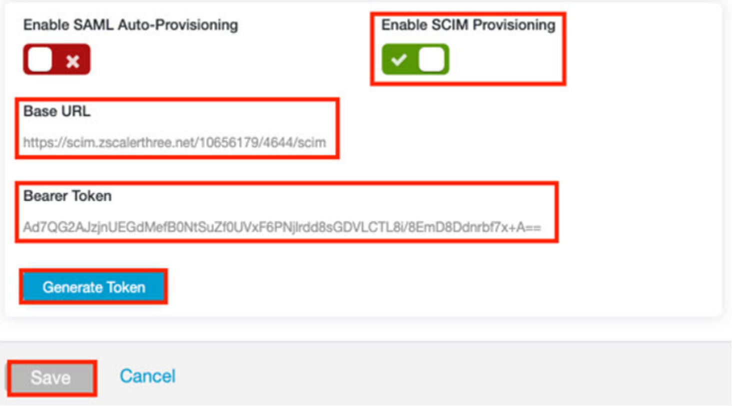
No.	ID	Name	Status	Location	IdP SAML C...	Authenticati...	Default IdP
1	4615	azure	✓	None	December 07, 2...	testmypacket.com	○
2	3585	Default	✓	Any	August 13, 2030	Any	●

Figure 17. Edit the IdP to enable SCIM

Configure SCIM Detail on the ZIA Admin Portal

To enable SCIM on the Azure IdP in the ZIA Admin Portal:

1. Toggle the **Enable SCIM Provisioning** switch from a red X to a green checkmark.
2. Click **Generate Token** to display the **Base URL** and **Bearer Token**.
3. Copy the **Base URL** and **Bearer Token** values for use later in the Azure configuration.
4. Click **Save**.
5. **Activate** your changes.



Enable SAML Auto-Provisioning ☒

Enable SCIM Provisioning ✓

Base URL
https://scim.zscalerthree.net/10656179/4644/scim

Bearer Token
Ad7QG2AJzjnUEGdMefB0NtSuZf0UVxF6PNjlrdd8sGDVLCTL8i/8EmD8Ddnrbf7x+A==

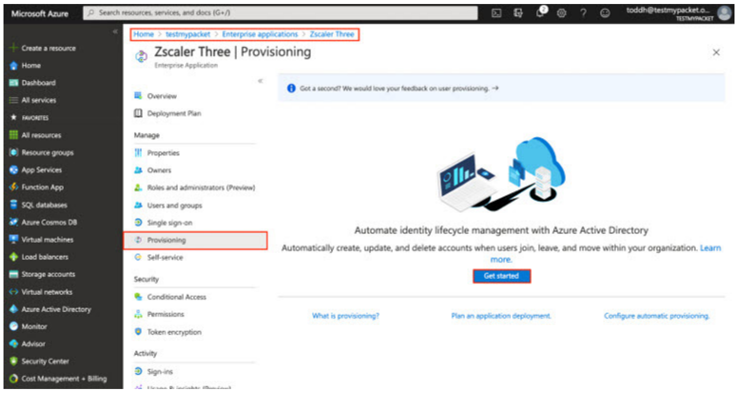
Figure 18. Edit the IdP to enable SCIM

Return to the Azure Portal to finish the SCIM configuration.

Configure SCIM on the Azure UI

To start the configuring process on Azure, select the ZIA IdP application:

1. Go to **Microsoft Entra ID** > **Enterprise Applications** > **Zscaler Three**.
2. Select **Provisioning**.
3. Click **Get Started**.



Home > testmypacket > Enterprise applications > Zscaler Three

Zscaler Three | Provisioning
Enterprise Application

Got a second? We would love your feedback on user provisioning. →

Automate identity lifecycle management with Azure Active Directory

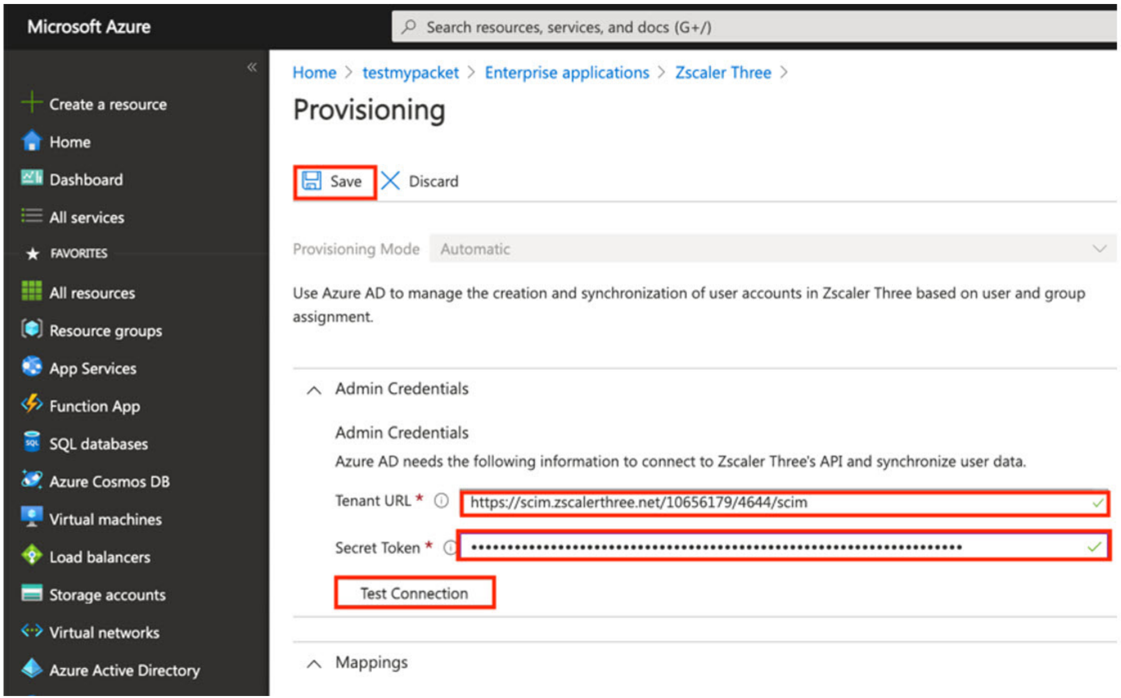
Automatically create, update, and delete accounts when users join, leave, and move within your organization. Learn more.

Figure 19. Select provisioning in the ZIA enterprise application

Configure Detailed SCIM Settings on the Azure UI

The SCIM Provisioning configuration builds out as you select the individual parameters:

1. Change the **Provisioning Mode** from **Manual** to **Automatic**.
2. Paste the **Base URL** value copied from the ZIA Admin Portal into the **Tenant URL**.
3. Paste the **Bearer Token** value into the **Secret Token**.
4. Click **Test Connection**.
5. Click **Save**.



Provisioning

Provisioning Mode: Automatic

Use Azure AD to manage the creation and synchronization of user accounts in Zscaler Three based on user and group assignment.

Admin Credentials

Azure AD needs the following information to connect to Zscaler Three's API and synchronize user data.

Tenant URL *: https://scim.zscalerthree.net/10656179/4644/scim

Secret Token *: ••

Figure 20. Configure SCIM on Azure

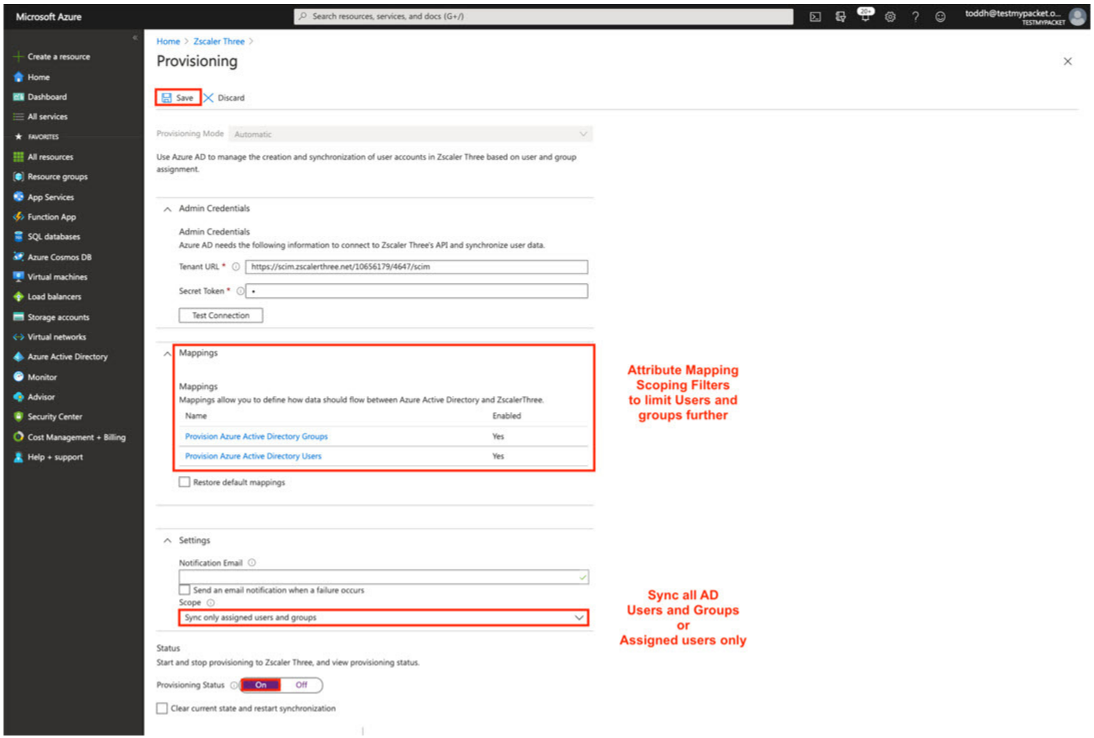
Azure tries to connect to Zscaler. The credentials must pass before you can save the Azure SCIM configuration. If the credentials pass, proceed to the next step.

If the credentials do not pass, make sure that you have saved and activated the SCIM configuration on the ZIA tenant.

Start Azure SCIM Sync and Set Basic Scoping

You can set detailed scoping filters for users and groups in the mapping section (shown in the following pages). To configure basic scoping and start the SCIM synchronization process:

1. Select **Settings.**
2. Select **Sync only assigned users and groups.**
3. Toggle the **Provisioning Status** to **On.**
4. **Save** the configuration.



Provisioning

Save Discard

Provisioning Mode: Automatic

Use Azure AD to manage the creation and synchronization of user accounts in Zscaler Three based on user and group assignment.

Admin Credentials

Admin Credentials

Azure AD needs the following information to connect to Zscaler Three's API and synchronize user data.

Tenant URL *: https://scim.zscalerthree.net/10656179/4647/scim

Secret Token *: •

Test Connection

Mappings

Mappings

Mappings allow you to define how data should flow between Azure Active Directory and ZscalerThree.

Name	Enabled
Provision Azure Active Directory Groups	Yes
Provision Azure Active Directory Users	Yes

□ Restore default mappings

Settings

Notification Email:

□ Send an email notification when a failure occurs

Scope: Sync only assigned users and groups

Status

Start and stop provisioning to Zscaler Three, and view provisioning status.

Provisioning Status: [✓ On] Off

□ Clear current state and restart synchronization

Attribute Mapping Scoping Filters to limit Users and groups further

Sync all AD Users and Groups or Assigned users only

Figure 21. Starting SCIM in Azure

> Limit the number of users and groups to the Users and Groups used for policies. Don't simply send everything. SCIM API calls are rate limited. APIs should only sync required users and groups to enhance the performance of your system.

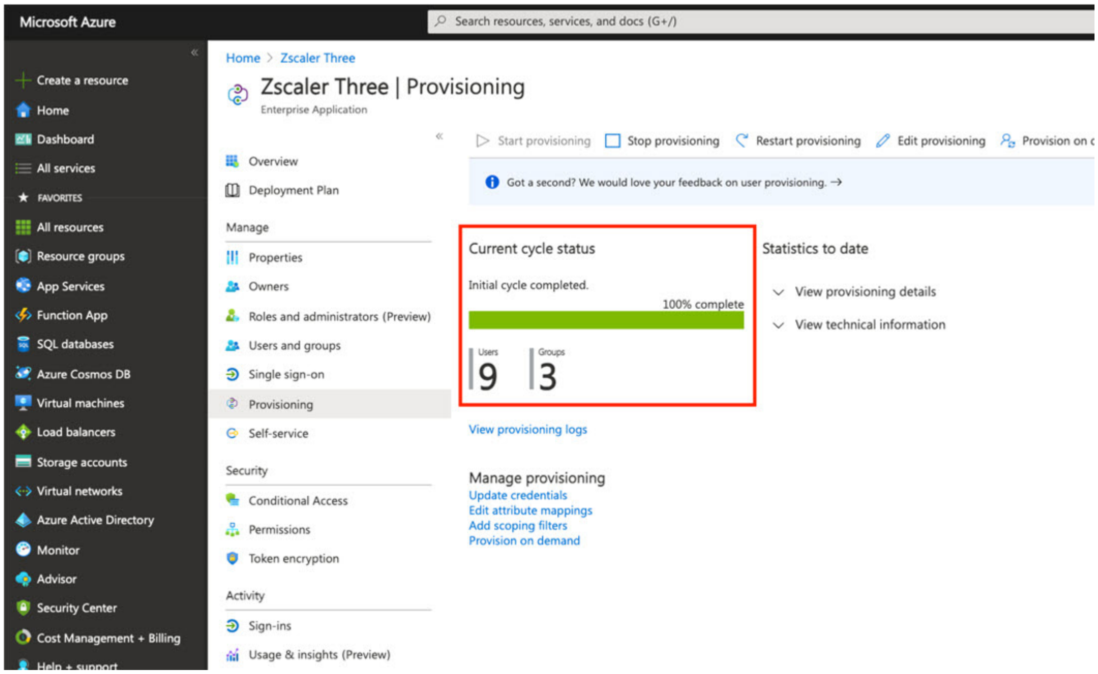
Verify SCIM on the Azure UI

The amount of time needed to complete an initial SCIM synchronization depends on the number of users and groups assigned to the ZIA application. If you sync thousands of users and groups, the delay in processing can slow next steps during installation or POV testing.

A best practice is to assign only the users and groups used in ZIA immediately, which is the ZPA Entitlement group (if ZPA is installed). Add the rest of the users after the initial sync. The SCIM interval for Azure is every 40 minutes, so changes can be delayed. If you need to sync an assigned user immediately, you can use the Provision on demand feature. This feature also tests SCIM and enables the POV or Installation to continue to move forward with ZIA or ZPA without delay.

To test and check the current SCIM Cycle Status on Azure, select the ZIA IdP application:

1. Go to Microso**ft Entra ID** > **Enterprise Applications** > **Zscaler Three**.
2. Select **Provisioning**.
3. Select **Provision on demand** to sync your test users.



Got a second? We would love your feedback on user provisioning. →

Current cycle status

Initial cycle completed.

100% complete

Users 9

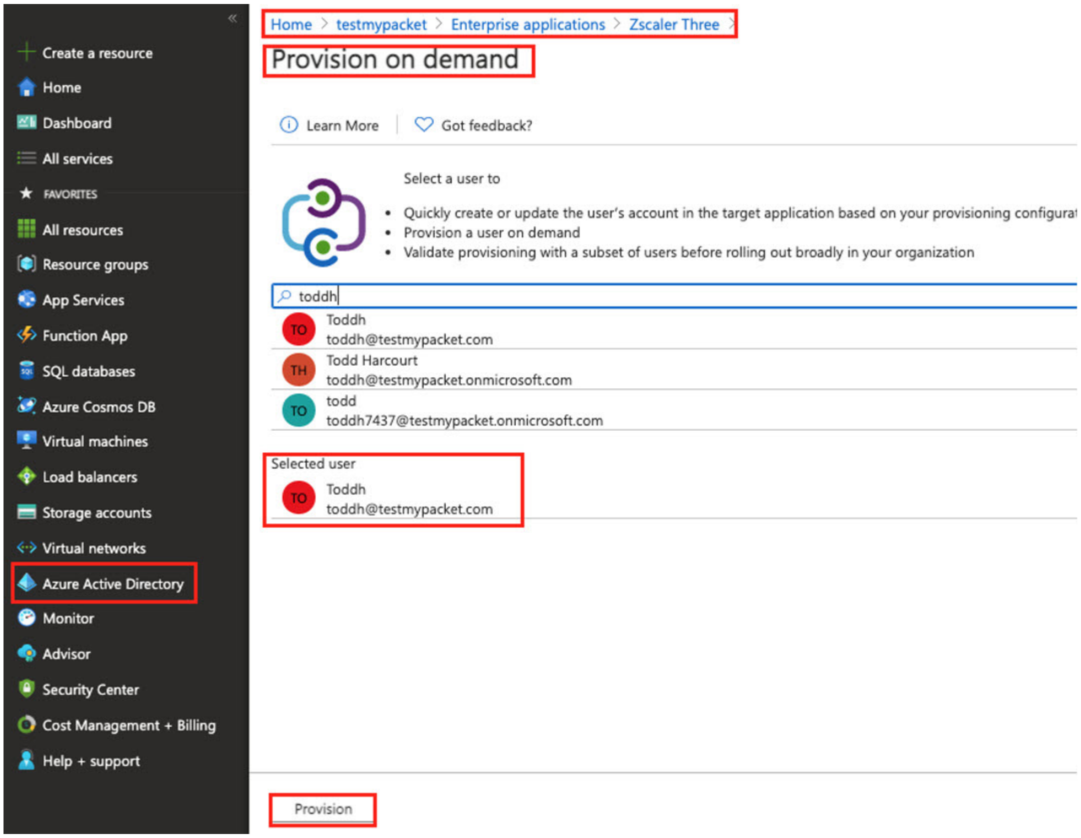
Groups 3

Figure 22. A successful SCIM sync

Provisioning on Demand

To sync a user immediately via SCIM, use the Provision on demand feature. This enables the POV or Installation to continue to move forward with ZIA or ZPA without delays and tests the SCIM functionality. To provision a user immediately using Provision on demand:

1. Go to **Microsoft Entra ID** > **Enterprise Applications** > **Zscaler Three** > **Provisioning** > **Provision on Demand**.
2. Search for and select users to be push into Zscaler via SCIM.
3. Click **Provision**.



Provision on demand

Select a user to

- Quickly create or update the user's account in the target application based on your provisioning configurat
- Provision a user on demand
- Validate provisioning with a subset of users before rolling out broadly in your organization

toddh

TO Toddh
toddh@testmypacket.com

TH Todd Harcourt
toddh@testmypacket.onmicrosoft.com

TO todd
toddh7437@testmypacket.onmicrosoft.com

Selected user

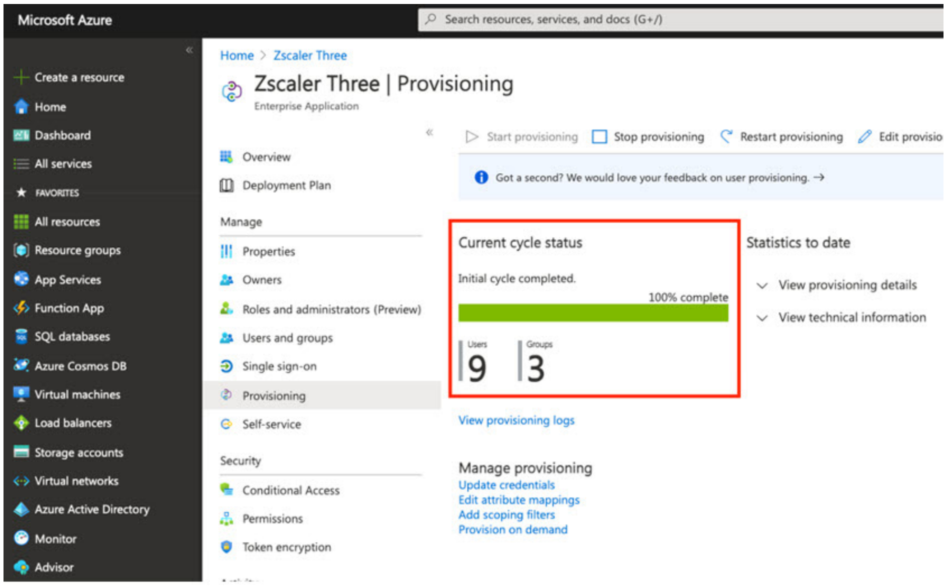
TO Toddh
toddh@testmypacket.com

Figure 23. Provisioning a User on Demand

SCIM User Scoping Filters

For more precise scoping, that selects only certain users or groups, create a scoping filter. Let's create a user scoping filter first:

1. Select **Add scoping filter** from the main provisioning page.



Got a second? We would love your feedback on user provisioning. →

Current cycle status

Initial cycle completed.

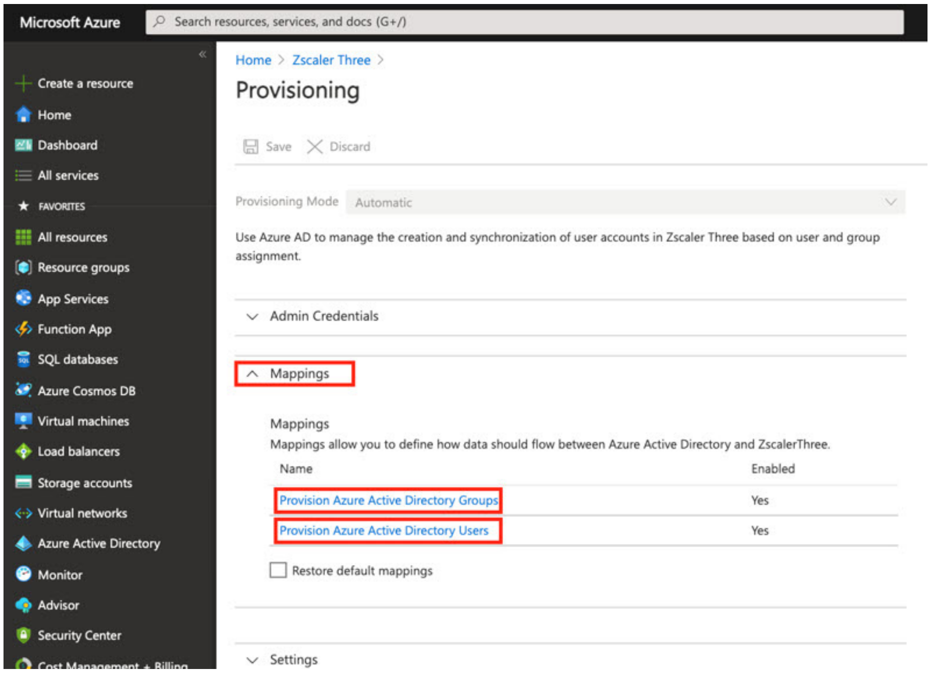
100% complete

Users 9

Groups 3

Figure 24. *Current cycle status for scoping filter*

2. Select **Mappings** to display the User and Group provisioning sections.
3. Select **Provision Microsoft Entra ID Users.**



Provisioning Mode: Automatic

Use Azure AD to manage the creation and synchronization of user accounts in Zscaler Three based on user and group assignment.

Mappings

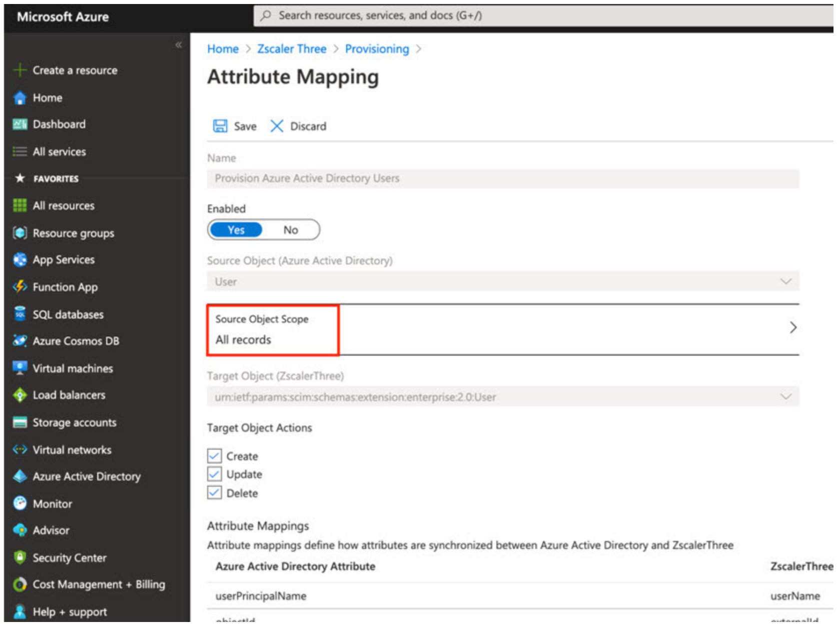
Mappings allow you to define how data should flow between Azure Active Directory and ZscalerThree.

Name	Enabled
Provision Azure Active Directory Groups	Yes
Provision Azure Active Directory Users	Yes

□ Restore default mappings

Figure 25. *Mapping*

4. Select **Source Object Scope**.



Attribute Mapping

Name
Provision Azure Active Directory Users

Enabled
Yes No

Source Object (Azure Active Directory)
User

Source Object Scope
All records

Target Object (ZscalerThree)
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

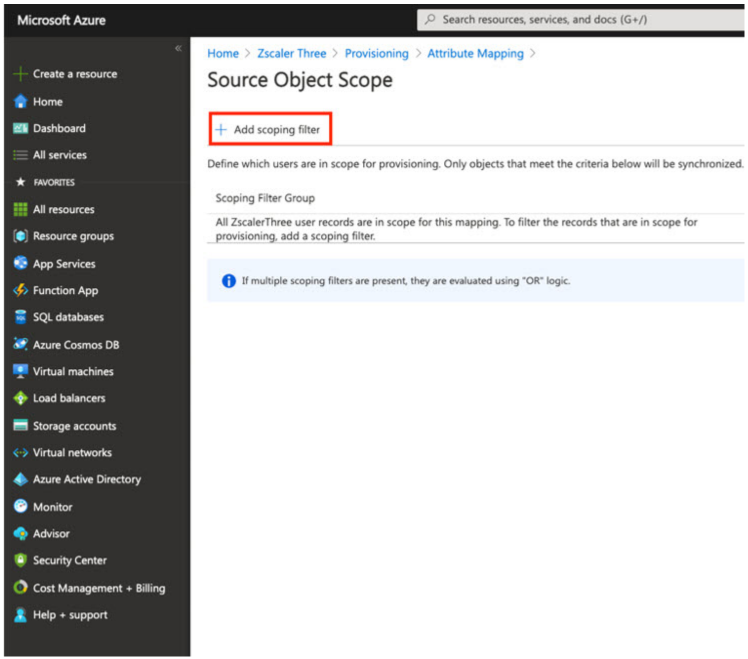
Target Object Actions
☑ Create
☑ Update
☑ Delete

Attribute Mappings
Attribute mappings define how attributes are synchronized between Azure Active Directory and ZscalerThree

Azure Active Directory Attribute	ZscalerThree
userPrincipalName	userName

Figure 26. Source scope

5. Select **Add scoping filter**.



Source Object Scope

Define which users are in scope for provisioning. Only objects that meet the criteria below will be synchronized.

Scoping Filter Group

All ZscalerThree user records are in scope for this mapping. To filter the records that are in scope for provisioning, add a scoping filter.

If multiple scoping filters are present, they are evaluated using "OR" logic.

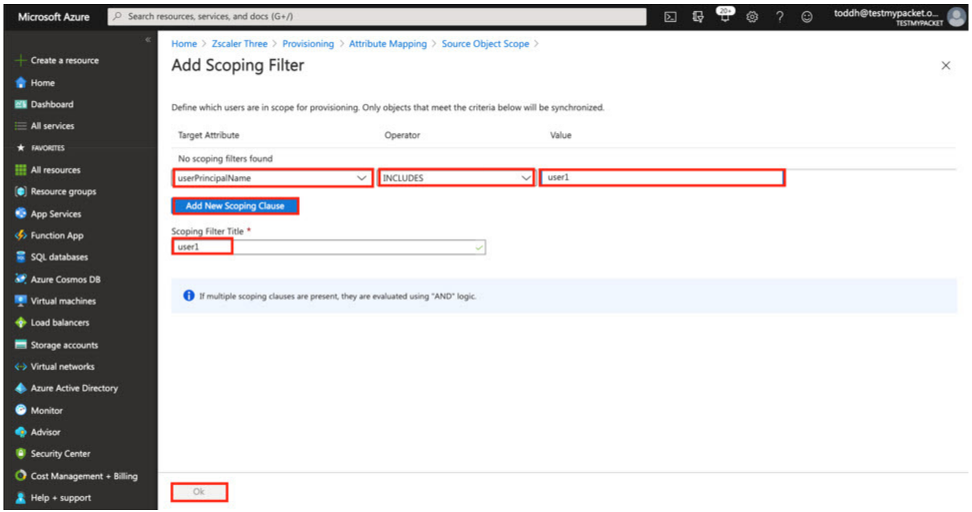
Figure 27. Add scoping filters

SCIM User Scoping Filters Detail

The following explains SCIM scoping filter setting details:

1. Verify that **Target Attribute** is set to `userPrincipalName`. The value is case-sensitive.
2. Select **INCLUDES** as the **Operator**.
3. Enter the portion of a user name that you want to allow to be synced by SCIM. In the preceding example, the **Value** is `user1`. Any user name that contains user1 is synchronized via SCIM.
4. **Name** the filter.
5. Click **Add New Scoping Clause**.
6. Click **OK**.
7. Click **OK** in the next window that appears.
8. Click **Save**.
9. Click **Yes**.

The **INCLUDES** operator can also be used with domains that are the **Target Attribute**.



Add Scoping Filter

Define which users are in scope for provisioning. Only objects that meet the criteria below will be synchronized.

Target Attribute	Operator	Value
No scoping filters found		
userPrincipalName	INCLUDES	user1

Scoping Filter Title *: user1

If multiple scoping clauses are present, they are evaluated using "AND" logic.

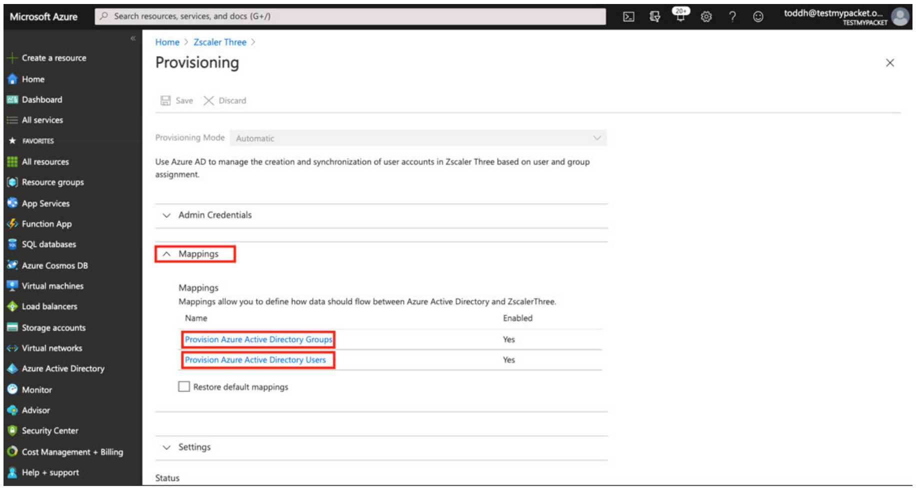
Figure 28. Add Scoping Filter Detail

In the preceding example, any Username that contains "user1" is synchronized via SCIM. The INCLUDES operator can also be used for domains.

SCIM Group Scoping Filters

Next, create a Group filter:

1. Select **Mappings** to display the User and Group provisioning sections.
2. Select **Provision Microsoft Entra ID Groups**.



Provisioning

Provisioning Mode: Automatic

Use Azure AD to manage the creation and synchronization of user accounts in Zscaler Three based on user and group assignment.

Admin Credentials

Mappings

Mappings

Mappings allow you to define how data should flow between Azure Active Directory and ZscalerThree.

Name	Enabled
Provision Azure Active Directory Groups	Yes
Provision Azure Active Directory Users	Yes

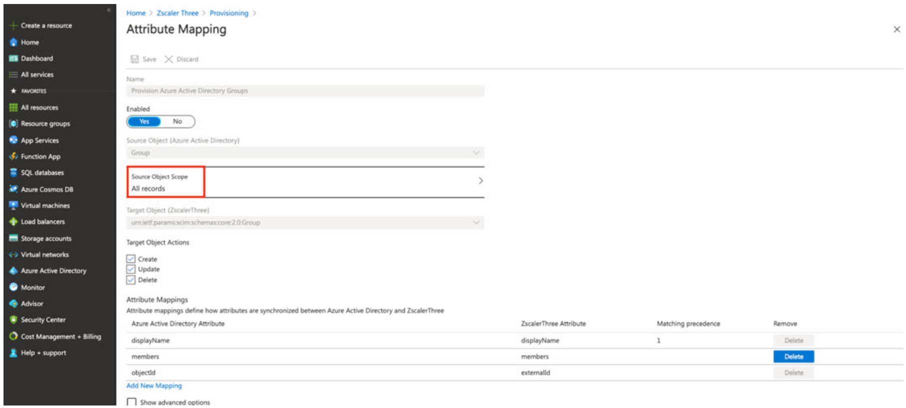
□ Restore default mappings

Settings

Status

Figure 29. Mapping

3. Select **Source Object Scope.**



Attribute Mapping

Name: Provision Azure Active Directory Groups

Enabled: Yes No

Source Object (Azure Active Directory): Group

Source Object Scope: All records

Target Object (ZscalerThree): urn:ietf:params:scim:schemas:core:2.0:Group

Target Object Actions

☑ Create
☑ Update
☑ Delete

Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Active Directory and ZscalerThree

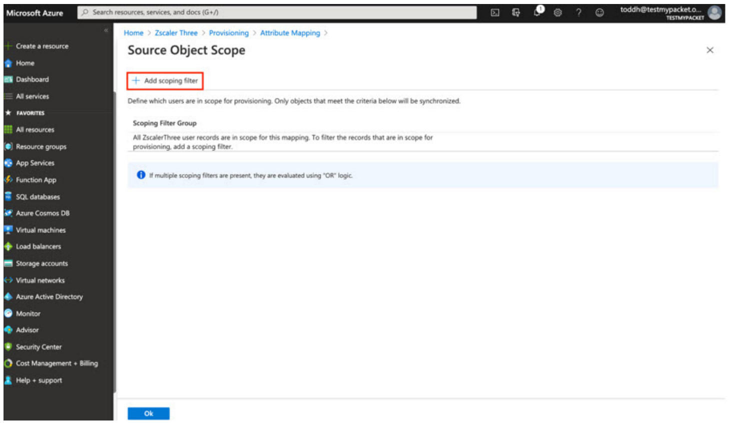
Azure Active Directory Attribute	ZscalerThree Attribute	Matching precedence	Remove
displayName	displayName	1	Delete
members	members		Delete
objectId	externalId		Delete

Add New Mapping

□ Show advanced options

Figure 30. Source object scope

4. Select **Add scoping filter.**



Source Object Scope

+ Add scoping filter

Define which users are in scope for provisioning. Only objects that meet the criteria below will be synchronized.

Scoping Filter Group

All ZscalerThree user records are in scope for this mapping. To filter the records that are in scope for provisioning, add a scoping filter.

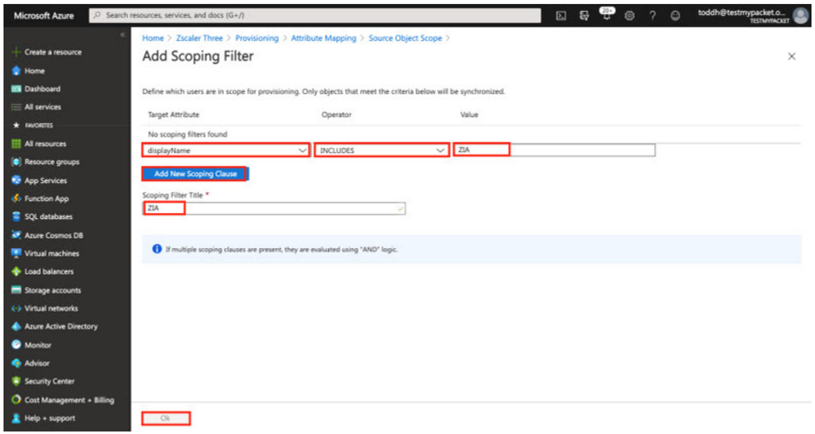
If multiple scoping filters are present, they are evaluated using "OR" logic.

Figure 31. Add scoping filter

SCIM Group Scoping Filter Detail

Set the SCIM group scoping filter:

1. Verify that the **Target Attribute** is set to `displayName`. The value is case-sensitive.
2. Select **INCLUDES** as the **Operator**.
3. Enter a text string value to search for in the group. In the preceding example, the **Value** is ZIA. Any security group that contains the text string, ZIA, is allowed.
4. Select **Add New Scoping Clause**.
5. Click **OK**.
6. Click **OK** again in the next window.
7. Click **Save**.
8. Click **Yes**.



Add Scoping Filter

Define which users are in scope for provisioning. Only objects that meet the criteria below will be synchronized.

Target Attribute	Operator	Value
No scoping filters found		
displayName	INCLUDES	ZIA

Scoping Filter Title *: ZIA

If multiple scoping clauses are present, they are evaluated using "AND" logic.

Figure 32. Group scope detail

The preceding example allows any security group that contains the text “ZIA” as part the group.

ZPA Entitlement

Along with ZIA, you can either enable ZPA for all ZIA users or you can enable a subset of ZIA users by configuring an Entitlement group that contains specific ZPA users. The Authentication flow for Zscaler Cloud Connector allows ZPA to be enabled for select users based on a group attribute that is applied after users authenticate into ZIA. The group attribute is traditionally tied to a Windows Security Group, which for a SAML IdP is provided as a memberOf user attribute and can be pushed as a SCIM Group dynamically.

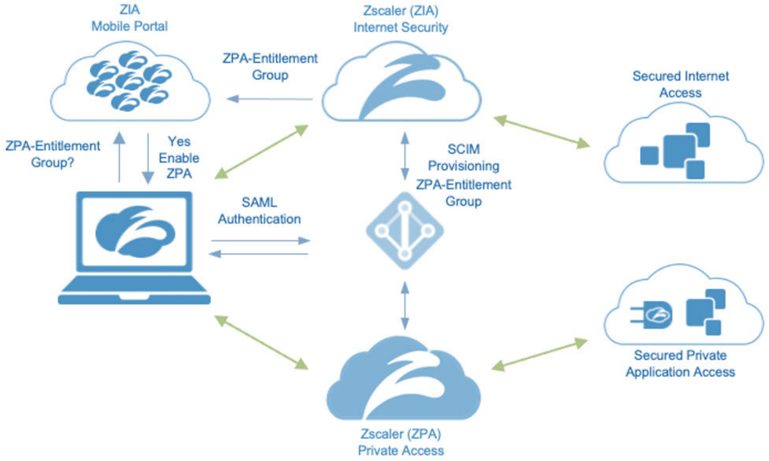
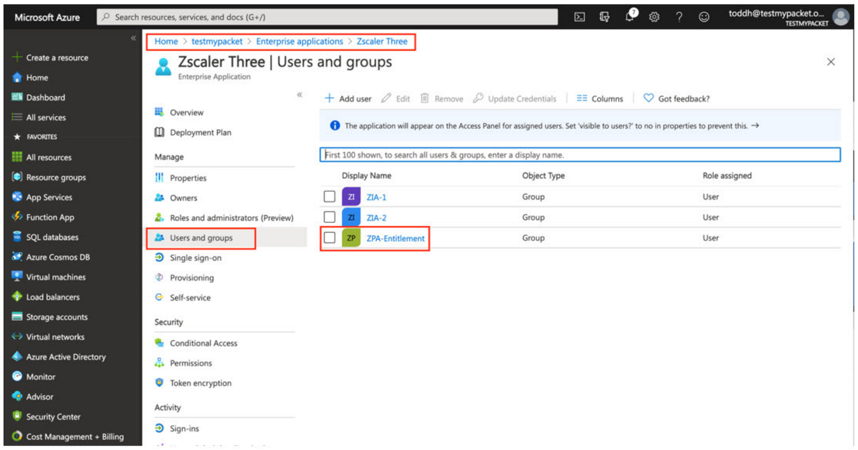


Figure 33. ZPA entitlement group

The group is provided during the authentication process by the ZIA IdP or pushed to ZIA via SCIM. The group is then configured and used by the Zscaler Cloud Connector during enrollment. ZIA Admin Portal enables ZPA for users that are part of the Entitlement group and the users can view the ZPA application the Zscaler Client Connector. You can also apply unique APP profiles for this entitled group during Zscaler Cloud Connector enrollment, if required by ZPA.

Configure ZPA Entitlement on the ZIA Azure IdP

In the Azure ZIA IdP User Management screen, use the Group ZPA-Entitlement to entitle ZPA for the users in that Security Group. To add the Security Group in Azure. Select **Microsoft Entra ID** > E**nterprise Applications** > **Zscaler Three** > **User and groups** > **Add user**



The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

	Display Name	Object Type	Role assigned
□	ZI ZIA-1	Group	User
□	ZI ZIA-2	Group	User
□	ZP ZPA-Entitlement	Group	User

Figure 34. Add the ZPA entitlement group to the ZIA Azure IdP

Your Cloud application might be one of the other Zscaler cloud names instead of Zscaler Three.

Configure ZPA Entitlement on the Zscaler Client Connector

Login to your organization's ZIA Admin Portal using admin credentials.

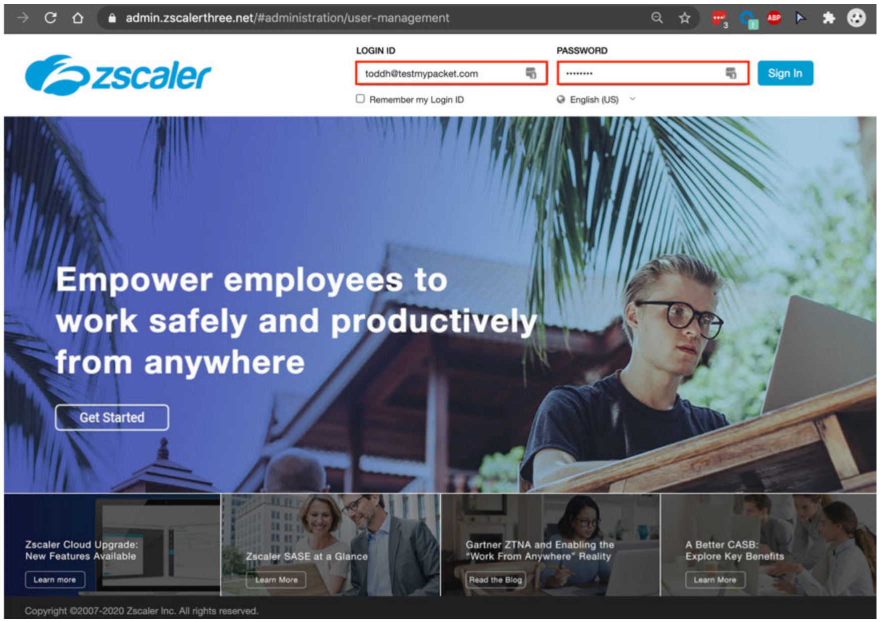

admin.zscalerthree.net/#administration/user-management
zscaler
LOGIN ID
toddh@testmypacket.com
PASSWORD
Sign In
Remember my Login ID
English (US)
Empower employees to work safely and productively from anywhere
Get Started
Zscaler Cloud Upgrade: New Features Available
Learn more
Zscaler SASE at a Glance
Learn More
Gartner ZTNA and Enabling the "Work From Anywhere" Reality
Read the Blog
A Better CASB: Explore Key Benefits
Learn More
Copyright ©2007-2020 Zscaler Inc. All rights reserved.

Figure 35. ZIA Admin Portal

Bring up your organization's Zscaler Client Connector to add the Entitlement group.

Select **Policy** > **Zscaler Client Connector**.

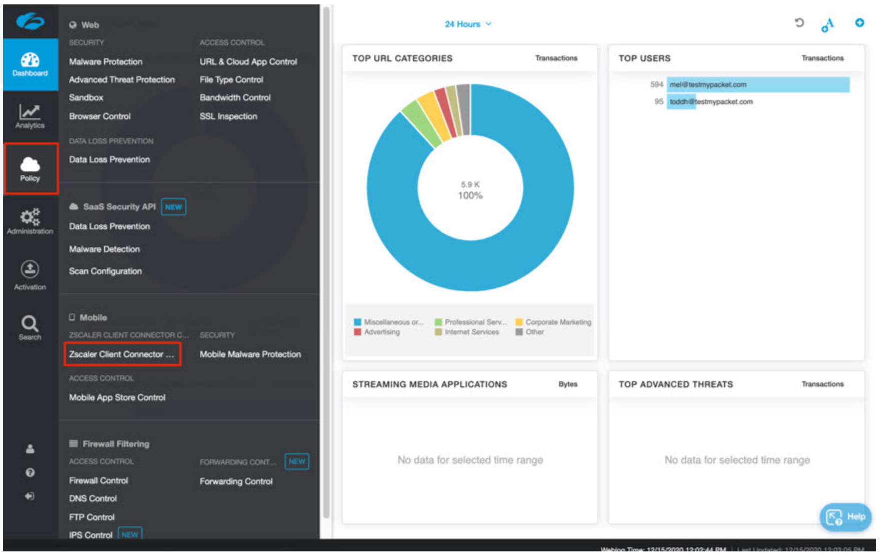
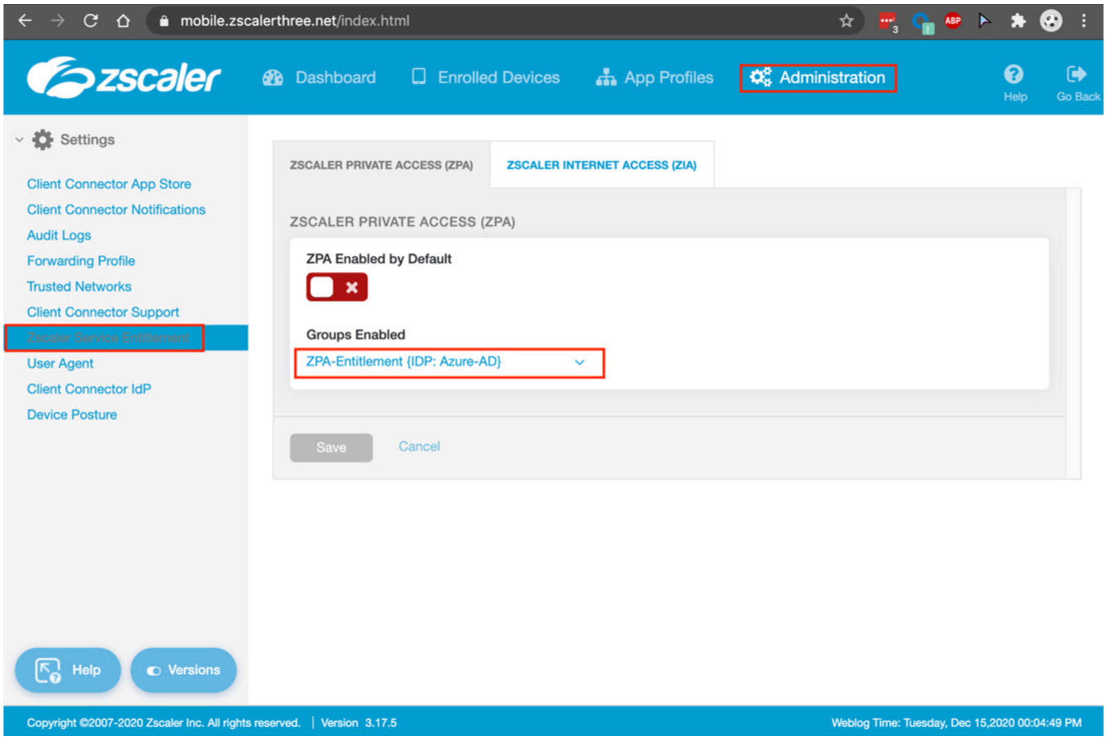


Figure 36. Entering the Zscaler Client Connector Portal

This brings up Zscaler Cloud Connector.

When Zscaler Cloud Connector displays:

1. Select **Administration** > **Zscaler Service Entitlement** > **Zscaler Private Access (ZPA)**.
2. Select the **ZPA-Entitlement group**.
3. Click **Save**.


mobile.zscalerthree.net/index.html
zscaler
Dashboard
Enrolled Devices
App Profiles
Administration
Help
Go Back
Settings
Client Connector App Store
Client Connector Notifications
Audit Logs
Forwarding Profile
Trusted Networks
Client Connector Support
Zscaler Service Entitlement
User Agent
Client Connector IdP
Device Posture
Help
Versions
ZSCALER PRIVATE ACCESS (ZPA)
ZSCALER INTERNET ACCESS (ZIA)
Save
Cancel
Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version 3.17.5
Weblog Time: Tuesday, Dec 15,2020 00:04:49 PM

ZSCALER PRIVATE ACCESS (ZPA)

ZPA Enabled by Default ☒

Groups Enabled: ZPA-Entitlement {IDP: Azure-AD}

Figure 37. Select the Entitlement Group

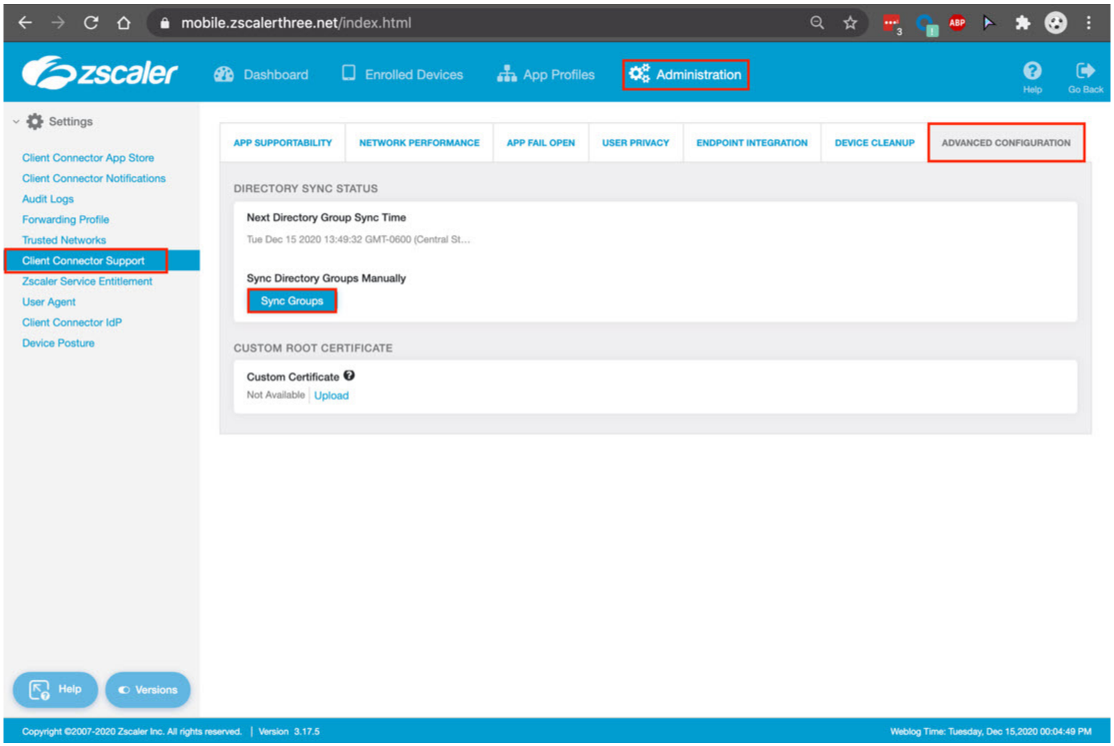
This creates a suffix for the ZIA Azure IdP name that is shown in the preceding example {IDP: Azure-AD}. The **Zscaler Service Entitlement** link is present only if ZPA is enabled and authentication is working on ZPA (confirmed by the Zscaler Support team). If ZPA is enabled and the link is not present, open a ticket with Zscaler Support.

Do not select the group and toggle the **ZPA Enabled by Default** switch. The default enables ZPA on all ZIA users. Select either the **Group Enabled** setting or the default.

Manually Sync Zscaler Client Connector Groups

The group synchronization between ZIA and the Zscaler Cloud Connector occurs every six hours automatically. Therefore, you might experience a gap between the group creation and availability in the Zscaler Cloud Connector. If the group is not present, try syncing the ZIA Admin Portal to Zscaler Cloud Connector manually.

To manually initiate a group synchronization, select **Administration** > **Client Connector Support** > **Advanced Configuration** > **Sync Groups**.



DIRECTORY SYNC STATUS

Next Directory Group Sync Time

Tue Dec 15 2020 13:49:32 GMT-0600 (Central St...

Sync Directory Groups Manually

CUSTOM ROOT CERTIFICATE

Custom Certificate

Not Available | Upload

Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version 3.17.5

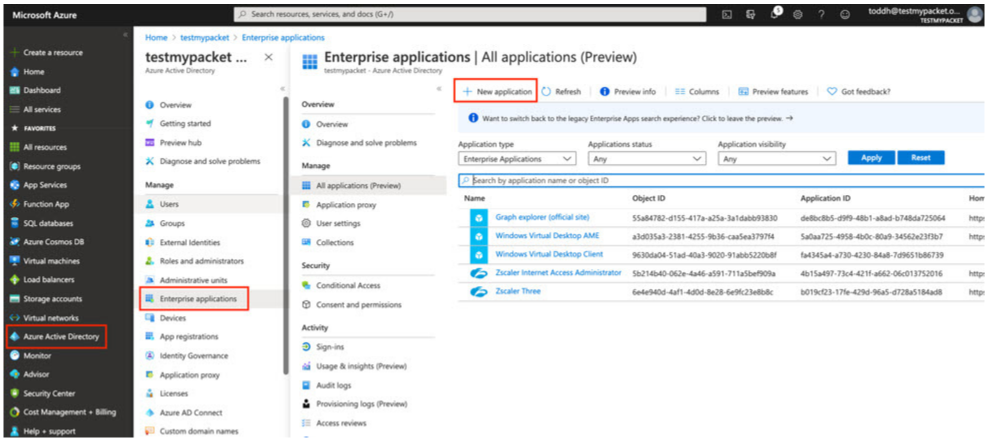
Weblog Time: Tuesday, Dec 15,2020 00:04:49 PM

Figure 38. Manually update the Mobile Portal groups

ZPA Authentication

To configure SAML Authentication for Zscaler ZPA, you must install and configure the Zscaler Private Access (ZPA) enterprise application from the Microsoft Entra ID Gallery.

To start the installation process, select **Microsoft Entra ID** > **Enterprise applications** > **New application**.



Want to switch back to the legacy Enterprise Apps search experience? Click to leave the preview. →

Application type: Enterprise Applications
Applications status: Any
Application visibility: Any

Search by application name or object ID

Name	Object ID	Application ID	Hom
Graph explorer (official site)	55a84782-d155-417a-a25a-3a1dabb93830	de8bc8b5-d9f9-48b1-a8ad-b748da725064	http
Windows Virtual Desktop AME	a3d035a3-2381-4255-9b36-caa5ea3797f4	5a0aa725-4958-4b0c-80a9-34562e23f3b7	http
Windows Virtual Desktop Client	9630da04-51ad-40a3-9020-91abb5220b8f	fa4345a4-a730-4230-84a8-7d9651b86739	
Zscaler Internet Access Administrator	5b214b40-062e-4a46-a591-711a5bef909a	4b15a497-73c4-421f-a662-06c013752016	http
Zscaler Three	6e4e940d-4af1-4d0d-8e28-6e9fc23e8b8c	b019cf23-17fe-429d-96a5-d728a5184ad8	http

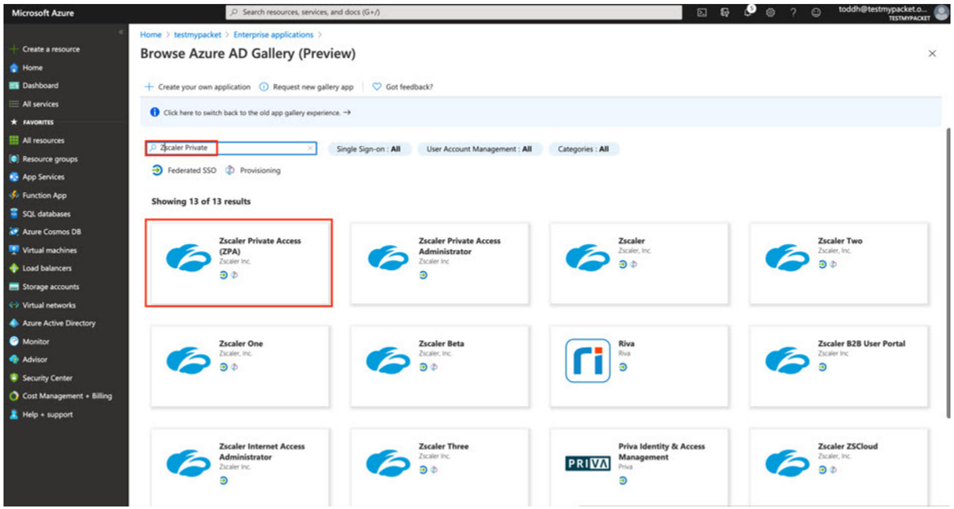
Figure 39. Add the Azure IdP ZPA application in Microsoft Entra ID

This brings up the Microsoft Entra ID Gallery.

Install the Microsoft Entra ID Zscaler Private Access (ZPA) Application

To begin installation:

1. Search for **Zscaler Private Access**.
2. Select the **Zscaler Private Access** tile.



Click here to switch back to the old app gallery experience. →

Zscaler Private

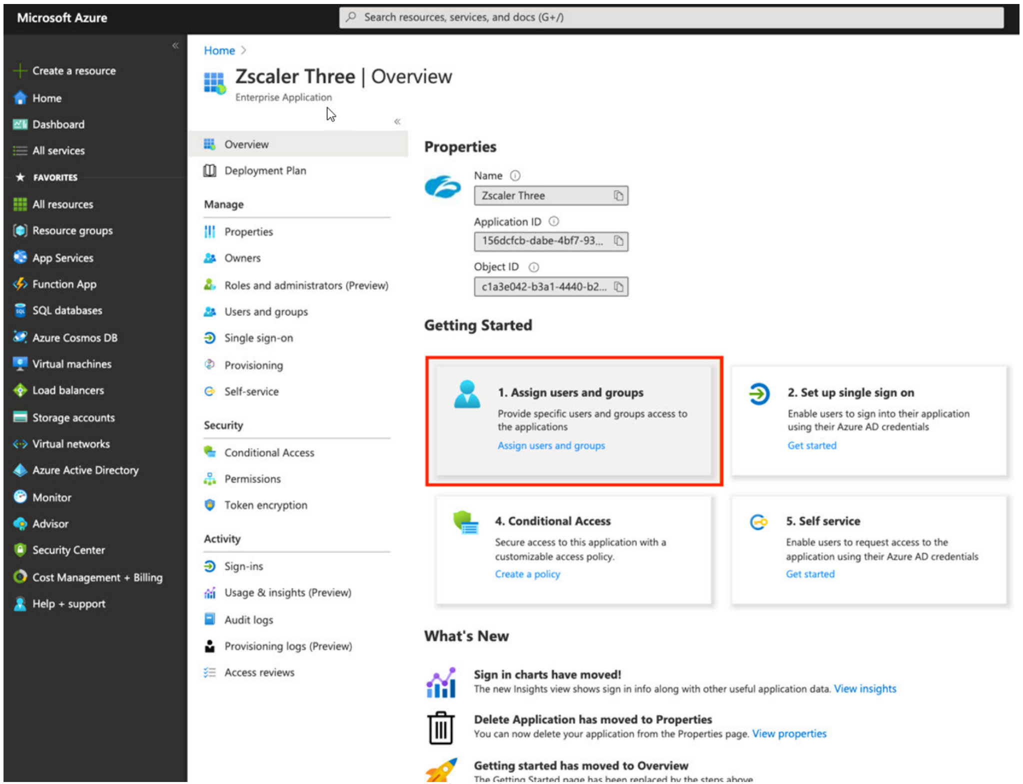
Showing 13 of 13 results

Figure 40. ZPA Application in the Microsoft Entra ID Gallery

Configure Users for Azure ZPA IdP Assignment

You must add the users using ZPA and authenticate to Microsoft Entra ID. These same Users and Groups get synchronized to ZPA via SCIM. To add ZPA users:

1. Select **Users and groups** > **Add user**. This opens the **Add Assignment** window.



Zscaler Three | Overview
Enterprise Application

Properties

Name: Zscaler Three

Application ID: 156dcfcb-dabe-4bf7-93...

Object ID: c1a3e042-b3a1-4440-b2...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

What's New

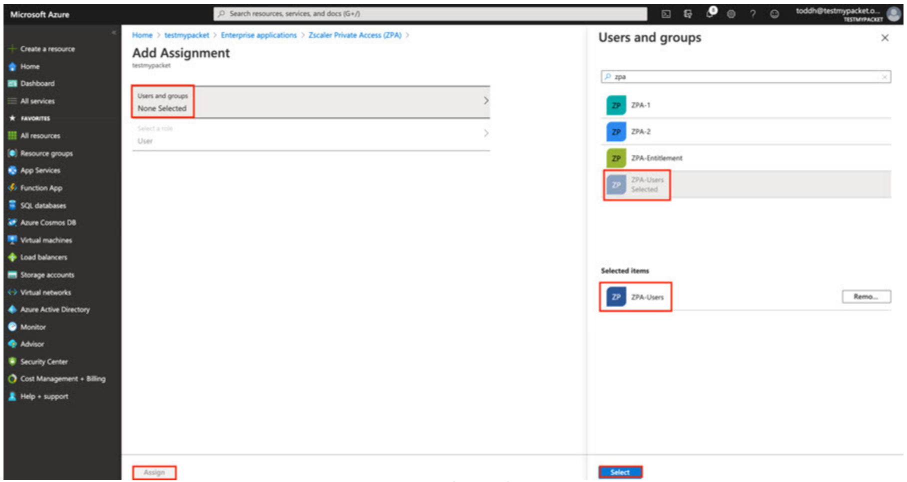
Sign in charts have moved!
The new Insights view shows sign in info along with other useful application data. View insights

Delete Application has moved to Properties
You can now delete your application from the Properties page. View properties

Getting started has moved to Overview
The Getting Started page has been replaced by the steps above

Figure 41. Assign users to the ZPA application (1 of 2)

2. Select the **Users and groups** link.
3. Select all users and groups authenticated to Azure.
4. Click **Select**.
5. Click **Assign**.



Add Assignment
testmypacket

Users and groups: None Selected

Select a role: User

Users and groups

zpa

ZPA-1
ZPA-2
ZPA-Entitlement
ZPA-Users Selected

Selected items

ZPA-Users

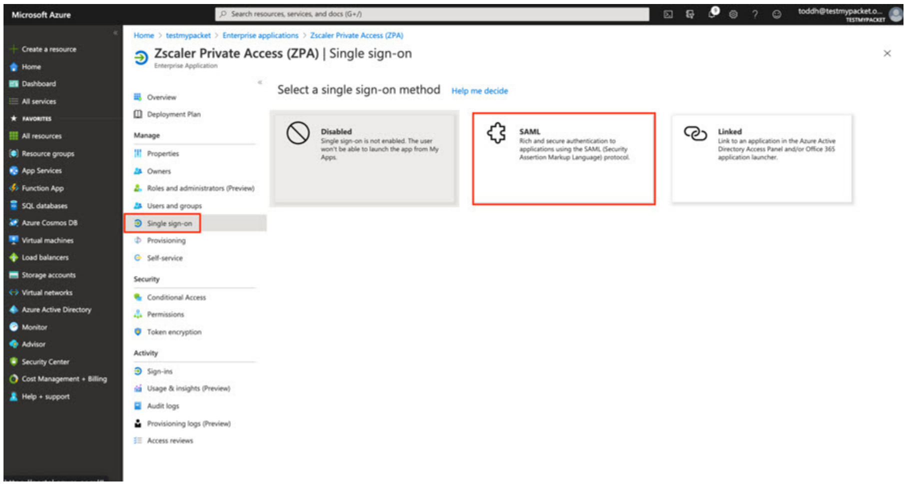
Figure 42. Assign users to the ZPA application (2 of 2)

You can add more users and groups later, if needed. Selectively add only necessary users and groups, because the size of the list can affect SCIM sync times.

Configure SAML SSO Azure ZPA IdP

To configure the SAML parameters for the IdP:

1. Select **Single Sign-on.**
2. Select the **SAML** tile. This opens the configuration procedures.



Zscaler Private Access (ZPA) | Single sign-on

Enterprise Application

Select a single sign-on method

Disabled Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

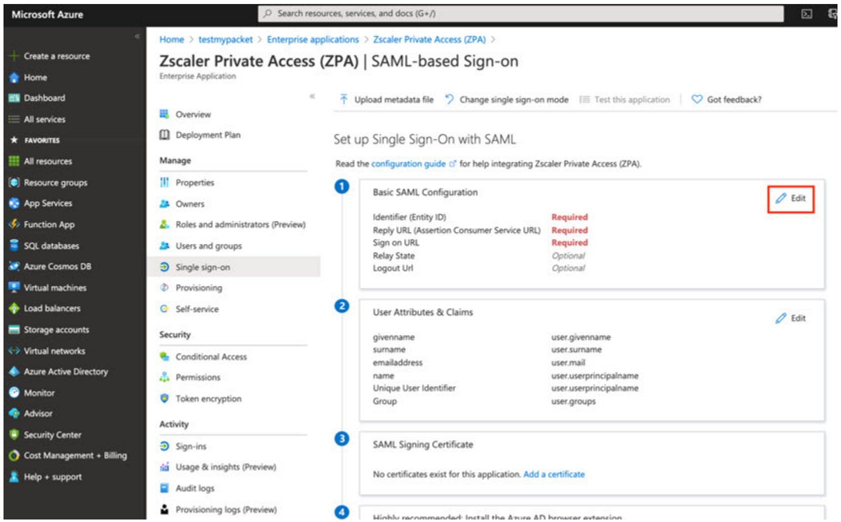
SAML Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Linked Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

Figure 43. The SAML settings tile

Configure Basic SAML Settings for Azure ZPA IdP

To configure basic SAML parameters, click **Edit**.



Zscaler Private Access (ZPA) | SAML-based Sign-on

Enterprise Application

Set up Single Sign-On with SAML

Read the configuration guide for help integrating Zscaler Private Access (ZPA).

1 Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Required
Relay State	Optional
Logout Url	Optional

2 User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
Group	user.groups

3 SAML Signing Certificate

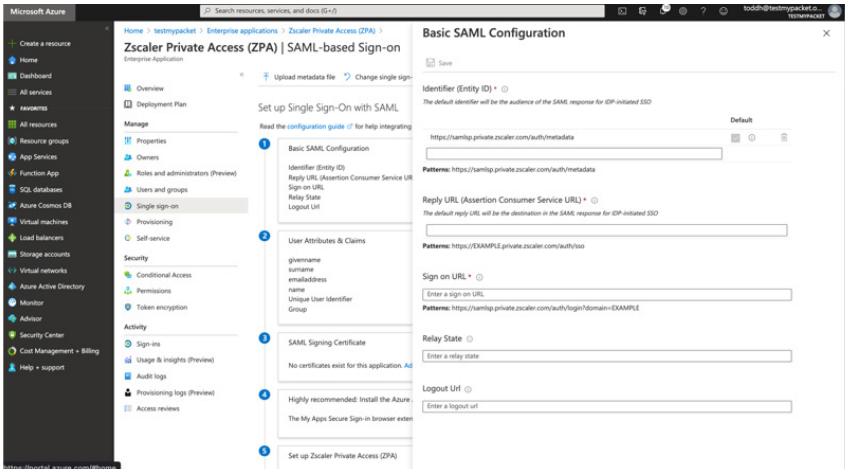
No certificates exist for this application. Add a certificate

4 Highly recommended: Install the Azure AD browser extension

Figure 44. Setting up single sign-on with SAML

On the **Basic SAML Configuration** page, you configure URLs from the ZPA Admin Portal:

1. Open a new tab in your browser or open another browser window.
2. Sign into the [ZPA Admin Portal](), with administrator credentials.



Basic SAML Configuration

Save

Identifier (Entity ID) *
The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

https://samlsp.private.zscaler.com/auth/metadata

Patterns: https://samlsp.private.zscaler.com/auth/metadata

Reply URL (Assertion Consumer Service URL) *
The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Patterns: https://EXAMPLE.private.zscaler.com/auth/sso

Sign on URL *
Enter a sign on URL
Patterns: https://samlsp.private.zscaler.com/auth/login?domain=EXAMPLE

Relay State
Enter a relay state

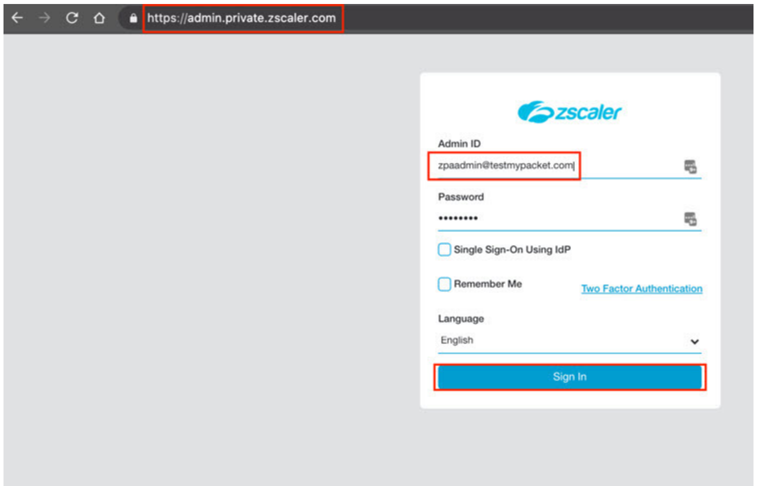
Logout Url
Enter a logout url

Figure 45. A basic SAML configuration

Configure the Azure IdP on ZPA

To start the configuration on the ZPA Admin Portal:

1. Enter your **Admin ID** and **Password** for your organization's ZPA tenant.
2. Click **Sign In**.



https://admin.private.zscaler.com

Admin ID
zpaadmin@testmypacket.com

Password
••••••••

□ Single Sign-On Using IdP

□ Remember Me

Language
English

Figure 46. ZPA Admin Portal

To add the Azure IdP:

1. Select **Administration** > **IdP Configuration**.
2. Select **Add IdP Configuration**.

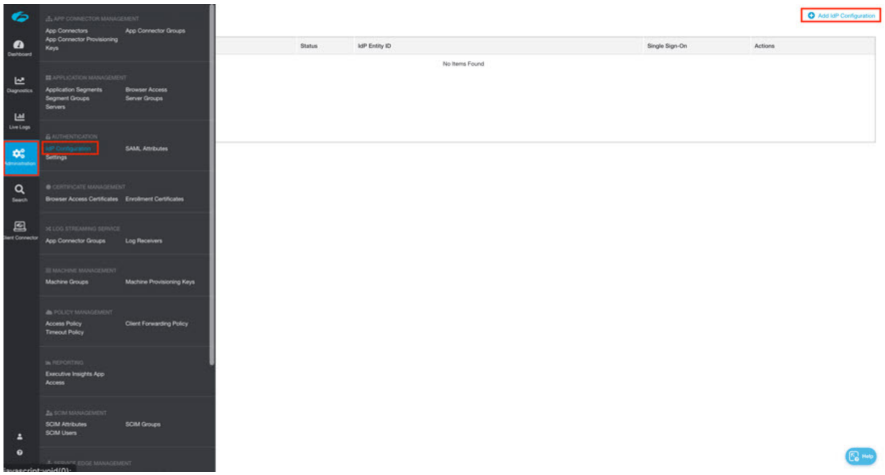
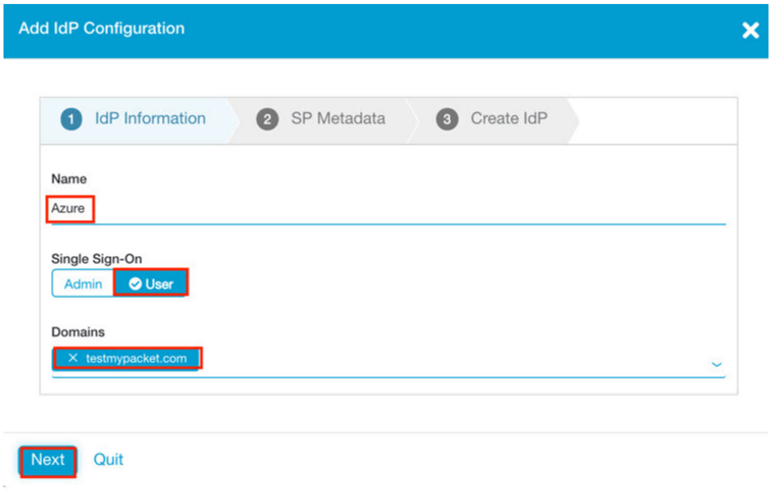


Figure 47. Add a new IdP

Configure the IdP Information for the Azure IdP on ZPA

In the **Add IdP Configuration** window:

1. Give the IdP a **Name**.
2. Select **User** under **Single Sign-On**.
3. Select the authentication under **Domains** (you can add more than one) authenticated by Azure.
4. Click **Next**.



Name: Azure

Single Sign-On: User

Domains: testmypacket.com

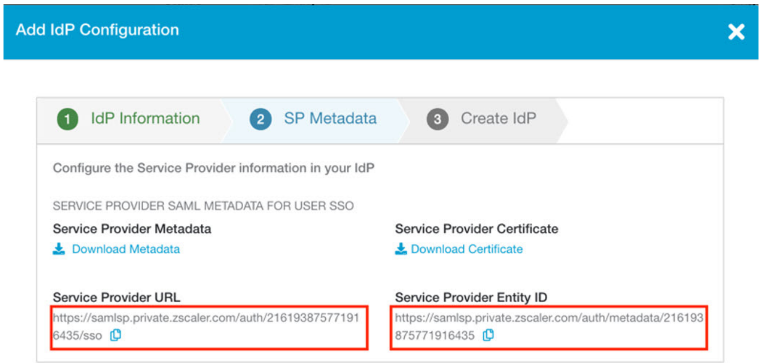
Figure 48. Add the IdP configuration

Zscaler Support must add all authentication domains to be added to your tenant.

SP Details for Use on the Azure IdP

Copy the two URLs, shown in the preceding image, into the Azure configuration:

1. Copy the **Service Provider URL**.
2. Paste the URL into the **Identifier (Entity ID)** on Azure.
3. Copy the **Service Provider Entity ID URL**.
4. Paste the URL into both the **Reply URL** and the **Sign on URL** on Azure.
5. Click **Next**.



Add IdP Configuration

Configure the Service Provider information in your IdP

SERVICE PROVIDER SAML METADATA FOR USER SSO

Service Provider Metadata: Download Metadata

Service Provider Certificate: Download Certificate

Service Provider URL: https://samlsp.private.zscaler.com/auth/216193875771916435/sso

Service Provider Entity ID: https://samlsp.private.zscaler.com/auth/metadata/216193875771916435

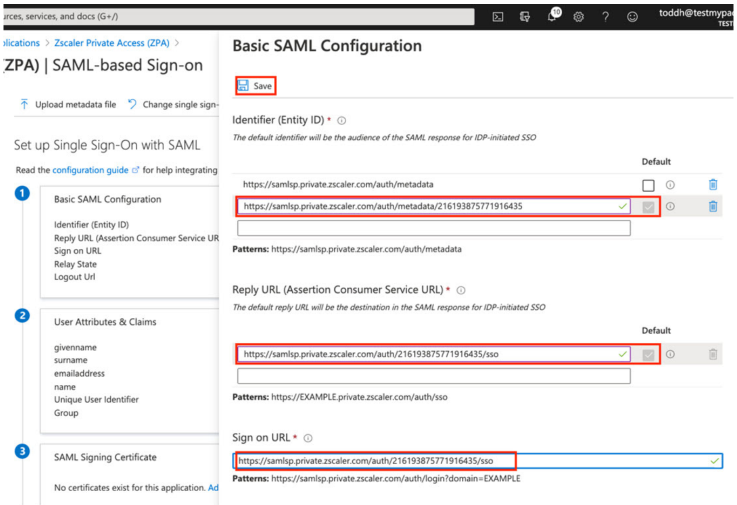
Figure 49. Service provider URLs for the Azure IdP configuration

Go to the Azure configuration browser to gather the information that is needed to finish the ZPA configuration.

Enter the SP Information to Finish the Azure IdP

Finish the Azure IdP configuration:

1. Verify that the **Identifier (Entity ID)** is the Service Provider URL from ZPA.
2. Verify that both the **Reply URL** and the **Sign on URL** are the Service Provider Entity ID URL.
3. Make sure the checkbox is selected to indicate the default value for the new URLs.
4. Click **Save**.



rces, services, and docs (G+/)
toddh@testmypa
TEST
lications > Zscaler Private Access (ZPA) >
Upload metadata file
Change single sign-
Save
Default

ZPA) | SAML-based Sign-on

Set up Single Sign-On with SAML

Read the configuration guide for help integrating

1 Basic SAML Configuration
Identifier (Entity ID)
Reply URL (Assertion Consumer Service UR
Sign on URL
Relay State
Logout Url

2 User Attributes & Claims
givenname
surname
emailaddress
name
Unique User Identifier
Group

3 SAML Signing Certificate
No certificates exist for this application. Ad

Basic SAML Configuration

Identifier (Entity ID) *
The default identifier will be the audience of the SAML response for IDP-initiated SSO

	Default
https://samlsp.private.zscaler.com/auth/metadata	□
https://samlsp.private.zscaler.com/auth/metadata/216193875771916435	☑

Patterns: https://samlsp.private.zscaler.com/auth/metadata

Reply URL (Assertion Consumer Service URL) *
The default reply URL will be the destination in the SAML response for IDP-initiated SSO

	Default
https://samlsp.private.zscaler.com/auth/216193875771916435/sso	☑

Patterns: https://EXAMPLE.private.zscaler.com/auth/sso

Sign on URL *
https://samlsp.private.zscaler.com/auth/216193875771916435/sso
Patterns: https://samlsp.private.zscaler.com/auth/login?domain=EXAMPLE

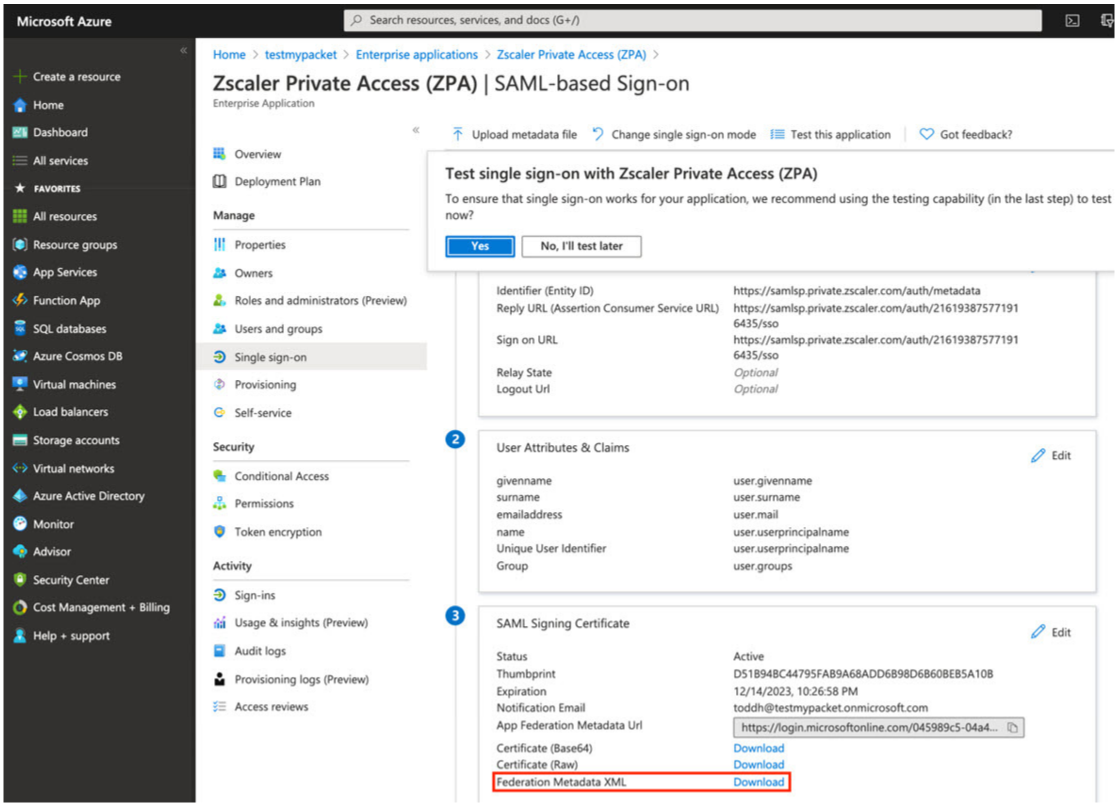
Figure 50. Finish the Azure IdP configuration

After Azure finishes saving, it creates the SAML Signing Certificates and Federation Metadata XML file. You must download the XML file to finish the configuration on ZPA.

Copy the IdP Metadata to Finish the ZPA Configuration

To finish the ZPA configuration:

1. Click **No, I'll test later** in the window.
2. Download the **Federation Metadata XML** file.



Zscaler Private Access (ZPA) | SAML-based Sign-on

Enterprise Application

Test single sign-on with Zscaler Private Access (ZPA)

To ensure that single sign-on works for your application, we recommend using the testing capability (in the last step) to test now?

Identifier (Entity ID)	https://samlsp.private.zscaler.com/auth/metadata
Reply URL (Assertion Consumer Service URL)	https://samlsp.private.zscaler.com/auth/216193875771916435/sso
Sign on URL	https://samlsp.private.zscaler.com/auth/216193875771916435/sso
Relay State	*Optional*
Logout Url	*Optional*

User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
Group	user.groups

SAML Signing Certificate

Status	Active
Thumbprint	D51B94BC44795FAB9A68ADD6B98D6B60BEB5A10B
Expiration	12/14/2023, 10:26:58 PM
Notification Email	toddh@testmypacket.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/045989c5-04a4...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

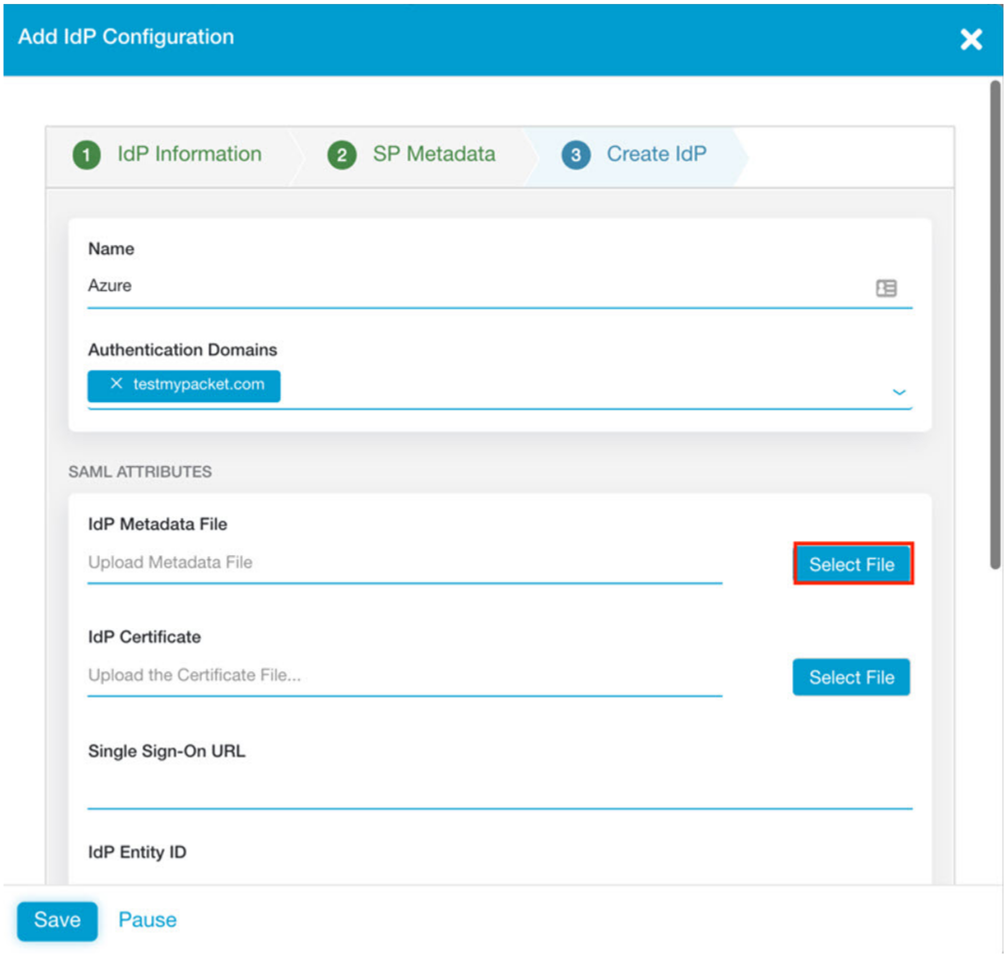
Figure 51. The XML data

Go back to the ZPA configuration window to finish the ZPA configuration.

Upload the Metadata to Finish the ZPA SP Configuration

To finish the configuration:

1. Upload the Federation Metadata XML file into the **Add IdP Configuration** page of the installation wizard.
2. Click **Save**.



Name: Azure

Authentication Domains: testmypacket.com

IdP Metadata File: Upload Metadata File

IdP Certificate: Upload the Certificate File...

Single Sign-On URL

IdP Entity ID

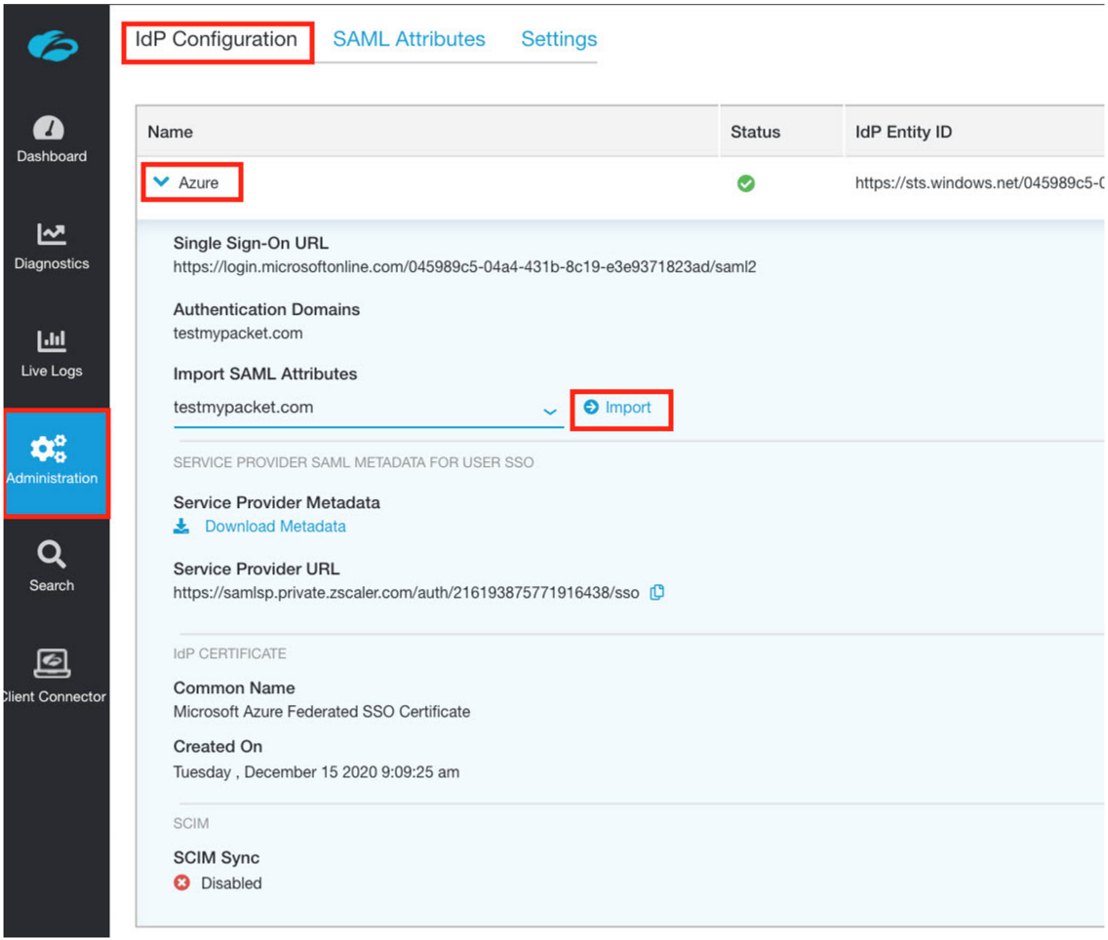
Figure 52. Upload the XML data

The XML file installs the signing certificate and the appropriate configuration information into ZPA.

Testing the ZPA and Azure IdP

Test the SAML configuration from the ZPA Admin Portal.

1. Go to **Administration** > **IdP Configuration**.
2. Click the blue arrow next to the Azure IdP.
3. Select **Import**, located next to the Authentication domain.



Name	Status	IdP Entity ID
Azure	✓	https://sts.windows.net/045989c5-(

Single Sign-On URL
https://login.microsoftonline.com/045989c5-04a4-431b-8c19-e3e9371823ad/saml2

Authentication Domains
testmypacket.com

Import SAML Attributes
testmypacket.com

SERVICE PROVIDER SAML METADATA FOR USER SSO

Service Provider Metadata
Download Metadata

Service Provider URL
https://samlsp.private.zscaler.com/auth/216193875771916438/sso

IdP CERTIFICATE

Common Name
Microsoft Azure Federated SSO Certificate

Created On
Tuesday , December 15 2020 9:09:25 am

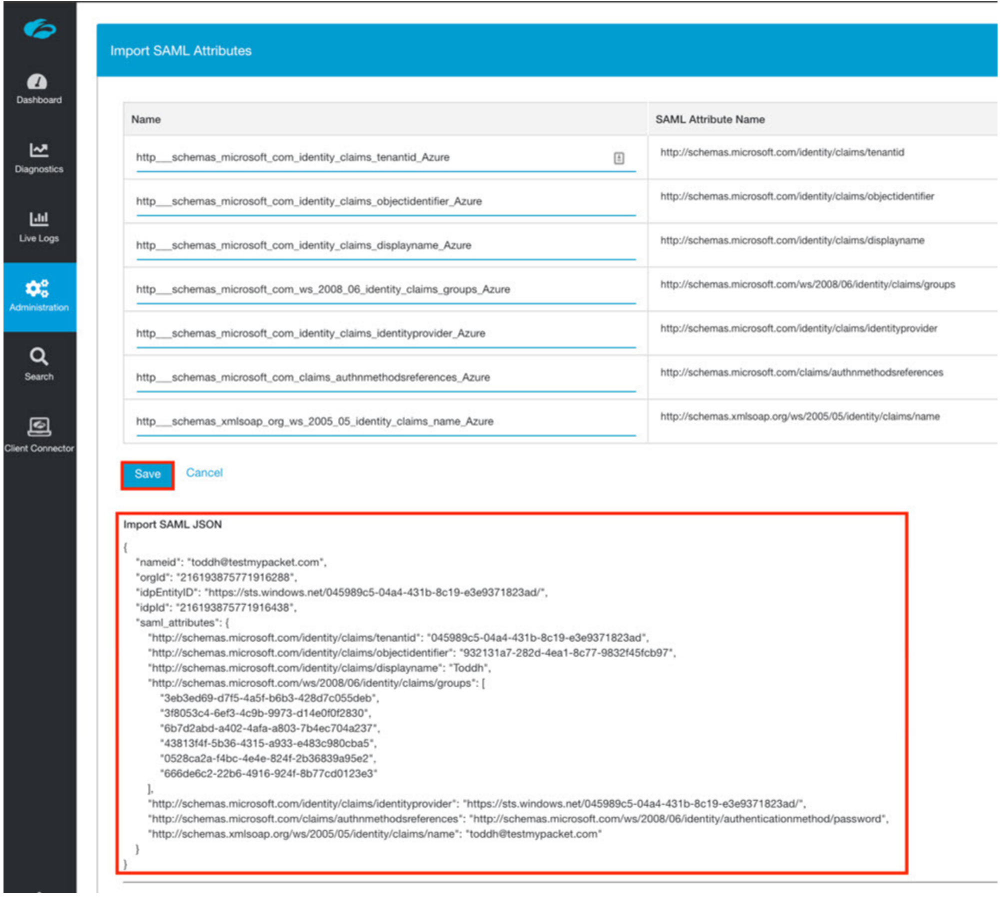
SCIM

SCIM Sync
Disabled

Figure 53. Test SAML Authentication to Azure

You are taken to Azure to authenticate. You then can see the test users SAML assertions.

If you receive a SAML assertion for your login, you have successfully authenticated and tested from the service provider to our IdP and you can move onto other installation aspects.



Import SAML Attributes

Name	SAML Attribute Name
http___schemas_microsoft_com_identity_claims_tenantid_Azure	http://schemas.microsoft.com/identity/claims/tenantid
http___schemas_microsoft_com_identity_claims_objectidentifier_Azure	http://schemas.microsoft.com/identity/claims/objectidentifier
http___schemas_microsoft_com_identity_claims_displayname_Azure	http://schemas.microsoft.com/identity/claims/displayname
http___schemas_microsoft_com_ws_2008_06_identity_claims_groups_Azure	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
http___schemas_microsoft_com_identity_claims_identityprovider_Azure	http://schemas.microsoft.com/identity/claims/identityprovider
http___schemas_microsoft_com_claims_authnmethodsreferences_Azure	http://schemas.microsoft.com/claims/authnmethodsreferences
http___schemas_xmlsoap_org_ws_2005_05_identity_claims_name_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

Import SAML JSON

```
{
   "nameid": "toddh@testmypacket.com",
   "orgId": "216193875771916288",
   "idpEntityID": "https://sts.windows.net/045989c5-04a4-431b-8c19-e3e9371823ad/",
   "idpId": "216193875771916438",
   "saml_attributes": {
      "http://schemas.microsoft.com/identity/claims/tenantid": "045989c5-04a4-431b-8c19-e3e9371823ad",
      "http://schemas.microsoft.com/identity/claims/objectidentifier": "932131a7-282d-4ea1-8c77-9832f45fcb97",
      "http://schemas.microsoft.com/identity/claims/displayname": "Toddh",
      "http://schemas.microsoft.com/ws/2008/06/identity/claims/groups": [
         "3eb3ed69-d7f5-4a5f-b6b3-428d7c055deb",
         "3f8053c4-6ef3-4c9b-9973-d14e0f0f2830",
         "6b7d2abd-a402-4afa-a803-7b4ec704a237",
         "43813f4f-5b36-4315-a933-e483c980cba5",
         "0528ca2a-f4bc-4e4e-824f-2b36839a95e2",
         "666de6c2-22b6-4916-924f-8b77cd0123e3"
      ],
      "http://schemas.microsoft.com/identity/claims/identityprovider": "https://sts.windows.net/045989c5-04a4-431b-8c19-e3e9371823ad/",
      "http://schemas.microsoft.com/claims/authnmethodsreferences": "http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password",
      "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name": "toddh@testmypacket.com"
   }
}
```

Figure 54. SAML assertion

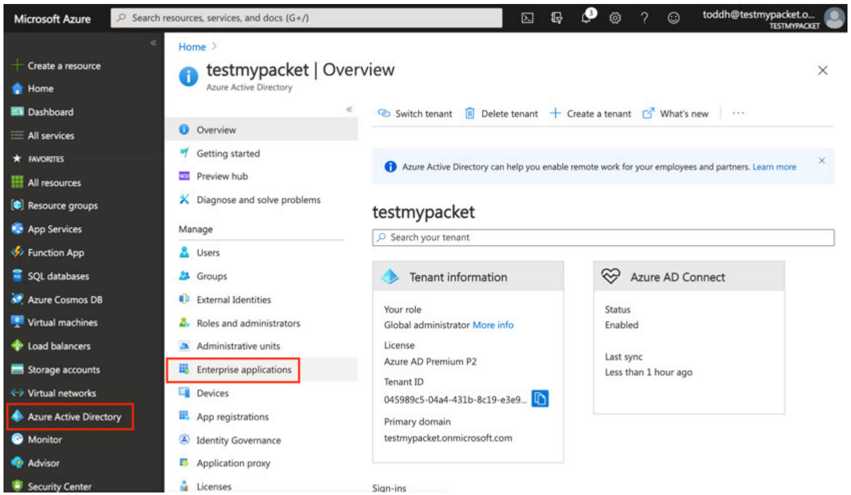
You can also **test the IdP authentication configuration**.

You can authenticate from a browser. This method of authentication is useful when working with clients who do not have access to the ZPA Admin Portal.

ZPA Provisioning

The SCIM specification is designed to make managing user and group identities in cloud-based applications and services easier. SCIM is used as best practice for user and group management with Zscaler Identity Partners. ZPA uses SCIM to sync user and group additions, removals, and changes. Managing groups with SCIM is a relatively new feature, but fully replaces SAML attributes for users and groups. The SCIM attributes are then used in the ZPA access and re-authentication policies.

To enable SCIM in Azure, select **Microsoft Entra ID** > **Enterprise applications** > **Zscaler Private Access (ZPA)**.



Your role
Global administrator More info

License
Azure AD Premium P2

Tenant ID
045989c5-04a4-431b-8c19-e3e9...

Primary domain
testmypacket.onmicrosoft.com

Status
Enabled

Last sync
Less than 1 hour ago

Figure 55. Configure SCIM provisioning on ZPA

Configure ZPA Provisioning

To configure ZPA provisioning:

1. Select **Provisioning**.
2. Click **Get started**.

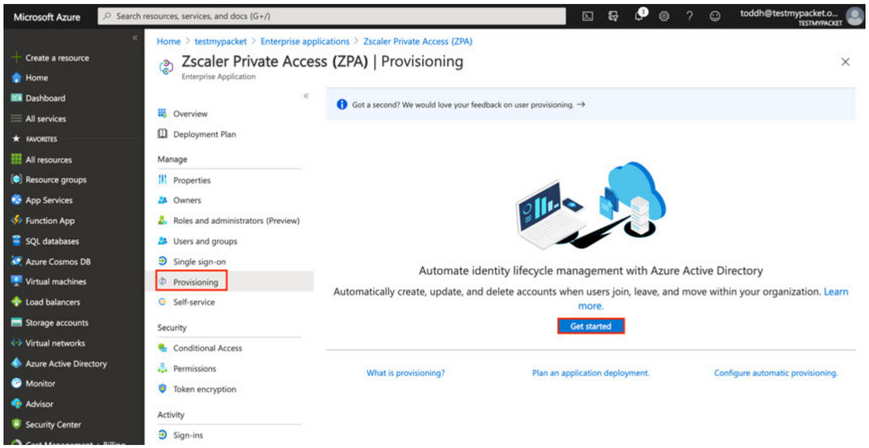
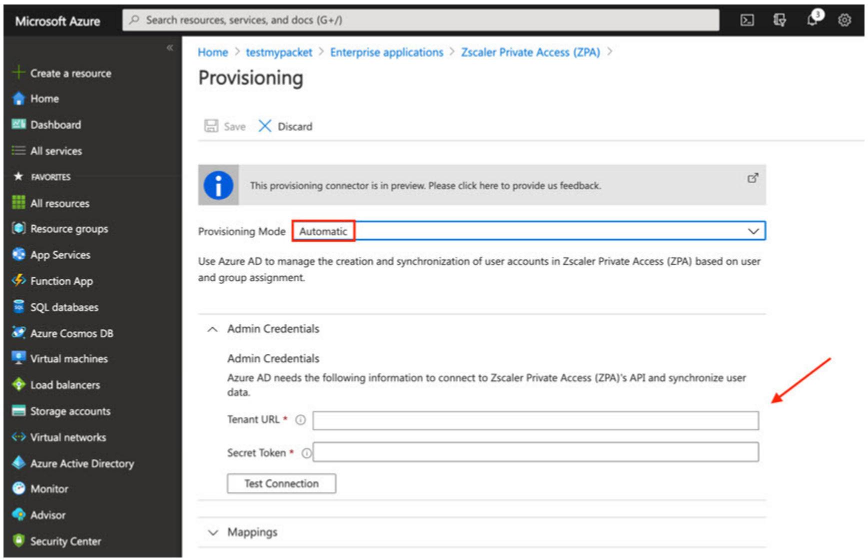


Figure 56. Provisioning

Configure SCIM Provisioning on Azure

The **Provisioning** configuration builds out as you select parameters. The **Admin Credential** fields are pulled from ZPA as you configure SCIM on ZPA.

1. Change the **Provisioning Mode** to **Automatic**.
2. Open a new tab or a new web browser.
3. Sign-in to the [ZPA Admin Portal]() with admin credentials.



Provisioning

Save Discard

This provisioning connector is in preview. Please click here to provide us feedback.

Provisioning Mode: Automatic

Use Azure AD to manage the creation and synchronization of user accounts in Zscaler Private Access (ZPA) based on user and group assignment.

Admin Credentials

Admin Credentials

Azure AD needs the following information to connect to Zscaler Private Access (ZPA)'s API and synchronize user data.

Tenant URL *

Secret Token *

Test Connection

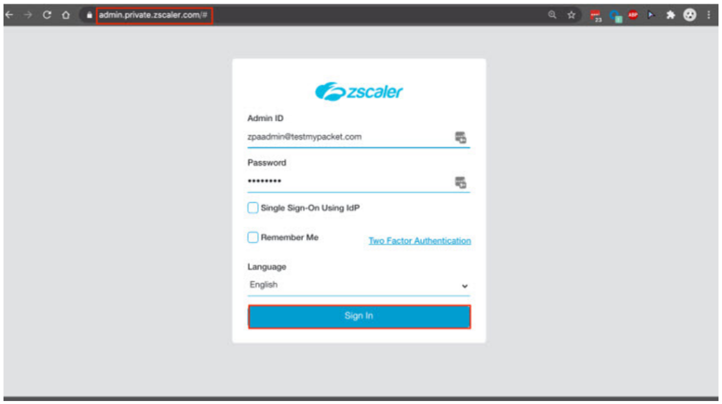
Mappings

Figure 57. Configure SCIM provisioning on ZPA

Configure SCIM Provisioning on ZPA

To configure SCIM provisioning:

1. Enter the **Admin ID** and **Password.**
2. Click **Sign In.** This opens the ZPA Admin Portal.



admin.private.zscaler.com/#

Admin ID: zpaadmin@testmypacket.com

Password: ••••••••

□ Single Sign-On Using IdP

□ Remember Me

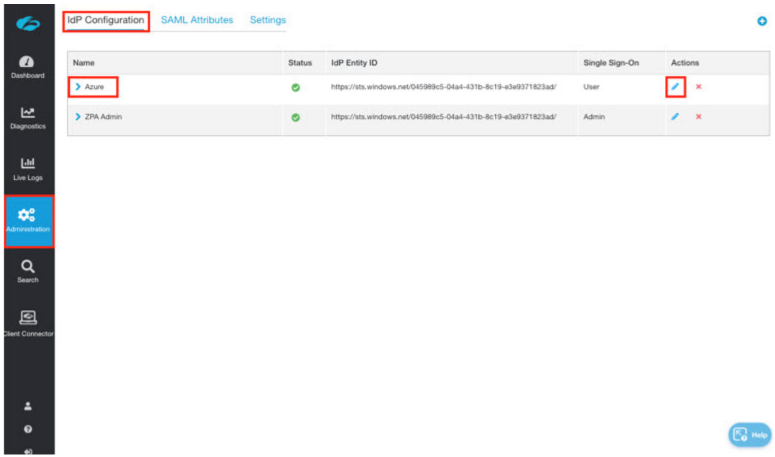
Two Factor Authentication

Language: English

Sign In

Figure 58. ZPA Admin Portal

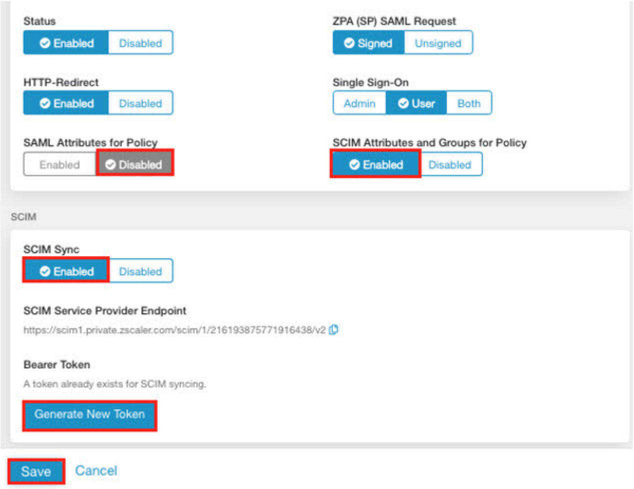
3. In the ZPA Admin Portal:
   a. Select **Administration** > **IdP Configuration**.
   b. Select the blue pencil for the Azure IdP. This launches the **Edit IdP Configuration** wizard.



Name	Status	IdP Entity ID	Single Sign-On	Actions
Azure	✓	https://sts.windows.net/045989c5-04a4-431b-8c19-e3e9371823ad/	User	✎ ✕
ZPA Admin	✓	https://sts.windows.net/045989c5-04a4-431b-8c19-e3e9371823ad/	Admin	✎ ✕

Figure 59. SCIM configuration

4. In the **Edit IdP Configuration** wizard:
   a. Disable **SAML Attributes for Policy**.
   b. Enable **SCIM Attributes for Policy**.
   c. Change **SCIM Sync** to **Enabled**.
   d. Click **Generate New Token**.
   e. Copy the **SCIM Service Provider Endpoint URL** and the **Bearer Token**. You need this information to finalize the configuration.
   f. Click **Save**.



Status: ● Enabled ○ Disabled

ZPA (SP) SAML Request: ● Signed ○ Unsigned

HTTP-Redirect: ● Enabled ○ Disabled

Single Sign-On: ○ Admin ● User ○ Both

SAML Attributes for Policy: ○ Enabled ● Disabled

SCIM Attributes and Groups for Policy: ● Enabled ○ Disabled

SCIM

SCIM Sync: ● Enabled ○ Disabled

SCIM Service Provider Endpoint

https://scim1.private.zscaler.com/scim/1/216193875771916438/v2

Bearer Token

A token already exists for SCIM syncing.

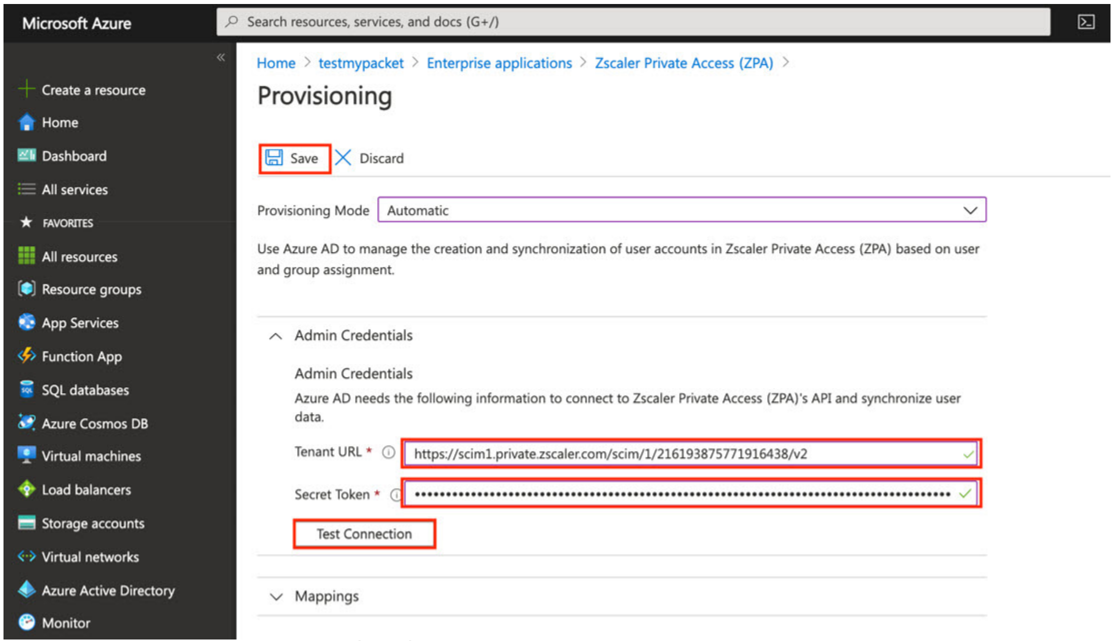
Figure 60. SCIM configuration

Go back to the Azure portal to finish your configuration.

Finish Azure SCIM Provisioning

To finish the SCIM configuration in Azure, paste the URLs from Zscaler into the Tenant URL and the Secret Token on your ZPA Application provisioning page. The credentials must pass before you can save the configuration.

1. Paste the **SCIM Service Provider Endpoint URL** from ZPA into the **Tenant URL**.
2. Paste the **Bearer Token** from ZPA into the **Secret Token** field.
3. Click the **Test Connection** button.
4. Click **Save**.



Provisioning

Provisioning Mode: Automatic

Use Azure AD to manage the creation and synchronization of user accounts in Zscaler Private Access (ZPA) based on user and group assignment.

Admin Credentials

Admin Credentials

Azure AD needs the following information to connect to Zscaler Private Access (ZPA)'s API and synchronize user data.

Tenant URL *: https://scim1.private.zscaler.com/scim/1/216193875771916438/v2

Secret Token *: ••

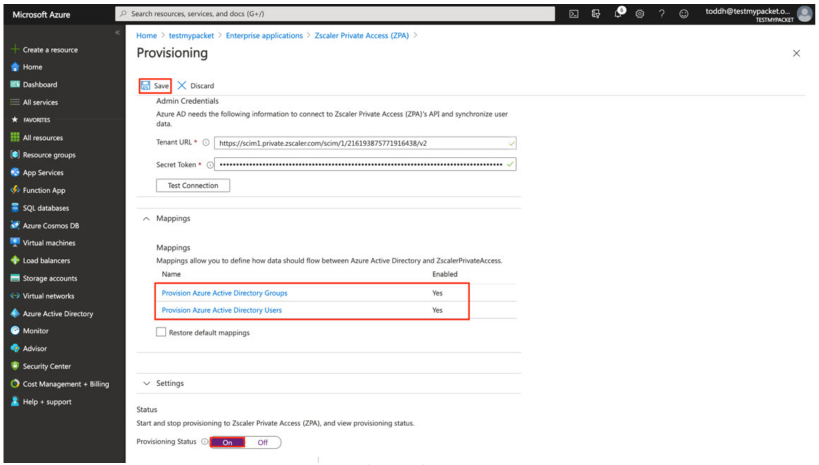
Figure 61. Azure SCIM configuration (1 of 2)

If you get a failure notice, verify that you saved the ZPA configuration.

Start the Azure SCIM Cycle

After you save the configuration, you must start provisioning on Azure. Go back into provisioning to finish the configuration steps:

1. Select **Microsoft Entra ID** > **Enterprise Applications** > **Zscaler Private Access (ZPA)** > **Provisioning**.
2. Select **On** for **Provisioning Status.**
3. Click **Save.**



Provisioning

Admin Credentials

Azure AD needs the following information to connect to Zscaler Private Access (ZPA)'s API and synchronize user data.

Tenant URL * https://scim1.private.zscaler.com/scim/1/216193875771916438/v2

Secret Token * ••

Mappings

Mappings allow you to define how data should flow between Azure Active Directory and ZscalerPrivateAccess.

Name	Enabled
Provision Azure Active Directory Groups	Yes
Provision Azure Active Directory Users	Yes

□ Restore default mappings

Status

Start and stop provisioning to Zscaler Private Access (ZPA), and view provisioning status.

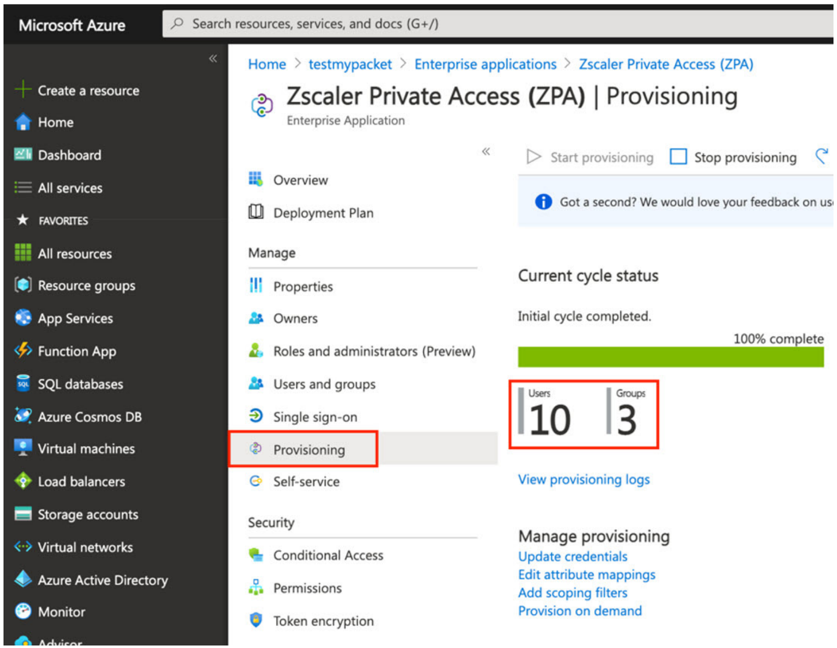
Provisioning Status [✓ On] Off

Figure 62. Azure SCIM configuration (2 of 2)

SCIM provisioning starts.

Configure ZPA SCIM Provisioning

The image shows the status as a completed SCIM interval. The SCIM cycle for Azure is every 40 minutes, but if you need to sync an assigned user immediately you can use **Provision on demand**.



Zscaler Private Access (ZPA) | Provisioning

Enterprise Application

Got a second? We would love your feedback on us

Current cycle status

Initial cycle completed.

100% complete

Users 10

Groups 3

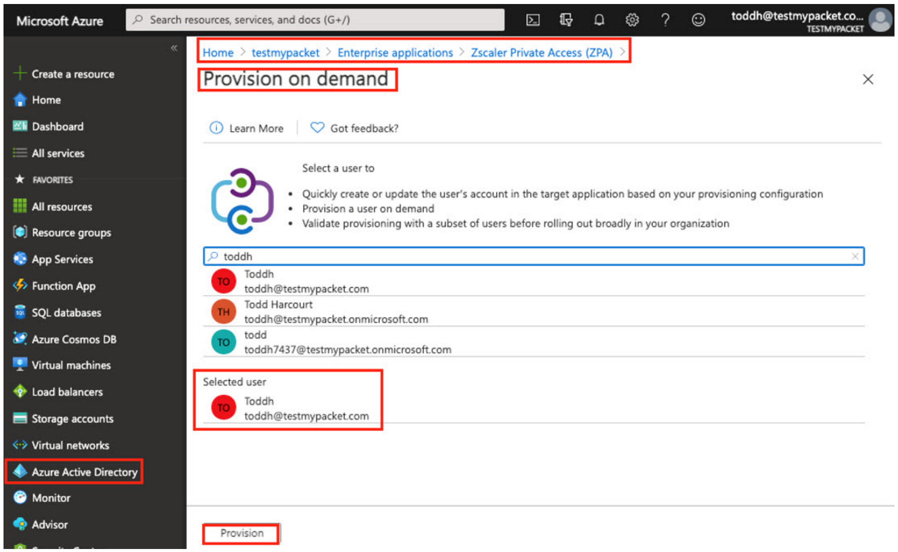
Figure 63. Completed SCIM cycle

Provisioning on Demand

To sync a user immediately via SCIM, use the Provision on demand feature. This enables you to move forward with the POV or Installation without delay and to test the SCIM functionality.

To provision a user immediately using Provision on demand:

1. Select **Microsoft Entra ID** > **Enterprise Applications** > **Zscaler Private Access (ZPA)** > **Provisioning** > **Provisioning on demand**.
2. Search and select your test users.
3. Click **Provision** to Initiate an immediate SCIM push of the selected users.



Provision on demand

Select a user to

- Quickly create or update the user's account in the target application based on your provisioning configuration
- Provision a user on demand
- Validate provisioning with a subset of users before rolling out broadly in your organization

toddh

TO Toddh toddh@testmypacket.com
TH Todd Harcourt toddh@testmypacket.onmicrosoft.com
TO todd toddh7437@testmypacket.onmicrosoft.com

Selected user
TO Toddh toddh@testmypacket.com

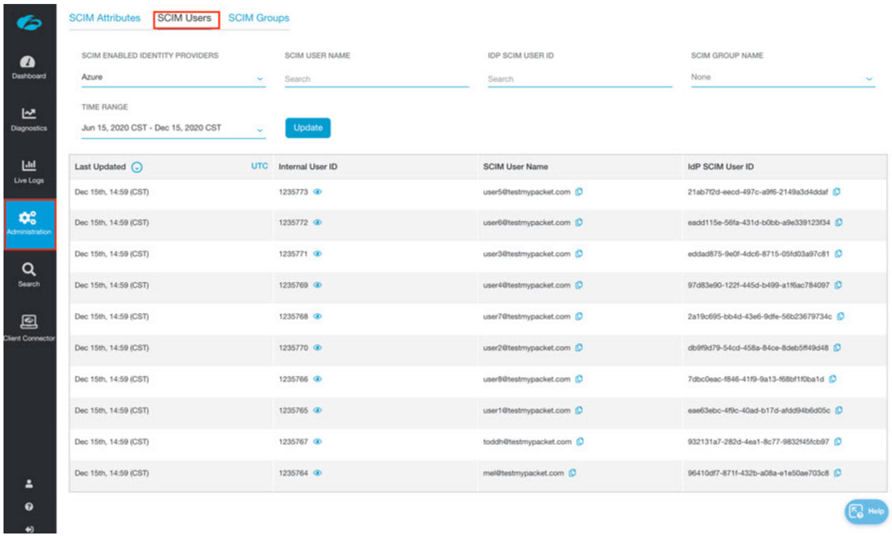
Figure 64. Provisioning on demand

The SCIM interval for Azure is every 40 minutes, so changes can be delayed.

ZPA SCIM Provisioned Users

To view users and groups that have been synced from Azure to ZPA, open the ZPA Admin Portal:

1. Go to **Administration** > **SCIM Users**.
2. Select the **SCIM Groups** tab to view the synced groups.



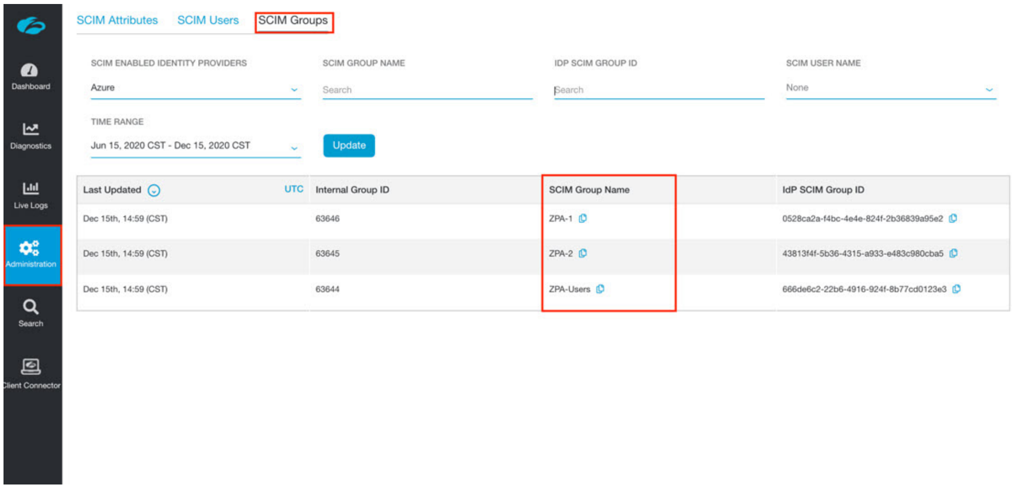
SCIM ENABLED IDENTITY PROVIDERS: Azure
SCIM USER NAME: Search
IDP SCIM USER ID: Search
SCIM GROUP NAME: None
TIME RANGE: Jun 15, 2020 CST - Dec 15, 2020 CST
Update

Last Updated UTC	Internal User ID	SCIM User Name	IdP SCIM User ID
Dec 15th, 14:59 (CST)	1235773	user5@testmypacket.com	21ab7f2d-eecd-497c-a9f6-2149a3d4ddaf
Dec 15th, 14:59 (CST)	1235772	user6@testmypacket.com	eadd115e-56fa-431d-b0bb-a9e339123f34
Dec 15th, 14:59 (CST)	1235771	user3@testmypacket.com	eddad875-9e0f-4dc6-8715-05fd03a97c81
Dec 15th, 14:59 (CST)	1235769	user4@testmypacket.com	97d83e90-122f-445d-b499-a1f6ac784097
Dec 15th, 14:59 (CST)	1235768	user7@testmypacket.com	2a19c695-bb4d-43e6-9dfe-56b23679734c
Dec 15th, 14:59 (CST)	1235770	user2@testmypacket.com	db9f9d79-54cd-458a-84ce-8deb5ff49d48
Dec 15th, 14:59 (CST)	1235766	user8@testmypacket.com	7dbc0eac-f846-41f9-9a13-f68bf1f0ba1d
Dec 15th, 14:59 (CST)	1235765	user1@testmypacket.com	eae63ebc-4f9c-40ad-b17d-afdd94b6d05c
Dec 15th, 14:59 (CST)	1235767	toddh@testmypacket.com	932131a7-282d-4ea1-8c77-9832f45fcb97
Dec 15th, 14:59 (CST)	1235764	mel@testmypacket.com	96410df7-871f-432b-a08a-e1e50ae703c8

Figure 65. SCIM users

ZPA SCIM Provisioned Groups

The list displays the groups synchronized via SCIM from Azure.



SCIM ENABLED IDENTITY PROVIDERS: Azure
SCIM GROUP NAME: Search
IDP SCIM GROUP ID: Search
SCIM USER NAME: None
TIME RANGE: Jun 15, 2020 CST - Dec 15, 2020 CST
Update

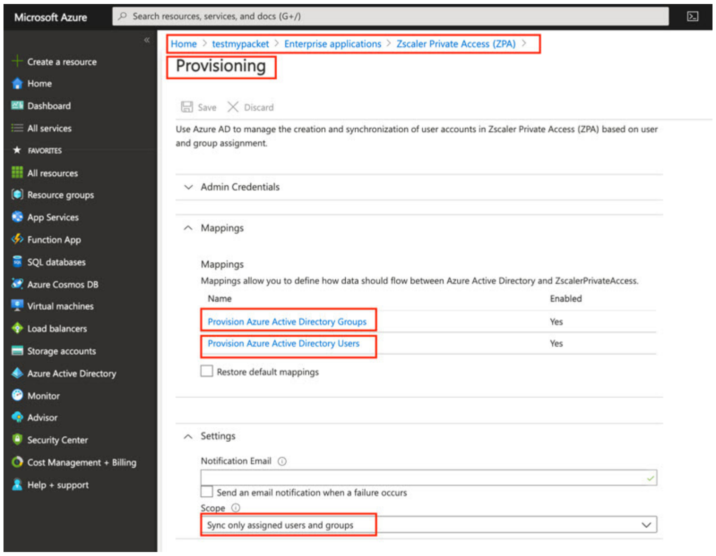
Last Updated UTC	Internal Group ID	SCIM Group Name	IdP SCIM Group ID
Dec 15th, 14:59 (CST)	63646	ZPA-1	0528ca2a-f4bc-4e4e-824f-2b36839a95e2
Dec 15th, 14:59 (CST)	63645	ZPA-2	43813f4f-5b36-4315-a933-e483c980cba5
Dec 15th, 14:59 (CST)	63644	ZPA-Users	666de6c2-22b6-4916-924f-8b77cd0123e3

Figure 66. SCIM groups

Configure ZPA SCIM Scoping

The time to complete an initial SCIM synchronization depends on the number of users and groups assigned to the ZPA application. If you sync thousands of users and groups, the delay can slow the next steps during installation or POV testing. A best practice is to assign only users and groups that use ZPA. To scope users and groups, you can enable general scoping from the **Provisioning** page and either sync all Microsoft Entra ID users, or sync only assigned users and groups. You can also define fine scoping filters. See detailed procedures in **SCIM User Scoping Filters** on how to configure scoping filters. To enable basic scoping to sync only assigned users and groups:

1. Select **Microsoft Entra ID** > **Enterprise Applications** > **Zscaler Private Access (ZPA)** > **Provisioning** > **Settings**.
2. Select S**ync only assigned users and groups**.
3. Click **Save**.



Provisioning

Use Azure AD to manage the creation and synchronization of user accounts in Zscaler Private Access (ZPA) based on user and group assignment.

Admin Credentials

Mappings

Mappings

Mappings allow you to define how data should flow between Azure Active Directory and ZscalerPrivateAccess.

Name	Enabled
Provision Azure Active Directory Groups	Yes
Provision Azure Active Directory Users	Yes

□ Restore default mappings

Settings

Notification Email

□ Send an email notification when a failure occurs

Scope: Sync only assigned users and groups

Figure 67. SCIM scoping

Configure ZPA Microsoft Entra ID Groups Role Mapping for SAML Attribute Policies

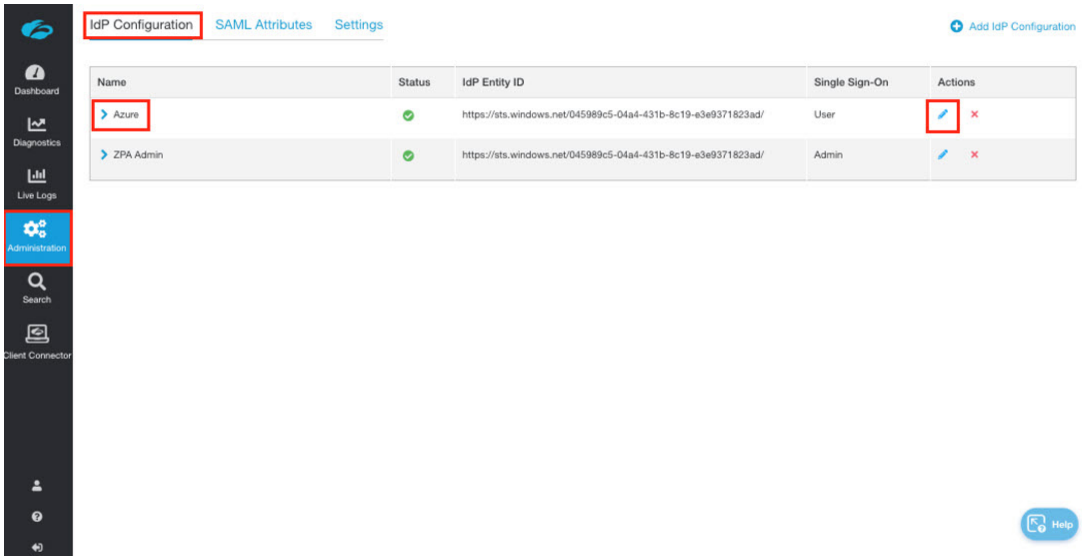
Before the addition of SCIM, one of the Azure SAML ZPA limitations was Azure's inability to provide security groups in human-readable form (except in certain circumstances). The 36-bit Azure numerical ID was sent in the SAML assertion instead of the Microsoft Entra ID Group name. This created an administration nightmare for managing groups. Implementing SCIM in ZPA for provisioning users and groups to and from Azure resolves this issue. However, at times you might not use SCIM and might need to use the original method of creating and mapping a role to an Microsoft Entra ID group so that you can pull the group into ZPA for use with policies.

The Azure configuration is a straight forward way to get your groups from Azure to ZPA via the clients SAML Assertion using SAML authentication attributes.

An example of role to group mapping is provided in case required and as a reference. The method is still prevalent in ZPA installations.

To start the process in the ZPA portal:

1. Select **Administration** > **IdP Configuration**.
2. Select the **Blue pencil** to edit the Azure IdP.



Name	Status	IdP Entity ID	Single Sign-On	Actions
› Azure	✓	https://sts.windows.net/045989c5-04a4-431b-8c19-e3e9371823ad/	User	✎ ✕
› ZPA Admin	✓	https://sts.windows.net/045989c5-04a4-431b-8c19-e3e9371823ad/	Admin	✎ ✕

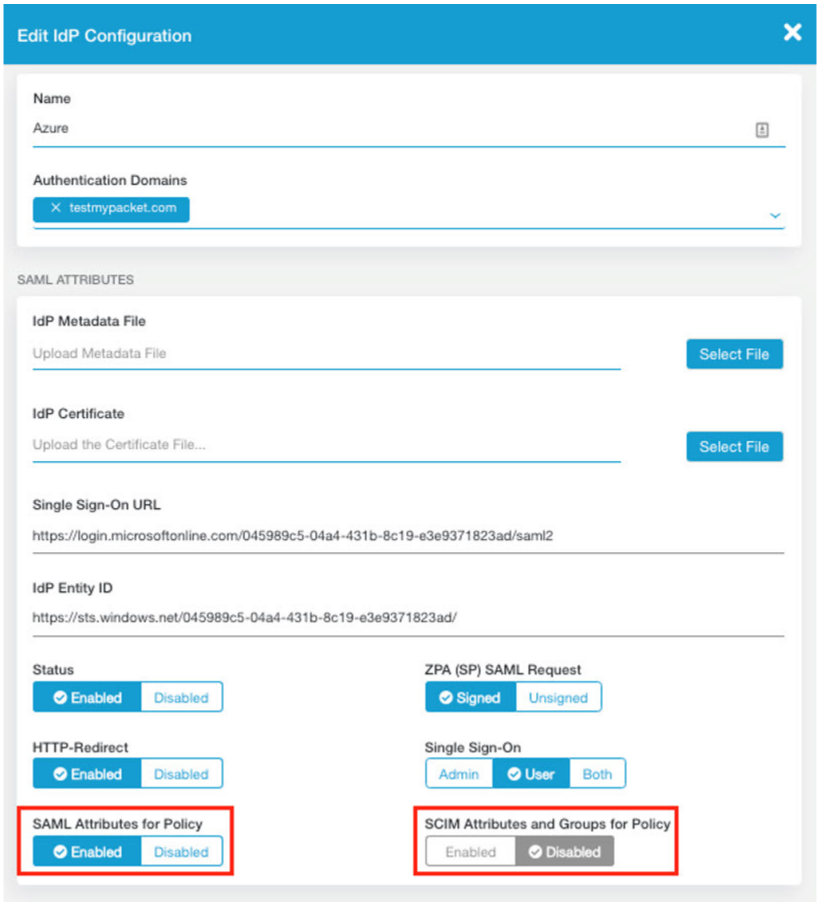
Figure 68. Edit the Azure IdP

Configure ZPA SAML Attributes for Policies

ZPA policies use either SAML attributes or SCIM attributes and groups for policies. SCIM is the best practice for implementations.

However, you can enable SAML attributes for policies:

1. Enable **SAML Attributes for Policy**.
2. Disable **SCIM Attributes and Groups for Policy**.
3. Click **Save**.



Edit IdP Configuration

Name: Azure

Authentication Domains: testmypacket.com

SAML ATTRIBUTES

IdP Metadata File: Upload Metadata File

IdP Certificate: Upload the Certificate File...

Single Sign-On URL: https://login.microsoftonline.com/045989c5-04a4-431b-8c19-e3e9371823ad/saml2

IdP Entity ID: https://sts.windows.net/045989c5-04a4-431b-8c19-e3e9371823ad/

Status: Enabled

ZPA (SP) SAML Request: Signed

HTTP-Redirect: Enabled

Single Sign-On: User

SAML Attributes for Policy: Enabled

SCIM Attributes and Groups for Policy: Disabled

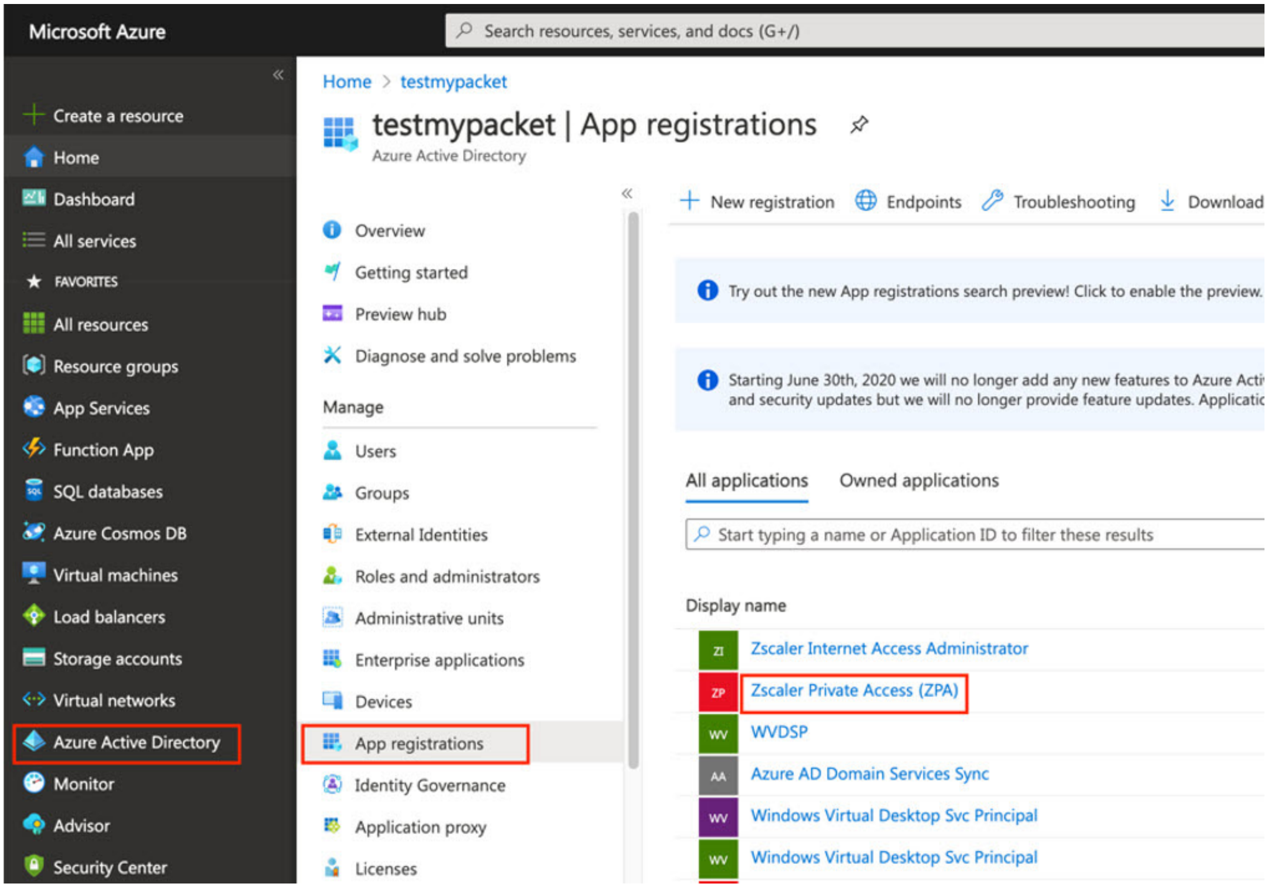
Figure 69. Select SAML attributes for policies

Configure Microsoft Entra ID Groups Role Mapping for SAML in Azure

To configure Azure to send the Microsoft Entra ID Group in readable form, you create a user role and map the role to the Microsoft Entra ID group that you want to use for policies in ZPA. Azure then sends the role as a SAML attribute in the SAML assertion, and the attribute is used for the Microsoft Entra ID Group policies in ZPA.

To start the Azure configuration, you must add the roles in the ZPA application App registrations:

1. Select **Microsoft Entra ID** > **App registrations** > **All Applications** > **Zscaler Private Access (ZPA)**.

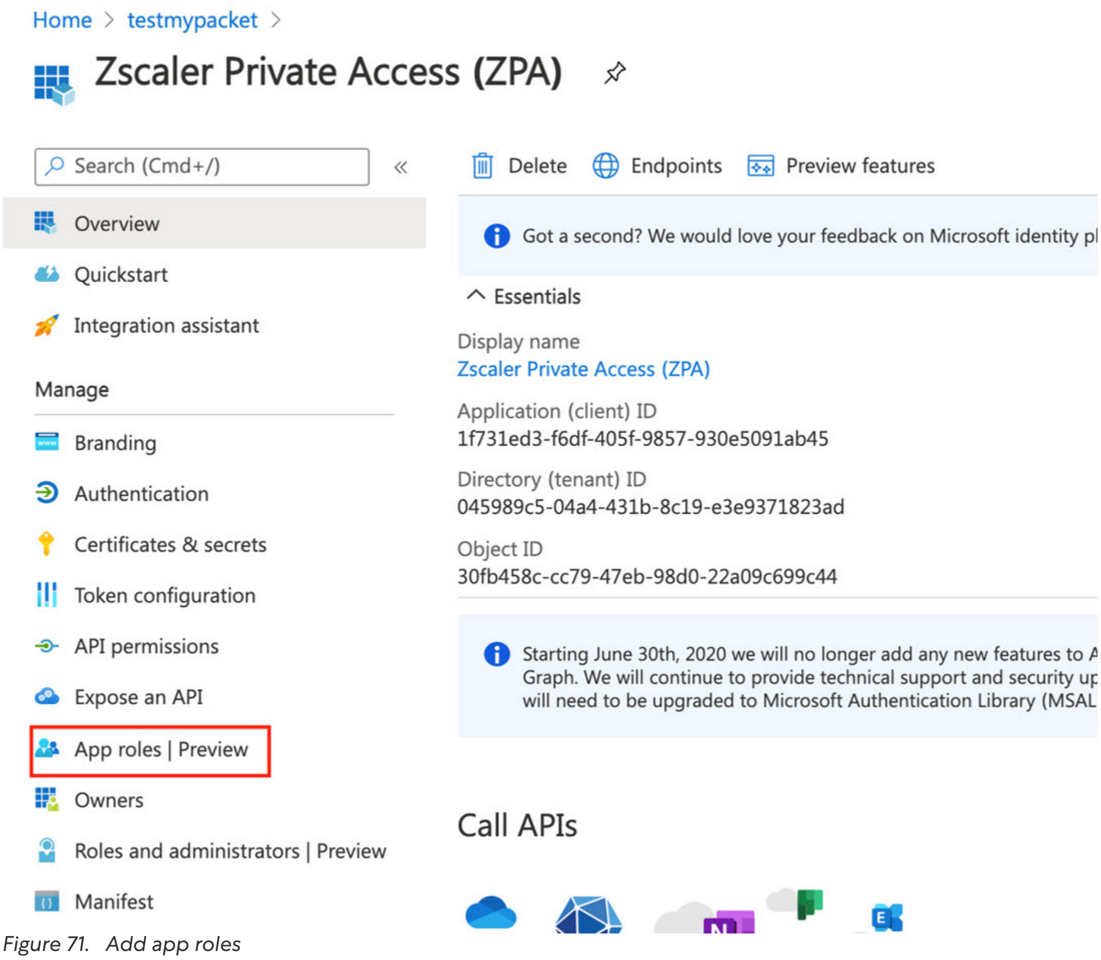


Try out the new App registrations search preview! Click to enable the preview.

Starting June 30th, 2020 we will no longer add any new features to Azure Acti and security updates but we will no longer provide feature updates. Applicatic

Figure 70. Select the ZPA IdP application

2. Select **App roles | Preview.** You are placed into ZPA application registration, in edit mode.



Got a second? We would love your feedback on Microsoft identity pl

Display name
Zscaler Private Access (ZPA)

Application (client) ID
1f731ed3-f6df-405f-9857-930e5091ab45

Directory (tenant) ID
045989c5-04a4-431b-8c19-e3e9371823ad

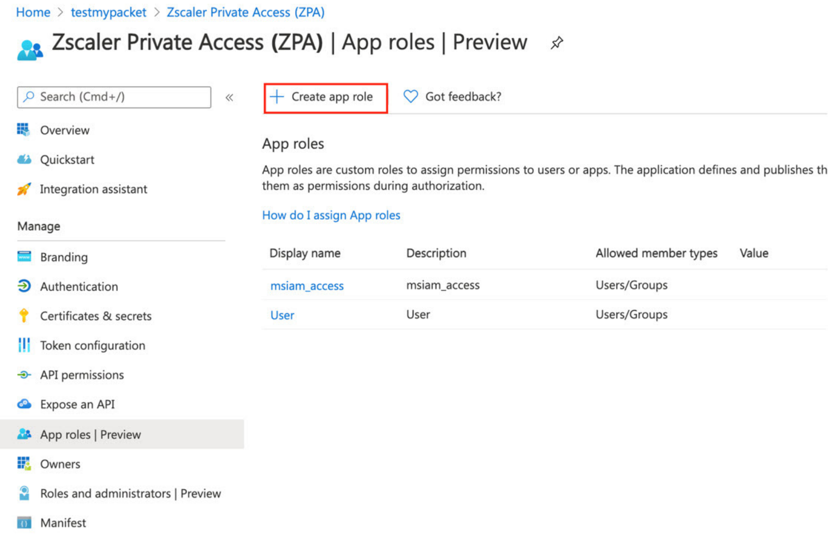
Object ID
30fb458c-cc79-47eb-98d0-22a09c699c44

Starting June 30th, 2020 we will no longer add any new features to A
Graph. We will continue to provide technical support and security up
will need to be upgraded to Microsoft Authentication Library (MSAL

Figure 71. Add app roles

Adding the Zscaler Private Access App Role

Select **Create app role**.



App roles

App roles are custom roles to assign permissions to users or apps. The application defines and publishes th them as permissions during authorization.

How do I assign App roles

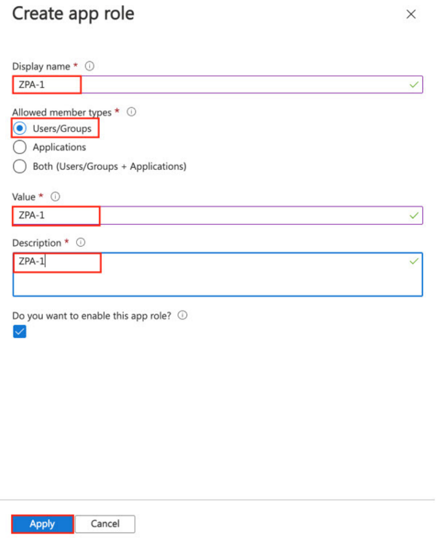
Display name	Description	Allowed member types	Value
msiam_access	msiam_access	Users/Groups	
User	User	Users/Groups	

Figure 72. Create the app role

Add the New Roles to the ZPA App Registration

Create two roles called ZPA-1 and ZPA-2. These names match the Microsoft Entra ID Groups to which they are mapped. The Microsoft Entra ID Groups have already been created. For each role:

1. Enter your Microsoft Entra ID Group name as the **Display** name. In this example, enter `ZPA-1`. The display name for the app role appears in the admin consent and app assignment views. This value can contain spaces.
2. Select **Users/Groups** as the **Allowed member types**.
3. Enter your Microsoft Entra ID Group name as the **Value**. In this example, enter `ZPA-1`. The value is what the application expects in the token. The value should exactly match the string referenced in the application's code. The value cannot contain spaces.
4. Enter your Microsoft Entra ID Group name as the **Description**.
5. Click **Apply**. Repeat for ZPA-2 and all required Microsoft Entra ID security groups used for ZIA policies.



Display name * ⓘ
ZPA-1

Allowed member types * ⓘ
● Users/Groups
○ Applications
○ Both (Users/Groups + Applications)

Value * ⓘ
ZPA-1

Description * ⓘ
ZPA-1

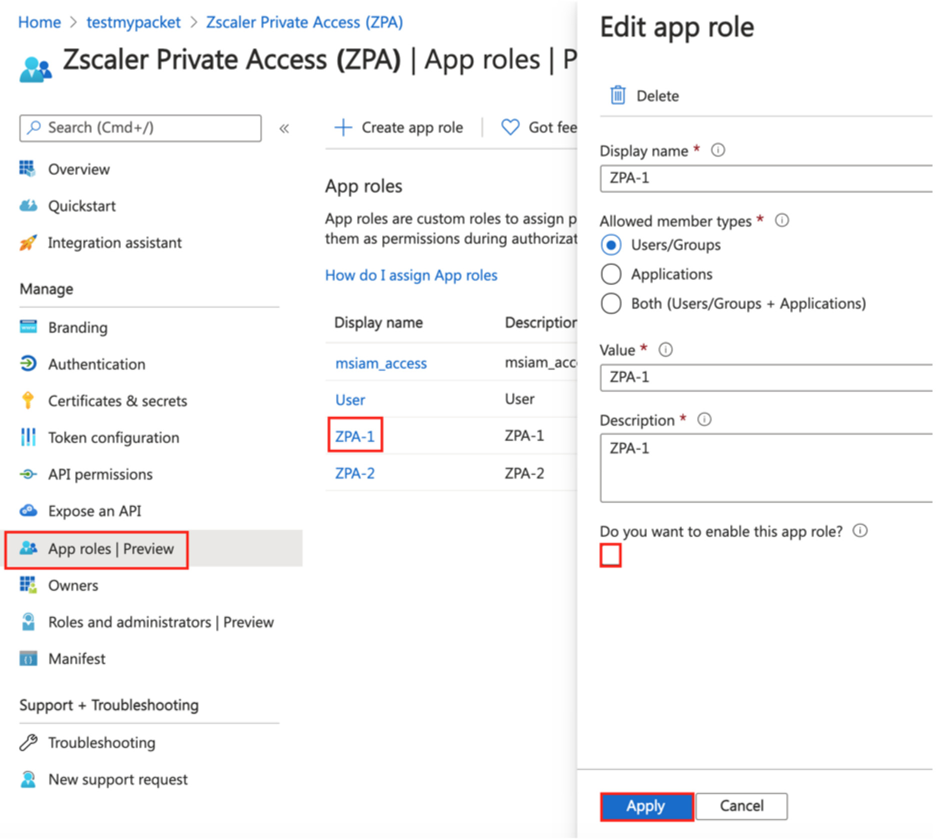
Do you want to enable this app role? ⓘ
☑

Figure 73. App role configuration detail

Deleting and App Roles in the ZPA App Registration

To delete app roles:

1. Select the App role that you want to delete.
2. Deselect the blue check mark under **Do you want to enable this app role**?
3. Click **Apply** to implement the configuration change.
4. Select the App role for deletion.
5. Click **Delete** and confirm the change.



Display name	Description
msiam_access	msiam_acc
User	User
ZPA-1	ZPA-1
ZPA-2	ZPA-2

Display name * ZPA-1

Allowed member types *
● Users/Groups
○ Applications
○ Both (Users/Groups + Applications)

Value * ZPA-1

Description * ZPA-1

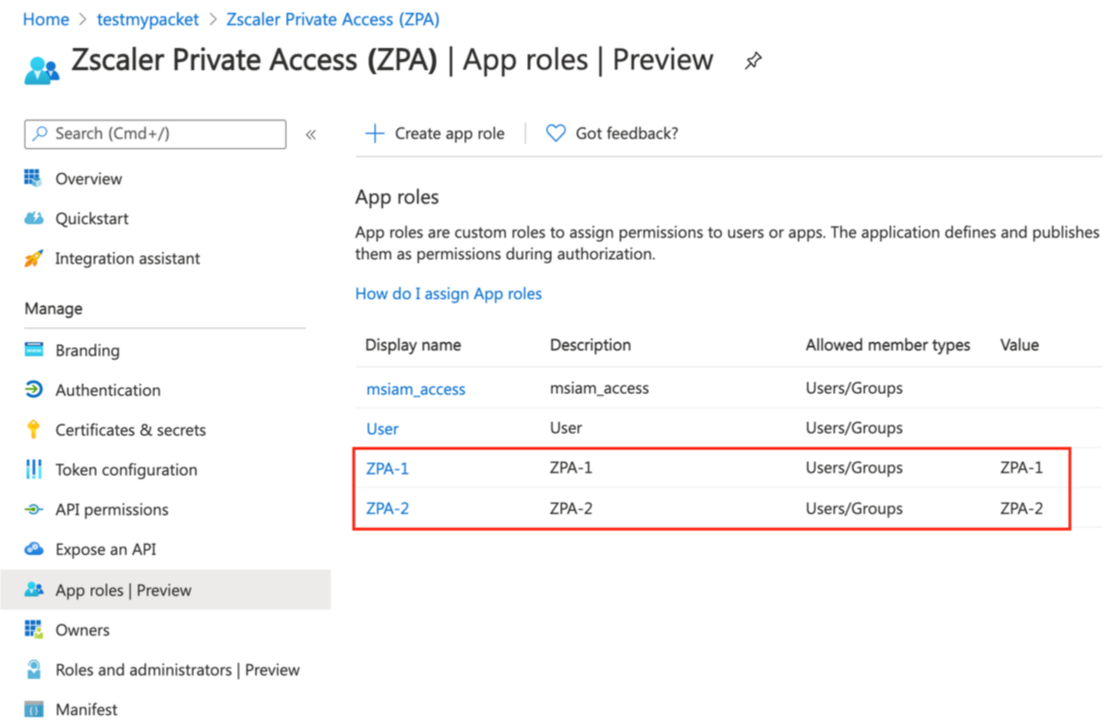
Do you want to enable this app role? □

Figure 74. Delete an app role

Deleting an App role can be confusing. To delete an App Role, you must first disable the role, save the configuration, and then go back into the role to delete it.

New Roles Added to the ZPA App Registration

Let's map the newly added roles to the ZPA-1 and ZPA-2 Microsoft Entra ID groups.



Home > testmypacket > Zscaler Private Access (ZPA)

Zscaler Private Access (ZPA) | App roles | Preview

App roles

App roles are custom roles to assign permissions to users or apps. The application defines and publishes them as permissions during authorization.

How do I assign App roles

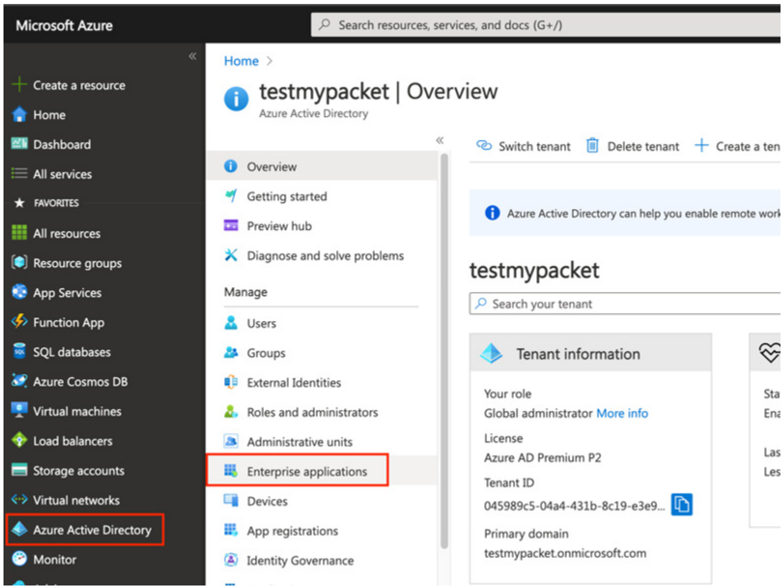
Display name	Description	Allowed member types	Value
msiam_access	msiam_access	Users/Groups	
User	User	Users/Groups	
ZPA-1	ZPA-1	Users/Groups	ZPA-1
ZPA-2	ZPA-2	Users/Groups	ZPA-2

Figure 75. Newly created app roles ready to be mapped to Microsoft Entra ID groups

Configure ZPA Role Mapping for Microsoft Entra ID Groups

To map the newly created roles to the Microsoft Entra ID groups:

1. Navigate to **Users and groups** under your installed ZPA application.
2. Select **Microsoft Entra ID** > **Enterprise applications** > **Zscaler Private Access (ZPA)**.



testmypacket | Overview

Azure Active Directory

Azure Active Directory can help you enable remote work

testmypacket

Search your tenant

Tenant information

Your role
Global administrator More info

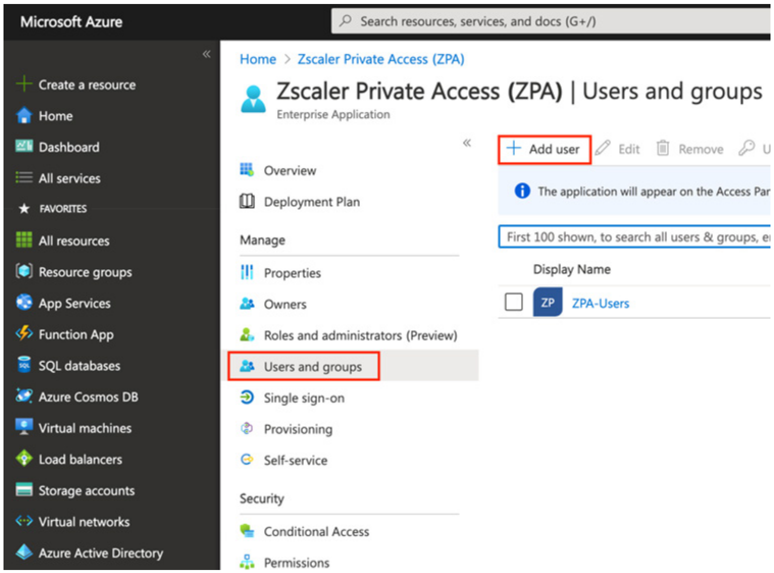
License
Azure AD Premium P2

Tenant ID
045989c5-04a4-431b-8c19-e3e9...

Primary domain
testmypacket.onmicrosoft.com

Figure 76. Select the ZPA from enterprise applications

3. Select **Users and groups**.
4. Select **Add User**.

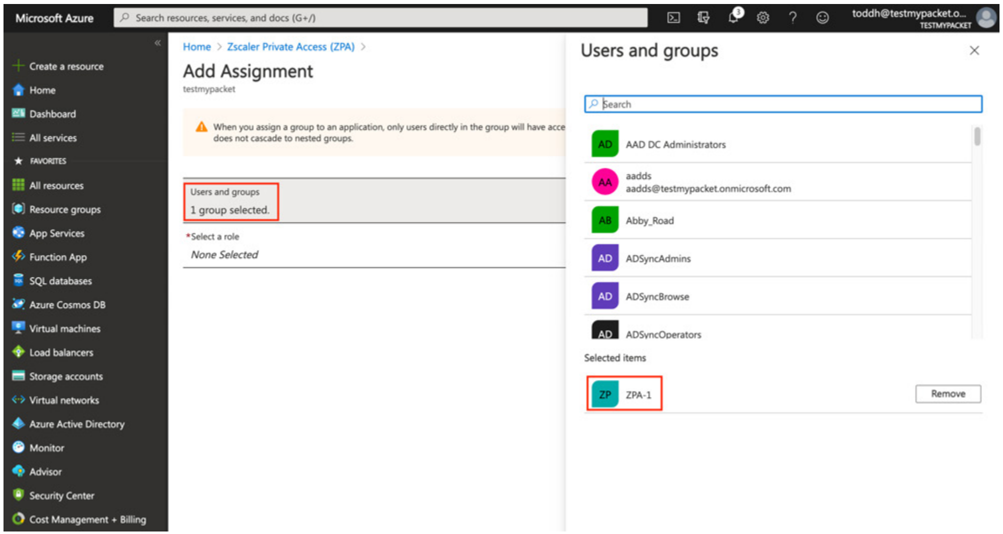


The application will appear on the Access Par

First 100 shown, to search all users & groups, e

Figure 77. Add User

5. Select **Users and groups**.
6. Search and select the Microsoft Entra ID group that you want to map to the role, in this case ZAP-1.
7. Click **Select** at the bottom of the page.



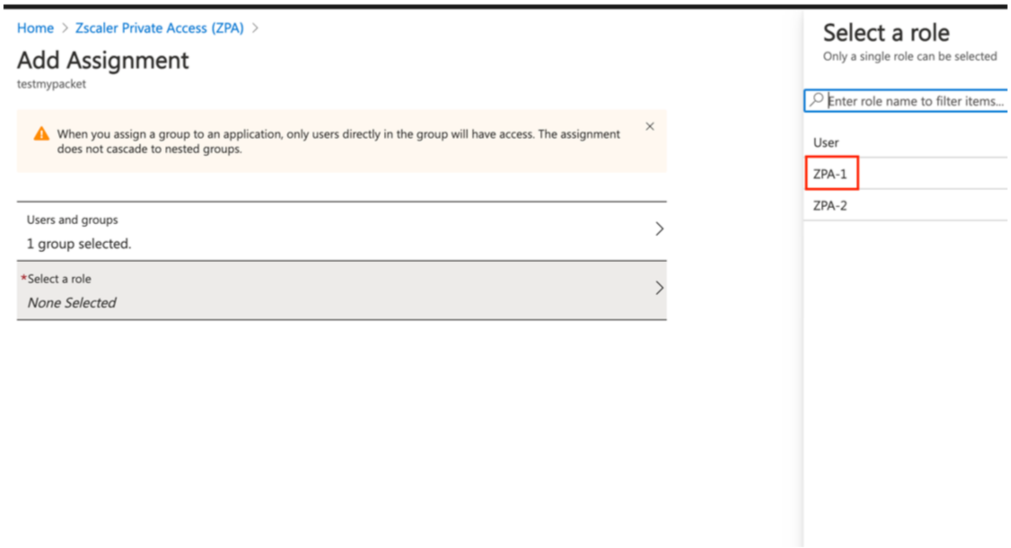
When you assign a group to an application, only users directly in the group will have acce does not cascade to nested groups.

Users and groups
1 group selected.

*Select a role
None Selected

Figure 78. Add assignment

8. Click **Select a role** to display the roles that you created. You can see the role that matches the name of our Microsoft Entra ID group, in this case ZPA-1.
9. Click **Select**, located at the bottom of the page.
10. Click **Assign** to finish the mapping.
11. Repeat similar steps for ZPA-2.


Home > Zscaler Private Access (ZPA) >

Add Assignment

testmypacket

When you assign a group to an application, only users directly in the group will have access. The assignment does not cascade to nested groups.

Users and groups

1 group selected.

*Select a role

None Selected

Select a role

Only a single role can be selected

Enter role name to filter items...

User

ZPA-1

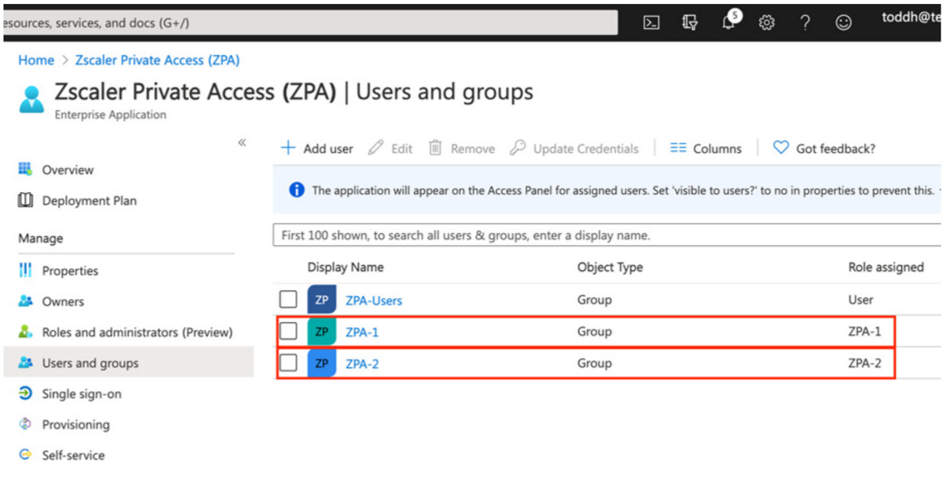
ZPA-2

Figure 79. Select the role

Review the ZPA Role Mapping for Microsoft Entra ID Groups

The image shows that groups are mapped to a role, and a user that is a part of a group with usable group names is shown in the Users SAML response, and the role can be applied to ZPA policies.

Next, clean up unreadable groups and add a department variable by updating the SAML attributes.



Zscaler Private Access (ZPA) | Users and groups

Enterprise Application

The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this.

First 100 shown, to search all users & groups, enter a display name.

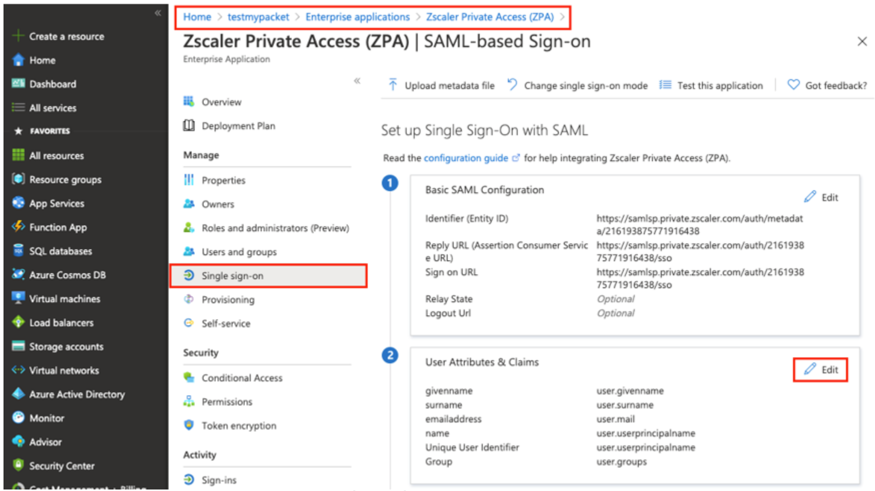
Display Name	Object Type	Role assigned
☐ ZP ZPA-Users	Group	User
☐ ZP ZPA-1	Group	ZPA-1
☐ ZP ZPA-2	Group	ZPA-2

Figure 80. Review the mappings

Mapping the Group SAML Attribute

Open the Attribute editor to edit the SAML variables that are returned in the SAML assertion.

1. Select **Microsoft Entra ID** > **Enterprise applications** > **Zscaler Private Access (ZPA)**.
2. Select **Single sign-on**.
3. Click **Edit** in the **User Attributes & Claims** area.



Zscaler Private Access (ZPA) | SAML-based Sign-on

Enterprise Application

Set up Single Sign-On with SAML

Read the configuration guide for help integrating Zscaler Private Access (ZPA).

1 Basic SAML Configuration

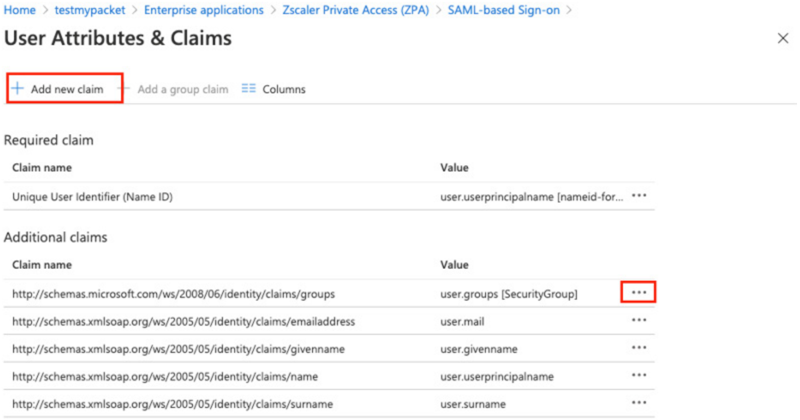
Identifier (Entity ID)	https://samlsp.private.zscaler.com/auth/metadata/216193875771916438
Reply URL (Assertion Consumer Service URL)	https://samlsp.private.zscaler.com/auth/216193875771916438/sso
Sign on URL	https://samlsp.private.zscaler.com/auth/216193875771916438/sso
Relay State	Optional
Logout Url	Optional

2 User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
Group	user.groups

Figure 81. SAML attribute mapping (1 of 5)

4. The user.groups [SecurityGroup] is the attribute that returns unusable group names in the SAML assertion. Let's delete it and add a new claim to be returned in the SAML assertion:
   a. Select the three dots next to the `user.groups [SecurityGroup]` value and delete the claim.
   b. Select **Add new claim** to open the **Manage claim** window.


Home > testmypacket > Enterprise applications > Zscaler Private Access (ZPA) > SAML-based Sign-on >
Add new claim
Add a group claim
Columns

User Attributes & Claims

Required claim

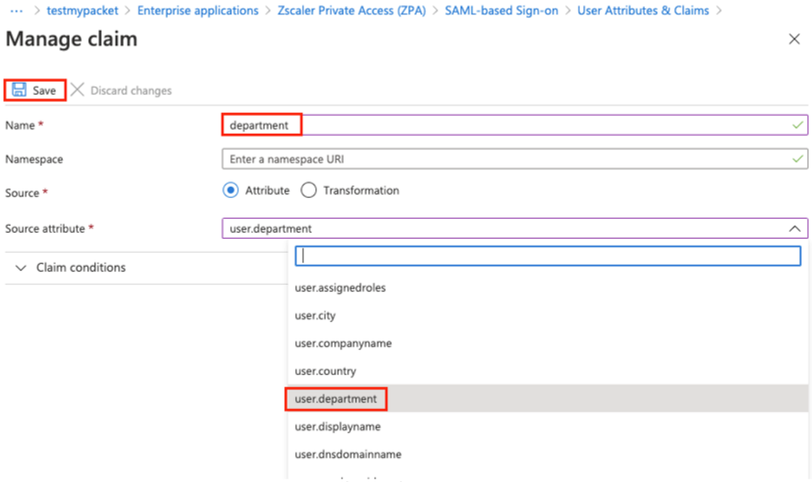
Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... •••

Additional claims

Claim name	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	user.groups [SecurityGroup] •••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail •••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname •••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname •••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname •••

Figure 82. SAML attribute mapping (2 of 5)

5. To create a new claim, you must map the source attribute to a variable name. The claim name is the attribute field, and the source is the variable that is populated by the user's department:
   a. Name the `Claim` department.
   b. Select **Attribute** as the **Source**.
   c. Select **user.department** as the **Source** attribute.
   d. **Save** your changes.



… > testmypacket > Enterprise applications > Zscaler Private Access (ZPA) > SAML-based Sign-on > User Attributes & Claims >

Manage claim

Save | Discard changes

Name *: department

Namespace: Enter a namespace URI

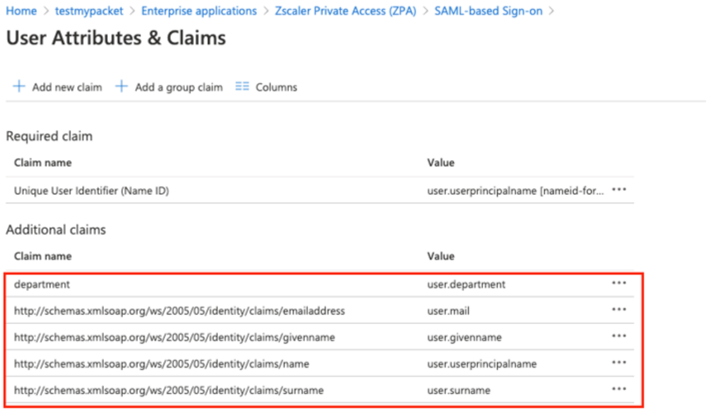
Source *: ● Attribute ○ Transformation

Source attribute *: user.department

Claim conditions

Figure 83. SAML attribute mapping (3 of 5)

6. You can see your completed SAML attribute changes.



Home > testmypacket > Enterprise applications > Zscaler Private Access (ZPA) > SAML-based Sign-on >

User Attributes & Claims

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... ···

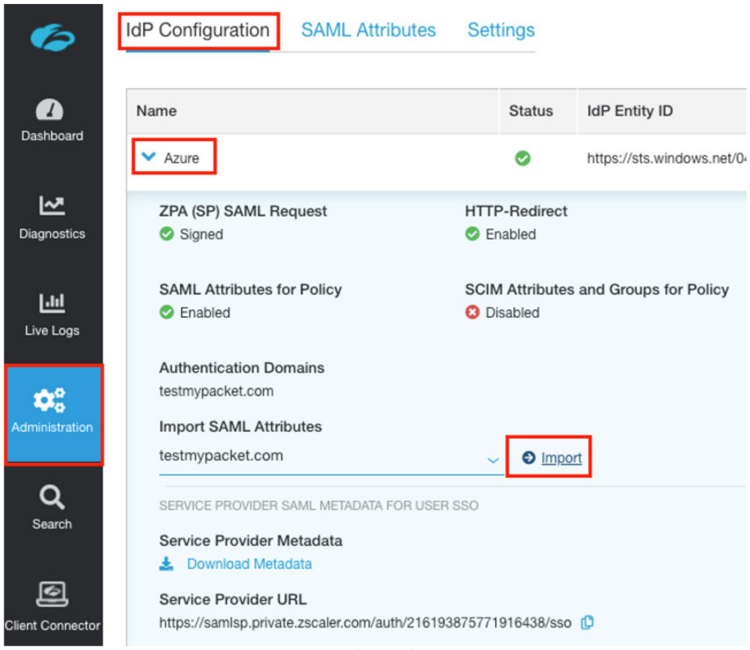
Additional claims

Claim name	Value
department	user.department ···
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail ···
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ···
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ···
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname ···

Figure 84. SAML attribute mapping (4 of 5)

7. Open the ZPA tenant and import the new attributes to be used in policies:
   a. Open the ZPA Admin Portal and enter the administrator credentials.

8. Rename the SAML Attribute name to be intuitive to the policy. Find the role Attribute and change the name to Microsoft Entra ID Groups.
   a. Select **Administrator** > **IdP Configuration**.
   b. Select the **Azure IdP**.
   c. Click the **blue arrow** to open the IdP detail.
   d. Click **Import**.



Name	Status	IdP Entity ID
Azure	✓	https://sts.windows.net/0

ZPA (SP) SAML Request
✓ Signed

HTTP-Redirect
✓ Enabled

SAML Attributes for Policy
✓ Enabled

SCIM Attributes and Groups for Policy
✕ Disabled

Authentication Domains
testmypacket.com

Import SAML Attributes
testmypacket.com

SERVICE PROVIDER SAML METADATA FOR USER SSO

Service Provider Metadata

Service Provider URL
https://samlsp.private.zscaler.com/auth/216193875771916438/sso

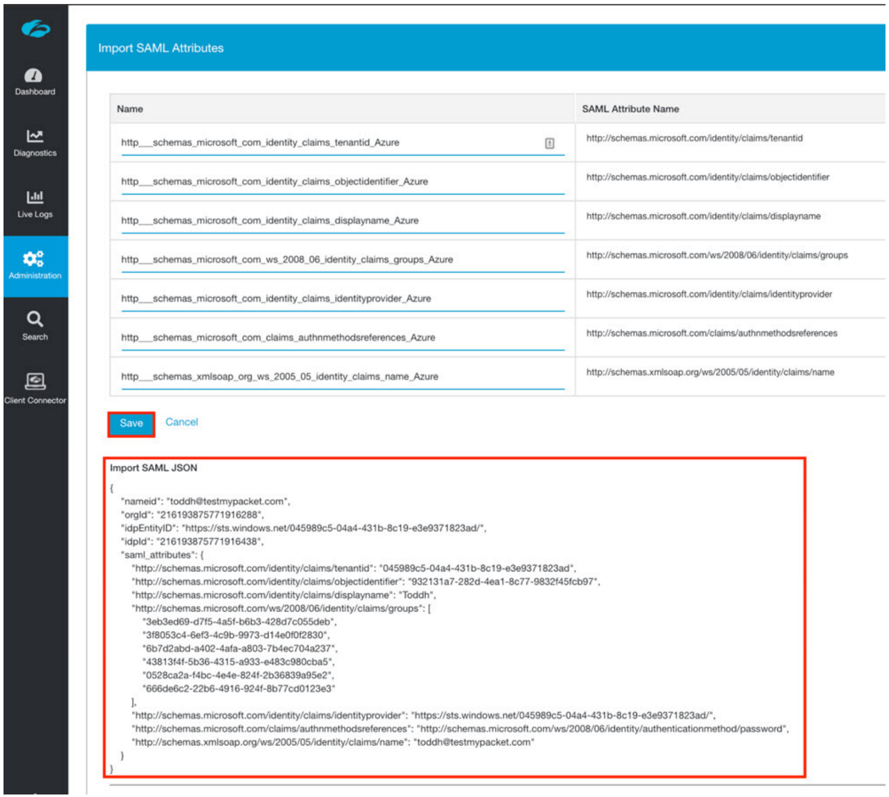
Figure 85. SAML attribute mapping (5 of 5)

ZPA Role Mapping SAML Assertion

You can see the SAML assertion that includes our ZPA groups and department.

Rename the SAML attributes to be intuitive to the policy. Find the role **Attribute** and change the name to `Groups` and find the department attribute and name it `Department`.

1. Rename the **Attributes** to be more intuitive.
2. **Save** the configuration.



Import SAML Attributes

Name	SAML Attribute Name
http___schemas_microsoft_com_identity_claims_tenantid_Azure	http://schemas.microsoft.com/identity/claims/tenantid
http___schemas_microsoft_com_identity_claims_objectidentifier_Azure	http://schemas.microsoft.com/identity/claims/objectidentifier
http___schemas_microsoft_com_identity_claims_displayname_Azure	http://schemas.microsoft.com/identity/claims/displayname
http___schemas_microsoft_com_ws_2008_06_identity_claims_groups_Azure	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
http___schemas_microsoft_com_identity_claims_identityprovider_Azure	http://schemas.microsoft.com/identity/claims/identityprovider
http___schemas_microsoft_com_claims_authnmethodsreferences_Azure	http://schemas.microsoft.com/claims/authnmethodsreferences
http___schemas_xmlsoap_org_ws_2005_05_identity_claims_name_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

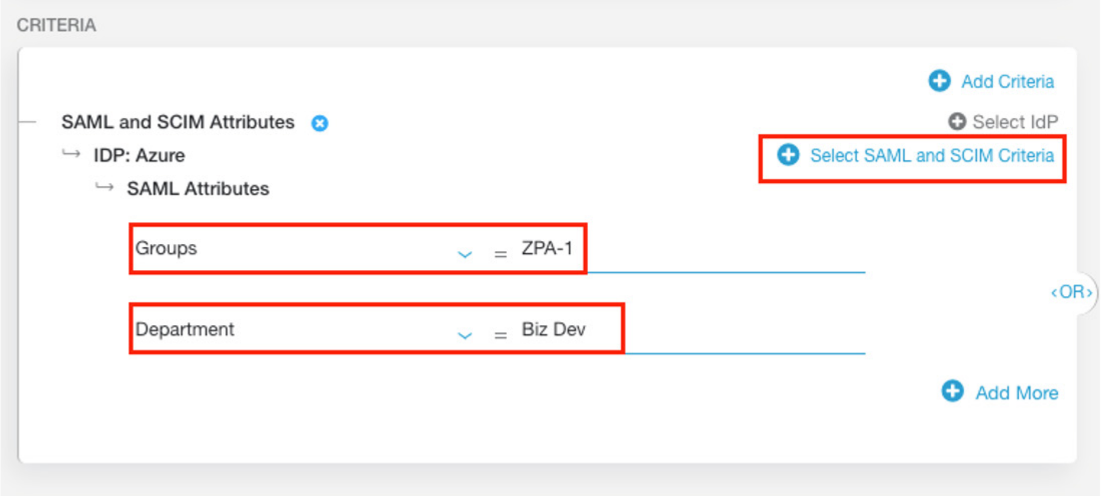
Import SAML JSON

```
{
  "nameid": "toddh@testmypacket.com",
  "orgId": "216193875771916288",
  "idpEntityID": "https://sts.windows.net/045989c5-04a4-431b-8c19-e3e9371823ad/",
  "idpId": "216193875771916438",
  "saml_attributes": {
    "http://schemas.microsoft.com/identity/claims/tenantid": "045989c5-04a4-431b-8c19-e3e9371823ad",
    "http://schemas.microsoft.com/identity/claims/objectidentifier": "932131a7-282d-4ea1-8c77-9832f45fcb97",
    "http://schemas.microsoft.com/identity/claims/displayname": "Toddh",
    "http://schemas.microsoft.com/ws/2008/06/identity/claims/groups": [
      "3eb3ed69-d7f5-4a5f-b6b3-428d7c055deb",
      "3f8053c4-6ef3-4c9b-9973-d14e0f0f2830",
      "6b7d2abd-a402-4afa-a803-7b4ec704a237",
      "43813f4f-5b36-4315-a933-e483c980cba5",
      "0528ca2a-f4bc-4e4e-824f-2b36839a95e2",
      "666de6c2-22b6-4916-924f-8b77cd0123e3"
    ],
    "http://schemas.microsoft.com/identity/claims/identityprovider": "https://sts.windows.net/045989c5-04a4-431b-8c19-e3e9371823ad/",
    "http://schemas.microsoft.com/claims/authnmethodsreferences": "http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password",
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name": "toddh@testmypacket.com"
  }
}
```

Figure 86. SAML assertion with ZPA groups

Configure ZPA Role Mapping for Microsoft Entra ID Groups

The SAML attribute can be used to create policies in ZPA.



Groups = ZPA-1

Department = Biz Dev

Figure 87. Policy with attribute selected

ZIA SAML Admin Authentication

By adding access to SAML Authentication for Zscaler Administrator, you enable ZIA administrators to connect to the ZIA tenant using single sign-on from the My-Apps Azure portal. The ZIA admins, authenticate using Microsoft Entra ID.

To add the ZIA Administrator App:

1. Select **Microsoft Entra ID** > **Enterprise applications** > **All applications**.
2. Select **New applications**.

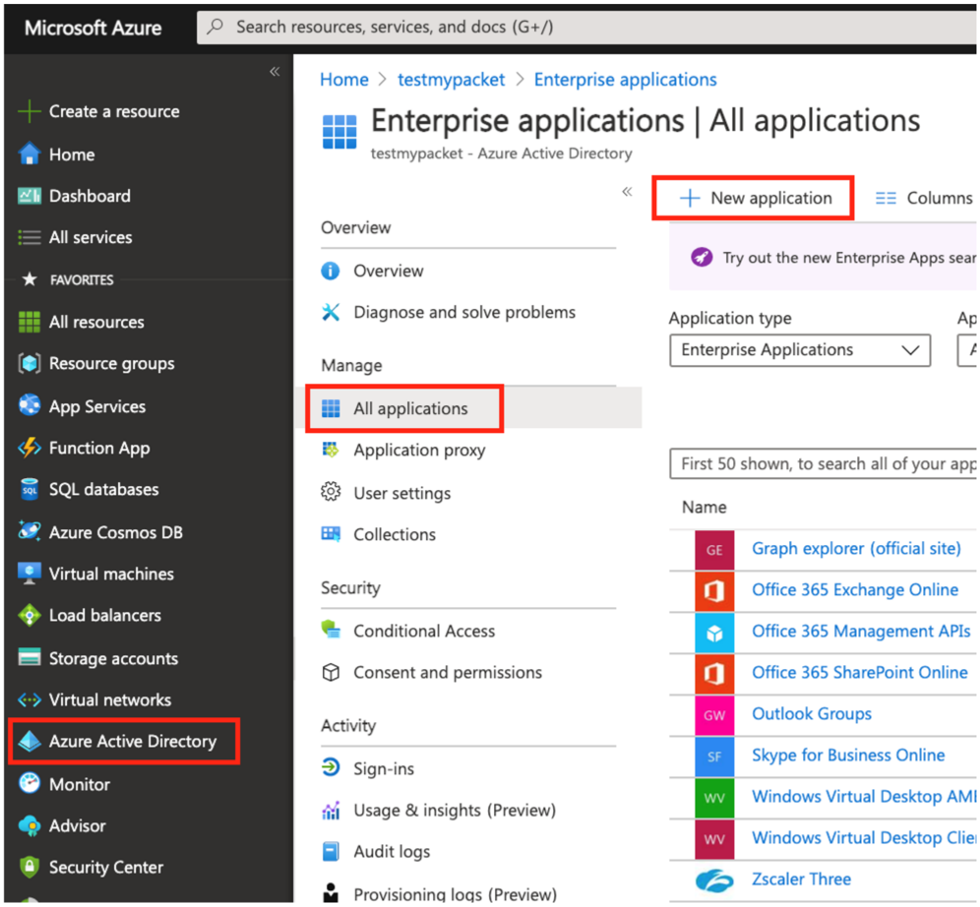

Microsoft Azure
Search resources, services, and docs (G+/)
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Home > testmypacket > Enterprise applications
Enterprise applications | All applications
testmypacket - Azure Active Directory
Overview
Overview
Diagnose and solve problems
Manage
All applications
Application proxy
User settings
Collections
Security
Conditional Access
Consent and permissions
Activity
Sign-ins
Usage & insights (Preview)
Audit logs
Provisioning logs (Preview)
New application
Columns
Try out the new Enterprise Apps sear
Application type
Enterprise Applications
Ap
First 50 shown, to search all of your app
Name
GE Graph explorer (official site)
Office 365 Exchange Online
Office 365 Management APIs
Office 365 SharePoint Online
GW Outlook Groups
SF Skype for Business Online
WV Windows Virtual Desktop AMI
WV Windows Virtual Desktop Clie
Zscaler Three

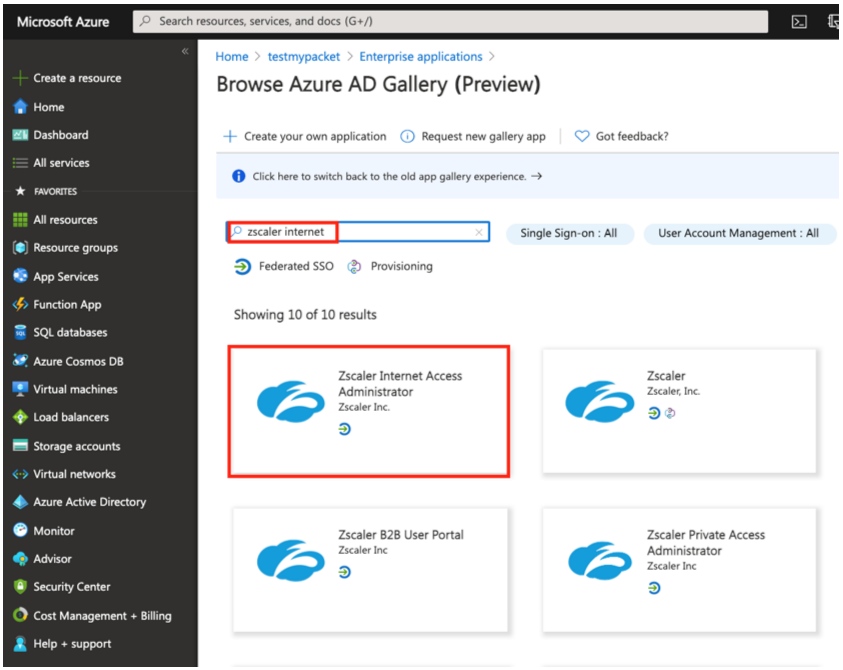
Figure 88. Adding the application for SAML admin access

This launches the **Microsoft Entra ID Application Gallery**.

SAML Authentication for ZIA Admin Access

Search for “zscaler internet”, and select the **Zscaler Internet Access Administrator** application.

1. Search for `zscaler internet`.
2. Select the **Zscaler Internet Access Administrator** application.



Browse Azure AD Gallery (Preview)

Click here to switch back to the old app gallery experience. →

zscaler internet

Showing 10 of 10 results

Zscaler Internet Access Administrator
Zscaler Inc.

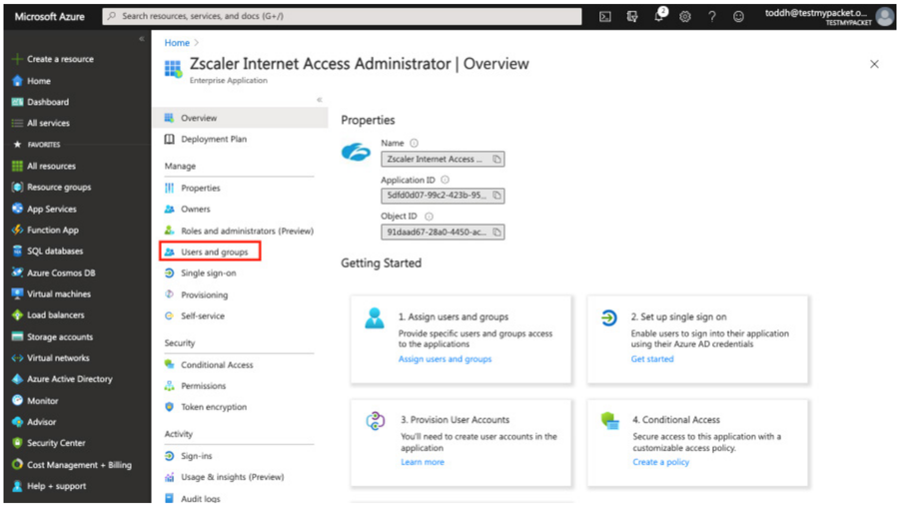
Zscaler
Zscaler, Inc.

Zscaler B2B User Portal
Zscaler Inc

Zscaler Private Access Administrator
Zscaler Inc

Figure 89. Administrator application

3. First, assign administrators to the application accessing the ZIA tenant.
4. Select **Users and group**.



Zscaler Internet Access Administrator | Overview
Enterprise Application

Properties

Name: Zscaler Internet Access ...

Application ID: 5dfd0d07-99c2-423b-95...

Object ID: 91daad67-28a0-4450-ac...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

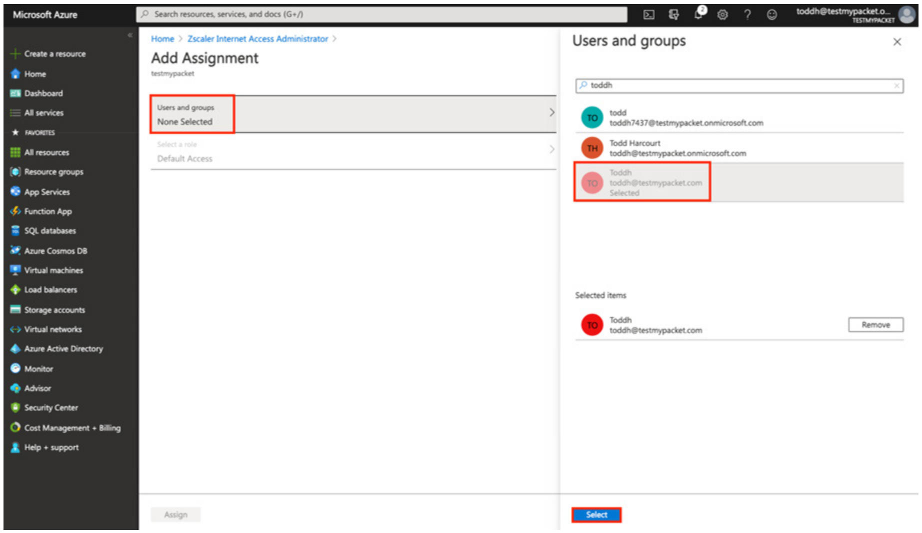
2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

3. Provision User Accounts
You'll need to create user accounts in the application
Learn more

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

Figure 90. Add ZIA administrators

5. Add the Administrators and Groups that contain your Zscaler Administrators, and click **Select**.



Add Assignment
testmypacket

Users and groups
None Selected

Select a role
Default Access

Users and groups

toddh

TO todd
toddh7437@testmypacket.onmicrosoft.com

TH Todd Harcourt
toddh@testmypacket.onmicrosoft.com

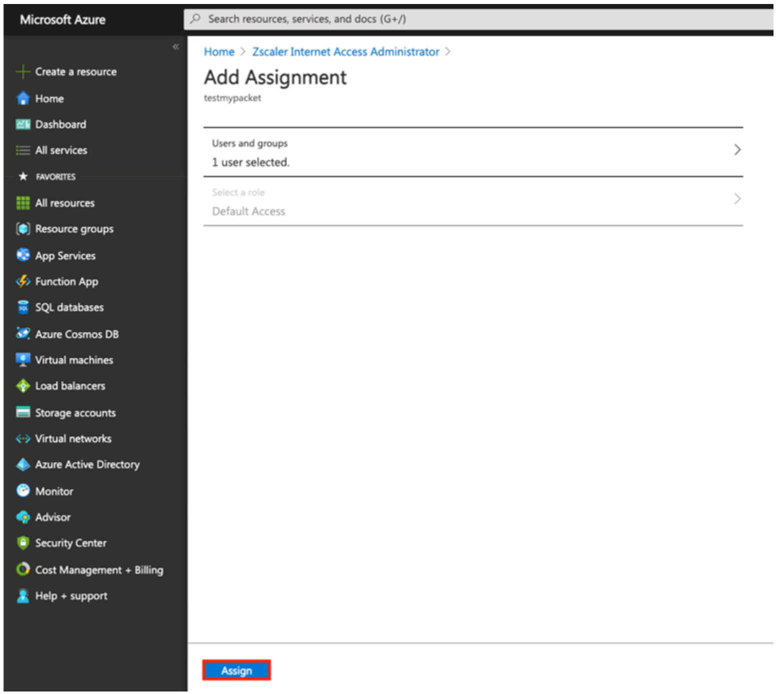
TO Toddh
toddh@testmypacket.com
Selected

Selected items

TO Toddh
toddh@testmypacket.com

Figure 91. *Add ZIA Administrators*

6. Click **Assign**.



Add Assignment
testmypacket

Users and groups
1 user selected.

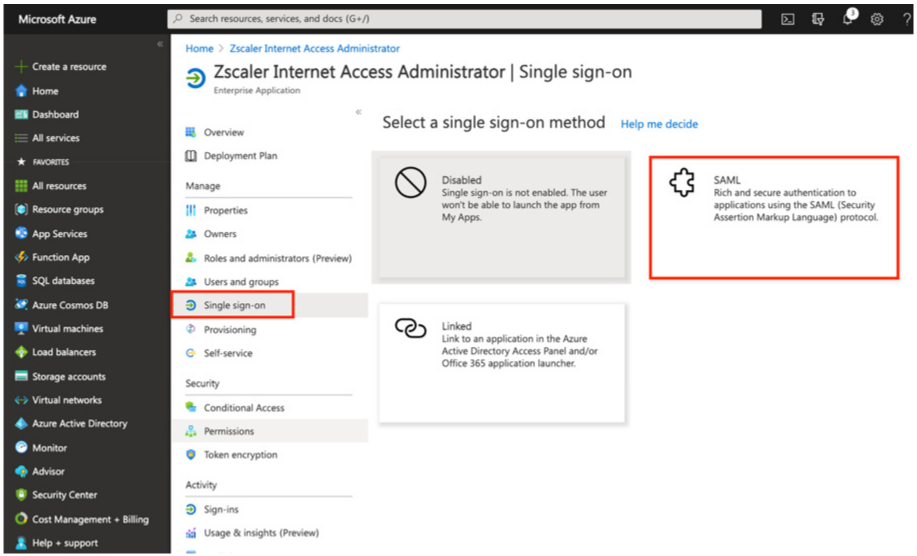
Select a role
Default Access

Figure 92. *Assign Administrators*

SAML Settings for ZIA Portal Admin Access

Configure SAML:

1. Select **Single sign-on** in the **Manage** section of the application.
2. Select the **SAML** tile.



Zscaler Internet Access Administrator | Single sign-on

Enterprise Application

Select a single sign-on method

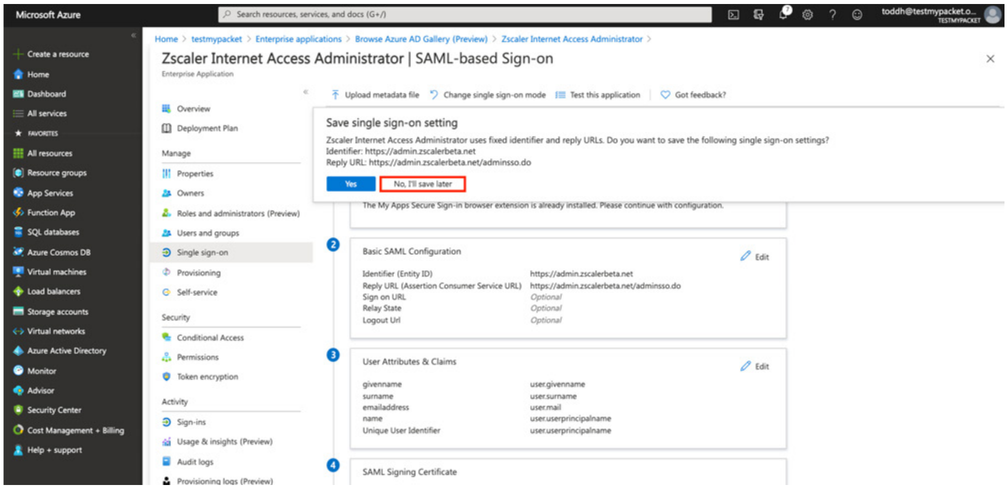
Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Linked
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

Figure 93. *Configure SAML*

3. Select **No I'll save later** at the prompt.



Zscaler Internet Access Administrator | SAML-based Sign-on

Enterprise Application

Save single sign-on setting

Zscaler Internet Access Administrator uses fixed identifier and reply URLs. Do you want to save the following single sign-on settings?
Identifier: https://admin.zscalerbeta.net
Reply URL: https://admin.zscalerbeta.net/adminsso.do

The My Apps Secure Sign-in browser extension is already installed. Please continue with configuration.

Basic SAML Configuration

Identifier (Entity ID)	https://admin.zscalerbeta.net
Reply URL (Assertion Consumer Service URL)	https://admin.zscalerbeta.net/adminsso.do
Sign on URL	*Optional*
Relay State	*Optional*
Logout Url	*Optional*

User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

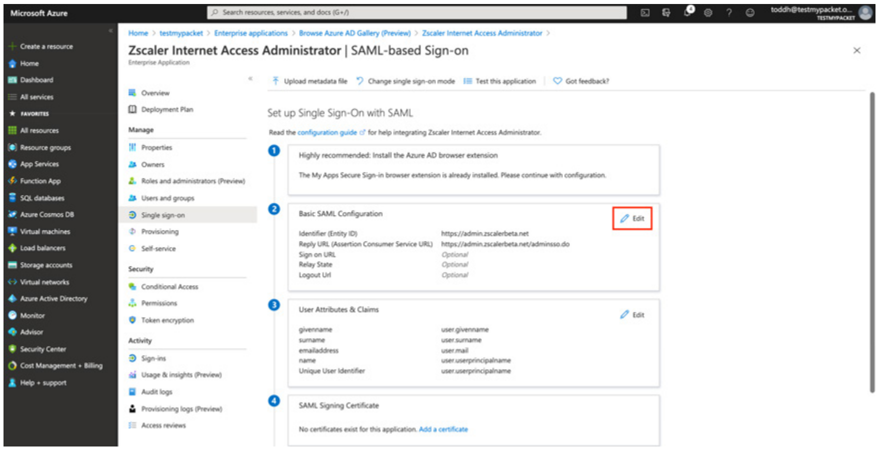
SAML Signing Certificate

Figure 94. *Configure SAML*

Configure Basic SAML Detail

To configure SAML details:

1. Select **Edit** under **Basic SAML Configuration**.



Zscaler Internet Access Administrator | SAML-based Sign-on

Enterprise Application

Set up Single Sign-On with SAML

Read the configuration guide for help integrating Zscaler Internet Access Administrator.

1 Highly recommended: Install the Azure AD browser extension

The My Apps Secure Sign-in browser extension is already installed. Please continue with configuration.

2 Basic SAML Configuration

Identifier (Entity ID)	https://admin.zscalerbeta.net
Reply URL (Assertion Consumer Service URL)	https://admin.zscalerbeta.net/adminsso.do
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

3 User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

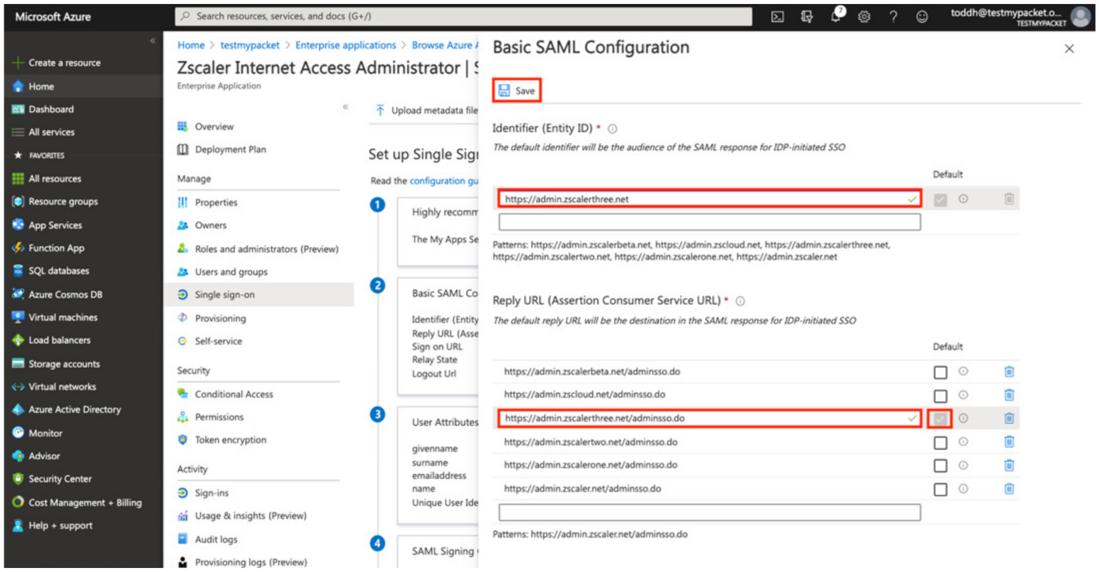
4 SAML Signing Certificate

No certificates exist for this application. Add a certificate

Figure 95. Configure Basic SAML

Under the **Entity ID** enter the ZIA administrator portal URL for the cloud that hosts your ZIA Tenant. The Zscaler cloud continues to expand, but currently it is one of the following cloud domains: zscaler.net, zscalerone.net, zscalertwo.net, zscalerthree.net, or zscloud.net. This information can be found in your ZIA Admin Portal under **Administration** > **Company Profile** > **Company ID**. In the following Company ID example (zscalerthree.net-3173833), zscalerthree.net is the Zscaler Cloud.

2. Enter `https://admin.zscalerthree.net` as the **EntityID**.
3. Select `https://login.zscalerthree.net/adminsso.do` for the **Reply URL**.
4. Make sure the check marks are selected on the new entries.
5. Select **Save** to save the configuration.
6. Replace “zscalerthree.net” with your ZIA cloud if it is different.



Basic SAML Configuration

Save

Identifier (Entity ID) * ⓘ

The default identifier will be the audience of the SAML response for IDP-initiated SSO

	Default
https://admin.zscalerthree.net ✓	☑

Patterns: https://admin.zscalerbeta.net, https://admin.zscloud.net, https://admin.zscalerthree.net, https://admin.zscalertwo.net, https://admin.zscalerone.net, https://admin.zscaler.net

Reply URL (Assertion Consumer Service URL) * ⓘ

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

	Default
https://admin.zscalerbeta.net/adminsso.do	☐
https://admin.zscloud.net/adminsso.do	☐
https://admin.zscalerthree.net/adminsso.do ✓	☑
https://admin.zscalertwo.net/adminsso.do	☐
https://admin.zscalerone.net/adminsso.do	☐
https://admin.zscaler.net/adminsso.do	☐

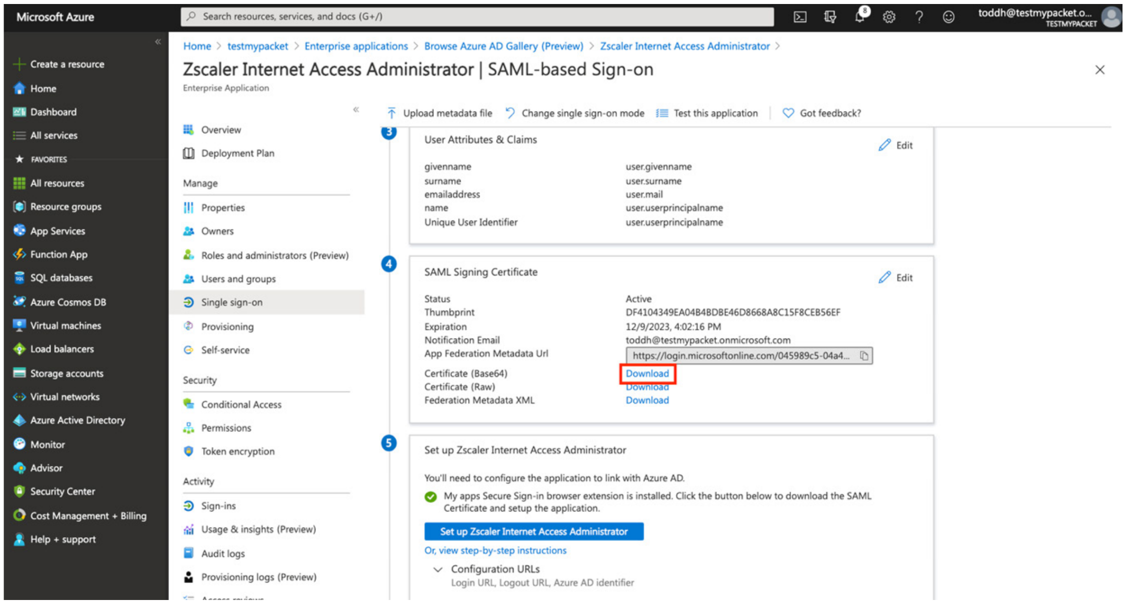
Patterns: https://admin.zscaler.net/adminsso.do

Figure 96. Configure basic SAML

Download and Save the Azure Signing Certificate

Saving the configuration creates the SAML Signing Certificate. It is unique to this portal.

1. Download the Base64 Certificate and save it for next steps.
2. Open the ZIA Admin Portal. `https://admin.zscalerthree.net` as an example of your cloud admin portal.



Zscaler Internet Access Administrator | SAML-based Sign-on
Enterprise Application

3 User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

4 SAML Signing Certificate

Status	Active
Thumbprint	DF4104349EA04B4BDBE46D8668A8C15F8CEB56EF
Expiration	12/9/2023, 4:02:16 PM
Notification Email	toddh@testmypacket.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/045989c5-04a4...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

5 Set up Zscaler Internet Access Administrator

You'll need to configure the application to link with Azure AD.

My apps Secure Sign-in browser extension is installed. Click the button below to download the SAML Certificate and setup the application.

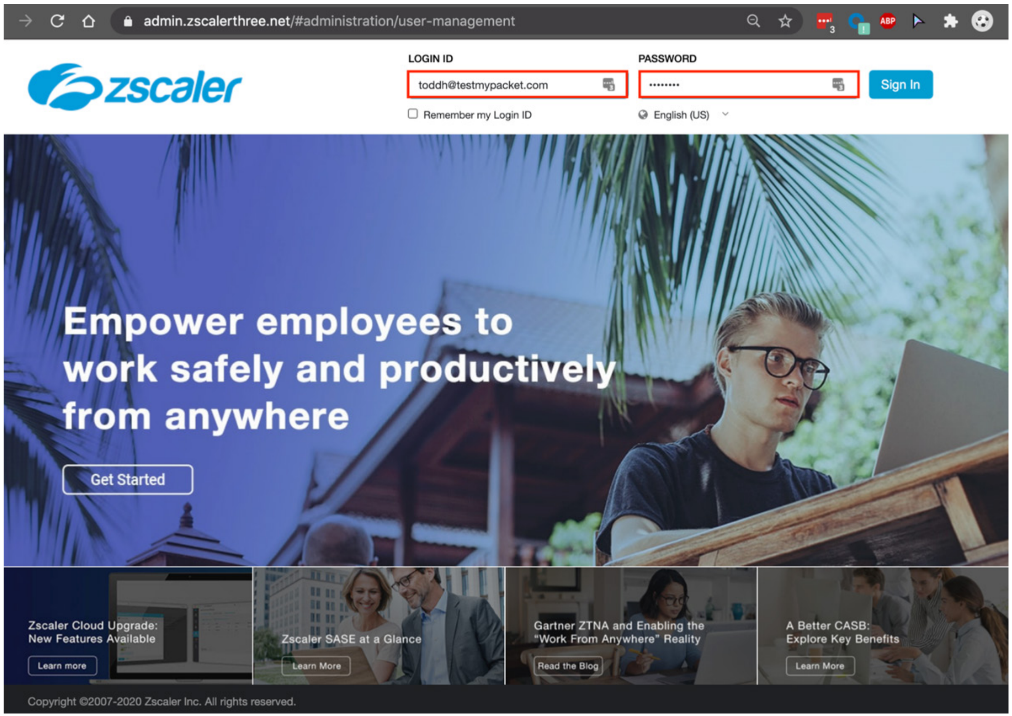
Or, view step-by-step instructions

Configuration URLs
Login URL, Logout URL, Azure AD identifier

Figure 97. Azure SAML signing certificate

Configure Zscaler for SAML Admin Access

Log in to your ZIA Admin Portal with your administrator credentials.


zscaler
Sign In
English (US)
Empower employees to work safely and productively from anywhere
Get Started
Zscaler Cloud Upgrade: New Features Available
Learn more
Zscaler SASE at a Glance
Learn More
Gartner ZTNA and Enabling the "Work From Anywhere" Reality
Read the Blog
A Better CASB: Explore Key Benefits
Learn More
Copyright ©2007-2020 Zscaler Inc. All rights reserved.

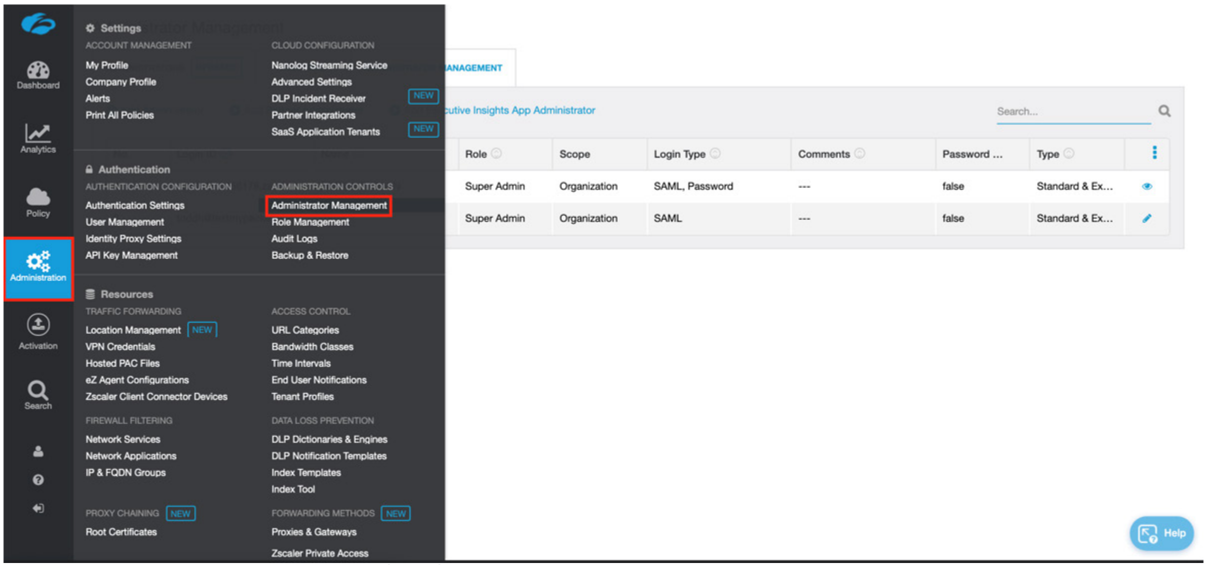
admin.zscalerthree.net/#administration/user-management

LOGIN ID: toddh@testmypacket.com
PASSWORD: ••••••••
□ Remember my Login ID

Figure 98. ZIA Admin Portal

Configure Zscaler to use SAML for Admin Accounts

Select **Administrator** > **Administrator Management**.



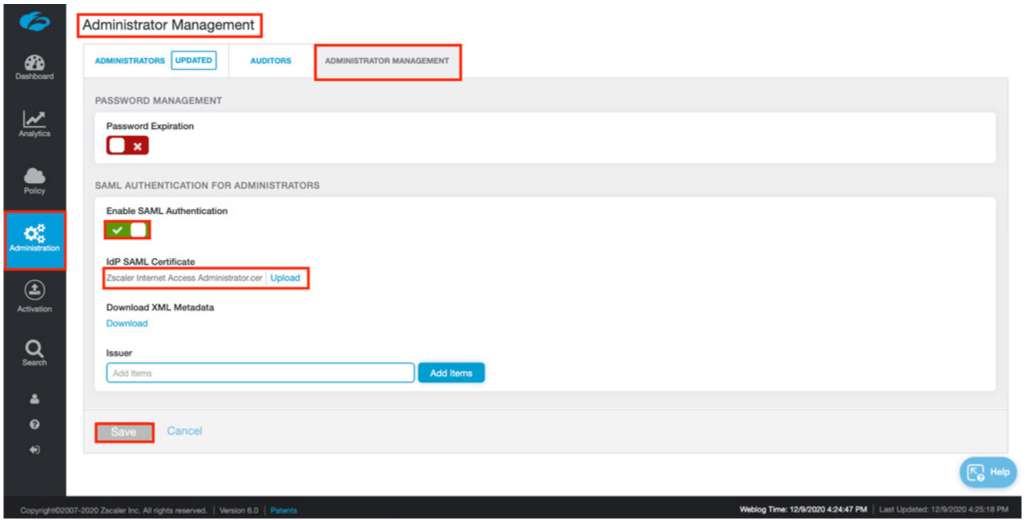
Role	Scope	Login Type	Comments	Password ...	Type
Super Admin	Organization	SAML, Password	---	false	Standard & Ex...
Super Admin	Organization	SAML	---	false	Standard & Ex...

Figure 99. Administrator Management (1 of 2)

Configure Zscaler Details to Use SAML for Admin Accounts

To configure Zscaler SAML administrator details:

1. Select the **Administrator Management** tab.
2. Select **Enable SAML Authentication**.
3. Upload the certificate that you downloaded in the previous step.
4. Select **Save**.



PASSWORD MANAGEMENT

Password Expiration ☒

SAML AUTHENTICATION FOR ADMINISTRATORS

Enable SAML Authentication ✓

IdP SAML Certificate: Zscaler Internet Access Administrator.cer | Upload

Download XML Metadata: Download

Issuer: Add Items

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents

Weblog Time: 12/9/2020 4:24:47 PM | Last Updated: 12/9/2020 4:25:18 PM

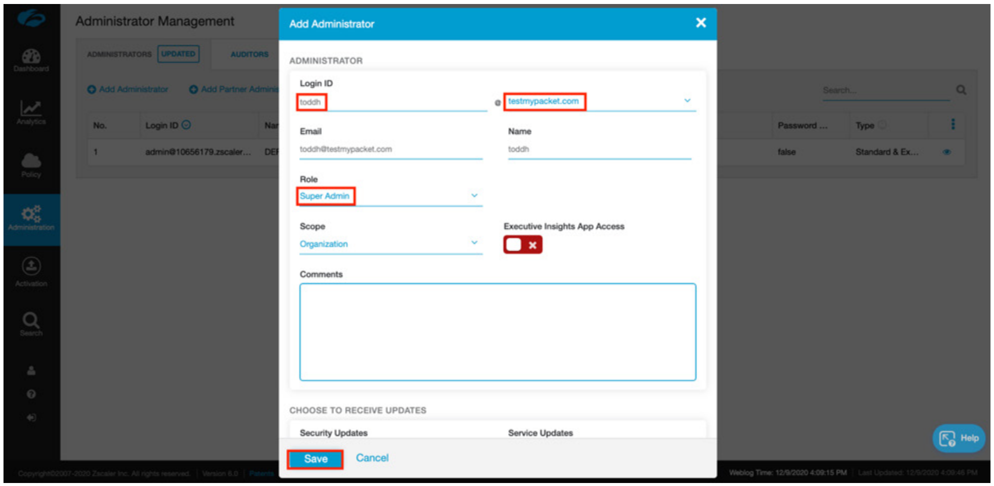
Figure 100. Administrator Management (2 of 2)

In the final step you create the administrators on Zscaler using the portal and SAML authentication.

Configure Admin Users for SAML Admin Access

To add administrators:

1. Select the **Administrators** tab.
2. Select **Add Administrator.**
3. Add the **Login ID** of the administrator.
4. Select an administrator role.
5. Select **Save**.



Add Administrator

ADMINISTRATOR

Login ID: toddh @ testmypacket.com

Email: toddh@testmypacket.com

Name: toddh

Role: Super Admin

Scope: Organization

Executive Insights App Access: ☒

Comments:

CHOOSE TO RECEIVE UPDATES

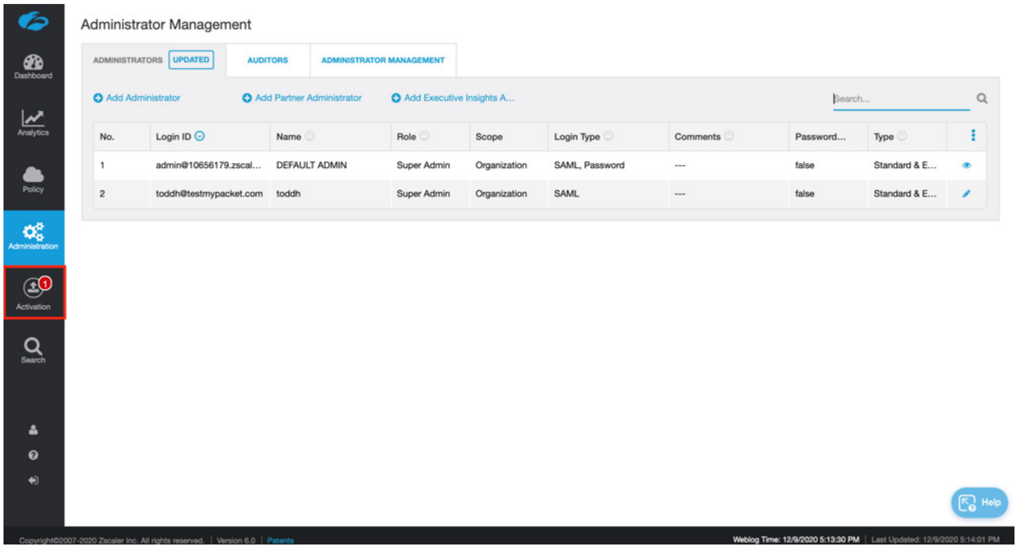
Security Updates

Service Updates

Figure 101. Add administrators

The administrator domain must use the domain that is supported by Microsoft Entra ID.

6. **Activate** the changes.



Administrator Management

No.	Login ID	Name	Role	Scope	Login Type	Comments	Password...	Type
1	admin@10656179.zscal...	DEFAULT ADMIN	Super Admin	Organization	SAML, Password	---	false	Standard & E...
2	toddh@testmypacket.com	toddh	Super Admin	Organization	SAML	---	false	Standard & E...

Figure 102. Activate the Changes

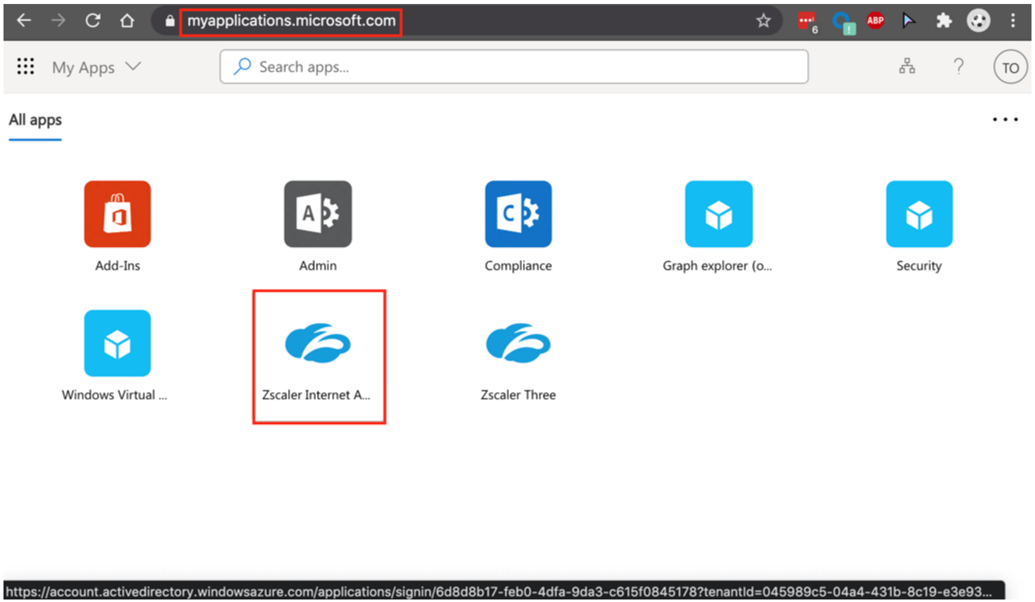
SAML Admin Access from Microsoft My Apps

From My Apps select the Zscaler Internet Admin icon to launch and automatically sign in to the ZIA Admin Portal. You can also test your access by using your Portal URL with a SAML-only user.

1. Launch **My Apps** at myapplications.microsoft.com.
2. Select the ZIA application.

In this exercise, you access ZIA Admin Portal for the Zscaler Three Cloud:

https://admin.zscalerthree.net



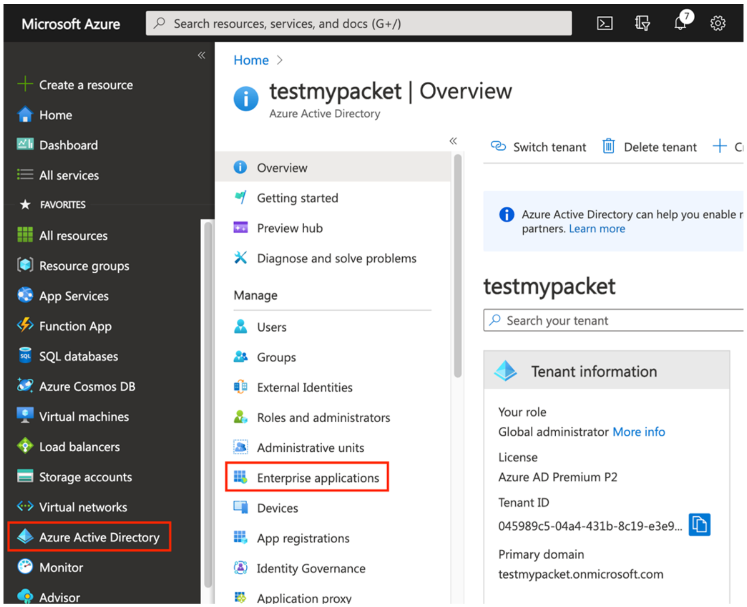
https://account.activedirectory.windowsazure.com/applications/signin/6d8d8b17-feb0-4dfa-9da3-c615f0845178?tenantId=045989c5-04a4-431b-8c19-e3e93...

Figure 103. Microsoft My-Apps

ZPA SAML Admin Authentication

To enable SAML authentication for ZPA administrators when accessing the ZPA tenant, you must install and configure the ZPA Administrator application from the Microsoft Entra ID Application Gallery.

To start the installation process, select **Microsoft Entra ID** > **Enterprise applications**.



Your role
Global administrator More info

License
Azure AD Premium P2

Tenant ID
045989c5-04a4-431b-8c19-e3e9...

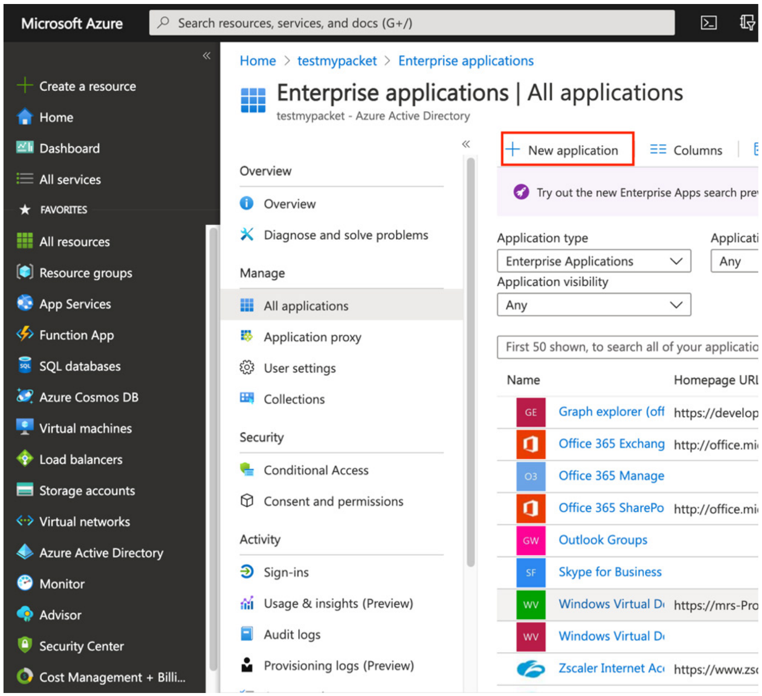
Primary domain
testmypacket.onmicrosoft.com

Figure 104. Add SAML admin application

Add the Zscaler Private Access Administrator Application

To add a ZPA admin application:

1. Select **New application**.



Application type: Enterprise Applications

Applicati: Any

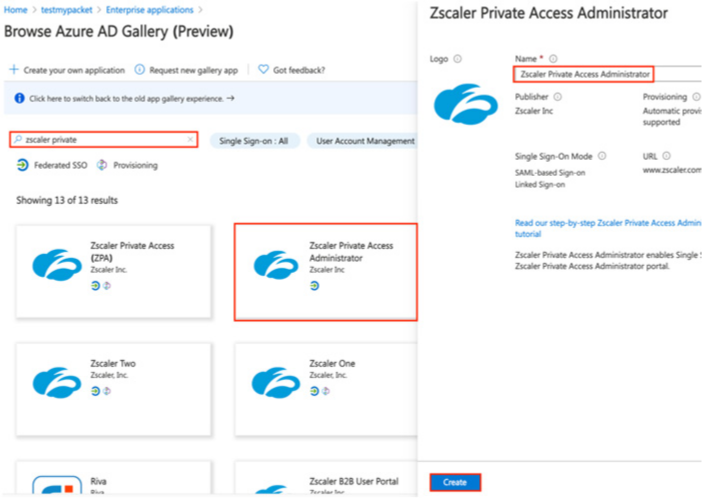
Application visibility: Any

First 50 shown, to search all of your applicatio

	Name	Homepage URL
GE	Graph explorer (off	https://develop
	Office 365 Exchang	http://office.mi
O3	Office 365 Manage	
	Office 365 SharePo	http://office.mi
GW	Outlook Groups	
SF	Skype for Business	
WV	Windows Virtual D	https://mrs-Pro
WV	Windows Virtual D	
	Zscaler Internet Ac	https://www.zs

Figure 105. Add new application

2. Search for `zscaler private access`.
3. Select the **Zscaler Private Access Administrator** tile.
4. Click **Create**.



Home > testmypacket > Enterprise applications >
Browse Azure AD Gallery (Preview)
+ Create your own application
Request new gallery app
Got feedback?
Click here to switch back to the old app gallery experience. →
Single Sign-on : All
User Account Management
Federated SSO
Provisioning
Zscaler Private Access (ZPA)
Zscaler Inc.
Zscaler Private Access Administrator
Zscaler Inc
Zscaler Two
Zscaler, Inc.
Zscaler One
Zscaler, Inc.
Riva
Zscaler B2B User Portal
Zscaler Private Access Administrator
Logo
Create

zscaler private

Showing 13 of 13 results

Name * : Zscaler Private Access Administrator

Publisher: Zscaler Inc

Provisioning: Automatic provi supported

Single Sign-On Mode: SAML-based Sign-on, Linked Sign-on

URL: www.zscaler.com

Read our step-by-step Zscaler Private Access Admin tutorial

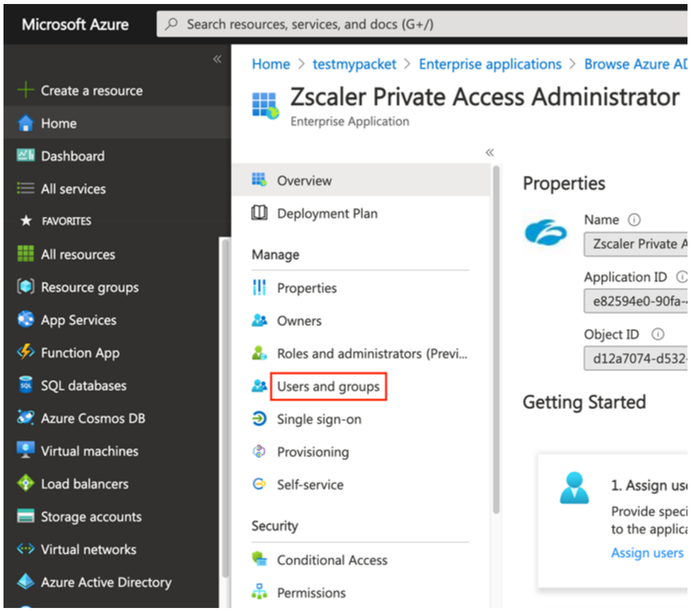
Zscaler Private Access Administrator enables Single Zscaler Private Access Administrator portal.

Figure 106. Zscaler Private Access Administrator app

Assign the Admin Accounts to the Application

First, assign your ZPA administrators to the application:

1. Select **Users and groups**. This launches the **Add user** page.



Name: Zscaler Private A

Application ID: e82594e0-90fa-

Object ID: d12a7074-d532

Figure 107. Assign users to the administrator app

2. Select **Add user**.

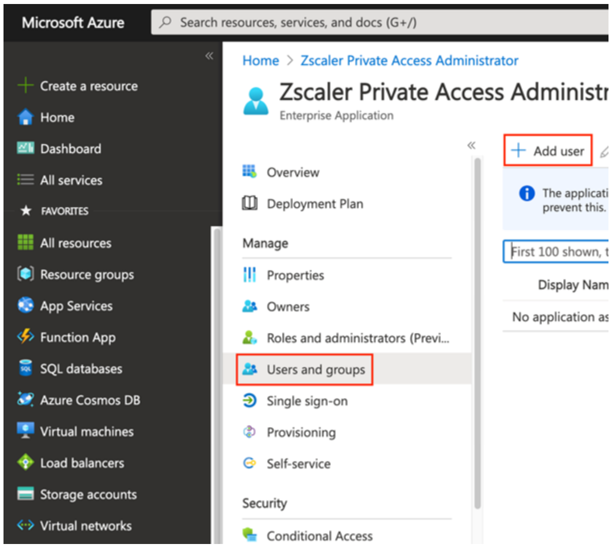


Figure 108. Add users

3. Select the **Users and groups** section.

4. Search and select all ZPA administrators or groups.

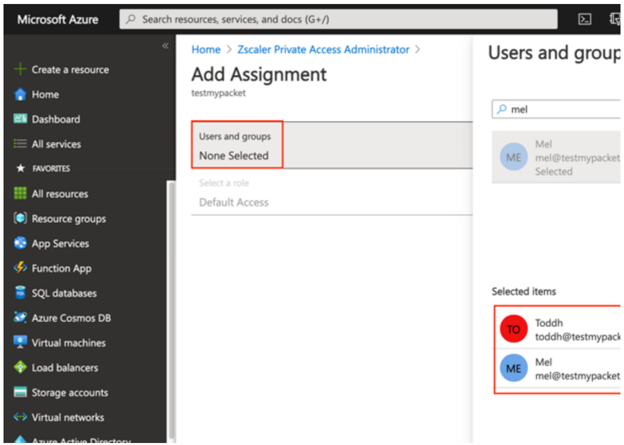


Figure 109. Selecting ZPA administrators

5. Click **Assign**.

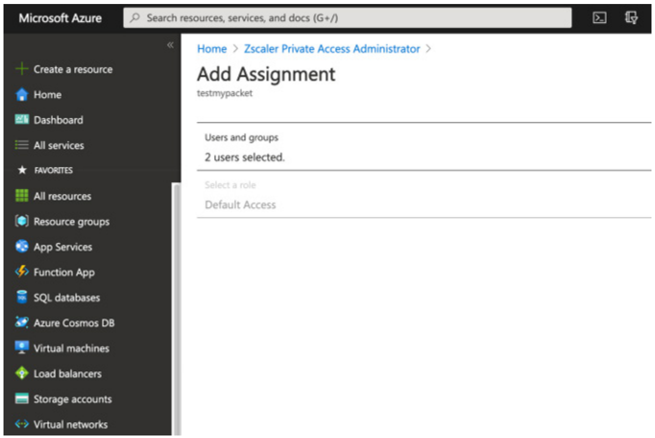
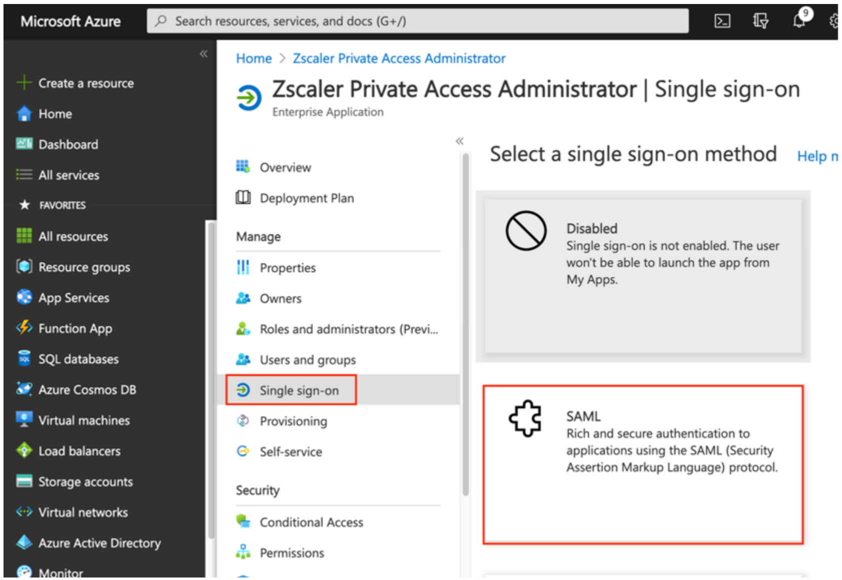


Figure 110. Assign ZPA administrators to the application

Configure SAML for the Application

The next step is to configure SAML for the single sign-on (SSO):

1. Select **Single sign-on**.
2. Select the **SAML** tile.



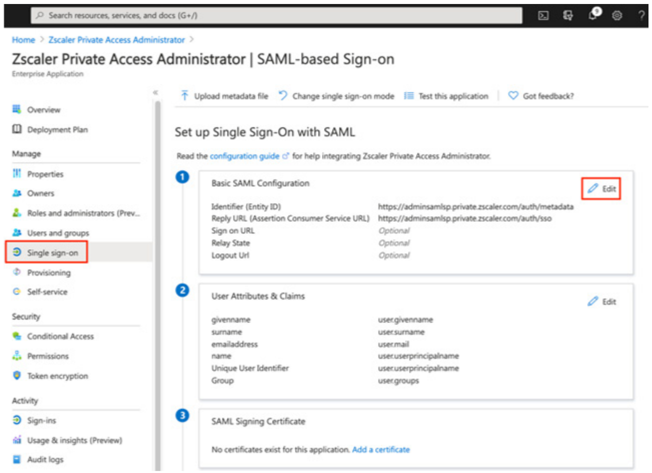
Select a single sign-on method

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Figure 111. Configure SAML

3. This brings up the **SAML configuration** wizard. Select **Edit** to open the **Basic SAML Configuration** page.



Set up Single Sign-On with SAML

Read the configuration guide for help integrating Zscaler Private Access Administrator.

1 Basic SAML Configuration

Identifier (Entity ID)	https://adminsamlsp.private.zscaler.com/auth/metadata
Reply URL (Assertion Consumer Service URL)	https://adminsamlsp.private.zscaler.com/auth/sso
Sign on URL	*Optional*
Relay State	*Optional*
Logout Url	*Optional*

2 User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
Group	user.groups

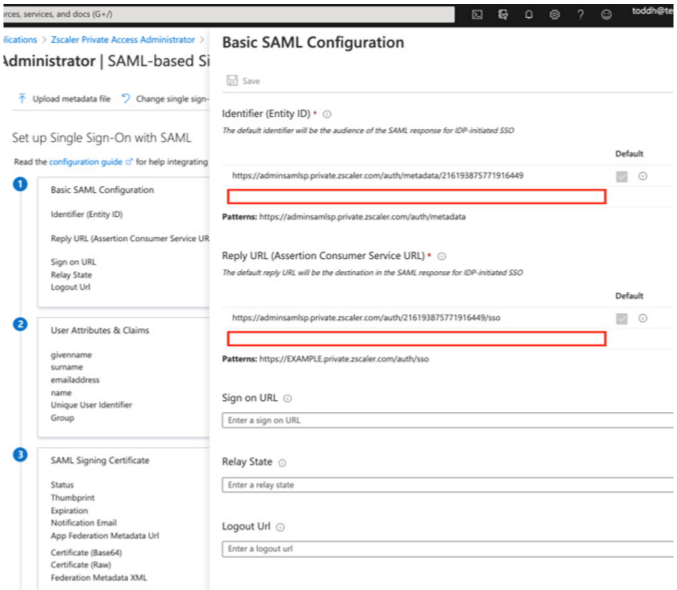
3 SAML Signing Certificate

No certificates exist for this application. Add a certificate

Figure 112. Basic SAML configuration

Copy the required SAML parameters from the ZPA portal and paste them into the fields as shown in the preceding image. Open the ZPA portal in a separate browser tab or window and leave the Azure Setup momentarily so that you can copy the values to insert on this page.

4. Open the ZPA Admin Portal to get the required URLs.



Basic SAML Configuration

Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

https://adminsamlsp.private.zscaler.com/auth/metadata/216193875771916449

Patterns: https://adminsamlsp.private.zscaler.com/auth/metadata

Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

https://adminsamlsp.private.zscaler.com/auth/216193875771916449/sso

Patterns: https://EXAMPLE.private.zscaler.com/auth/sso

Sign on URL: Enter a sign on URL

Relay State: Enter a relay state

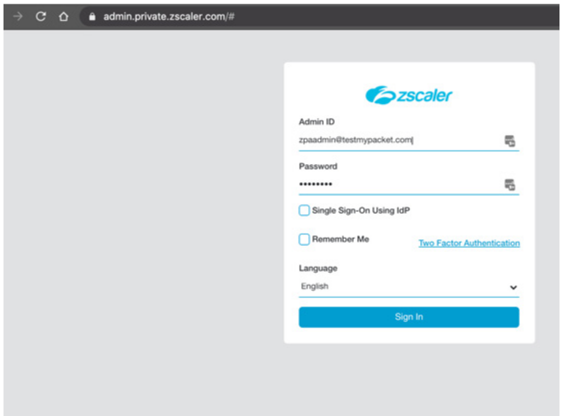
Logout Url: Enter a logout url

Figure 113. Required parameters

ZPA Configuration for SAML Admin Access

Sign-in to your organizations ZPA Admin Portal using administrator credentials.

1. Enter the credentials.
2. Click **Sign In**.



Admin ID: zpaadmin@testmypacket.com

Password: ••••••••

□ Single Sign-On Using IdP

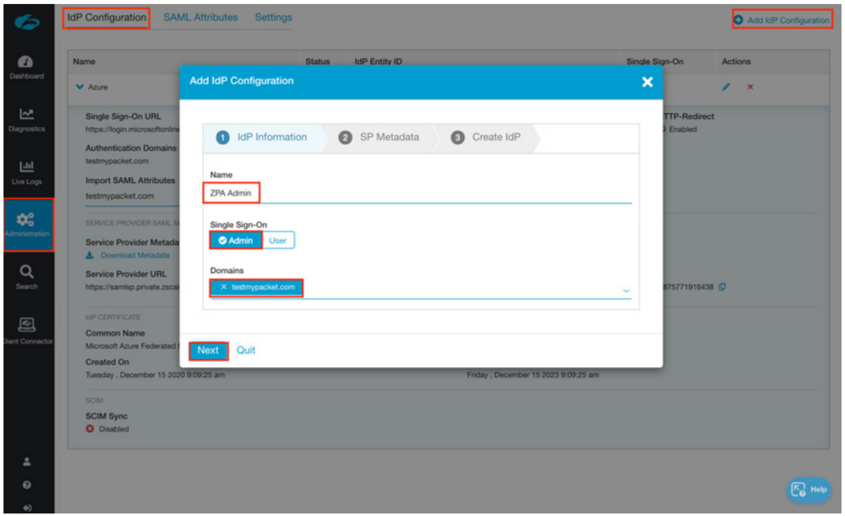
□ Remember Me

Language: English

Figure 114. The ZPA Admin Portal

3. To configure ZPA for administrator SAML authentication from the **Add IdP Configuration** wizard select **Administration** > **IdP Configuration** > **Add IdP Configuration**.
4. **Name** the IdP Profile.
5. Select **Admin** for the **Single Sign-On** type.
6. Select the domains the administrators authenticate against in Azure.

7. Click **Next**. This moves you to the **SP Metadata** setup.



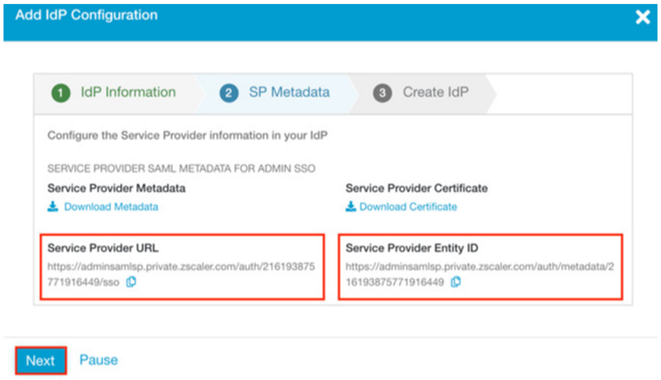
Name: ZPA Admin

Single Sign-On: Admin | User

Domains: testmypacket.com

Figure 115. Add the IdP configuration

8. Two URLs need to be copied and pasted into the Azure configuration.
   a. Copy the **Service Provider URL**.
   b. Copy the **Service Provider Entity ID**.
9. Click **Next**.
10. Open the **Azure configuration** window.



Configure the Service Provider information in your IdP

SERVICE PROVIDER SAML METADATA FOR ADMIN SSO

Service Provider Metadata

Service Provider Certificate

Service Provider URL
https://adminsamlsp.private.zscaler.com/auth/216193875771916449/sso

Service Provider Entity ID
https://adminsamlsp.private.zscaler.com/auth/metadata/216193875771916449

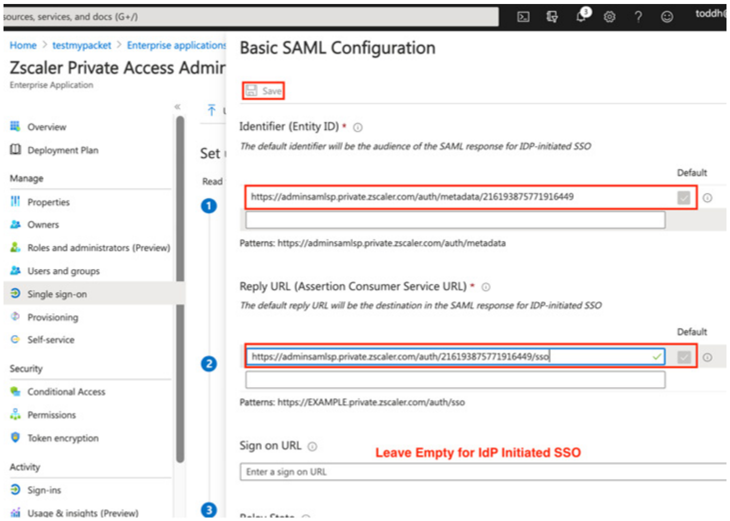
Figure 116. SP Metadata to copy and paste into the Azure configuration

Leave this window open and go to the Azure window to finish the Azure configuration.

Finish the Azure Configuration for SAML Admin Access

To finish the Azure configuration:

1. Paste the **Service Provider URL** into the **Reply URL** field.
2. Paste the **Service Provider Entity ID** into the **ID (Entity ID)**.
3. Select the URLs as **Default**.
4. Click **Save.**



Basic SAML Configuration

Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

https://adminsamlsp.private.zscaler.com/auth/metadata/216193875771916449

Patterns: https://adminsamlsp.private.zscaler.com/auth/metadata

Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

https://adminsamlsp.private.zscaler.com/auth/216193875771916449/sso

Patterns: https://EXAMPLE.private.zscaler.com/auth/sso

Sign on URL

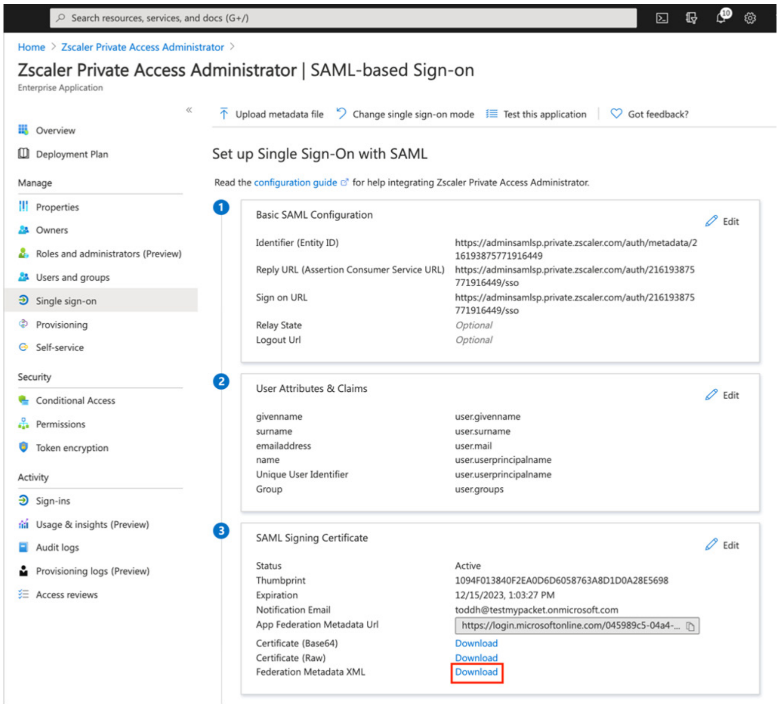
Leave Empty for IdP Initiated SSO

Enter a sign on URL

Figure 117. Finish the Azure configuration

Saving the Azure configuration generates the Signing Certificates and the Metadata that uniquely identify the instance and provide an authenticated session when authenticating the administrators:

1. Download and save the `Federation Metadata XML` file.
2. Open the ZPA window to finish the ZPA configuration.



Zscaler Private Access Administrator | SAML-based Sign-on

Set up Single Sign-On with SAML

Read the configuration guide for help integrating Zscaler Private Access Administrator.

Basic SAML Configuration

Identifier (Entity ID)	https://adminsamlsp.private.zscaler.com/auth/metadata/216193875771916449
Reply URL (Assertion Consumer Service URL)	https://adminsamlsp.private.zscaler.com/auth/216193875771916449/sso
Sign on URL	https://adminsamlsp.private.zscaler.com/auth/216193875771916449/sso
Relay State	*Optional*
Logout Url	*Optional*

User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
Group	user.groups

SAML Signing Certificate

Status	Active
Thumbprint	1094F013840F2EA0D6D6058763A8D1D0A28E5698
Expiration	12/15/2023, 1:03:27 PM
Notification Email	toddh@testmypacket.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/045989c5-04a4-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

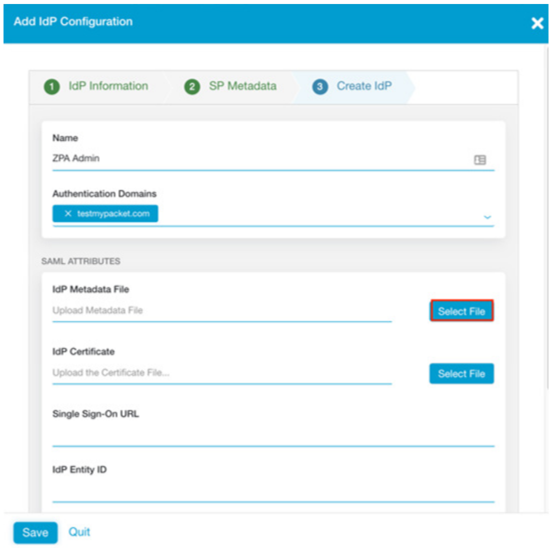
Figure 118. Download the Federation Metadata to upload to ZPA

Finish the ZPA Configuration for SAML Admin Access

The Federation Metadata XML file populates the required URLs and installs the signing certificate.

In the ZPA IdP Configuration window:

- Select and upload the **Federation Metadata XML** file from Azure.



Add IdP Configuration

1 IdP Information 2 SP Metadata 3 Create IdP

Name: ZPA Admin

Authentication Domains: testmypacket.com

SAML ATTRIBUTES

IdP Metadata File: Upload Metadata File — Select File

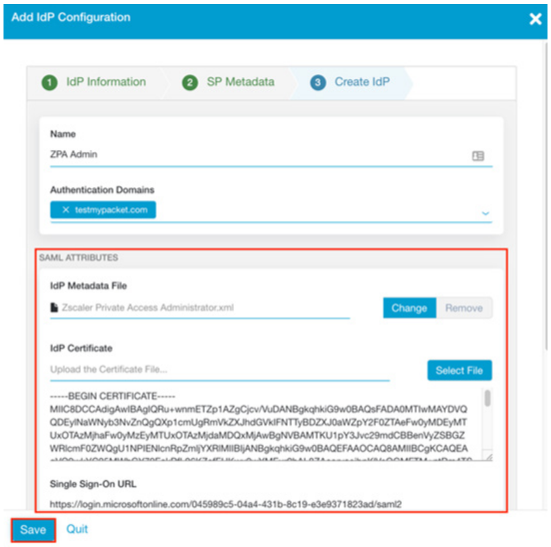
IdP Certificate: Upload the Certificate File... — Select File

Single Sign-On URL

IdP Entity ID

Figure 119. Upload the Federation metadata to ZPA

- Click **Save**.



Add IdP Configuration

1 IdP Information 2 SP Metadata 3 Create IdP

Name: ZPA Admin

Authentication Domains: testmypacket.com

SAML ATTRIBUTES

IdP Metadata File: Zscaler Private Access Administrator.xml — Change Remove

IdP Certificate: Upload the Certificate File... — Select File

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAdigAwIBAgIQRu+wnmETZp1AZgCjcv/VuDANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQ
QDEylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMDEyMT
UxOTAzMjhaFw0yMzEyMTUxOTAzMjdaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZ
WRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
```

Single Sign-On URL: https://login.microsoftonline.com/045989c5-04a4-431b-8c19-e3e9371823ad/saml2

Figure 120. Completed ZPA Configuration

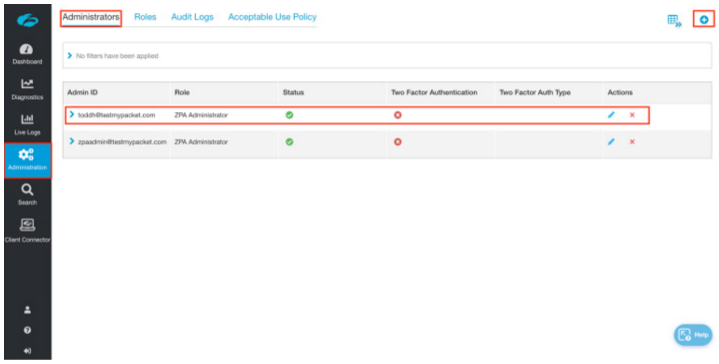
This completes the SAML configuration. Next, add administrators to ZPA.

Add ZPA Admin Accounts to ZPA

All administrators for ZPA must be added to the ZPA portal as administrators. SAML to Azure authenticates the administrators, but the admins still must be configured in both ZPA and Azure.

To add the administrator:

1. Select **Administration** > **Administrators**.
2. Select **Add administrator** or the **Blue Plus** sign.



No filters have been applied

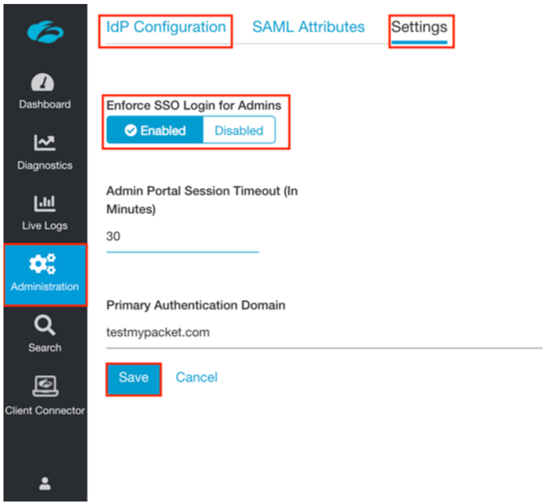
Admin ID	Role	Status	Two Factor Authentication	Two Factor Auth Type	Actions
toddh@testmypacket.com	ZPA Administrator	✓	⊗		✎ ×
zpaadmin@testmypacket.com	ZPA Administrator	✓	⊗		✎ ×

Figure 121. Adding ZPA administrators

Enforce SSO for all Administrators

Select Enforce SSO for all Administrators to force all administrators, except for the primary ZPA administrator, to use SAML for authentication.

1. Select **Administrator** > **IdP Configuration** > **Settings**.
2. Select **Enabled** for the **Enforce SSO Login for Admins** field.
3. Click **Save**.



Enforce SSO Login for Admins
[✓ Enabled] Disabled

Admin Portal Session Timeout (In Minutes)
30

Primary Authentication Domain
testmypacket.com

Figure 122. Enforcing SSO for ZPA administrators

Open the ZPA Portal from Azure My-Apps

After the configuration is complete, the admin can launch the ZPA portal from their My-Apps portal with SSO/SAML and without having to enter credentials:

- Select the **Zscaler Private Access Administrator** application from the **My Apps** portal.

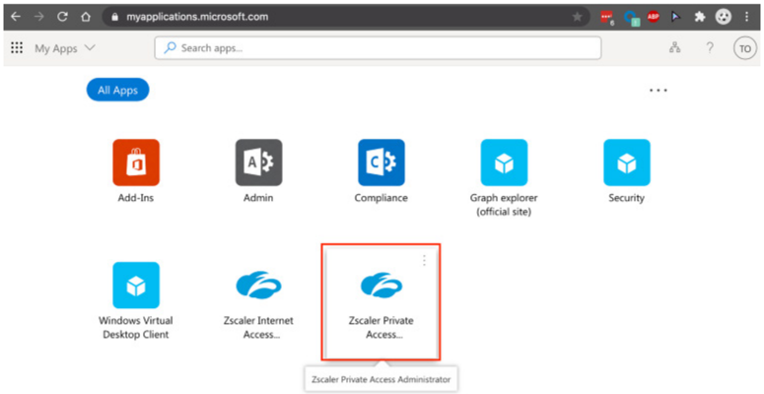

myapplications.microsoft.com
My Apps
Search apps...
TO
All Apps
Add-Ins
Admin
Compliance
Graph explorer (official site)
Security
Windows Virtual Desktop Client
Zscaler Internet Access...
Zscaler Private Access...
Zscaler Private Access Administrator

Figure 123. Launch the ZPA Portal from the Admins My-App page

ZPA Administrator Portal Launched from My-Apps

The following image shows that the implementation was successful. You can access the ZPA Portal.

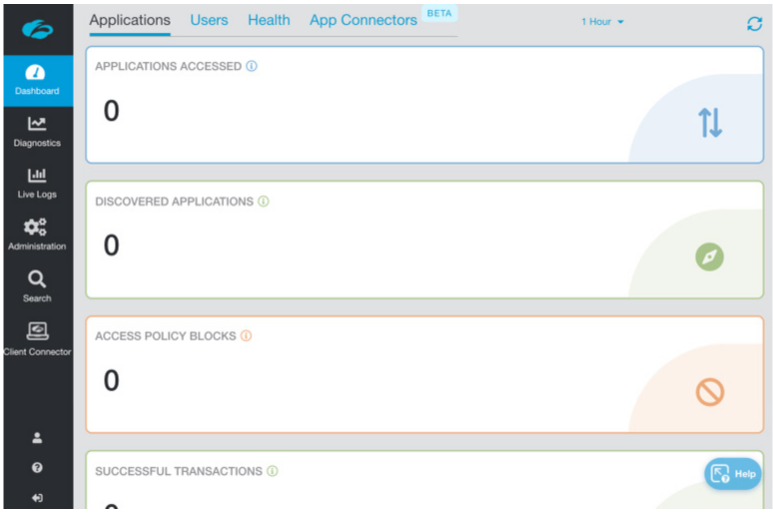


Figure 124. The ZPA Portal launched from the My-Apps page

The Processes Summarized

The following steps are a no-frills outline of what you need to configure for Zscaler authentication and provisioning for ZIA and ZPA. Use your Zscaler Cloud account information to complete application and URL fields. `Zscalerthree` is used in these summary steps as an example, but your cloud might be different.

ZIA Authentication

1. Add the Microsoft Entra ID ZIA application for your cloud.
    a. Select **Microsoft Entra ID** > **Enterprise Applications** > **New application**.
    b. Search and install the Zscaler Three Application from the Microsoft Entra ID gallery.
2. Assign users to the Zscaler Three application.
    a. Select **Microsoft Entra ID** > **Enterprise Applications** > **Zscaler Three** > **Users and Groups**.
    b. Add ZIA users and groups.
3. Configure Authentication Azure UI SAML for ZIA Authentication.
    a. Select **Microsoft Entra ID** > **Enterprise Applications** > **Zscaler Three** > **Sign-On** > **SAML**.
    b. Edit the basic SAML configuration.
        i. Enter the **Entity ID** (**zscalerthree.net**).
        ii. Enter the **Sign-on URL** (**https://login.zscalerthree.net/sfc_sso**).
        iii. Enter the **Reply URL** (**https://login.zscalerthree.net/sfc_sso**).
        iv. **Save** the configuration.
    c. Get the **SAML Signing Certificate**.
        i. Download the Base64 SAML signing certificate.
        ii. Rename the certificate for `ZscalerThree.cer` to `ZscalerThree.pem`.
    d. Set Up Zscaler Three and Configuration URLs.
        iii. Copy the **Login URL**.
4. Configure Authentication Zscaler Three.
    a. Select **Administration** > **Authentication Settings** > **Authentication Profile**.
        i. Set **Authentication Type** as **Enable SAML**.
        ii. **Save** the configuration.
        iii. **Activate** changes.
    b. Select **Administration** > **Authentication Settings** > **Identity Providers** > **Add Identity Provider**.
        i. **Name** the IdP.
        ii. Toggle the **Status** to **Enable**.
        iii. Paste the **Azure Login URL** into the **SAML Portal URL** field.
        iv. Enter **NameID** as the **Login Name Attribute**.
        v. Upload the ZscalerThree.cer file as the **IdP SAML Certificate**.
        vi. Select **Microsoft Entra ID** as the **Vendor**.
        vii. Select the **Authentication Domain or Leave** as **Default**.
        viii. **Save** the configuration.

ix. **Activate** the changes.

ZIA Provisioning

1. Configure Provisioning Zscaler Three.
    a. Select **Administration** > **Authentication Settings** > **Identity Providers** > **Edit the Azure IdP**.
        i. If using SAML provisioning.
            1. Enable **SAML Auto-Provisioning**.
            2. Enter **userName** as the **User Display Name Attribute**.
            3. Enter **memberOf** for the **Group Name Attribute**.
            4. Enter **department** for the **Department Name Attribute**.
            5. **Save** the configuration.
            6. **Activate** the changes.
        ii. If using SCIM provisioning (recommended, must be **E5**, or **P1 / P2 Azure**).
            1. Enable **SCIM Provisioning**.
            2. Select **Generate Token**.
            3. Copy the **Base URL** to paste in Azure.
            4. Copy the **Bearer Token** to paste in Azure.
            5. **Save** the configuration.
            6. **Activate** the changes.
            7. Configure **Provisioning Azure**.
    b. Select **Microsoft Entra ID** > **Enterprise Applications** > **Zscaler Three** > **Provisioning**.
        i. Change **Provisioning Mode** to **Automatic**.
        ii. Under **Admin Credentials**.
            1. Enter the **Zscaler Base URL** into the **Azure Tenant URL**.
            2. Enter the **Zscaler Bearer Token** into the **Azure Secret Token**.
            3. **Test** the connection.
            4. **Save** the configuration.
        iii. Enable provisioning synchronization.
            1. Toggle **Provisioning Status** to **On**.
            2. **Save** the configuration.
        iv. (Optional) Push immediate users needed for test.
            1. Select **Provisioning** > **Provision on Demand**.
            2. Select **User**.
            3. Select **Provision**.
            4. Repeat.
        v. (Optional) Enable scoping filters.
            1. Create **User or Group SCIM scoping filters**.

ZPA Entitlement

1. Enable ZPA Entitlement.
    a. Azure: **Microsoft Entra ID** > **Enterprise Applications** > **Zscaler Three** > **Users and Groups**.
        i. Add the ZPA group that contains the ZPA users.
    b. Zscaler Three: **Policy** > **Zscaler Client Connector Portal**.
        i. Select **Administration**.
        ii. Select **Zscaler Service Entitlement**.
        iii. Select the **ZPA Entitlement Group** for **Groups Enabled**.
            1. Do not select **ZPA Enabled by Default**.
        iv. **Save** the configuration.
    c. To manually sync group in Zscaler Three: **Policy** > **Zscaler Client Connector Portal**.
        i. Select **Administration**.
        ii. Select **Client Connector Support**.
        iii. Select A**dvanced Configuration**.
        iv. Select **Sync Groups**.

ZPA Authentication

1. Add the Microsoft Entra ID ZPA Private Access (ZPA) application for your cloud.
    a. Select **Microsoft Entra ID** > **Enterprise Applications** > **New application**.
    b. Search and install the **Zscaler Private Access (ZPA)** application from the **Microsoft Entra ID Gallery**.
2. Assign users to the Zscaler Private Access (ZPA) application.
    a. Select **Microsoft Entra ID** > **Enterprise Applications** > **Zscaler Private Access** > **Users and Groups**.
    b. Add ZPA users and groups.
3. Configure authentication Azure: SAML for ZPA authentication.
    a. Select **Microsoft Entra ID** > **Enterprise Applications** > **Zscaler Private Access** > **Sign-On > SAML**.
    b. Edit the basic SAML configuration (need URLs from ZPA to proceed).
4. Configure authentication Zscaler Private Access.
    a. Select **Administration** > **Authentication** > **IdP Configuration**.
        i. Add IdP.
    b. Add IdP configuration.
        i. Name the IdP.
        ii. Select **User** for **Single Sign-On**.
        iii. Select authentication domains.
        iv. Select **Next**.
    c. Add SP metadata.
        v. Copy the **Service Provider URL** to paste in Azure **Reply** and **Sign-On** URL.
        vi. Copy **Service Provider Entity ID** to paste in Azure **Entity ID**.
        vii. Select **Next**.

5. Configure authentication Azure: SAML for ZPA authentication.
    a. Select **Microsoft Entra ID** > **Enterprise Applications** > **Zscaler Private Access** > **Sign-On** > **SAML**.
        i. Paste the **ZPA Service Provider URL** to in the Azure **Reply** and **Sign-On** URL.
        ii. Paste the **ZPA Service Provider Entity ID** in the Azure **Entity ID**.
        iii. **Save** the configuration.
        iv. Download the **Federation Metadata XML** file.
6. Configure authentication Zscaler Private Access.
    a. **Administration** > **Authentication** > **IdP Configuration**.
        i. Select and upload the **Federation Metadata XML** file saved from the Azure Portal.
        ii. **Save** the configuration.
        iii. **Test** authentication.

ZPA Provisioning

1. Configure SCIM provisioning Zscaler Private Access.
    a. Select **Administration** > **IdP Configuration** > **Edit the Azure IdP**.
        i. Enable **SCIM Sync**.
        ii. Select **Generate New Token**.
        iii. Copy the **SCIM Service Provider Endpoint URL** for the Azure configuration.
        iv. Copy the **Bearer Token** for the Azure configuration.
        v. Disable SAML Attributes for Policy (Ignore the Error).
        vi. Enable SCIM Attributes for Policy.
        vii. **Save** the configuration.
2. Configure SCIM provisioning Azure.
    a. Select **Microsoft Entra ID** > **Enterprise Applications** > **ZPA** > **Provisioning**.
        i. Change **Provisioning Mode** to **Automatic**.
        ii. Under **Admin Credentials**.
            1. Enter the Zscaler Base URL into the Azure **Tenant URL**.
            2. Enter the Zscaler Bearer Token into the Azure **Secret Token**.
            3. **Test** the connection.
            4. **Save** the configuration.
        iii. Enable provisioning synchronization.
            1. Toggle **Provisioning Status** to **On**.
            2. **Save** the configuration.
        iv. (Optional) Push immediate users needed for test.
            1. Select **Provisioning** > **Provision on Demand**.
            2. Select **User**.
            3. Select **Provision**.
            4. Repeat.

v. (Optional) Enable scoping filters.

1. Create **User or Group SCIM scoping filters**.

3. Configure SAML Provisioning Zscaler (optional).

a. Select **Administration** > **IdP Configuration** > **Edit the Azure IdP**.

i. Disable **SCIM Sync**.

ii. Enable **SAML Attributes** for **Policy**.

iii. Disable **SCIM Attributes** for **Policy**.

iv. **Save** the configuration.

4. Configure Microsoft Entra ID Group Mapping Azure.

a. Select **Microsoft Entra ID** > **Enterprise Applications** > **ZPA**.

i. See the configuration details in the body of the document.

ZIA SAML Admin Authentication

1. Add the Microsoft Entra ID Zscaler Internet Access Administrator application for your cloud.

a. Select **Microsoft Entra ID** > **Enterprise Applications** > **New application**.

b. Search and install the **Zscaler Internet Access Administrator** application from the Microsoft Entra ID gallery.

2. Assign users to the Zscaler Three application.

a. Select **Microsoft Entra ID** > **Enterprise Applications** > **Zscaler Internet Access Administrator Application** > **Users and Groups**.

b. Add ZIA administrator users and groups.

3. Configure Authentication Azure: SAML for ZIA Authentication.

a. Select **Microsoft Entra ID** > **Enterprise Applications** > **Zscaler Three** > **Sign-On** > **SAML**.

b. Edit the basic SAML configuration.

i. Enter the **Entity ID** (`https://admin.zscalerthree.net`).

ii. Enter the **Reply URL** (`https://admin.zscalerthree.net/adminsso.do`).

iii. **Save** the configuration.

c. Get the **SAML Signing Certificate**.

i. Download the Base64 SAML Signing Certificate.

4. Configure Authentication Zscaler Three.

a. Select **Administration** > **Administrator Management** > **Administrator Management**.

i. Enable **SAML authentication**.

ii. Upload the Internet Access Administrator.cer certificate saved from Azure.

iii. **Save** the configuration.

b. Select **Administration** > **Administrator Management** > **Administrators**.

i. Add administrators that use SAML authentication.

ii. **Save** the configuration.

iii. **Activate** changes.

ZPA SAML Admin Authentication

1. Add the Microsoft Entra ID Zscaler Private Access Administrator application for your cloud.
    a. Select **Microsoft Entra ID** > **Enterprise Applications** > **New application**.
    b. Search and install the Zscaler Private Access Administrator from the Microsoft Entra ID gallery.
2. Assign users to the Zscaler Private Access Administrator application.
    a. Select **Microsoft Entra ID** > **Enterprise Applications** > **Zscaler Private Access Administrator** > **Users and Groups**.
    b. Add ZPA users and groups.
3. Configure Authentication Azure: SAML for ZPA Admin Authentication.
    a. Select **Microsoft Entra ID** > **Enterprise Applications** > **Zscaler Private Access Administrator** > **Sign-On** > **SAML**.
    b. Edit the basic SAML Configuration (you need URLs from ZPA to proceed).
4. Configure Authentication Zscaler Private Access.
    a. Select **Administration** > **Authentication** > **IdP Configuration**.
        i. **Add** IdP.
    b. Add IdP configuration.
        i. **Name** the IdP.
        ii. Select **Admin** for **Single Sign-On**.
        iii. Select **Authentication Domains**.
        iv. Click **Next**.
    c. SP metadata.
        i. Copy the **Service Provider URL** to paste in Azure **Reply URL**.
        ii. Copy **Service Provider Entity ID** to paste in Azure **Entity ID**.
        iii. Click **Next**.
5. Configure Authentication Azure: SAML for ZPA Admin Authentication.
    a. Select **Microsoft Entra ID** > **Enterprise Applications** > **Zscaler Private Access** > **Sign-On** > **SAML**.
        i. Paste the **ZPA Service Provider URL** in the Azure **Reply URL**.
        ii. Paste the **ZPA Service Provider Entity ID** in the Azure **Entity ID**.
        iii. **Save** the configuration.
        iv. Download the **Federation Metadata XML** file.
6. Configure Authentication Zscaler Private Access.
    a. Select **Administration** > **Authentication** > **IdP Configuration**.
        i. Select and upload the **Federation Metadata XML** file.
        ii. **Save** the configuration.
        iii. **Test** the authentication.
    b. Select **Administration** > **Administrator Management** > **Administrators**.
        i. Add administrators that use SAML authentication.
        ii. **Save** the configuration.

Transparent SSO Using IWA with Microsoft Entra ID

One of the advantages of using Microsoft Entra ID is that you can often use Integrated Windows Authentication (IWA) to provide SSO to your Zscaler installation. SSO provides a better user experience by automatically authenticating users with their Windows domain credentials. Zscaler can take advantage of IWA if IWA is configured for the Microsoft Entra ID environment. IWA is not a Zscaler feature or Zscaler configuration, and works between Microsoft Entra ID and the Windows Active Directory Server. However, Zscaler can take advantage of a working IWA environment. IWA is a Microsoft feature that allows you to automatically authenticate using your Windows Active Directory authentication credentials.

IWA works in two Azure architectures:

- An Microsoft Entra ID and On-Site Microsoft Entra ID hybrid environment.
- An all-Microsoft Entra ID environment with Microsoft Entra ID Directory Services installed as an Azure service.

IWA uses Kerberos ticketing, and the Windows device must authenticate to the FQDN of the authenticating service in Azure.

To enable IWA for Zscaler in either the Hybrid Microsoft Entra ID or AADDS environments, you install two URLs as trusted sites in your intranet zone on your browser and install the Zscaler Client Connector with the `--userDomain` and `--cloudName` command line installation parameters.

[Microsoft Azure online documentation](#) provides detailed configuration options, including GPO options to push the browser settings.

Why do you need to add the domains as trusted domains? By default, the browser automatically calculates the correct zone, either internet or intranet, from a specific URL. For example, `https:/testmypacket/` maps to the intranet zone, whereas `https://internet.testmypacket.com/` maps to the internet zone (because the URL contains a period).

Browsers don't send Kerberos tickets to a cloud endpoint, like the Microsoft Entra ID URL, unless you explicitly add the URL to the browser's intranet zone.

- Add `*.yourlogindomain.com` and `autologon.microsoftazuread-sso.com` to your browsers trusted intranet sites.

See [Appendix A: Capture the SAML Request for Troubleshooting](#) in the back of this guide.

PAC File and Zscaler Client Connector: Authentication Bypasses

When using ZIA, you must bypass the IdP login URLs for authentication to succeed.

For ZPA, you are not required to bypass the IdP login URL.

Destination URLs can flow through ZIA, but bypassing the URLs for ZIA is a requirement for both browser PAC files and for the Zscaler Client Connector. You can also apply these bypasses as authentication bypasses in Zscaler ZIA.

The difference between the two methods is what IP Microsoft Entra ID sees. A ZIA authentication bypass shows the Zscaler IP range, while the PAC file / Zscaler Cloud Connector bypass shows the egress IP of the customer. Both methods work, but you might have requirements for which method works better.

You must add the following entries to your browser PAC or the Zscaler Client Connector custom PAC file for the application profile.

For more information see Appendix A: Capture the SAML Request for Troubleshooting.

```
PAC File Bypasses:

// Microsoft Entra ID Authentication Bypass

if (

dnsDomainIs(host, “login.microsoftonline.com”) ||

dnsDomainIs(host, “clientconfig.microsoftonline-p.net”) ||

dnsDomainIs(host, “*.autodiscover.yourdomain.com”))

return “DIRECT”;
```

Appendix A: Capture the SAML Request for Troubleshooting

Troubleshooting SAML can be challenging. The troubleshooting procedures find and decode the SAML assertion and look at the attributes returned by the IdP. The following steps capture the assertion by using the Chrome browser's Developer Tools. You can then decode the assertion using a base 64 decoder on the desktop. Use of a decoder on the local computer is the most secure method. Alternatively, you can use browser extensions, or cloud based base64 decoders, but when clear text passwords are present in the data, keeping things in house- such as using a decoder on the desktop- is always more secure. You can use any browser to capture the SAML assertion. The procedures for the most common browsers are in the next sections.

How to View a SAML Response in Your Browser for Troubleshooting

Retrieving your service provider SAML response in your browser can help you troubleshoot single sign-on (SSO) login issues.

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 view the Headers tab located at the bottom of the window. 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 the options icon (the small 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 Internet Explorer: To View a SAML Response in Internet Explorer

The best way analyze network traffic in Internet Explorer is through a third-party tool.

Follow the steps at How to Use Fiddler Web Debugger to Analyze a WS-Federation Passive Sign-In to download and install Fiddler and capture the data.

What to do with the Base64-encoded SAML response

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

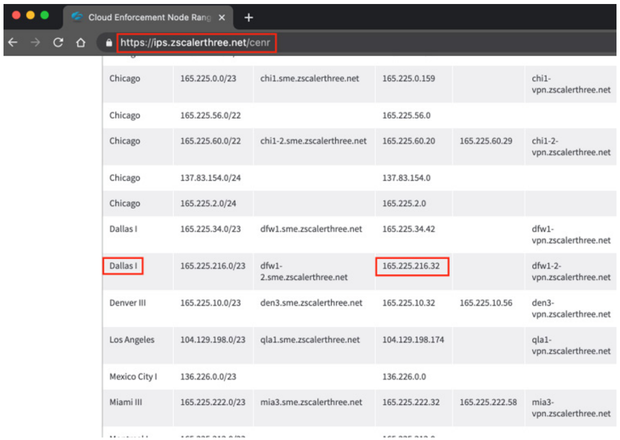
Security Tip

Because the SAML response data might contain sensitive security data, Zscaler recommends that you do not use an online base64 decoder. Instead, use a tool that is installed on your local system.

Configuring Your Browser to Capture the SAML Response

First, configure Zscaler as a proxy for your browser. You can configure the automatic FQDN to select the fastest gateway response as the proxy. The FQDN is `gateway.zscalerthree.net`, where zscalerthree is replaced by your cloud (i.e., `gateway.zscloud.net`, `gateway.zscalertwo.net`, etc.).

For this exercise, manually select the proxy from your list of enforcement nodes. Enter your cloud information center (in the preceding example, the URL is `ips.zscalerthree.net/cenr`). In the example, the URL lists the enforcement nodes for the `Zscalerthree` cloud. The Dallas IP is used as the proxy address defined in our example browser.



https://ips.zscalerthree.net/cenr

Chicago	165.225.0.0/23	chi1.sme.zscalerthree.net	165.225.0.159		chi1-vpn.zscalerthree.net
Chicago	165.225.56.0/22		165.225.56.0		
Chicago	165.225.60.0/22	chi1-2.sme.zscalerthree.net	165.225.60.20	165.225.60.29	chi1-2-vpn.zscalerthree.net
Chicago	137.83.154.0/24		137.83.154.0		
Chicago	165.225.2.0/24		165.225.2.0		
Dallas I	165.225.34.0/23	dfw1.sme.zscalerthree.net	165.225.34.42		dfw1-vpn.zscalerthree.net
Dallas I	165.225.216.0/23	dfw1-2.sme.zscalerthree.net	165.225.216.32		dfw1-2-vpn.zscalerthree.net
Denver III	165.225.10.0/23	den3.sme.zscalerthree.net	165.225.10.32	165.225.10.56	den3-vpn.zscalerthree.net
Los Angeles	104.129.198.0/23	qla1.sme.zscalerthree.net	104.129.198.174		qla1-vpn.zscalerthree.net
Mexico City I	136.226.0.0/23		136.226.0.0		
Miami III	165.225.222.0/23	mia3.sme.zscalerthree.net	165.225.222.32	165.225.222.58	mia3-vpn.zscalerthree.net

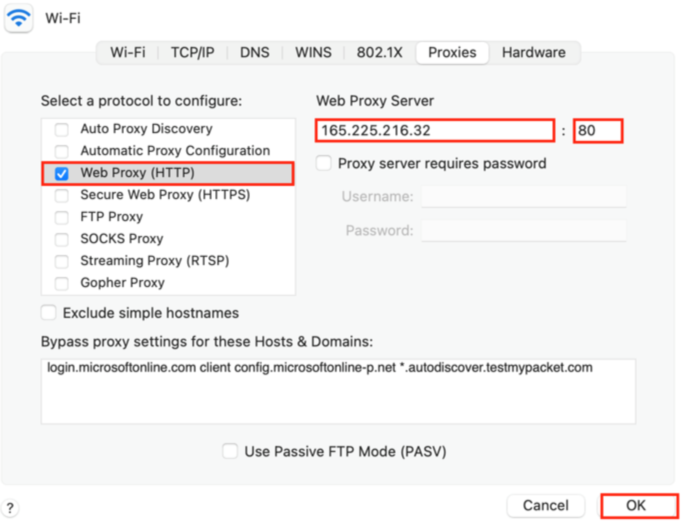
Figure 125. Select a test proxy

Open the proxy configuration screen for your test browser and enter in the proxy IP address. You must also enter in the Microsoft Entra ID domains as bypasses so that the request reaches Microsoft Entra ID and isn't blocked by ZIA.

The three Microsoft Entra ID domains to bypass are as follows:

- login.microsoftonline.com
- config.microsoftonline-p.net
- *.autodiscover.testmypacket.com

Save the changes. You are now ready to test.


Wi-Fi
Wi-Fi | TCP/IP | DNS | WINS | 802.1X | Proxies | Hardware
Select a protocol to configure:
□ Auto Proxy Discovery
□ Automatic Proxy Configuration
□ Secure Web Proxy (HTTPS)
□ FTP Proxy
□ SOCKS Proxy
□ Streaming Proxy (RTSP)
□ Gopher Proxy
□ Proxy server requires password
Username:
Password:
□ Exclude simple hostnames
□ Use Passive FTP Mode (PASV)
?
Cancel
OK

☑ Web Proxy (HTTP)

Web Proxy Server: 165.225.216.32 : 80

Bypass proxy settings for these Hosts & Domains:
login.microsoftonline.com client config.microsoftonline-p.net *.autodiscover.testmypacket.com

Figure 126. Setting your browser proxy settings

To validate the authorization, complete the following steps.

1. Enter any URL in the browser, and ZIA prompts you for authentication credentials.
2. Start your developer tools.
3. Select the three dots at the top right of the browser to open a drop-down menu, Select **More Tools**, and then **Developer Tools**. This starts the developer screen.

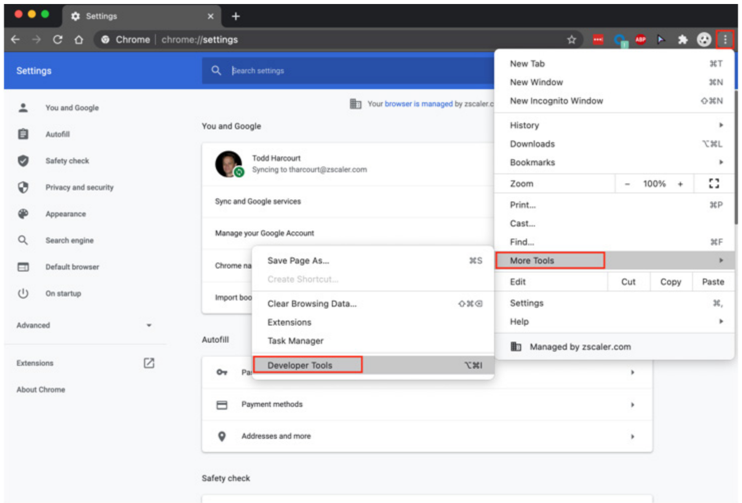
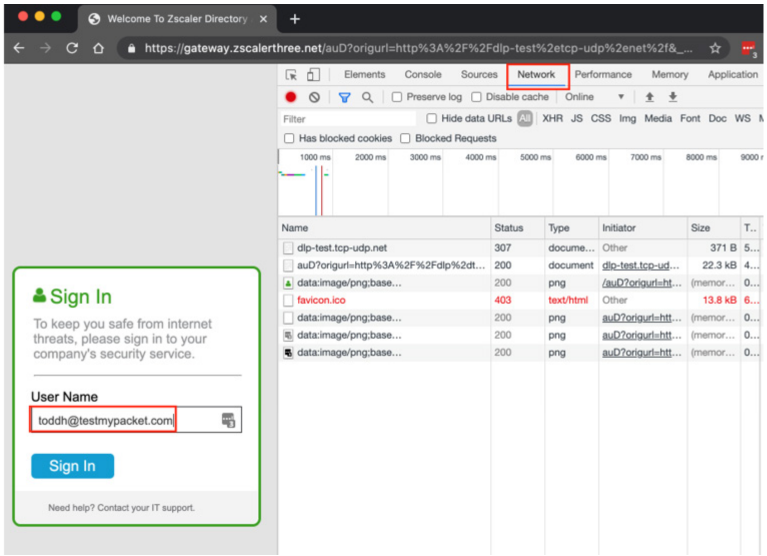


Figure 127. Selecting Developer Tools

The network trace shows you the connection and packet information as both authenticate into Zscaler and Microsoft Entra ID.

The initial authentication screen, shown in the preceding image, is looking for only the user domain that is appended to the User ID, so that Zscaler knows which Zscaler instance to direct the request to. In this case, the domain is `testmypacket.com`.



https://gateway.zscalerthree.net/auD?origurl=http%3A%2F%2Fdlp-test%2etcp-udp%2enet%2f&_...

To keep you safe from internet threats, please sign in to your company's security service.

User Name: toddh@testmypacket.com

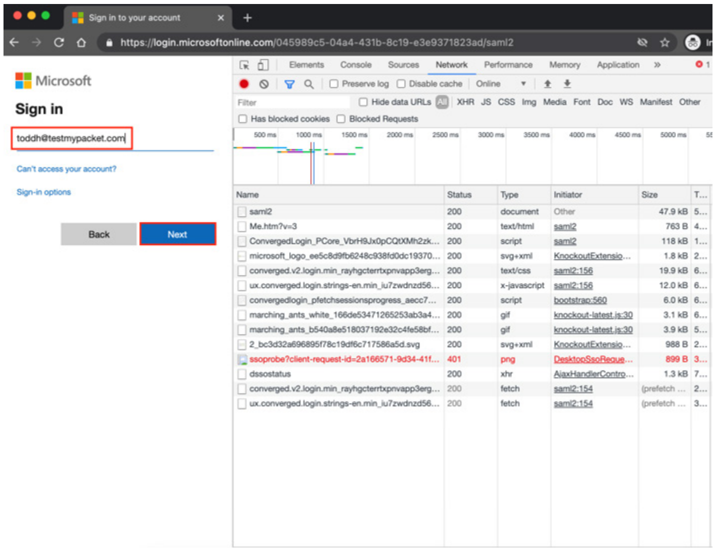
Need help? Contact your IT support.

Name	Status	Type	Initiator	Size	T..
dlp-test.tcp-udp.net	307	docume...	Other	371 B	5...
auD?origurl=http%3A%2F%2Fdlp%2dt...	200	document	dlp-test.tcp-ud...	22.3 kB	4...
data:image/png;base...	200	png	/auD?origurl=ht...	(memor...	0...
favicon.ico	403	text/html	Other	13.8 kB	6...
data:image/png;base...	200	png	auD?origurl=htt...	(memor...	0...
data:image/png;base...	200	png	auD?origurl=htt...	(memor...	0...
data:image/png;base...	200	png	auD?origurl=htt...	(memor...	0...

Figure 128. Capturing the SAML Request

Zscaler redirects the authentication request to Microsoft Entra ID, and you see the Microsoft Entra ID authentication screen.

Log in with a valid user ID from the Microsoft Entra ID database associated with the Zscaler instance.



https://login.microsoftonline.com/045989c5-04a4-431b-8c19-e3e9371823ad/saml2

toddh@testmypacket.com

Name	Status	Type	Initiator	Size	T...
saml2	200	document	Other	47.9 kB	5...
Me.htm?v=3	200	text/html	saml2	763 B	4...
ConvergedLogin_PCore_VbrH9Jx0pCQtXMh2zk...	200	script	saml2	118 kB	1...
microsoft_logo_ee5c8d9fb6248c938fd0dc19370...	200	svg+xml	KnockoutExtensio...	1.8 kB	2...
converged.v2.login.min_rayhgcterrtxpnvapp3erg...	200	text/css	saml2:156	19.9 kB	6...
ux.converged.login.strings-en.min_iu7zwdnzd56...	200	x-javascript	saml2:156	12.0 kB	6...
convergedlogin_pfetchsessionsprogress_aecc7...	200	script	bootstrap:560	6.0 kB	6...
marching_ants_white_166de53471265253ab3a4...	200	gif	knockout-latest.js:30	3.1 kB	6...
marching_ants_b540a8e518037192e32c4fe58bf...	200	gif	knockout-latest.js:30	3.9 kB	5...
2_bc3d32a696895f78c19df6c717586a5d.svg	200	svg+xml	KnockoutExtensio...	988 B	2...
ssoprobe?client-request-id=2a166571-9d34-41f...	401	png	DesktopSsoReque...	899 B	3...
dssostatus	200	xhr	AjaxHandlerContro...	1.3 kB	7...
converged.v2.login.min_rayhgcterrtxpnvapp3erg...	200	fetch	saml2:154	(prefetch ...	2...
ux.converged.login.strings-en.min_iu7zwdnzd56...	200	fetch	saml2:154	(prefetch ...	3...

Figure 129. Authenticate to the Microsoft Entra ID IdP

After authentication has completed:

1. Select the packet called **sfc_sso**, that is destined to login.zscalerthree.net. This is the SAML response from Microsoft Entra ID and contains the SAML assertion. The assertion is base64 encoded and requires a decoder to get the clear text information.
2. Select the SAML response data excluding "SAMLResponse:" we want only the data.

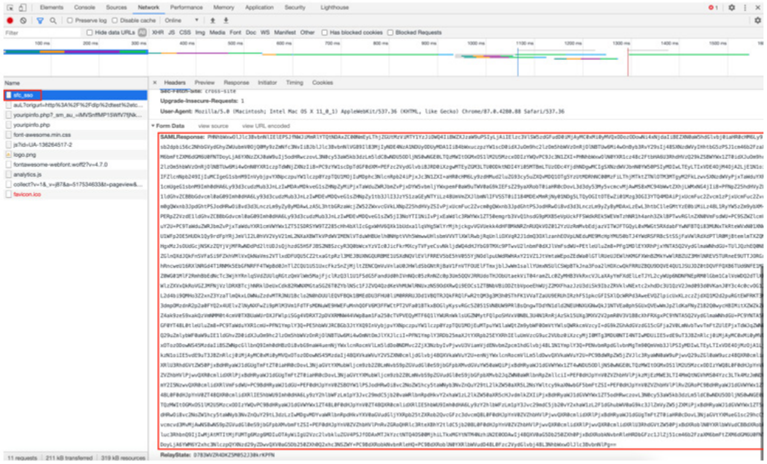
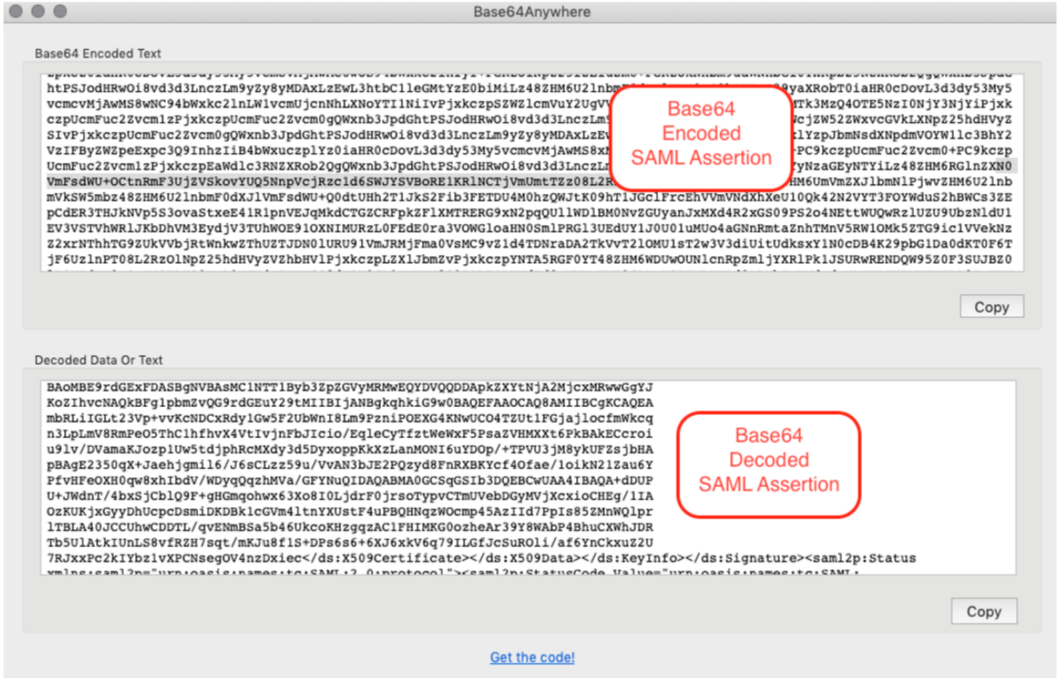


Figure 130. SAML response containing the assertion

Using a base64 decoder:

1. Paste the encoded text into the application.
2. Copy the decoded SAML assertion.

(For this demonstration, we used the **Base64Anywhere** app downloaded free from the Mac App store. There are also free decoders in the Windows store if you are a Microsoft user, and command line options. For example, for macOS you can use a CLI command "base64 -D data" to decode the assertion.)

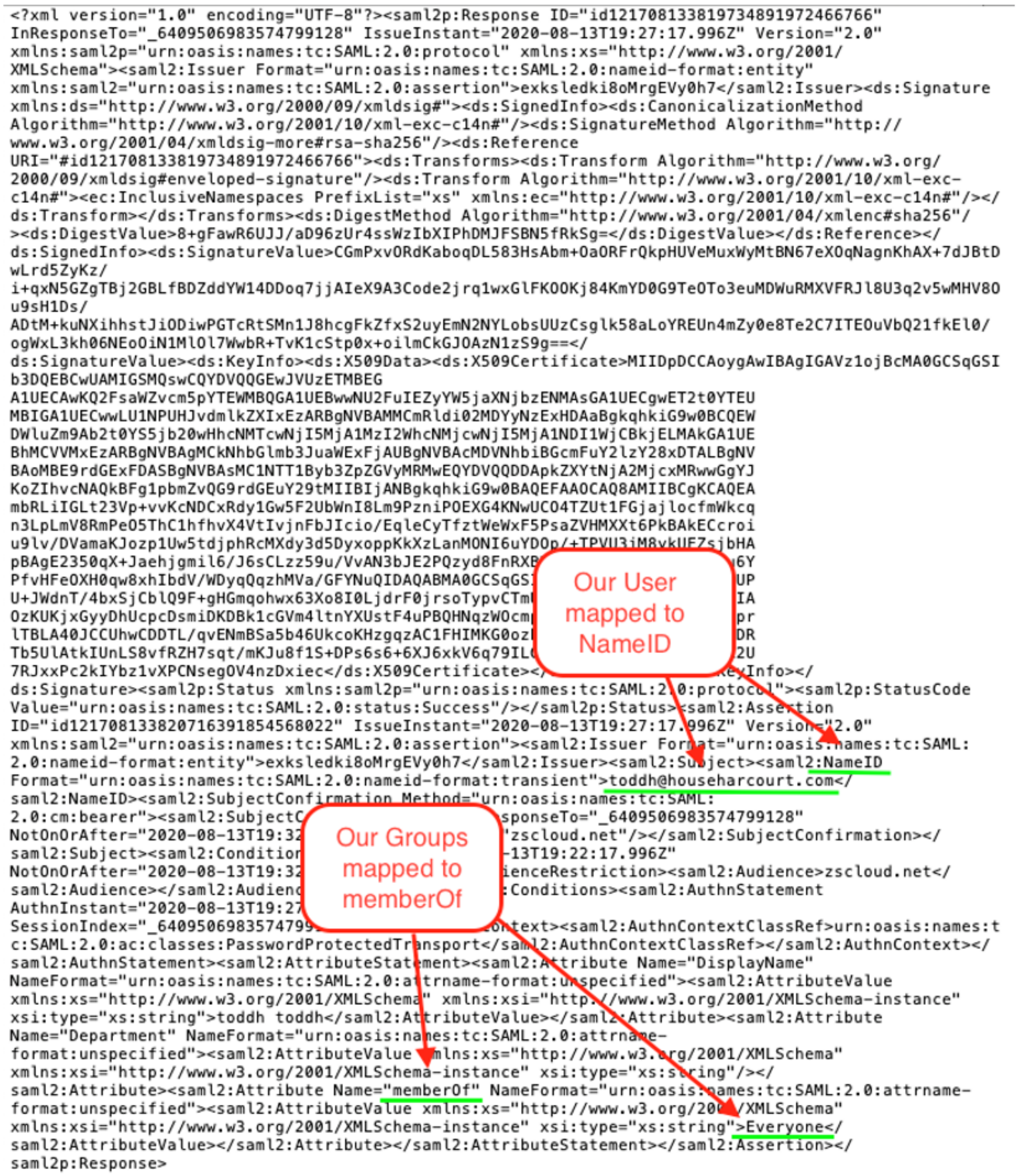


```
htPSJodHRwOi8vd3d3LnczLm9yZy8yMDAxLzEwL3htbC1leGMtYzE0biMiLz48ZHM6U2lnbm 9yaXRobT0iaHR0cDovL3d3dy53My5
vcmcvMjAwMS8wNC94bWxkc2lnLW1vcmUjcnNhLXNoYTI1NiIvPjxkczpSZWZlcmVuY2UgVV MTk3MzQ4OTE5NzI0NjY3NjYiPjxk
czpUcmFuc2Zvcm1zPjxkczpUcmFuc2Zvcm0gQWxnb3JpdGhtPSJodHRwOi8vd3d3LnczLm9 WcjZW52ZWxvcGVkLXNpZ25hdHVyZ
SIvPjxkczpUcmFuc2Zvcm0gQWxnb3JpdGhtPSJodHRwOi8vd3d3LnczLm9yZy8yMDAxLzEv xlYzpJbmNsdXNpdmVOYW1lc3BhY2
VzIFByZWZpeExpc3Q9InhzIiB4bWxuczplYz0iaHR0cDovL3d3dy53My5vcmcvMjAwMS8xM +PC9kczpUcmFuc2Zvcm0+PC9kczp
UcmFuc2Zvcm1zPjxkczpEaWdlc3RNZXRob2QgQWxnb3JpdGhtPSJodHRwOi8vd3d3LnczLn ZyNzaGEyNTYiLz48ZHM6RGlnZXN0
VmFsdWU+OCtnRmF3UjZVSkovYUQ5NnpVcjRzc1d6SWJYSVBoRE1KRlNCTjVmUmtTZz08L2R HM6UmVmZXJlbmNlPjwvZHM6U2lnb
mVkSW5mbz48ZHM6U2lnbmF0dXJlVmFsdWU+Q0dtUHh2T1JkS2Fib3FETDU4M0hzQWJtK09hT1JGclFrcEhVVmVNdXhXeU10Qk42N2VYT3FOYWduS2hBWCs3ZE
pCdER3THJkNVp5S3ovaStxeE41R1pnVEJqMkdCTGZCRFpkZFlXMTRERG9xN2pqQUllWDlBM0NvZGUyanJxMXd4R2xGS09PS2o4NEttWUQwRzlUZU9UbzNldU1
EV3VSTVhWRlJKbDhVM3EydjV3TUhWOE91OXNIMURzL0FEdE0ra3VOWGloaHN0SmlPRGl3UEdUY1J0U01uMUo4aGNnRmtaZnhTMnV5RW1OMk5ZTG9ic1VVekNz
Z2xrNThhTG9ZUkVVbjRtWnkwZThUZTJDN0lURU91VmJRMjFma0VsMC9vZ1d4TDNraDA2TkVvT2lOMU1sT2w3V3diUitUdksxY1N0cDB4K29pbG1Da0dKT0F6T
jF6UzlnPT08L2RzOlNpZ25hdHVyZVZhbHVlPjxkczpLZXlJbmZvPjxkczpYNTA5RGF0YT48ZHM6WDUwOUNlcnRpZmljYXRlPk1JSURwRENDQW95Z0F3SUJBZ0
```

```
BAoMBE9rdGExFDASBgNVBAsMC1NTT1Byb3ZpZGVyMRMwEQYDVQQDDApkZXYtNjA2MjcxMRwwGgYJ
KoZIhvcNAQkBFg1pbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
mbRLiIGLt23Vp+vvKcNDCxRdy1Gw5F2UbWnI8Lm9PzniPOEXG4KNwUCO4TZUt1FGjajlocfmWkcq
n3LpLmV8RmPeO5ThC1hfhvX4VtIvjnFbJIcio/EqleCyTfztWeWxF5PsaZVHMXXt6PkBAkECcroi
u9lv/DVamaKJozp1Uw5tdjphRcMXdy3d5DyxoppKkXzLanMONI6uYDOp/+TPVU3jM8ykUFZsjbHA
pBAgE2350qX+Jaehjgmil6/J6sCLzz59u/VvAN3bJE2PQzyd8FnRXBKYcf4Ofae/1oikN21Zau6Y
PfvHFeOXH0qw8xhIbdV/WDyqQqzhMVa/GFYNuQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA+dDUP
U+JWdnT/4bxSjCblQ9F+gHGmqohwx63Xo8I0LjdrF0jrsoTypvCTmUVebDGyMVjXcxioCHEg/1IA
OzKUKjxGyyDhUcpcDsmiDKDBk1cGVm4ltnYXUstF4uPBQHNqzWOcmp45AzIId7PpIs85ZMnWQlpr
lTBLA40JCCUhwCDDTL/qvENmBSa5b46UkcoKHzgqzAC1FHIMKG0ozheAr39Y8WAbP4BhuCXWhJDR
Tb5UlAtkIUnLS8vfRZH7sqt/mKJu8f1S+DPs6s6+6XJ6xkV6q79ILGfJcSuROli/af6YnCkxuZ2U
7RJxxPc2kIYbz1vXPCNsegOV4nzDxiec</ds:X509Certificate></ds:X509Data></ds:KeyInfo></ds:Signature><saml2p:Status
```

Figure 131. Decoding the Base 64 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 a group called `Everyone`. All groups and attributes associated with the user can be seen in this response.



```
<?xml version="1.0" encoding="UTF-8"?><saml2p:Response ID="id121708133819734891972466766"
InResponseTo="_6409506983574799128" IssueInstant="2020-08-13T19:27:17.996Z" Version="2.0"
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:xs="http://www.w3.org/2001/
XMLSchema"><saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">exksledki8oMrgEVy0h7</saml2: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="#id121708133819734891972466766"><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#"><ec:InclusiveNamespaces PrefixList="xs" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/></
ds:Transform></ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/
><ds:DigestValue>8+gFawR6UJJ/aD96zUr4ssWzIbXIPhDMJFSBN5fRkSg=</ds:DigestValue></ds:Reference></
ds:SignedInfo><ds:SignatureValue>CGmPxvORdKaboqDL583HsAbm+OaORFrQkpHUVeMuxWyMtBN67eXOqNagnKhAX+7dJBtD
wLrd5ZyKz/
i+qxN5GZgTBj2GBLfBDZddYW14DDoq7jjAIeX9A3Code2jrq1wxGlFKOOKj84KmYD0G9TeOTo3euMDWuRMXVFRJl8U3q2v5wMHV8O
u9sH1Ds/
ADtM+kuNXihhstJiODiwPGTcRtSMn1J8hcgFkZfxS2uyEmN2NYLobsUUzCsglk58aLoYREUn4mZy0e8Te2C7ITEOuVbQ21fkEl0/
ogWxL3kh06NEoOiN1MlOl7WwbR+TvK1cStp0x+oilmCkGJOAzN1zS9g==</
ds:SignatureValue><ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIIDpDCCAoygAwIBAgIGAVz1ojBcMA0GCSqGSI
b3DQEBCwUAMIGSMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxEzARBgNVBAMMCmRldi02MDYyNzExHDAaBgkqhkiG9w0BCQEW
DWluZm9Ab2t0YS5jb20wHhcNMTcwNjI5MjA1MzI2WhcNMjcwNjI5MjA1NDI1WjCBkjELMAkGA1UE
BhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xDTALBgNV
BAoMBE9rdGExFDASBgNVBAsMC1NTT1Byb3ZpZGVyMRMwEQYDVQQDDApkZXYtNjA2MjcxMRwwGgYJ
KoZIhvcNAQkBFg1pbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
mbRLiIGLt23Vp+vvKcNDCxRdy1Gw5F2UbWnI8Lm9PzniPOEXG4KNwUCO4TZUt1FGjajlocfmWkcq
n3LpLmV8RmPeO5ThC1hfhvX4VtIvjnFbJIcio/EqleCyTfztWeWxF5PsaZVHMXXt6PkBAkECcroi
u9lv/DVamaKJozp1Uw5tdjphRcMXdy3d5DyxoppKkXzLanMONI6uYDOp/+TPVU3iM8ykUFZsjbHA
pBAgE2350qX+Jaehjgmil6/J6sCLzz59u/VvAN3bJE2PQzyd8FnRXB                  6Y
PfvHFeOXH0qw8xhIbdV/WDyqQqzhMVa/GFYNuQIDAQABMA0GCSqGSI                  UP
U+JWdnT/4bxSjCblQ9F+gHGmqohwx63Xo8I0LjdrF0jrsoTypvCTm                   IA
OzKUKjxGyyDhUcpcDsmiDKDBk1cGVm4ltnYXUstF4uPBQHNqzWOcm                   pr
lTBLA40JCCUhwCDDTL/qvENmBSa5b46UkcoKHzgqzAC1FHIMKG0oz                   DR
Tb5UlAtkIUnLS8vfRZH7sqt/mKJu8f1S+DPs6s6+6XJ6xkV6q79IL                   2U
7RJxxPc2kIYbz1vXPCNsegOV4nzDxiec</ds:X509Certificate></           KeyInfo></
ds:Signature><saml2p:Status xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"><saml2p:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></saml2p:Status><saml2:Assertion
ID="id121708133820716391854568022" IssueInstant="2020-08-13T19:27:17.996Z" Version="2.0"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"><saml2:Issuer Format="urn:oasis:names:tc:SAML:
2.0:nameid-format:entity">exksledki8oMrgEVy0h7</saml2:Issuer><saml2:Subject><saml2:NameID
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">toddh@househarcourt.com</
saml2:NameID><saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:
2.0:cm:bearer"><saml2:SubjectC                   sponseTo="_6409506983574799128"
NotOnOrAfter="2020-08-13T19:32                   "zscloud.net"/></saml2:SubjectConfirmation></
saml2:Subject><saml2:Condition                   -13T19:22:17.996Z"
NotOnOrAfter="2020-08-13T19:32                   ienceRestriction><saml2:Audience>zscloud.net</
saml2:Audience></saml2:Audienc                   :Conditions><saml2:AuthnStatement
AuthnInstant="2020-08-13T19:27
SessionIndex="_640950698357479                   ntext><saml2:AuthnContextClassRef>urn:oasis:names:t
c:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef></saml2:AuthnContext></
saml2:AuthnStatement><saml2:AttributeStatement><saml2:Attribute Name="DisplayName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"><saml2:AttributeValue
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">toddh toddh</saml2:AttributeValue></saml2:Attribute><saml2:Attribute
Name="Department" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified"><saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string"/></
saml2:Attribute><saml2:Attribute Name="memberOf" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified"><saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Everyone</
saml2:AttributeValue></saml2:Attribute></saml2:AttributeStatement></saml2:Assertion></
saml2p:Response>
```

Figure 132. SAML Attributes in the Decoded Assertion

Appendix B: Requesting Zscaler Support

You might need Zscaler Support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler Support is available 24/7 hours a day, year-round.

To contact Zscaler Support

1. Go to **Administration** > **Settings** > **Company profile**.

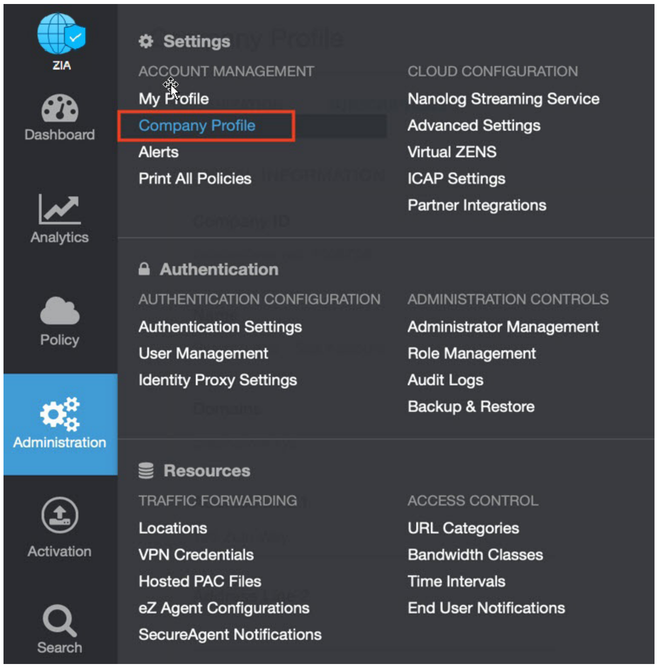
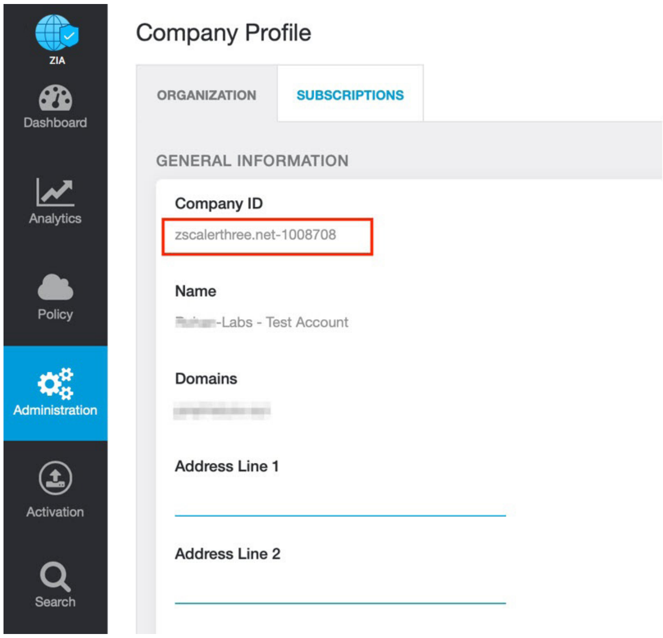


Figure 133. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.



Company Profile

GENERAL INFORMATION

Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 134. Company ID

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

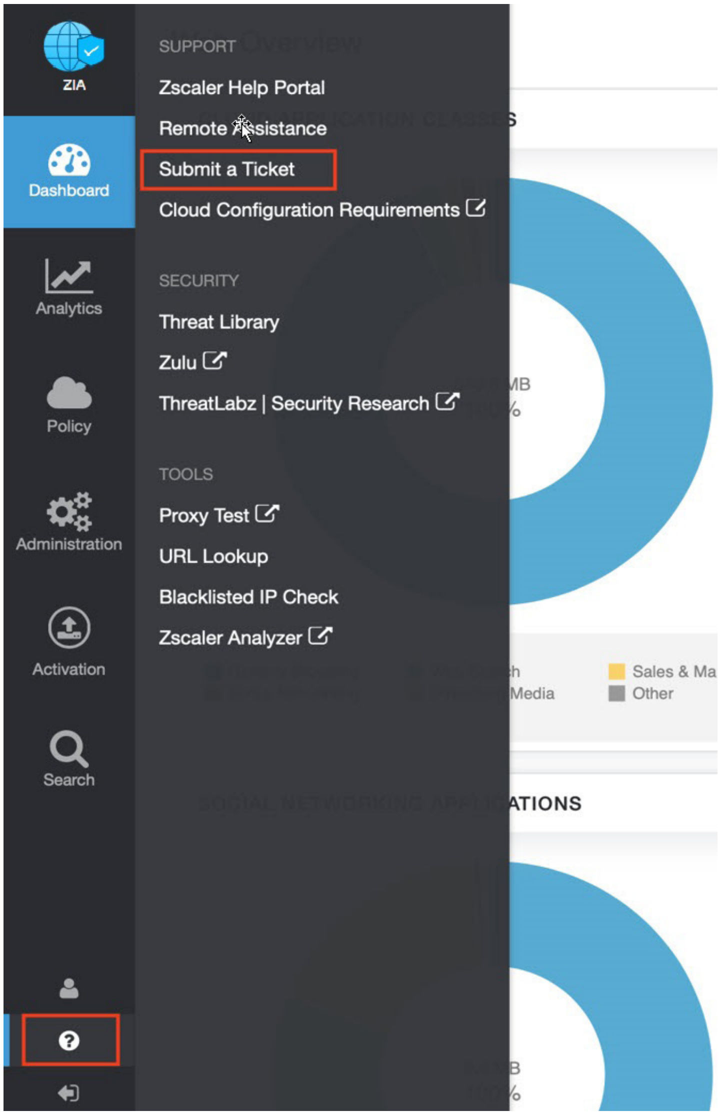


Figure 135. Submit a ticket