



ZSCALER AND IBM VERIFY SSO DEPLOYMENT GUIDE

Contents

Terms and Acronyms	4
Trademark Notice	5
About This Document	6
Zscaler Overview	6
IBM Overview	6
Audience	6
Software Versions	6
Request for Comments	6
Zscaler and IBM Introduction	7
ZIA Overview	7
ZPA Overview	7
Zscaler Resources	7
IBM Security Verify Overview	8
IBM Resources	8
ZIA Configuration	9
Configure Zscaler Application in IBM Security Verify	12
Create or Update Zscaler Application	12
Configure Sign-On	13
Configure Account Lifecycle	14
Define Adoption Policy for Account Synchronization	15
Define Entitlements for the Application	17
Zscaler Provisioning Use Cases	18
Account Synchronization with Zscaler	18
New User Provisioning to Zscaler	20
Create New User	20
Test that the New User Can Login	21
Provisioning Use Case	22
Add User to Group	22
Check that the User is Provisioned to Zscaler	24
Check New User Can Access Zscaler via SSO	25

Deprovisioning Use Case	26
Remove User from Zscaler User Group	26
Zscaler App Role Management Use Cases	28
Assign User to the Zscaler Group Through Permissions	28
Check that the User is Added to the Zscaler Group from Zscaler	30
Remove User from the Zscaler Group Through Permissions	30
Check that the User is Removed from the Zscaler Group	32
Provision a New User and Assign to a Zscaler Group Through Permissions	33
Check that the User is Added to the Zscaler Group from Zscaler	35
Add the User to the Zscaler Group through Roles	35
ZPA Configuration	38
Before you begin	38
Zscaler Configuration	38
IBM Security Verify Zscaler Application Configuration	40
Enable SCIM Configuration for Zscaler	43
Enable Lifecycle for Zscaler Application	44
Define Entitlements for Application	46
Zscaler Provisioning Use Cases	47
New User Provisioning to Zscaler	47
Create New User	47
Test that the New User Can Login	48
Provisioning Use Case	49
Add the User to Group	49
Check that the User is Provisioned to ZPA	51
Check that the New User Can Access Zscaler via SSO	52
Deprovisioning Use Case	52
Remove User from ZPA User Group	52
Check the User is Removed from ZPA	53
Appendix A: Requesting Zscaler Support	54
Save Company ID	54
Enter Support Section	55

Terms and Acronyms

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

Acronym	Definition
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
IKE	Internet Key Exchange (RFC2409)
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SSL	Secure Socket Layer (RFC6101)
XFF	X-Forwarded-For (RFC7239)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

© 2023 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

About This Document

Zscaler Overview

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

IBM Overview

IBM (NYSE: [IBM](#)) looks to be a part of every aspect of an enterprise's IT needs. The company primarily sells software, IT services, consulting, and hardware. IBM operates in 175 countries and employs approximately 350,000 people. The company has a robust roster of 80,000 business partners to service 5,200 clients—which includes 95% of all Fortune 500. While IBM is a B2B company, IBM's outward impact is substantial. For example, IBM manages 90% of all credit card transactions globally and is responsible for 50% of all wireless connections in the world. To learn more, refer to the [IBM Security Verify website](#).

Audience

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

- [Zscaler Resources](#)
- [IBM Resources](#)
- [Appendix A: Requesting Zscaler Support](#)

Software Versions

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

Request for Comments

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

Zscaler and IBM Introduction

This section contains overviews of the Zscaler and IBM applications described in this deployment guide.

ZIA Overview

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

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via 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 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 and Link	Description
ZIA Help Portal	Help articles for ZIA.
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.
ZPA Help Portal	Help articles for ZPA.

IBM Security Verify Overview

Organizations need unified identity repositories and policies to deliver cloud transformation and IT modernization, while enabling a remote workforce and increasing user productivity and security. Simultaneously as consumers pivot faster to digital channels, these same organizations need to provide a consistent, secure, and frictionless experience across channels to their prospects, customers, and citizens.

IBM Security Verify protects users and applications both inside and outside the enterprise, while enabling technical agility and operational efficiency as a cloud-native solution. Beyond single-sign on and multifactor authentication, IBM Security Verify is a modernized, modular IDaaS that provides deep AI-powered context for risk-based authentication and adaptive access decisions, guided experiences for developer time-to-value and comprehensive cloud IAM capabilities. From privacy and consent management to holistic risk detection and identity analytics, IBM Security Verify centralizes workforce and consumer IAM for any hybrid cloud deployment.

IBM Resources

The following table contains links to IBM support resources.

Name and Link	Description
IBM Security Verify product documentation	Online help for IBM Security Verify.
IBM Security Verify developer guides	Online help for IBM developers.
IBM Community Forum	IBM community forum webpages.
IBM Support	IBM support portal for submitting requests and issues.

ZIA Configuration

To allow user provisioning in IBM Security Verify, follow these steps to generate the SCIM URL and token.

1. Log in as an admin user to your ZIA Admin Portal using the following URL:

<https://admin.zscalerbeta.net>

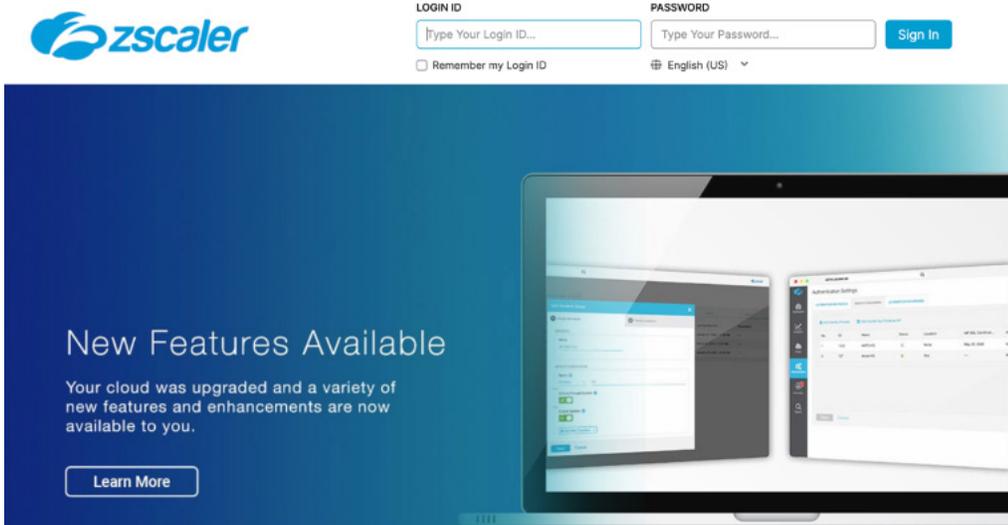


Figure 1. Login to ZIA Admin Portal

2. Go to **Administration > Authentication > Authentication Settings**.

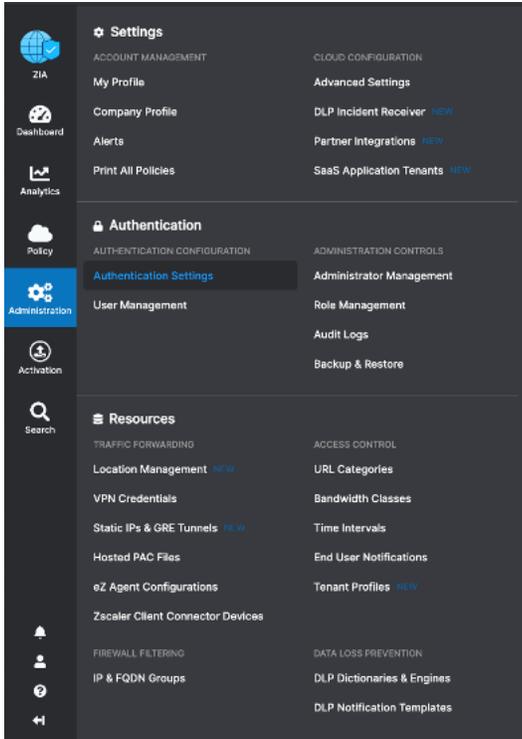


Figure 2. ZIA authentication settings

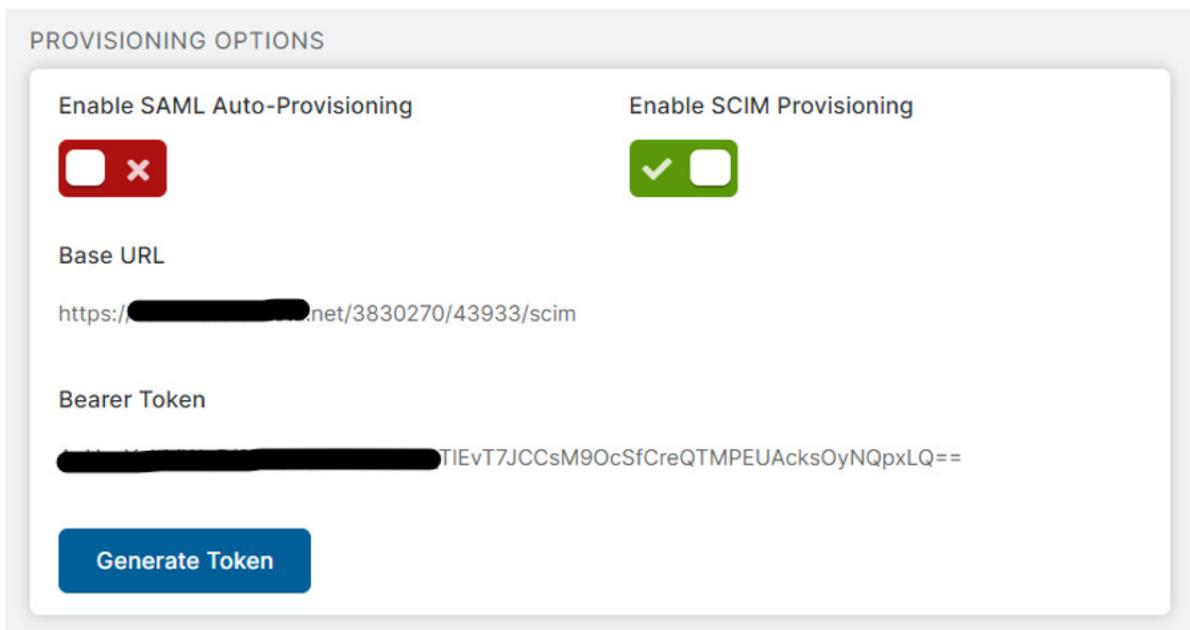
3. For the **Authentication Type** field, select **SAML**.
4. Click **Open Identity Providers**. The **Identity Providers** tab is displayed.
5. Click **Add IdP** (or select the identity provider that you want to modify and click the Edit icon).
6. Provide the following details in the **Add IdP** window:
 - a. For the **General Info** section, specify the following settings:
 - i. **Name**: Provide a name for your identity provider configuration.
 - ii. **Status**: Select **Enabled**.
 - iii. **SAML Portal URL**: `https://xxxxx.verify.ibm.com/saml/sps/saml20ip/saml20/login`
 - iv. **Login Name Attribute**: Provide the login name attribute as **NameID**.
 - v. **Entity ID**: The name of the Zscaler cloud.
 - vi. **Org-Specific Entity ID**: Enable if you have more than one organization instance on the same Zscaler cloud.
 - vii. **IdP SAML Certificate**: Upload the certificate which you can download from IBM Security Verify.
 - viii. **Vendor**: Select **Others**.
 - b. For the **Criteria** section, specify the following settings:
 - i. **Locations**: Select a value from the drop-down menu based on your requirements.
 - ii. **Authentication Domains**: Select a value from the drop-down menu based on your requirements.

The screenshot shows the 'Add IdP' window with the following configuration details:

GENERAL INFO	
Name New Prod	Status Enabled
SAML Portal URL https://[redacted].verify.ibm.com/sa...	Login Name Attribute NameID
Entity ID zscalerbeta.net	Org-Specific Entity ID Disabled
IdP SAML Certificate cic_certificate.pem Upload	IdP SAML Certificate Expiration Date July 25, 2030
Vendor Others	Default IdP Disabled
CRITERIA	
Locations None	Authentication Domains [redacted].com

Figure 3. Add IdP window

- c. In the **Provisioning Options** section:
 - i. **Enable SAML Auto-Provisioning**: Disabled.
 - ii. **Enable SCIM Provisioning**: Enabled.
 - iii. Copy the **Base URL**.
 - iv. Click **Generate Token** to create a bearer token, and copy it.



PROVISIONING OPTIONS

Enable SAML Auto-Provisioning **X**

Enable SCIM Provisioning **✓**

Base URL

https://[REDACTED].net/3830270/43933/scim

Bearer Token

[REDACTED]TIEvT7JCCsM9OcSfCreQTMPEUAcksOyNQpxLQ==

Generate Token

Figure 4. Provisioning options

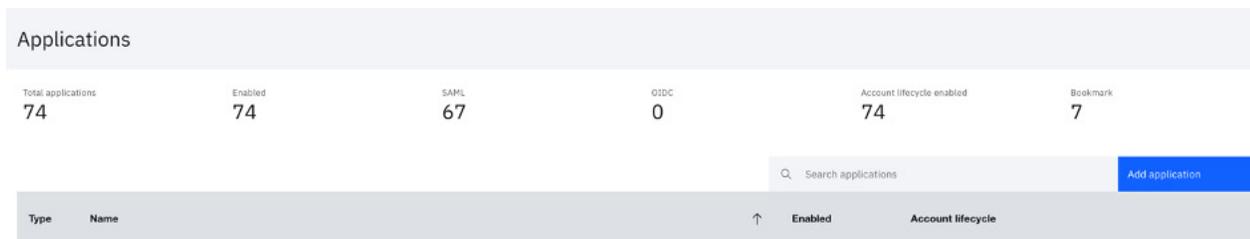
7. Click **Save**.
8. In order to apply the new changes, logout from the ZIA Admin Portal. Changes won't start until you logout.

Configure Zscaler Application in IBM Security Verify

The following sections describe configuring Zscaler in the IBM Security Verify application.

Create or Update Zscaler Application

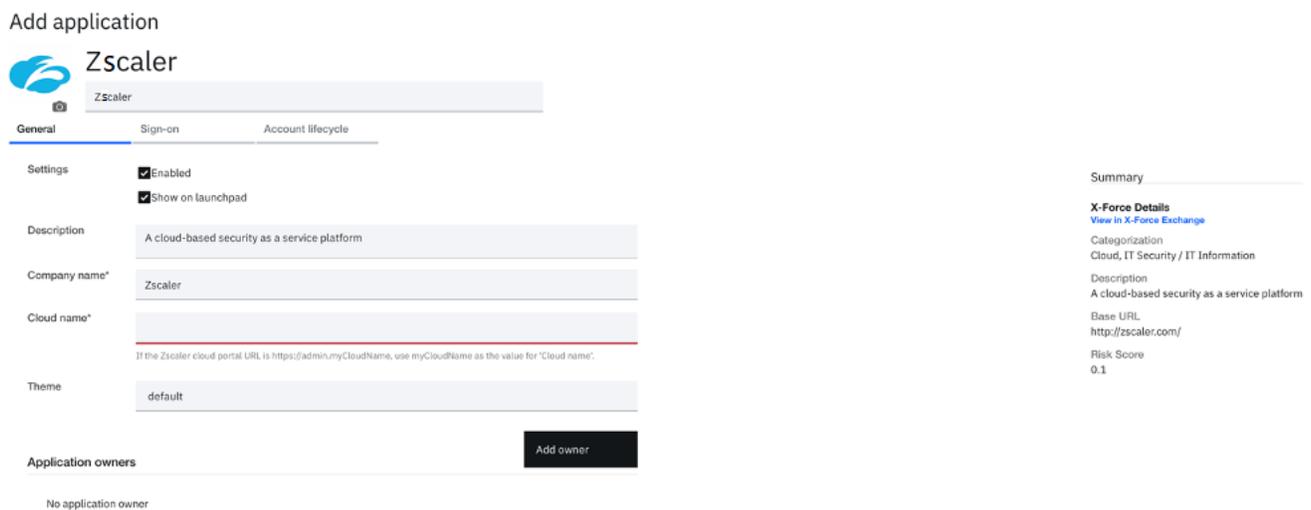
1. Login to IBM Security Verify as a tenant admin.
2. Go to **Applications** page, then click **Add application**.



Applications						
Total applications	Enabled	SAML	OIDC	Account lifecycle enabled	Bookmark	
74	74	67	0	74	7	
<input type="text" value="Search applications"/> Add application						
Type	Name	Enabled	Account lifecycle			

Figure 5. IBM Security Verify Applications

3. On the **Select Application Type** dialog, enter `Zscaler` into the search box.
4. When displayed, select the Zscaler application and then click **Add application**.
5. On the **Add Application** page, leave Zscaler as the **Company name**.
6. Enter the Zscaler cloud portal name (it is part of the URL: `https://admin.<myCloudName>`) as the value for **Cloud name**.



Add application

Zscaler

General Sign-on Account lifecycle

Settings

- Enabled
- Show on launchpad

Description

A cloud-based security as a service platform

Company name*

Zscaler

Cloud name*

If the Zscaler cloud portal URL is `https://admin.myCloudName`, use `myCloudName` as the value for "Cloud name".

Theme

default

Application owners Add owner

No application owner

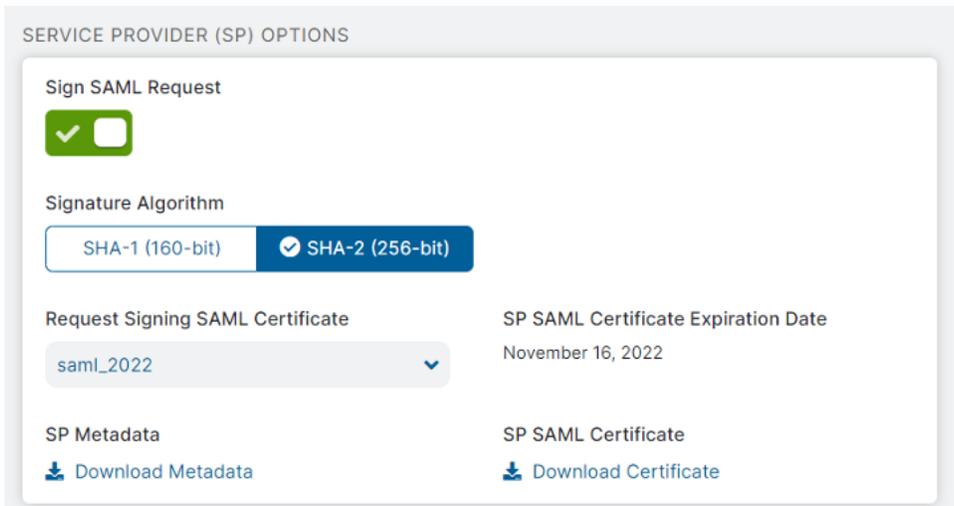
Summary

X-Force Details
[View in X-Force Exchange](#)
 Categorization
 Cloud, IT Security / IT Information
 Description
 A cloud-based security as a service platform
 Base URL
<http://zscaler.com/>
 Risk Score
 0.1

Figure 6. Zscaler application

Configure Sign-On

1. Go to the Zscaler **Sign-on** tab. Follow the on-screen instructions.
2. In another browser, login to your Zscaler account as an admin user. The URL varies depending on your Zscaler cloud, but looks like: `https://admin.<Zscaler Cloud>`.
3. For the **Authentication Type** field, click **Open Identity Providers**. The **Identity Providers** tab is displayed.
4. Select the previously created identity provider and click the **Edit** icon.
5. For the **Service Provider (SP) Options** section, specify the following settings:
 - a. **Sign SAML Request**: Enable this option (If you want to sign the SAML request).
 - b. **Signature Algorithm**: Select SHA-2 (256-bit).
 - c. **Request Signing SAML Certificate**: Select a certificate from the drop-down based on your requirements.
 - d. **SP Metadata**: Click this to download Zscaler metadata.
 - e. **SP SAML Certificate**: If Sign SAML Request is enabled, click this to download Zscaler certificate.



SERVICE PROVIDER (SP) OPTIONS

Sign SAML Request

Signature Algorithm
 SHA-1 (160-bit) | **SHA-2 (256-bit)**

Request Signing SAML Certificate
 saml_2022

SP SAML Certificate Expiration Date
 November 16, 2022

SP Metadata
[Download Metadata](#)

SP SAML Certificate
[Download Certificate](#)

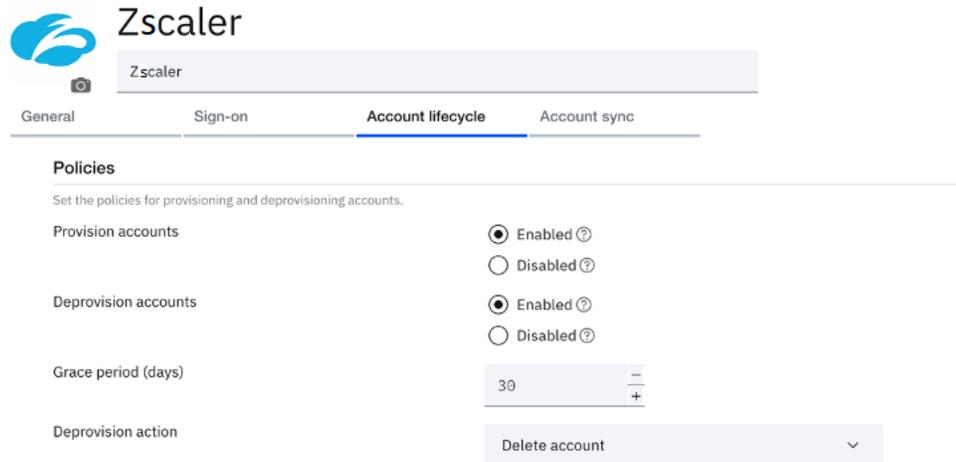
Figure 7. Service Provider options

6. In order to apply the new changes, logout from ZIA Admin Portal. Changes won't apply until you logout.

Configure Account Lifecycle

1. Go to the Zscaler **Account lifecycle** tab.
2. Enable the provisioning and deprovisioning. Zscaler allows **Suspend account** and **Delete account** (with a **Grace period**) as a **Deprovision action**.

Add application



Zscaler

General Sign-on **Account lifecycle** Account sync

Policies

Set the policies for provisioning and deprovisioning accounts.

Provision accounts Enabled ? Disabled ?

Deprovision accounts Enabled ? Disabled ?

Grace period (days) 30 - +

Deprovision action Delete account ▾

Figure 8. Zscaler policies

3. Scroll down to the **API authentication** section.
4. In the **SCIM base URL** field, enter the SCIM URL that you generated earlier.
5. In the **Bearer token** field, enter the token that you generated earlier.



API authentication

API authentication information about the application.

SCIM base URL*

Provide the SCIM URL of your application.

Bearer token*

Bearer token that is required for API calls.

Test connection

Test your connection before you continue.

Figure 9. API authentication

6. Click **Test connection** to confirm the settings.
7. Confirm that connection successful message is shown. If not, verify that **SCIM base URL** and **Bearer token** are entered correctly.

8. Scroll down to the **API Attribute mapping** section and set the following:
 - a. **given_name** = displayName
 - b. **preferred_username** = userName
 - c. **given_name** = name.givenName
 - d. **family_name** = name.familyName
 - e. **email** = Email

Leave the other attributes as-is.

Attribute mapping

Map the attributes that are used to provision accounts in the target application.

Verify attribute Choose from existing attributes	Transformation Transform the value	Target attribute Attribute name in the target app	Keep updated
given_name x v	None x v	→ displayName x v	<input type="checkbox"/>
preferred_username x v	None x v	→ userName x v	<input type="checkbox"/>
department x v	None x v	→ department x v	<input type="checkbox"/>
given_name x v	None x v	→ name.givenName x v	<input type="checkbox"/>
family_name x v	None x v	→ name.familyName x v	<input type="checkbox"/>
email x v	None x v	→ Email x v	<input type="checkbox"/>

[+ Add attribute mapping](#)

Figure 10. Zscaler attribute mapping

9. Click **Save**.

Define Adoption Policy for Account Synchronization

As the Zscaler connection is successfully tested, you must define the adoption policy in order to synchronize the accounts with IBM Security Verify. In order to define the adoption policy, click the Account sync tab from the details of the Zscaler application.

Add application

 **Zscaler**

Zscaler_demo_24thJune

General Sign-on Account lifecycle **Account sync**

Adoption policy

Specify how the account sync operation finds an account's owner in IBM Security Verify. Select at least one attribute pair for the accounts to be adopted.

All of these must be true

[+ Attribute pairs](#)

Figure 11. Account sync tab

1. Click **+ Attribute pairs** to add the attribute rule to match the users from Zscaler with the existing users in IBM Security Verify. Define the rules as:

```
userName = preferred_username
```

Add application

The screenshot shows the Zscaler 'Add application' interface. At the top, the Zscaler logo is on the left, and the application name 'Zscaler' is in the center. Below the name is a text field containing 'Zscaler_demo_24thJune'. A navigation bar below the text field has four tabs: 'General', 'Sign-on', 'Account lifecycle', and 'Account sync', with 'Account sync' being the active tab. Below the tabs is the 'Adoption policy' section. It contains a heading 'Adoption policy' and a sub-heading 'All of these must be true'. Underneath, there is a table with two columns: 'Target attributes' and 'IBM Security Verify attributes'. A single row is visible with 'userName' in the 'Target attributes' column, an equals sign in the middle, and 'preferred_username' in the 'IBM Security Verify attributes' column. There is a dropdown arrow next to 'preferred_username' and a trash icon to its right. At the bottom left of the table area, there is a link '+ Attribute pairs'.

Figure 12. Zscaler Add Application window

2. Click **Save**.

Define Entitlements for the Application

Define the entitlement for users and groups that should get access to this application. When you saved application, the **Entitlements** tab displays:

1. On the **Entitlements** tab, select the radio button for **Select Users and Groups, and assign individual accesses**.
2. Click **Add**.

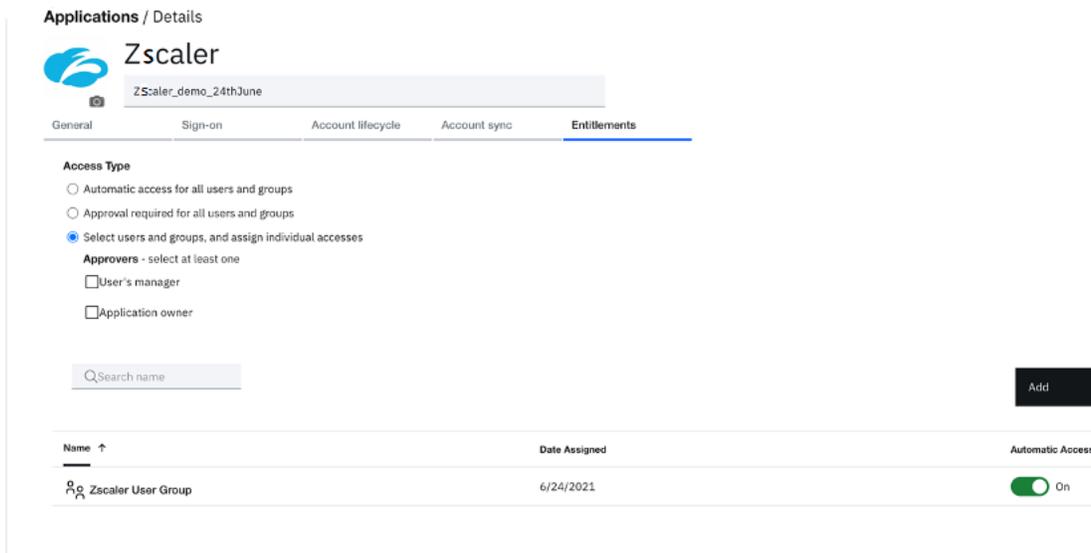


Figure 13. Zscaler Applications/Details window

3. On the **Select User/Group** dialog, search for Zscaler User Group (this group must have been already created by admin).
4. Select **Zscaler User Group** and click **Add**.
5. Click **OK**.

Select User/Group

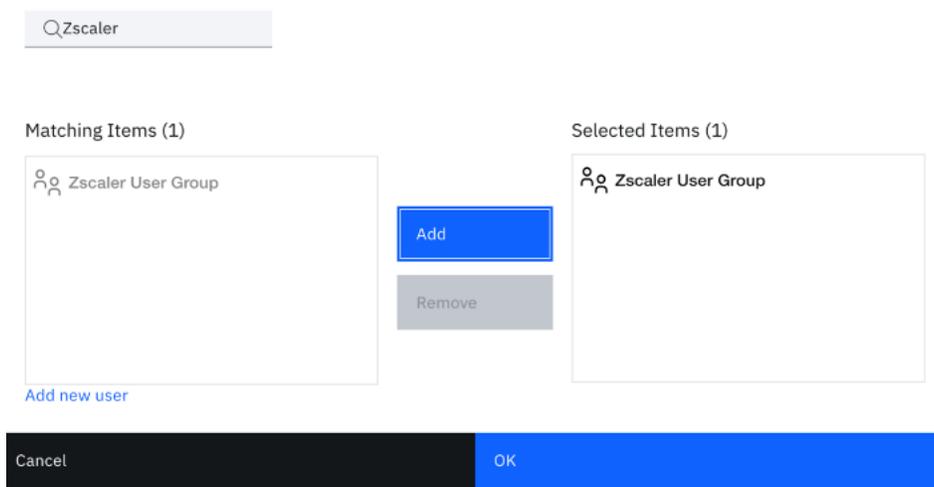


Figure 14. Select User/Group dialog

Zscaler Provisioning Use Cases

After the **Zscaler application** is successfully configured, the tenant admin can synchronize the **Zscaler account data** with IBM Security Verify.

Account Synchronization with Zscaler

1. Login to IBM Security Verify as tenant admin.
2. From the admin console, go to **Applications**.
3. Select **Accounts** from the three dot action menu for the Zscaler application.

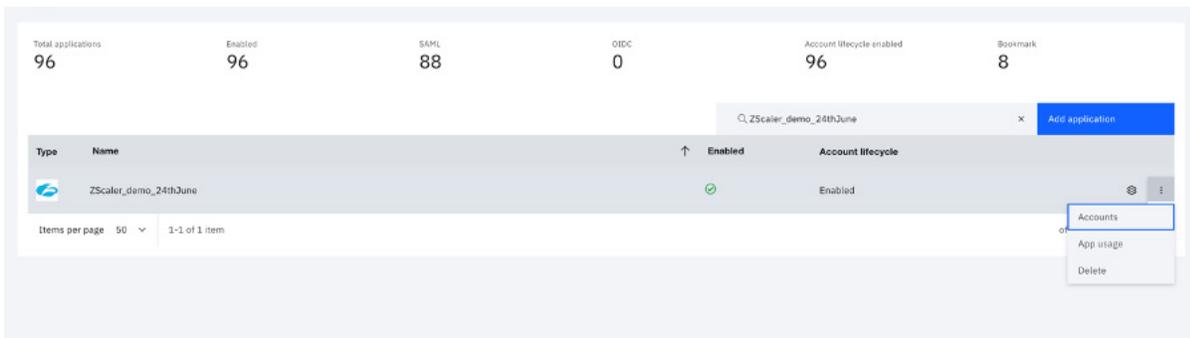


Figure 15. IBM Security Verify accounts

4. Click **Start account synchronization**.

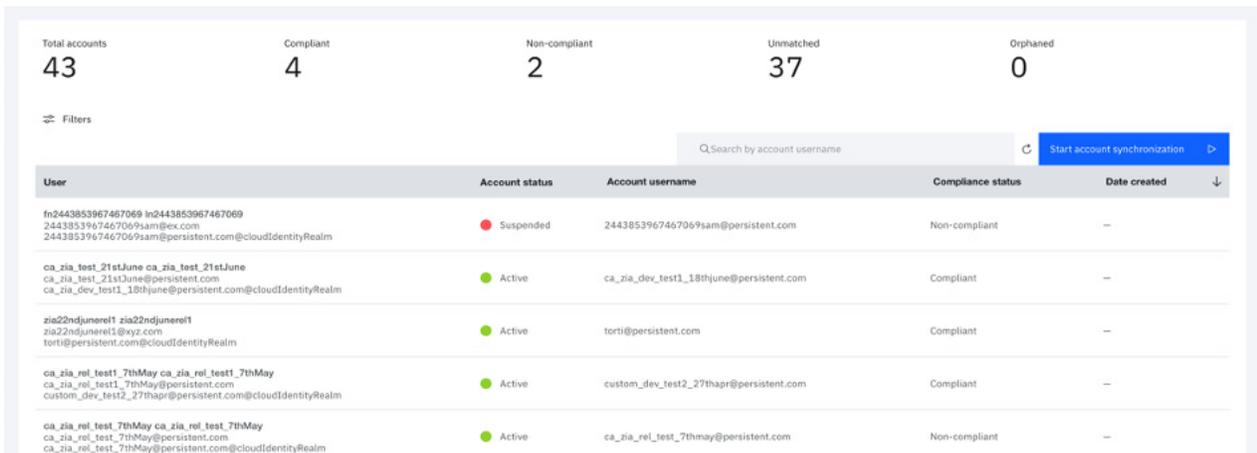


Figure 16. Start account synchronization

5. In order to monitor the account synchronization, go to the **Governance** menu and click the **Account sync** tab

Type	Application name	Status	Start time	End time
	ZScaler_demo_24thJune	Completed	Jun 24, 2021 2:01 PM IST	Jun 24, 2021 2:01 PM IST
	ZScaler_demo_24thJune	Completed	Jun 24, 2021 1:48 PM IST	Jun 24, 2021 1:48 PM IST

Figure 17. Account sync tab

6. Click the row on which you must see the details. The account sync details are opened in the right-side pane and provide the summary of various accounts fetched from the Zscaler.

Type	Application name	Status	Start time	End time
	ZScaler_demo_24thJune	Completed	Jun 24, 2021 2:01 PM IST	Jun 24, 2021 2:01 PM IST
	ZScaler_demo_24thJune	Completed	Jun 24, 2021 1:48 PM IST	Jun 24, 2021 1:48 PM IST

Summary ×

Status
Completed

General
Reconciliation ID
a9f91c87-9f9c-4850-acef-8603c8d717a1
Application name
ZScaler_demo_24thJune

Details

Compliant	4
Non-compliant	2
Unmatched	37
Failed	0

Figure 18. Account details



Account sync rule: Accounts are matched on the attributes mapping defined in the [Define Adoption Policy for Account Synchronization](#) of the application window. So, the admin must define attribute mapping carefully.

New User Provisioning to Zscaler

Create a new user in IBM Security Verify and make sure they can log in.

Create New User

1. Login to IBM Security Verify tenant as an administrative user.
2. From the admin console, go to **Users & groups**.
3. Click **Add user**.
4. Create a user. You can create any user you like (as long as it doesn't clash with existing ones). For example:
 - **Identity Source:** Cloud Directory.
 - **User name:** `zscaleruser01@ex.com` (use the domain name that is registered or associated with the Zscaler identity provider).
 - **Given name:** `User01`.
 - **Surname:** `Zscaler`.
 - **Email:** a valid email address.

×

Add user

On

Basic user profile

Given name
User01

Middle name (optional)

Surname
Zscaler

User name
zscaleruser01@~~example.com~~

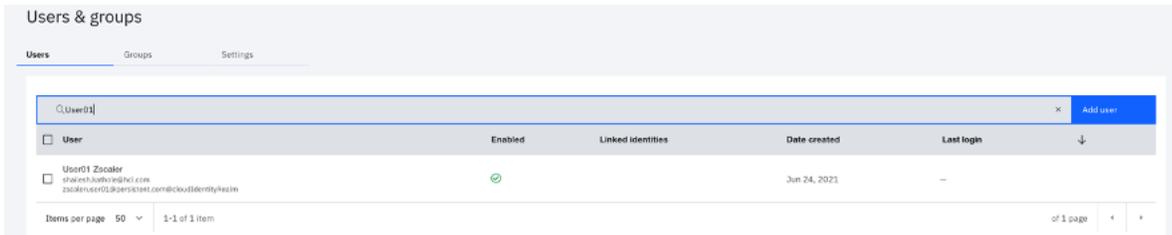
External ID (optional)

Preferred language (optional)

User information

Figure 19. Add user dialog

5. Click **Save**, which creates the user and displays the new user in the Users table.



The screenshot shows the 'Users & groups' management interface. At the top, there are tabs for 'Users', 'Groups', and 'Settings'. Below the tabs is a search bar containing 'User01' and an 'Add user' button. A table lists the user details:

User	Enabled	Linked identities	Date created	Last login
User01 Zscaler shakesh.karthik@hel.com zscaleruser01@prod-eu01a.com@cloudidentity.ibm	<input checked="" type="checkbox"/>		Jun 24, 2023	—

At the bottom, there are controls for 'Items per page' (set to 50) and '1-1 of 1 item'. A pagination indicator shows 'of 1 page'.

Figure 20. New user

Test that the New User Can Login

The new user gets the initial password via email. Go to your email client of the newly created user and look for an email indicating a user has been created.

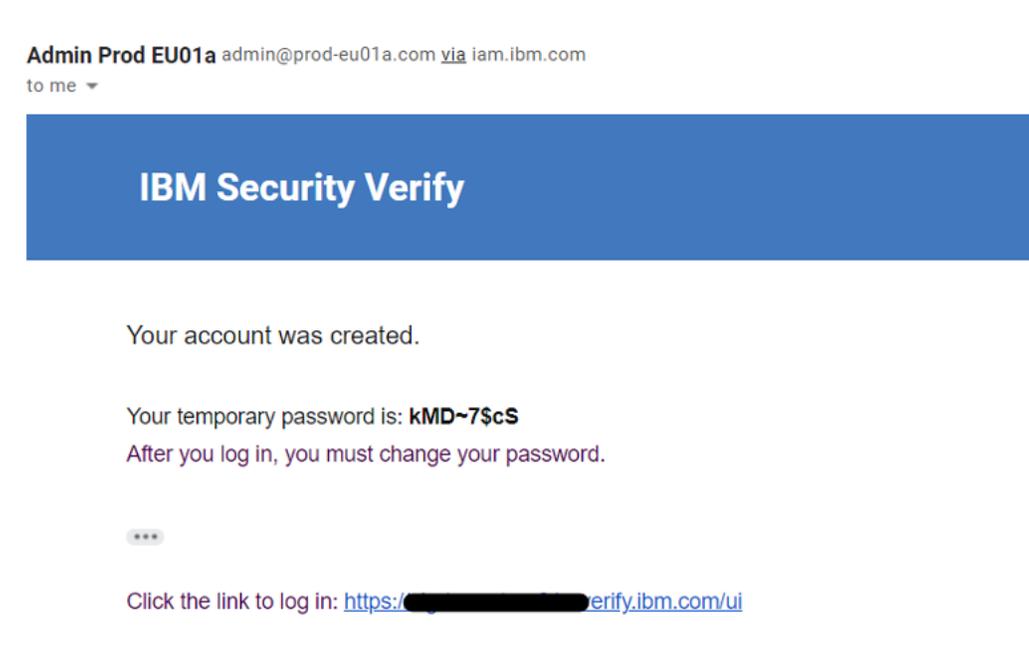


Figure 21. New user email

1. Open a new browser session, copy the link from the email, and log in with the username and password from the email.
2. When prompted, enter a **New password** and **Confirm password**, then click **Change Password**.
3. Validate that the user has access to the IBM Security Verify launchpad.

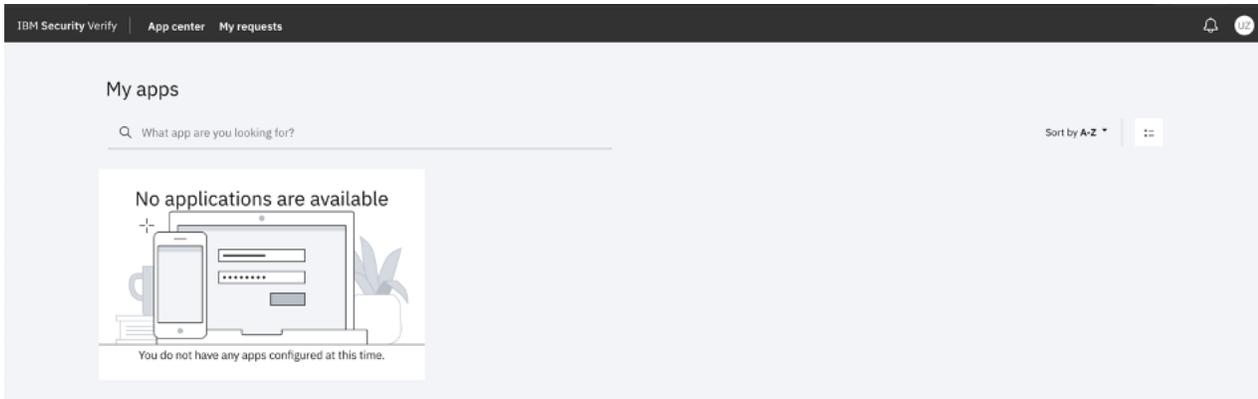


Figure 22. New user in IBM Security Verify

Provisioning Use Case

You have entitled the **Zscaler User Group** with **Automatic access** for the Zscaler application. In order to provision a new Zscaler account for a newly created user, add the new user as a member of the **Zscaler User Group**. Adding a user to this group triggers the automatic provisioning for the Zscaler account.

Add User to Group

Return to the IBM Security Verify admin console as the admin user. You might still have the window open from previous steps.

1. Go to the **Users & groups** section and click the **Groups** tab.
2. Hover over the **Zscaler User Group** and click the **Edit** icon.

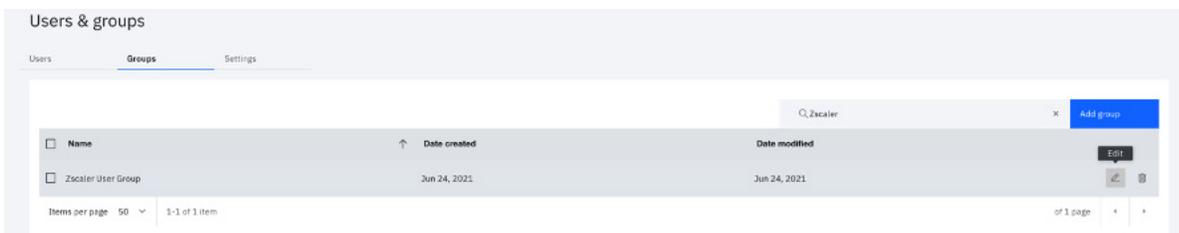


Figure 23. IBM Security Verify Users & groups screen

3. Click **Add** beside **Group Members**.
4. Search for the name of the new user.

- Choose the listed user and click **Select**. This moves the user to **Selected users & groups**.

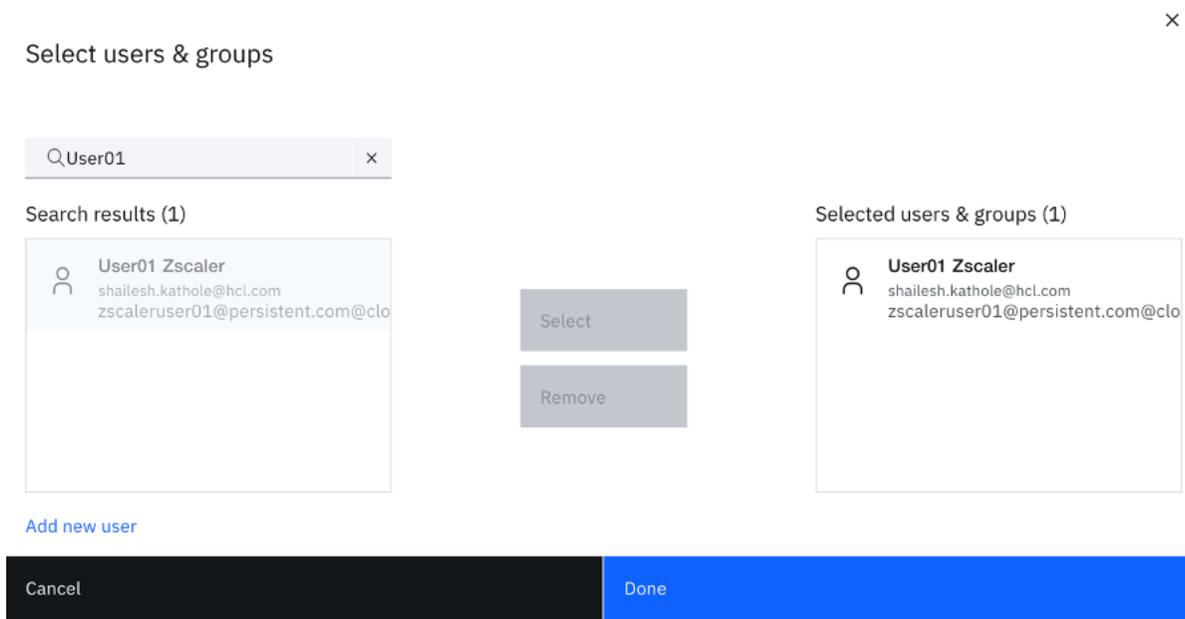


Figure 24. Select users & groups screen

- Click **Done**, then **Save** on the **Edit Group** dialog.
- Return to the **Users** tab, hover over your new user and click the **User Details** icon on the right side.
- Confirm the new user is in the **Zscaler User Group** under **Groups**.

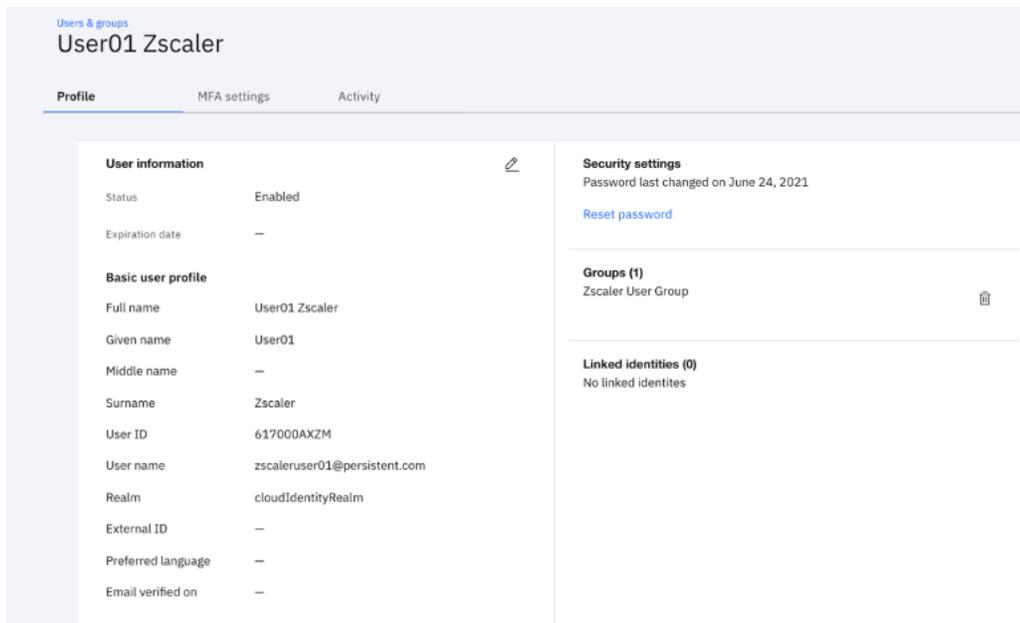
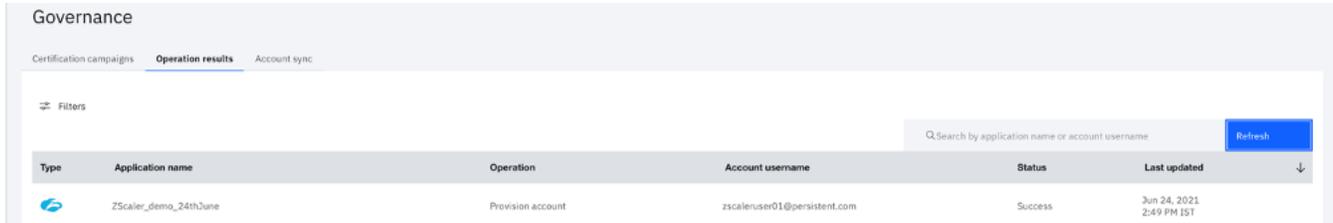


Figure 25. IBM Security Verify user details

Check that the User is Provisioned to Zscaler

Now that the user is added to the **Zscaler User Group**, Zscaler's automatic user provisioning is triggered by IBM Security Verify.

1. From the admin console, go to **Governance > Operation results** tab.



Type	Application name	Operation	Account username	Status	Last updated
	ZScaler_demo_24thJune	Provision account	zscaleruser01@persistent.com	Success	Jun 24, 2021 2:49 PM IST

Figure 26. Operations results tab

2. Validate the new user provisioning by logging in to the ZIA Admin Portal. Go to **Administration > Authentication > User Management**.

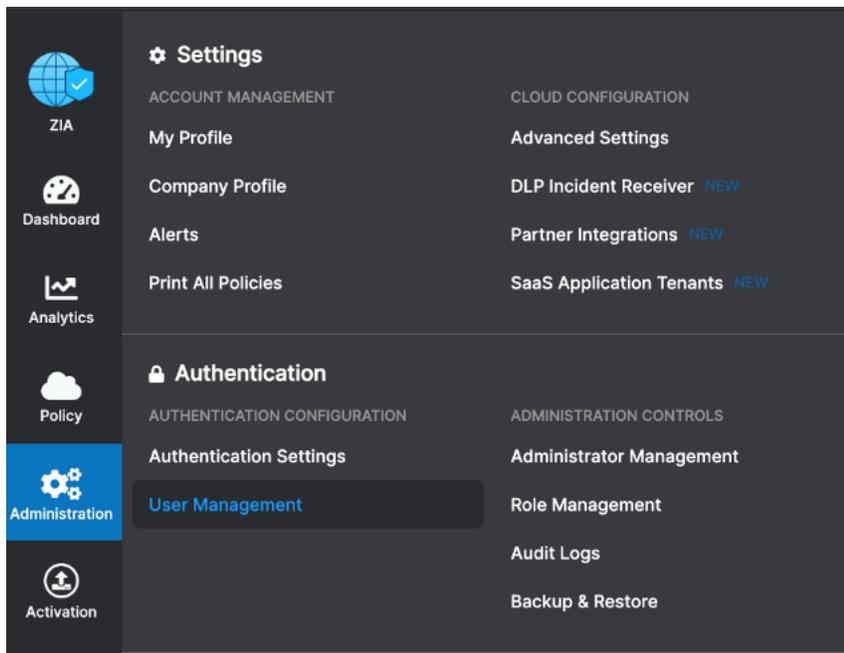
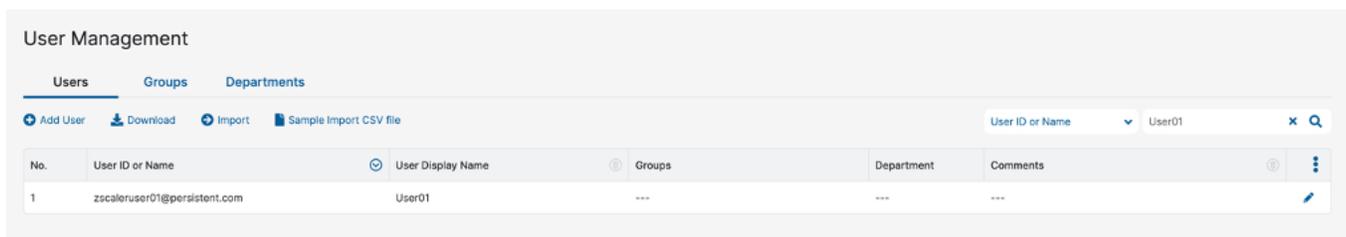


Figure 27. ZIA User Management

3. Look for the newly provisioned user.



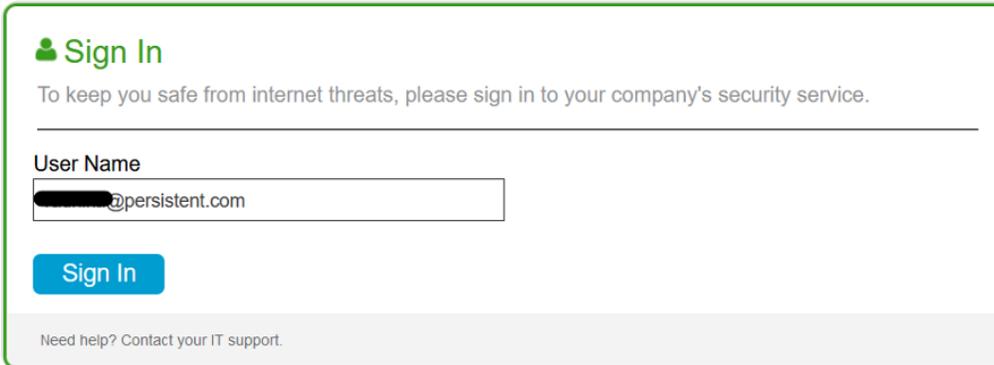
No.	User ID or Name	User Display Name	Groups	Department	Comments
1	zscaleruser01@persistent.com	User01	---	---	---

Figure 28. Newly provisioned user

4. Validate the user details such as:
 - The new user is listed in Zscaler with the correct user name.
 - Other user attributes are created per attribute mapping rules.

Check New User Can Access Zscaler via SSO

1. Access the SP init URL to Zscaler (`http://gateway.your.domain/test`).
2. Enter the **User Name**.



Sign In

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

User Name

██████████@persistent.com

Sign In

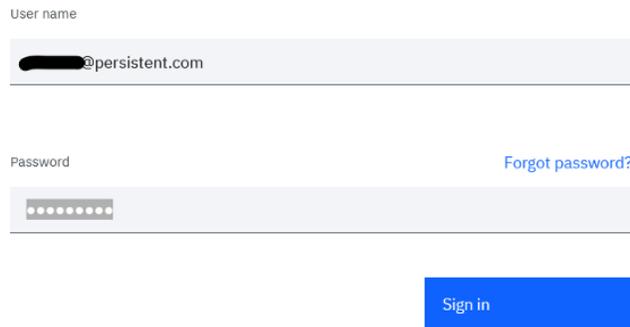
Need help? Contact your IT support.

Figure 29. Zscaler gateway login

3. Validate that user is redirected to IBM Security Verify for SSO.
4. Provide the **User name** and **Password**.

IBM **Security** Verify

Sign in with Cloud Directory



User name

██████████@persistent.com

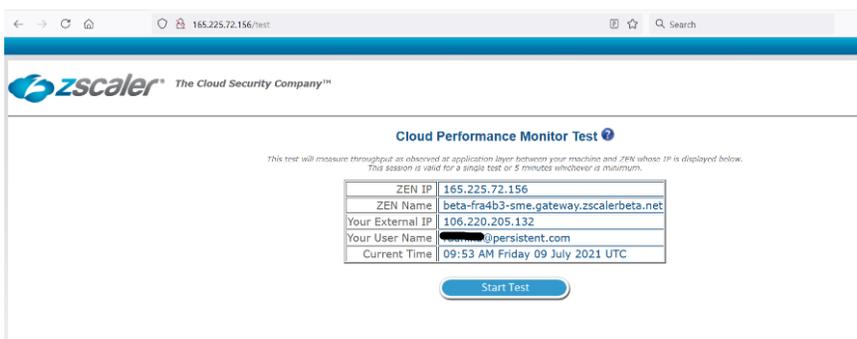
Password [Forgot password?](#)

.....

Sign in

Figure 30. IBM Security Verify admin credentials

5. Verify that the user has access to Zscaler.



zscaler The Cloud Security Company™

Cloud Performance Monitor Test

This test will measure throughput as observed at application layer between your machine and ZEN whose IP is displayed below. This session is valid for a single test or 5 minutes whichever is minimum.

ZEN IP	165.225.72.156
ZEN Name	beta-fra4b3-sme.gateway.zscalerbeta.net
Your External IP	106.220.205.132
Your User Name	██████████@persistent.com
Current Time	09:53 AM Friday 09 July 2021 UTC

Start Test

Figure 31. Zscaler monitor test

Deprovisioning Use Case

Test deprovisioning the user from Zscaler.

Remove User from Zscaler User Group

1. Return to the IBM Security Verify admin console.
2. Go to **Users & groups** and select the **Groups** tab.
3. Edit the **Zscaler User Group**.
4. Select the newly added user and click **Remove**.

The screenshot displays the 'Edit group' interface in the IBM Security Verify admin console. The group name is 'Zscaler User Group'. The description field is empty. The group was created and last modified on June 24, 2021. Below the metadata, there are 'Add' and 'Remove' buttons for managing group members. A search bar is provided to find users or groups by name. A single user, 'User01 Zscaler', is listed with the email addresses shailesh.kathole@hcl.com and zscaleruser01@persistent.com@cloudIdentityRealm. At the bottom, there is a checkbox to 'Send the end-user an email notification regarding this change.' with a note: 'Note: Notification applies when the group's user membership is modified. Notification is not sent to nested group members.' The 'Cancel' and 'Save' buttons are located at the bottom of the form.

Figure 32. IBM Security Verify Edit Group screen

5. Click **Save**.
6. Review the user details in the **Users** tab. Confirm that no groups are listed in the **Groups** section.

The screenshot shows the 'User01 Zscaler' profile page. It has three tabs: 'Profile' (selected), 'MFA settings', and 'Activity'. The 'Profile' tab is divided into two columns. The left column contains 'User information' and 'Basic user profile'. The right column contains 'Security settings', 'Groups (0)', and 'Linked identities (0)'. The 'User information' section shows: Status: Enabled; Expiration date: —. The 'Basic user profile' section shows: Full name: User01 Zscaler; Given name: User01; Middle name: —; Surname: Zscaler; User ID: 617000AXZM; User name: zscaleruser01@persistent.com; Realm: cloudIdentityRealm. The 'Security settings' section shows: Password last changed on June 24, 2021; a 'Reset password' link. The 'Groups (0)' section shows: No groups. The 'Linked identities (0)' section shows: No linked identities.

Figure 33. Users & Groups user details

The admin can monitor the user deprovisioning task by selecting the **Governance > Operation results** tab.

The screenshot shows the 'Governance' section with the 'Operation results' tab selected. Below the tabs are 'Filters' and a search bar 'Search by application name or account username' with a 'Refresh' button. A table displays the operation results:

Type	Application name	Operation	Account username	Status	Last updated
	ZScaler_demo_24thJune	Deprovision account	zscaleruser01@persistent.com	Success	Jun 24, 2021 3:14 PM IST

Figure 34. Operations results tab

Check that the user has been removed from Zscaler:

1. Return to the ZIA Admin Portal and search the **User ID** or **Name**.
2. Verify that no users are listed.

The screenshot shows the 'User Management' section with the 'Users' tab selected. Below the tabs are 'Add User', 'Download', 'Import', and 'Sample Import CSV file' buttons. A search bar contains 'User ID or Name' and 'user01'. Below the search bar is a table with columns: No., User ID or Name, User Display Name, Groups, Department, and Comments. The table is empty and displays the message 'No matching items found'.

Figure 35. User Management tab

Zscaler App Role Management Use Cases

Permission is managed through App Role Management where you can add a user to Zscaler groups. These groups are fetched during account synchronization.

Assign User to the Zscaler Group Through Permissions

1. Login to IBM Security Verify as a tenant admin.
2. From the admin console, go to **App Role Management > Permissions**.
3. Filter your created Zscaler application and check the Zscaler groups.

The screenshot shows the 'App role management' interface in IBM Security Verify. The 'Permissions' tab is active, displaying a list of permissions for the application 'ZScaler_demo_24thJune'. The 'Service Admin' permission is selected, and its details are shown in a modal window.

Permission name	Description	Application	Category
Basic access	Provides access to the application with basic authorization	ZScaler_demo_24thJune	Default
GROUP_NAME_tmj84	—	ZScaler_demo_24thJune	Group
Q2KON	—	ZScaler_demo_24thJune	Group
r2oCk	—	ZScaler_demo_24thJune	Group
Service Admin	—	ZScaler_demo_24thJune	Group

Figure 36. App role management

4. Click any of the GROUPS and click **Manage membership**.

The screenshot shows the 'App role management' interface in IBM Security Verify. The 'Service Admin' group details are displayed in a modal window. The 'Manage membership' button is highlighted at the bottom of the modal window.

Permission name	Description	Application	Category
Basic access	Provides access to the application with basic authorization	ZScaler_demo_24thJune	Default
GROUP_NAME_tmj84	—	ZScaler_demo_24thJune	Group
Q2KON	—	ZScaler_demo_24thJune	Group
r2oCk	—	ZScaler_demo_24thJune	Group
Service Admin	—	ZScaler_demo_24thJune	Group

Figure 37. Manage groups

5. Click **Assign new users**.

Figure 38. Assign new users

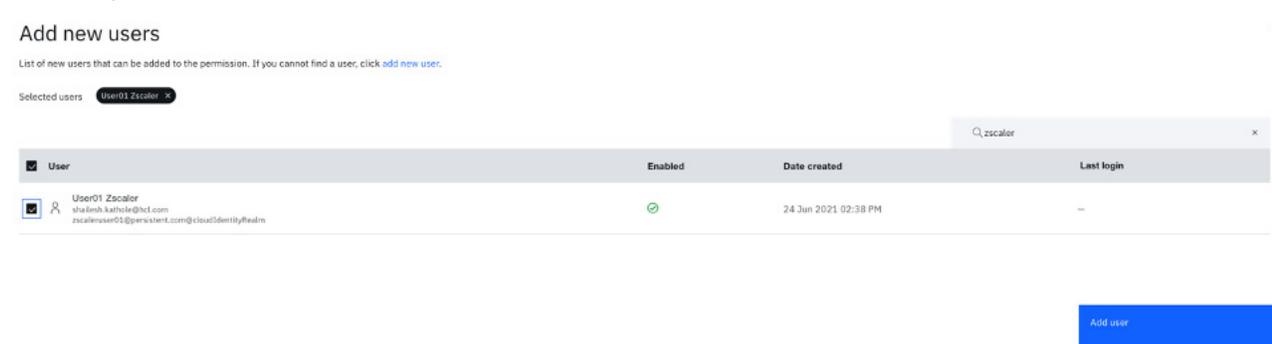
6. Search by the user name, select the user, and click **Add User**.

Figure 39. Add user

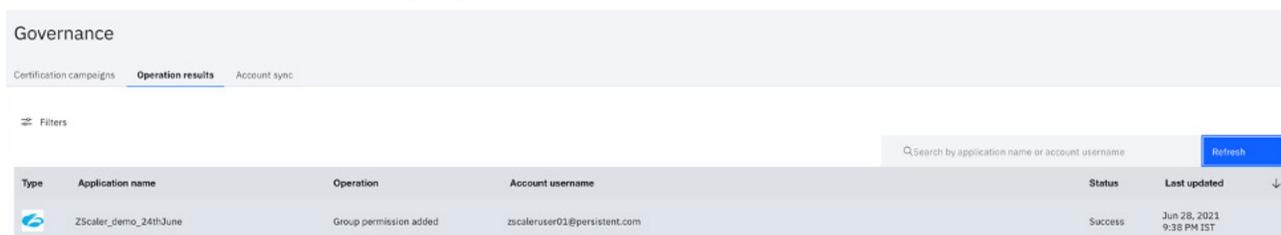
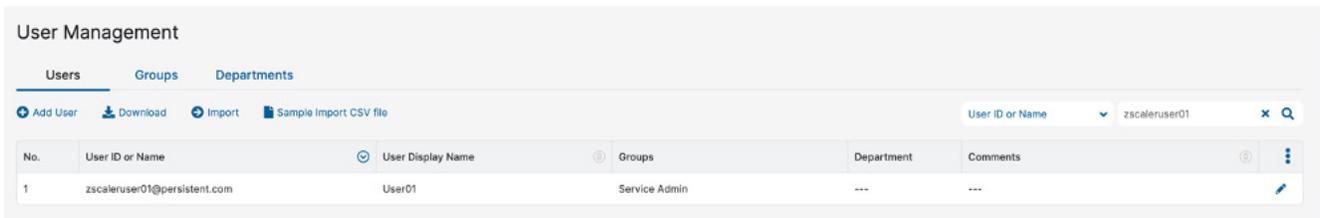
7. Monitor the group permission by going to the **Governance > Operation results** tab.

Figure 40. Operations results tab

Check that the User is Added to the Zscaler Group from Zscaler

1. Return to the Zscaler application and search the user name (zscaleruser01).
2. Ensure that the user has been added to the **Groups** column.



The screenshot shows the 'User Management' interface with tabs for 'Users', 'Groups', and 'Departments'. The 'Users' tab is active. At the top, there are buttons for 'Add User', 'Download', 'Import', and 'Sample Import CSV file'. A search bar contains 'zscaleruser01'. Below is a table with columns: No., User ID or Name, User Display Name, Groups, Department, and Comments. One user is listed with ID 'zscaleruser01@persistent.com', display name 'User01', and group 'Service Admin'.

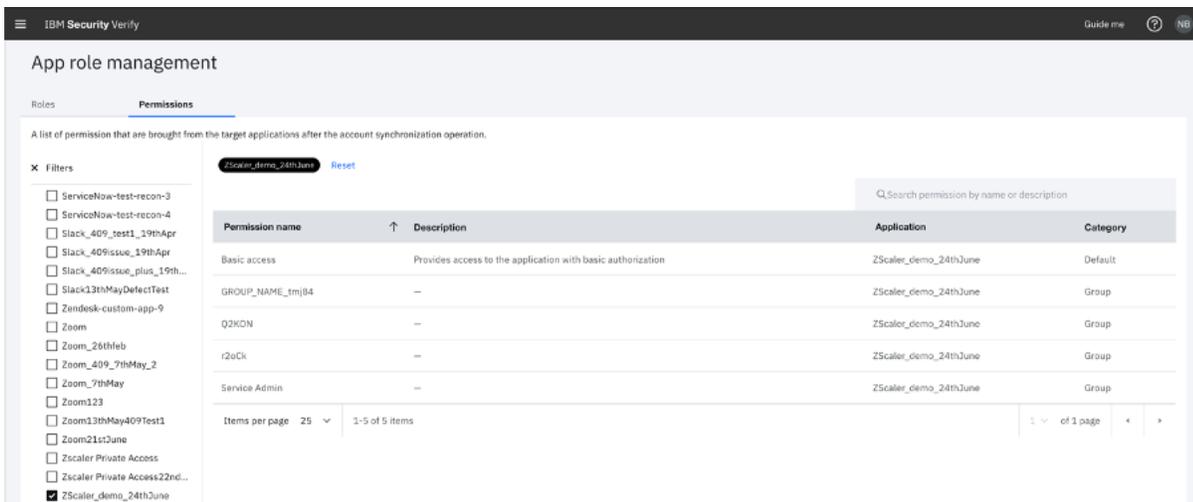
No.	User ID or Name	User Display Name	Groups	Department	Comments
1	zscaleruser01@persistent.com	User01	Service Admin	---	---

Figure 41. User groups

Remove User from the Zscaler Group Through Permissions

When a user is revoked from a Zscaler group, the user is also deprovisioned from the Zscaler application:

1. Login to IBM Security Verify as a tenant admin.
2. From the admin console, go to **App Role Management > Permissions**.
3. Filter your created Zscaler application and check the Zscaler groups.



The screenshot shows the 'App role management' interface in IBM Security Verify. The 'Permissions' tab is active. A search filter 'Zscaler_demo_24thJune' is applied. A table lists permissions with columns: Permission name, Description, Application, and Category. The 'Service Admin' permission is highlighted.

Permission name	Description	Application	Category
Basic access	Provides access to the application with basic authorization	Zscaler_demo_24thJune	Default
GROUP_NAME_fm 84	—	Zscaler_demo_24thJune	Group
Q2KDN	—	Zscaler_demo_24thJune	Group
r2uCK	—	Zscaler_demo_24thJune	Group
Service Admin	—	Zscaler_demo_24thJune	Group

Figure 42. Zscaler groups

4. Click any of the group and click **Manage membership**.

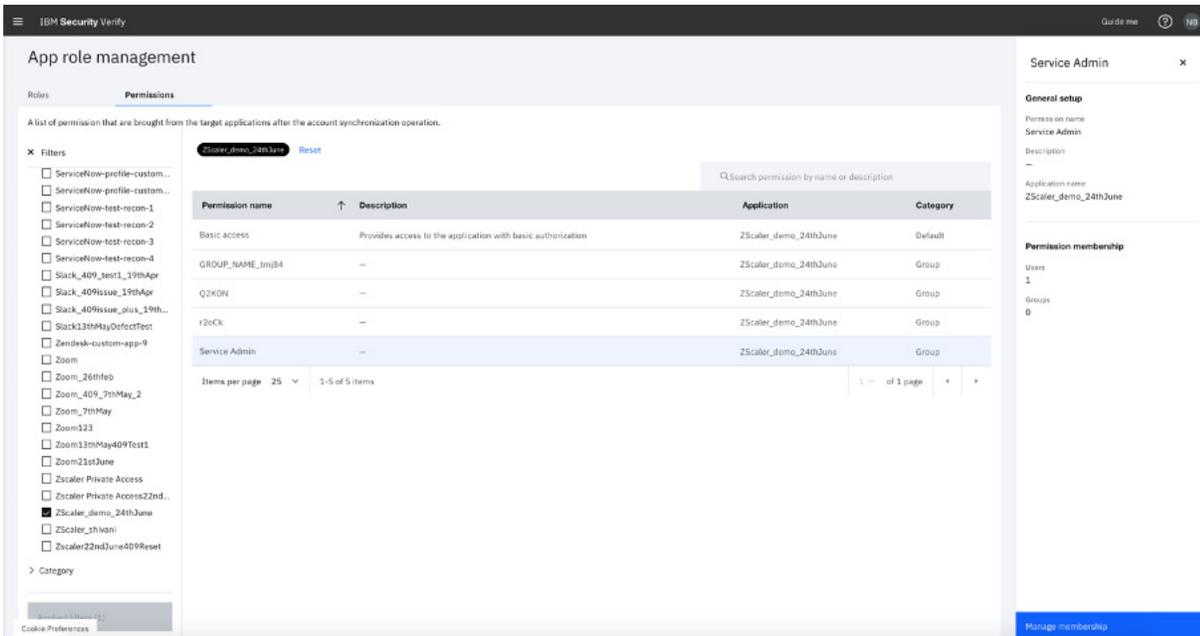


Figure 43. Manage membership

5. Hover over the user whose permission you want to remove and click the **Delete** icon.

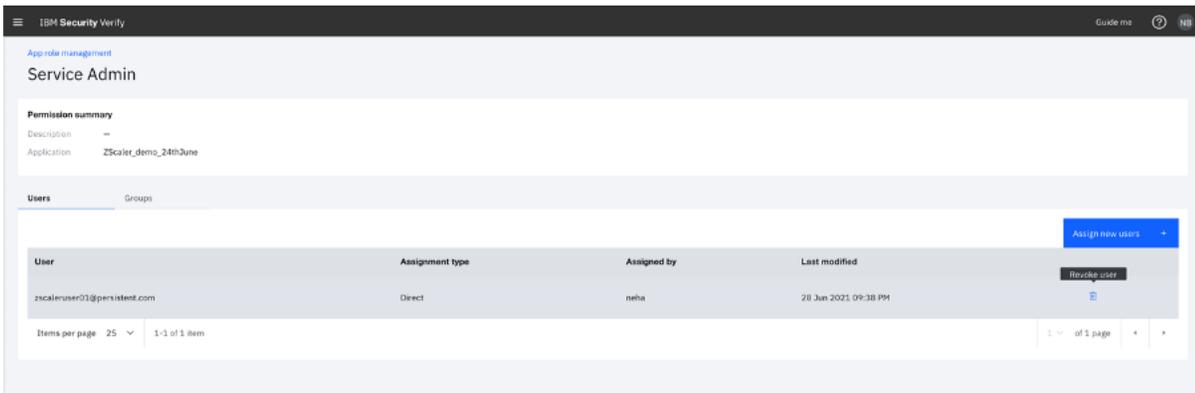


Figure 44. Revoke user

6. Confirm by clicking **Revoke user**.

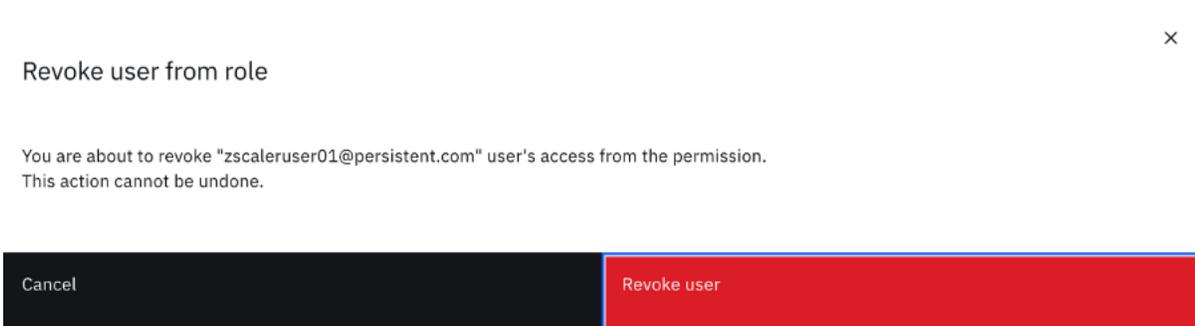


Figure 45. Confirm revoke user

- Monitor the group permission by going to **Governance > Operation results**.

Type	Application name	Operation	Account username	Status	Last updated
	ZScaler_demo_24thJune	Group permission removed	zscaleruser01@persistent.com	Success	Jun 28, 2021, 10:49 PM IST
	ZScaler_demo_24thJune	Devision account	zscaleruser01@persistent.com	Success	Jun 28, 2021, 10:49 PM IST

Figure 46. Review group permissions removed

If your Zscaler application deprovision action is set to **Delete**, then the user is deleted.

Check that the User is Removed from the Zscaler Group

- Return to the ZIA Admin Portal and search by the **User ID** or **Name**.
- Verify that no groups are listed in the **Groups** column.

No.	User ID or Name	User Display Name	Groups	Department	Comments
1	zscaleruser01@persistent.com	User01	---	---	---

Figure 47. Groups column

Provision a New User and Assign to a Zscaler Group Through Permissions

You can also provision a new from to Zscaler through App Role management.

1. Login to IBM Security Verify as a tenant admin.
2. From the admin console, go to **App Role Management > Permissions**.
3. Filter your created Zscaler application and check the Zscaler groups.

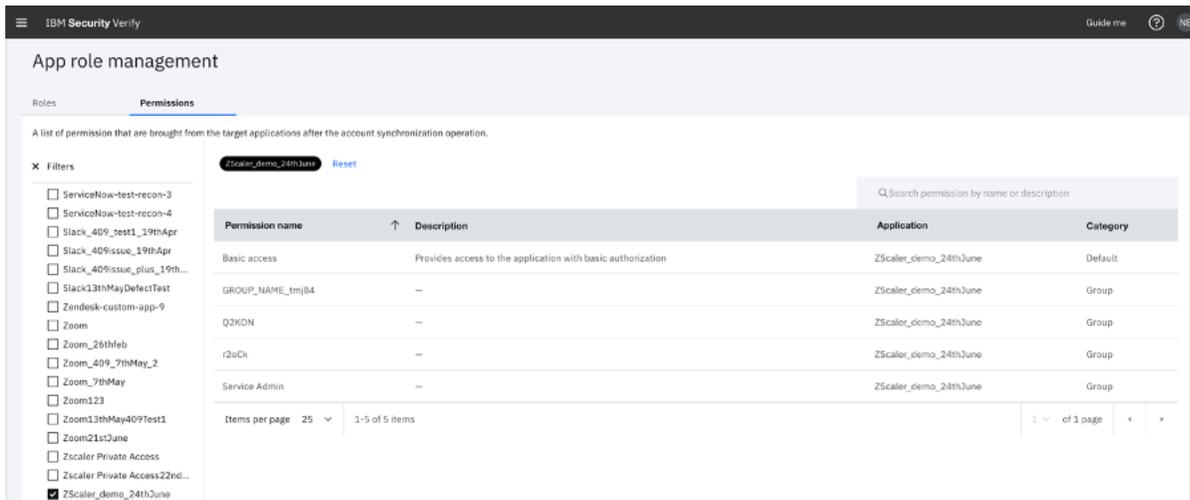


Figure 48. Groups

4. Click any of the groups and click **Manage membership**.

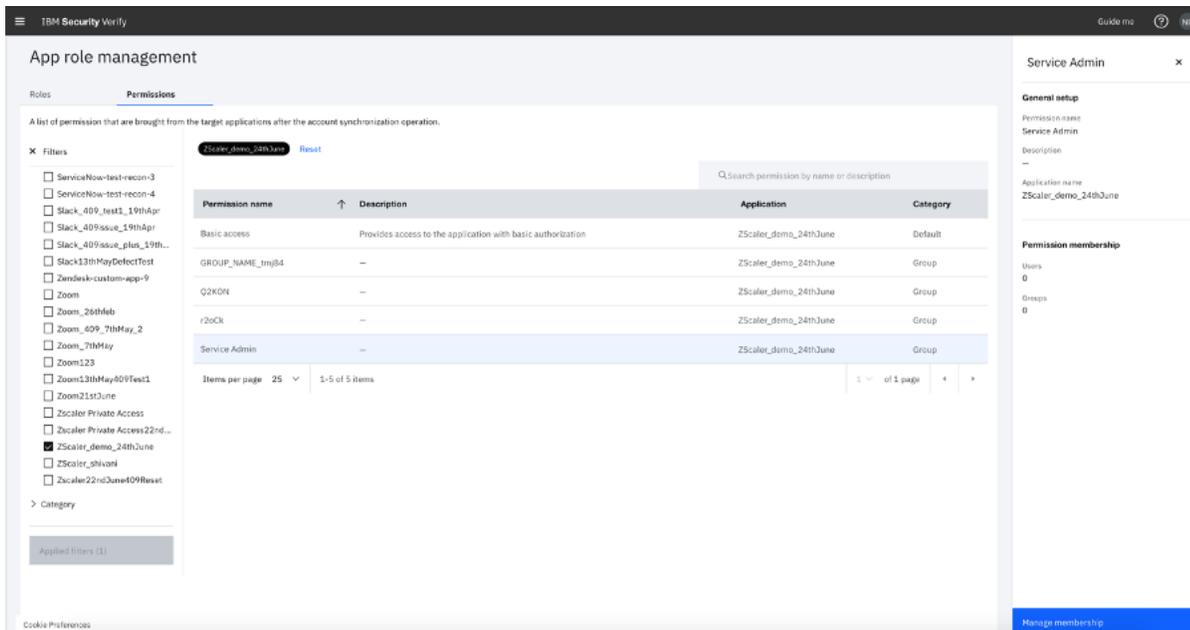


Figure 49. Manage group membership

5. Click **Assign new user**.

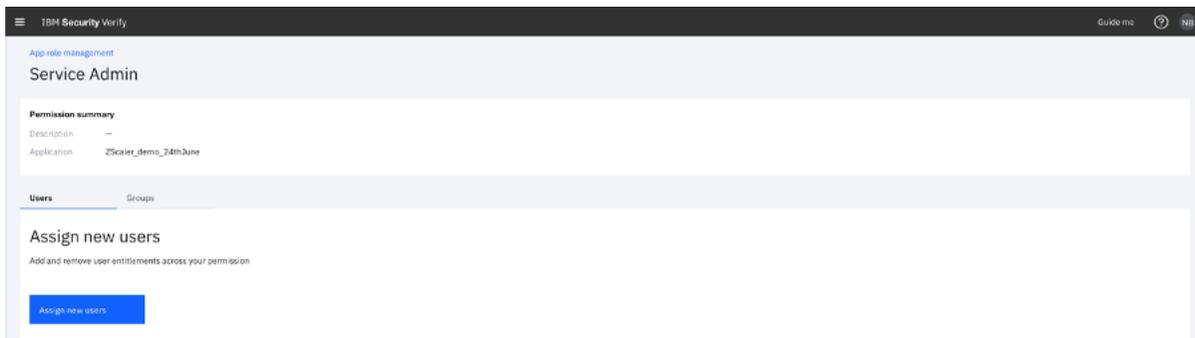


Figure 50. Assign new user

6. Click the **add new user** link. This navigates to the **Users & Groups**.



Figure 51. Add new users

7. Add a new user. To learn more, see [New User Provisioning to Zscaler](#).
8. After the user is created, follow the same steps under [Add the User to the Zscaler Group through Roles](#) section.

You can monitor the group permission.

1. From the admin console, go to **Governance > Operation results**.

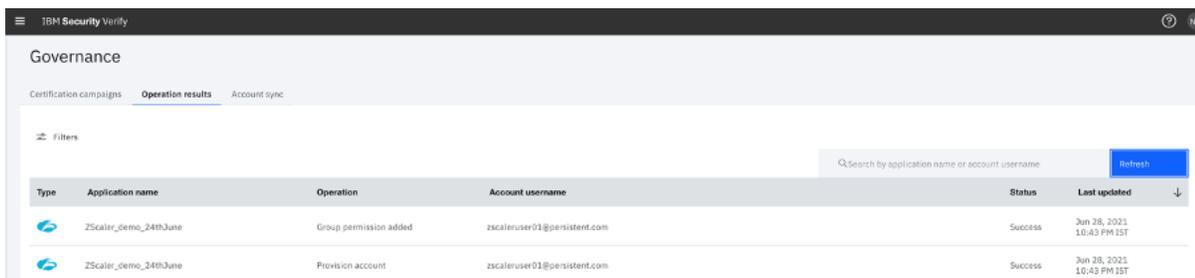
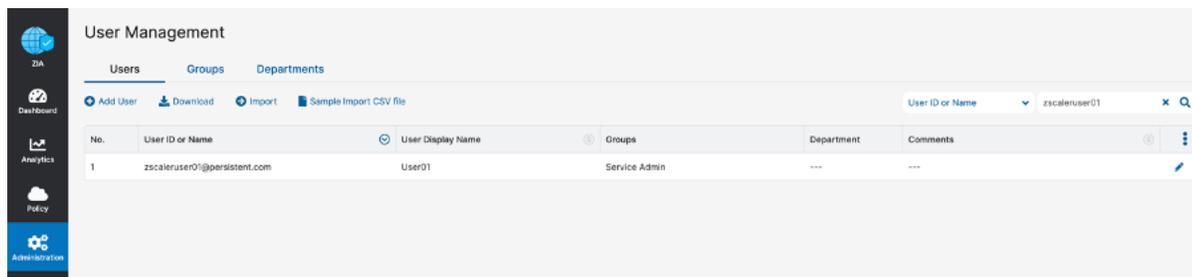


Figure 52. Operations results

2. Provision the user account before adding the group permission when you create a new user.
3. Assign the new user to a group through App Role Management.

Check that the User is Added to the Zscaler Group from Zscaler

1. Return to the ZIA Admin Portal and search by the **User ID** or **Name**.
2. Ensure that the user is added to the Zscaler group in the **Groups** column.



The screenshot shows the 'User Management' page in the ZIA Admin Portal. The 'Users' tab is selected. A search bar at the top right contains 'zscaleruser01'. Below the search bar is a table with the following data:

No.	User ID or Name	User Display Name	Groups	Department	Comments
1	zscaleruser01@persistent.com	User01	Service Admin	---	---

Figure 53. Groups column

Add the User to the Zscaler Group through Roles

You can assign Zscaler groups to the user accounts for the Zscaler application that are enabled with account lifecycle management.

1. Login to IBM Security Verify as a tenant admin.
2. From the admin console, go to **App Role Management > Roles**.
3. Click **Create role**.

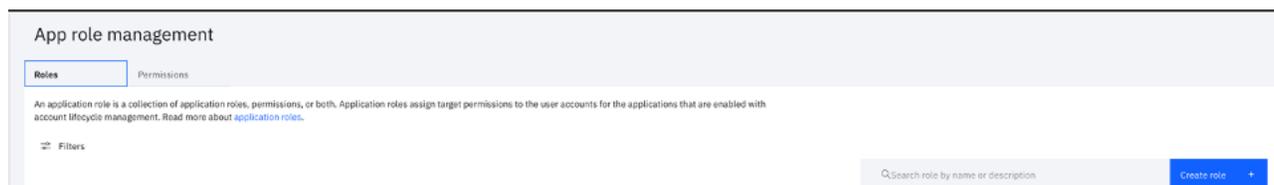


Figure 54. App role management

4. Add the following details:
 - **Role name:** Enter `Zscaler_Role`.
 - **Description:** (Optional) Add a meaningful description.
 - **Select application:** Select the Zscaler application.

5. Click **Next**.

Create role

- General setup (selected)
- Role composition
- Preview

General setup

Give your role a name, description, and select an application.

Role name:

Description (optional):

Select application:

[Cancel setup](#)
Information is not saved on exit.

Next

Figure 55. General setup

6. Go to the **Permissions** tab, select the group, and click **Next**.

Create role

- General setup
- Role composition (selected)
- Preview

Role composition

Select the permissions or roles both that are used to create a role.

Roles: **Permissions**

Selected permissions: **Service Admin**

Search permission by name or description

Permission name	Description	Category	Rights
<input type="checkbox"/> Basic access	Provides access to the application with basic authorization	Default	—
<input type="checkbox"/> GROUP_NAME_tmjB4	—	Group	—
<input type="checkbox"/> Q2KON	—	Group	—
<input type="checkbox"/> r2oCk	—	Group	—
<input checked="" type="checkbox"/> Service Admin	—	Group	—

Items per page: 25 | 1-5 of 5 items | 1 of 1 page

[Cancel setup](#)
Information is not saved on exit.

Back **Next**

Figure 56. Role composition

7. Click **Next**.

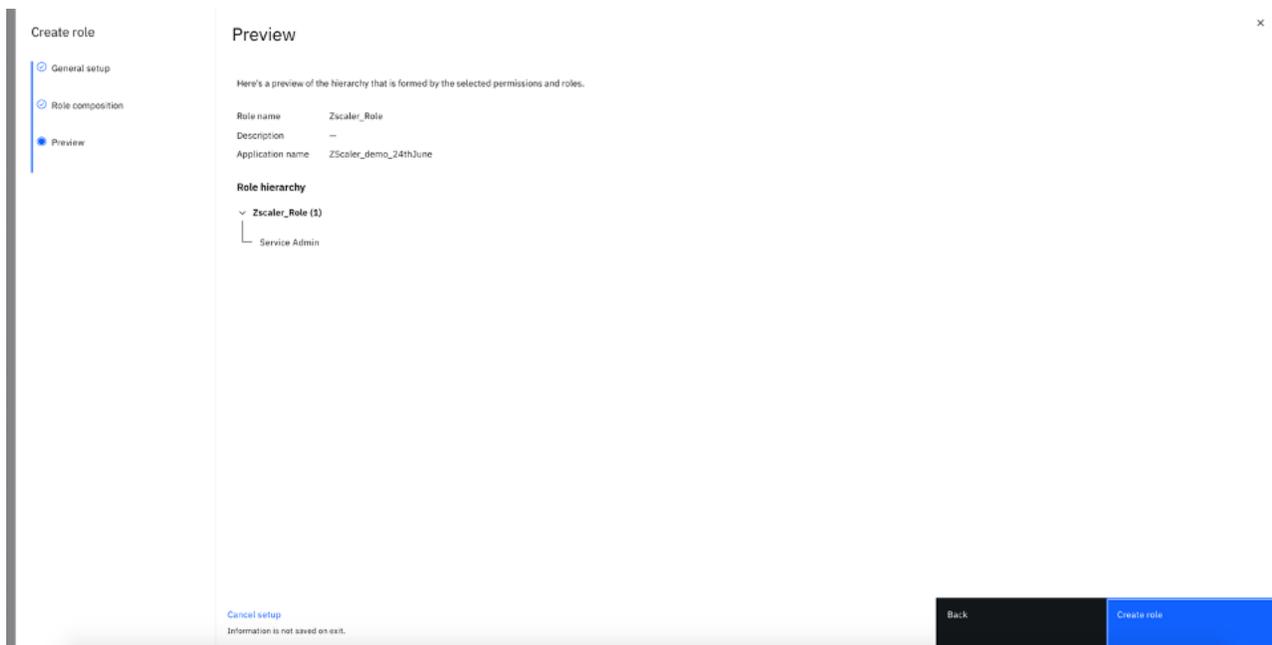


Figure 57. Role preview

8. Click **Create Role**.

9. Search for the **Role Name**.

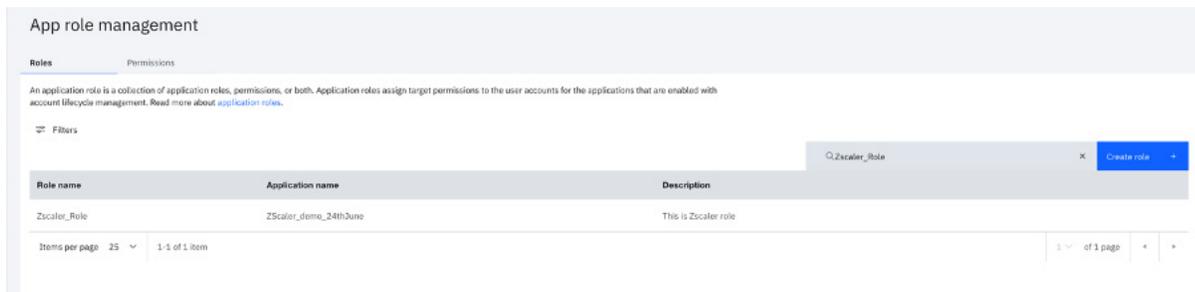


Figure 58. Role name search

10. In order to Manage membership, click the created Role and follow the same steps as mentioned in the [Assign User to the Zscaler Group Through Permissions](#) section or [Provision a New User and Assign to a Zscaler Group Through Permissions](#).

ZPA Configuration

IBM Security Verify provides support for single sign-on (SSO), multifactor authentication (MFA), adaptive access, and account lifecycle management for several applications out of the box. This document provides instructions for configuring IBM Security Verify with ZPA as an application leveraging these capabilities.

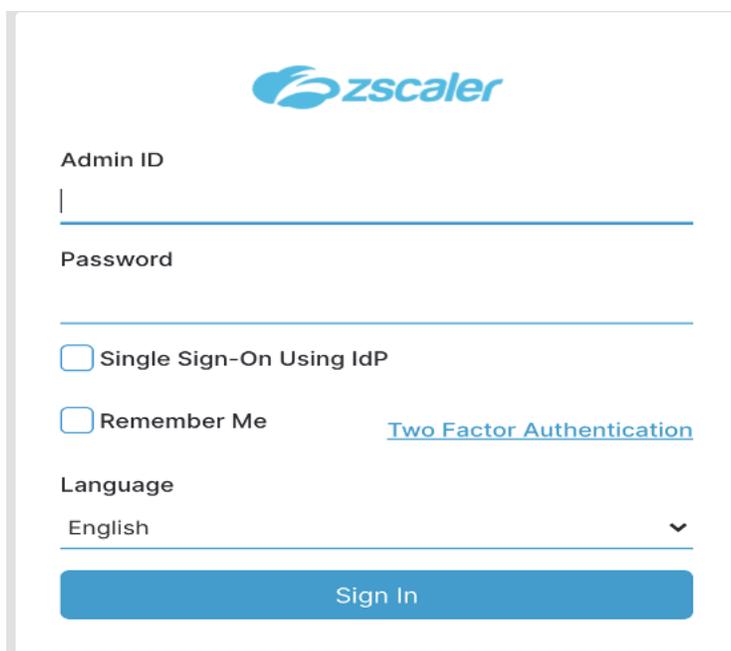
Before you begin

Make sure to have a ZPA account with administrator access.

Zscaler Configuration

To allow Single Sign-on and user provisioning for the ZPA application:

1. Log in as an admin user to your ZPA Admin Portal account.



The screenshot shows the Zscaler Admin Portal login interface. At the top center is the Zscaler logo. Below it, there are two input fields: 'Admin ID' and 'Password'. Under the 'Password' field, there are two checkboxes: 'Single Sign-On Using IdP' and 'Remember Me'. To the right of the 'Remember Me' checkbox is a link for 'Two Factor Authentication'. Below these options is a 'Language' dropdown menu currently set to 'English'. At the bottom of the form is a blue 'Sign In' button.

Figure 59. ZPA log in

2. Go to **Administration > IdP Configuration**.

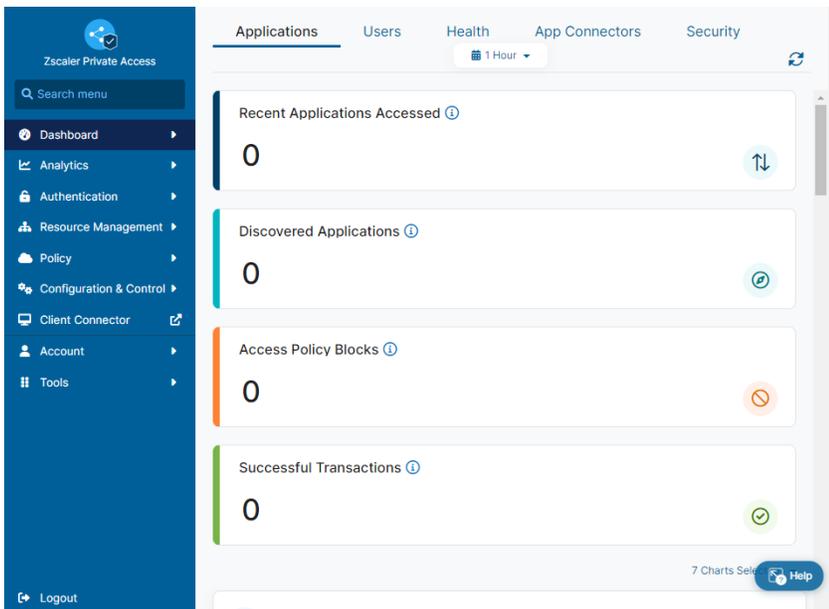


Figure 60. IdP configuration

3. Click **Add IdP Configuration**.
4. Enter a **Name**
5. Select **User** for **Single Sign-on**.
6. Select **User SP Certificate Rotation** from the available list.
7. Select the domains from the available list.

Add IdP Configuration
✕

1 IdP Information
2 SP Metadata
3 Create IdP

Name

Verify User SSO

Single Sign-On

Admin User

User SP Certificate Rotation

ZPA Admin SSO SP cert - Commercial Prod - 1

Domains

✕ nfr.ibm.com

Next
Cancel

Figure 61. Add IdP Configuration

8. Click **Next**. The **SP Metadata** tab is displayed.
9. Download **Service Provider Metadata** and **Service Provider Certificate**.
10. The **Service Provider URL** is displayed. Copy this URL (which is inserted in the **Assertion Consumer Service URL** text field of the ZPA application configuration in IBM Security Verify).
11. The **Service Provider Entity ID** is displayed. Copy this ID (which is inserted in the **Provider ID** text field of ZPA application configuration in IBM Security Verify).

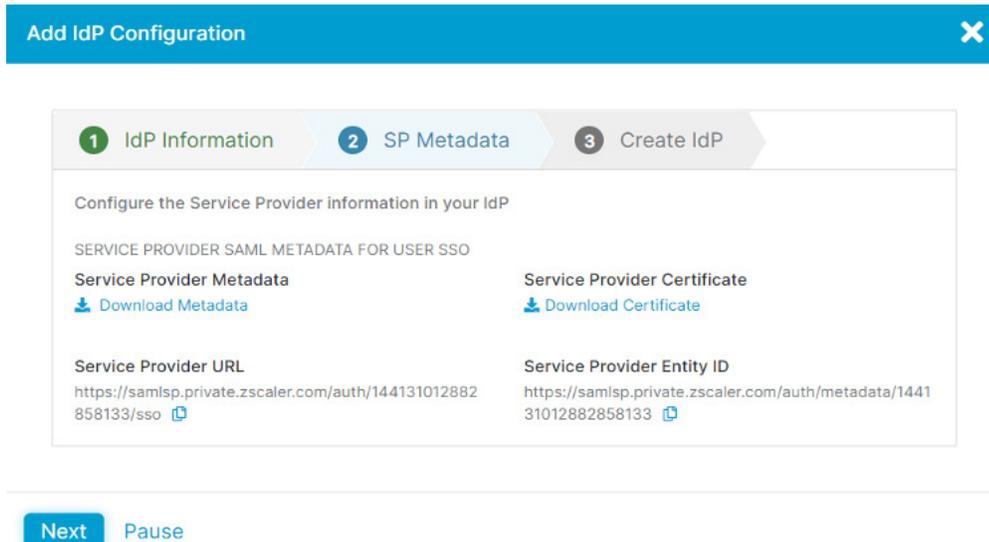


Figure 62. Add IdP Configuration

12. Click **Next**. The **Create IdP** section is displayed.
13. Open a new browser to gather some details.

IBM Security Verify Zscaler Application Configuration

1. In the new browser, login to IBM Security Verify as tenant admin.
2. From the admin console, go to the **Applications** page.
3. Click **Add application**.

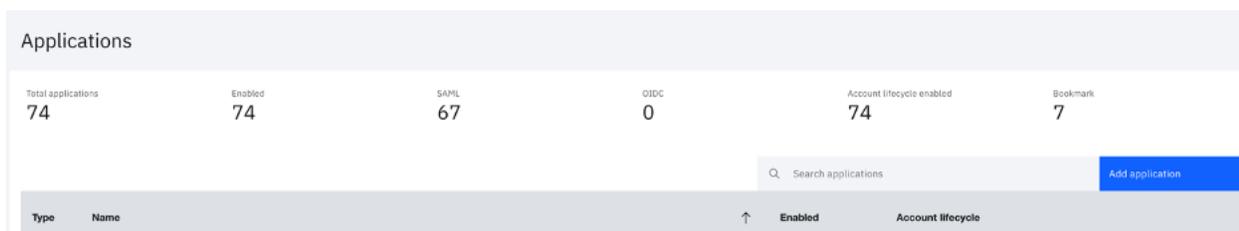


Figure 63. Applications page

4. On the **Select Application Type** dialog, enter `Zscaler Private Access` into the search box.
5. Select the ZPA application when it displays and then click **Add application**.
6. On the **Add Application** page, provide `Zscaler Private Access` as the **Company name**.

Add application

Zscaler Private Access

Zscaler Private Access

General Sign-on Account lifecycle

Settings

- Enabled
- Show on launchpad

Description

A cloud service from Zscaler that provides seamless, zero trust access to private applications running on public cloud or within the data center

Company name*

Zscaler Private Access

Theme

default

Application owners

Add owner

No application owner

Summary

X-Force Details

[View in X-Force Exchange](#)

Categorization

Cloud, IT Security / IT Information

Description

A cloud service from Zscaler that provides seamless, zero trust access to private applications running on public cloud or within the data center

Base URL

http://zscaler.com/products/zscaler-private-access

Risk Score

0.1

Figure 64. Add Application dialog

7. Click the **Sign-on** tab.
8. Follow the instructions displayed in right-side pane.

Add application

Zscaler Private Access

Zscaler Private Access

General Sign-on Account lifecycle

Provider ID*

https://samisp.private.zscaler.com/auth/metadata/144131012882856132

Unique Identifier of the service provider. Use the 'Service Provider Entity ID' value from the Zscaler Private Access (ZPA) IDP Configuration page.

Use unique ID

Assertion consumer service URL (HTTP-POST)*

https://samisp.private.zscaler.com/auth/144131012882856132/sso

The service provider endpoint that receives the SAML assertion. Use the 'Service Provider URL' value from the Zscaler Private Access (ZPA) IDP Configuration page.

Signature options

Use digital signatures to establish trust between IBM Security Verify and the service provider.

Validate SAML request signature

Service Provider Entity ID

Service Provider Entity ID is display Identify provider.

Click Next.

Next tab is displayed.

SAML CONFIGURATION

In the SAML CONFIGURATION sect

IDP Metadata File

https://cig-tenant-eu01a.verify.ibm.com/metadata

If the Use unique ID check box is s

https://cig-tenant-eu01a.verify.ibm.com/metadata/v1/tusID=00c089b2c9

IDP Certificate

Download the certificate for uplo

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

Cancel Save

Figure 65. ZPA Add application

9. Update the **Assertion Consumer Service URL** text field with the **Service Provider URL** copied from Zscaler.
10. Update the **Provider ID** text field with the **Service Provider Entity ID** copied from Zscaler.
11. In the **Instructions** pane, go to the **SAML CONFIGURATION** section and download the IdP Metadata file.
12. Save the application configuration in IBM Security Verify.
13. Return to the ZPA Admin Portal and upload the downloaded IdP Metadata in the **IdP Certificate** section of the **Edit IdP Configuration** window.

Edit IdP Configuration

IdP Metadata File

metadata.xml Change Remove

IdP Certificate

Upload the Certificate File... Select File

```
-----BEGIN CERTIFICATE-----
MIIDPjCCAiagAwIBAgIERZV5vTANBgqhkiG9w0BAQsFADBhMQkwBwYDVQQGEwAxCTAHBgNVBAGTADEJ
MAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAStADEoMcyGA1UEAxMFY2InLXRlbnFudC1ldTAxYS55
2ZXJpZnkuZWJlLnNvbTAeFw0yMDA3Mjc3MjA3MTA3MjA3MjA3MjA3MjA3MjA3MjA3MjA3MjA3MjA3
EJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADEJMAcGA1UECzMAMScGwJgYDVQQDEx9ja
-----
```

Single Sign-On URL

https://cig-tenant-eu01a.verify.ibm.com/saml/sps/saml20ip/saml20/login

IdP Entity ID

https://cig-tenant-eu01a.verify.ibm.com/saml/sps/saml20ip/saml20

Figure 66. Edit IdP Configuration

14. Set **Status** as **Enabled**.
15. Set **SAML Attributes for Policy** as **Enabled**.
16. **Save** the configuration.

Enable SCIM Configuration for Zscaler

1. Log in as an admin user to your ZPA Admin Portal (continue to use an existing session if not logged out).
2. From the admin console, go to **Administration > IdP Configuration**.
3. Edit the IdP configuration created earlier.

Name	Status	IDP Entity ID	Single Sign-On	Actions
Admin	Enabled	https://fivibm2021.net/verify/ibmcloudsecurity.com/saml/https://saml20p/saml20	Admin	Edit Delete
ZPA User SSO	Enabled	https://ocp-test1.prep-cn.cloudidentity.ibm.com/saml/https://saml20p/saml20	User	Edit Delete

Figure 67. IdP Configuration

4. In the **Edit IdP Configuration** window, select **Enabled** for **SCIM Sync**.
5. Copy the **SCIM Service Provider Endpoint**.
6. Click **Generate New Token** to create a bearer token and copy it.
7. Click **Save**.

SCIM CONFIGURATION

SCIM Sync: Enabled Disabled

SCIM Attributes for Policy: Enabled Disabled

SCIM Service Provider Endpoint
<https://scim1.private.zscaler.com/scim/1/144131012882858133/v2>

Bearer Token
 This client secret will not display again. Copy it to your clipboard before exiting.
 KtpBnLF-daH-W3id6JPAAf0t3tMuAWD9V38u5... [REDACTED] ...MQL1Ghw

[Generate New Token](#)

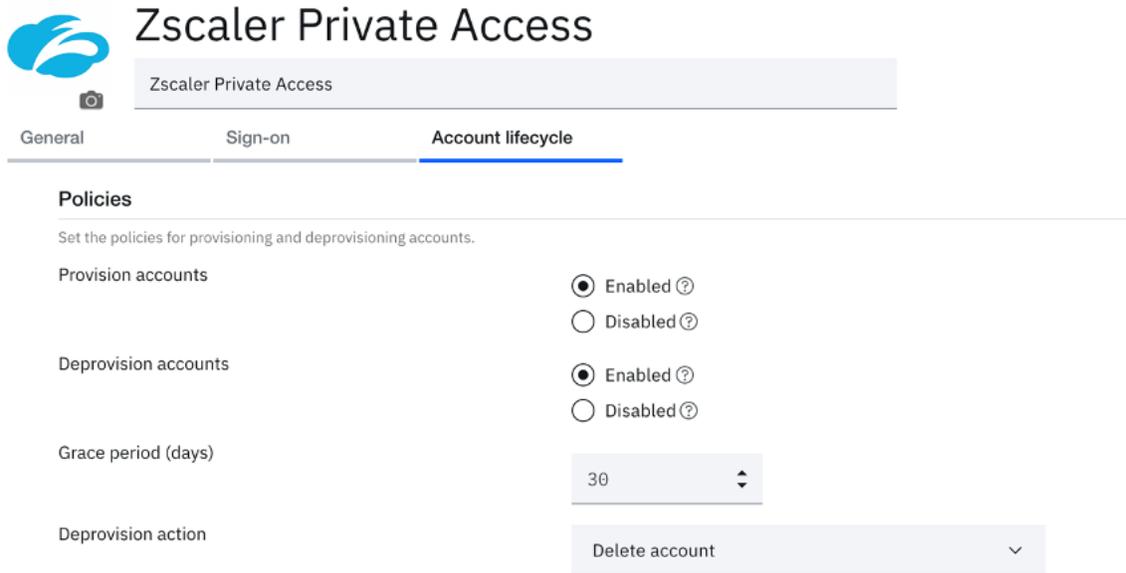
[Save](#) [Cancel](#)

Figure 68. SCIM configuration

Enable Lifecycle for Zscaler Application

1. Login to IBM Security Verify as tenant admin (continue to use the existing session if not logged out).
2. From the admin console, go to **Applications** page.
3. Select the **Zscaler Private Access** application.
4. Go to the **Account lifecycle** tab.
5. Enable the **Provision accounts** and **Deprovision accounts**. ZPA allows **Suspend account** or **Delete account** (with a **Grace Period**) as a **Deprovision** action.

Add application



Zscaler Private Access

Zscaler Private Access

General Sign-on **Account lifecycle**

Policies

Set the policies for provisioning and deprovisioning accounts.

Provision accounts Enabled ? Disabled ?

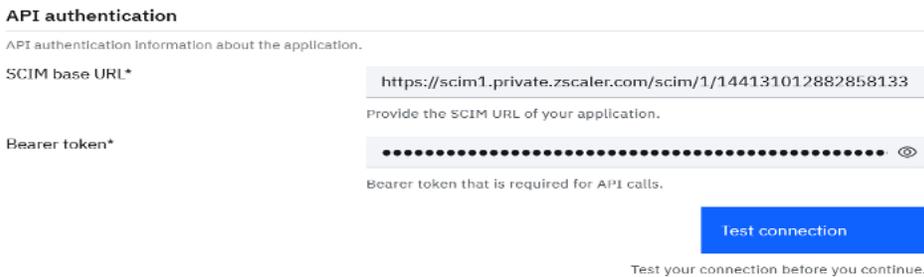
Deprovision accounts Enabled ? Disabled ?

Grace period (days) 30

Deprovision action Delete account

Figure 69. Add application

6. Scroll down to the **API Authentication** section.
7. In the **SCIM base URL** field, enter the **SCIM Service Provider Endpoint** URL copied from Zscaler.
8. In the **Bearer token**, enter the token copied from Zscaler.
9. Click **Test connection** to confirm the settings.



API authentication

API authentication information about the application.

SCIM base URL*

Provide the SCIM URL of your application.

Bearer token*

Bearer token that is required for API calls.

Test connection

Test your connection before you continue.

The connection test was successful.

Figure 70. API authentication

10. Confirm that connection successful message is shown. If not, verify that the **SCIM Base URL** and **Bearer Token** are entered correctly.
11. Scroll down to the **API Attribute Mappings** section and set the following:
 - **preferred_username** = userName
 - **given_name** = name.givenName
 - **family_name** = name.familyName
 - **email** = Email

Leave the other mappings as-is.

Attribute mapping

Map the attributes that are used to provision accounts in the target application.

Verify attribute Choose from existing attributes	Transformation Transform the value	Target attribute Attribute name in the target app	Keep updated	
preferred_username x v	None x v	→ userName x v	<input type="checkbox"/>	🗑️
given_name x v	None x v	→ name.givenName x v	<input type="checkbox"/>	🗑️
family_name x v	None x v	→ name.familyName x v	<input type="checkbox"/>	🗑️
email x v	None x v	→ Email x v	<input type="checkbox"/>	🗑️

Figure 71. Attribute mapping

12. Click **Save**.

Define Entitlements for Application

Define the entitlement for users and groups to get access to this application.

When you save the application, the **Entitlements** tab is displayed.

1. On the **Entitlements** tab, make sure to choose **Select users and groups, and the assign individual accesses**.
2. Click **Add**.

Applications / Details

Zscaler Private Access

Zscaler Private Access

General Sign-on Account lifecycle **Entitlements**

Access Type

Automatic access for all users and groups

Approval required for all users and groups

Select users and groups, and assign individual accesses

Approvers - select at least one

User's manager

Application owner

Search name

Add

Name ↑	Date Assigned	Automatic Access
ZPA User Group	6/16/2021	On

Figure 72. Application details

3. On the **Select User/Group** dialog, search for, select, and add **ZPA User Group** (this group must have been already created by admin).
4. Click **OK** to close the dialog.

Select User/Group

Q ZPA

Matching Items (1)

ZPA User Group

Selected Items (1)

ZPA User Group

Add

Remove

Add new user

Cancel OK

Figure 73. Select User/Group

5. Click **Save** to save application changes.

Zscaler Provisioning Use Cases

After ZPA is successfully configured, the tenant admin can provision user accounts.



IBM Security Verify does not support account synchronization with ZPA.

New User Provisioning to Zscaler

Create a new user in IBM Security Verify and make sure they can log in.

Create New User

1. Login to the IBM Security Verify tenant as an administrative user.
2. Go to **Users & groups**.
3. Click **Add user**.
4. Create a user. You can create any user you like (as long as it doesn't clash with existing ones). For example:
 - **Identity Source:** Select **Cloud Directory**.
 - **User name:** zpauser01
 - **Given name:** User01
 - **Surname:** ZPA
 - **Email:** Enter a valid email address

Add user ×

Identity source*

Cloud Directory

Status

On

Basic user profile

Given name

User01

Middle name (optional)

Surname

ZPA

User name

zpauser01

External ID (optional)

Cancel Save

Figure 74. Add user

- Click **Save** to create the user.

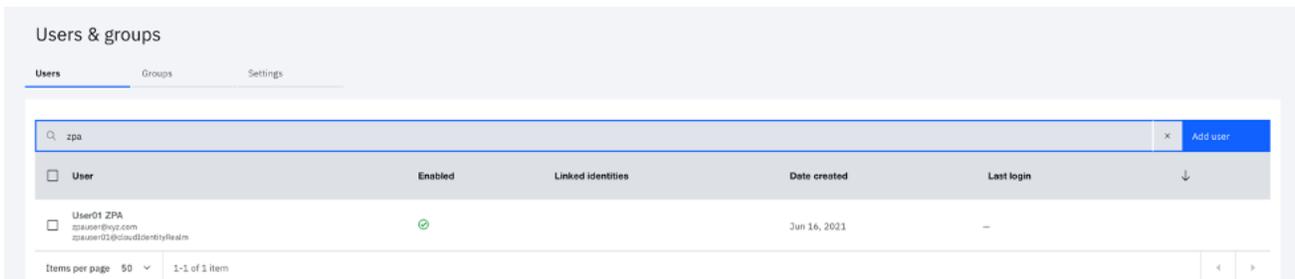


Figure 75. Users & groups

The new user is created and listed in the **Users** table.

Test that the New User Can Login

The new user gets the initial password via email. Go to your email client of the newly created user and look for a confirmation email.

Admin Prod EU01a admin@prod-eu01a.com via iam.ibm.com
to me ▾



Your account was created.

Your temporary password is: **KMD~7\$cs**

After you log in, you must change your password.

...

Click the link to log in: [https://\[redacted\].verify.ibm.com/ui](https://[redacted].verify.ibm.com/ui)

Figure 76. Confirmation email

- Open a new browser session, copy the link from the email and log in with the username and password from the email.
- When prompted, enter a **New password**, **Confirm password**, and click **Change Password**.

3. Validate that user is able to access the IBM Security Verify launchpad.

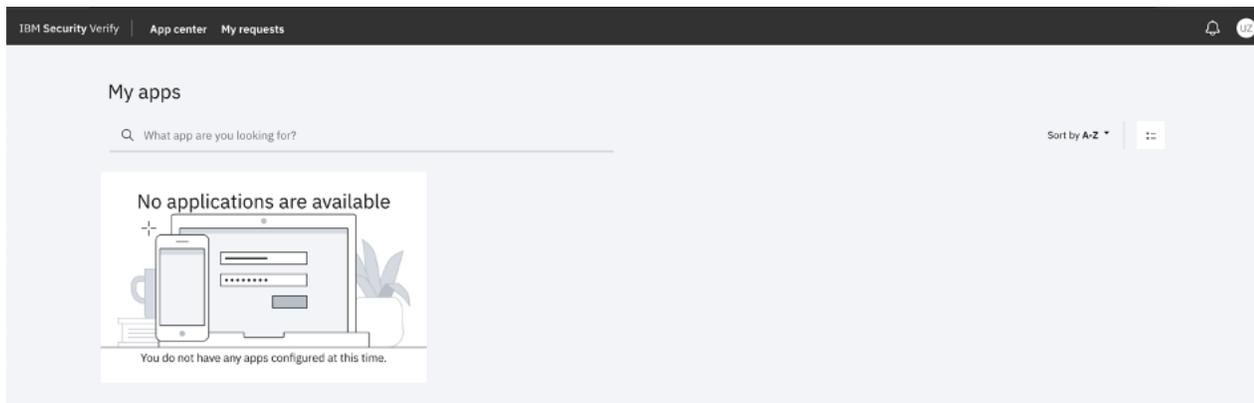


Figure 77. My apps

Provisioning Use Case

You have entitled the **Zscaler User Group** with `Automatic` access for the ZPA application. In order to provision a new Zscaler account for a newly created user, make the new user a member of the **ZPA User Group**. This triggers the automatic provisioning for the ZPA account.

Add the User to Group

Return to the IBM Security Verify admin console as the admin user.

1. Access the **Users & groups** section and click the **Groups** tab.
2. Hover over the **ZPA User Group** and click the **Edit** icon.



Figure 78. Users & groups

3. Click **Add** beside **Group Members**.
4. Search for the name of the new user that is listed in the **Search results**.

- Choose the listed user and click **Select**. This moves the user to **Selected users & groups**.

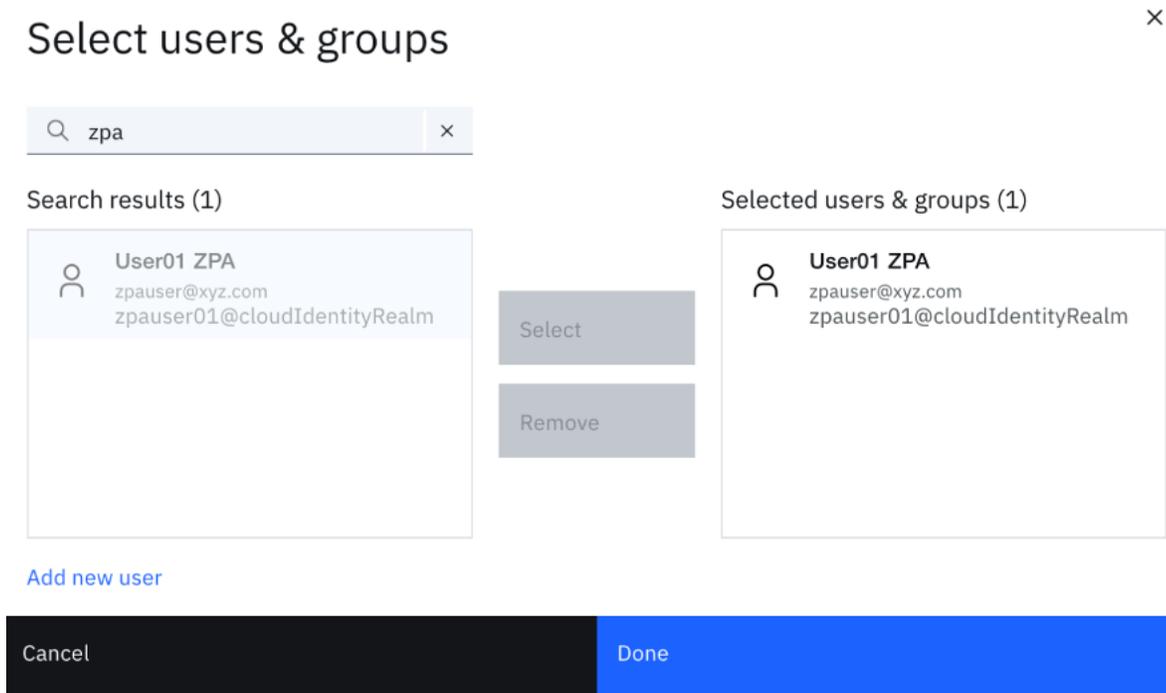


Figure 79. Select users & groups

- Click **Done**, then **Save** on the **Edit Group** dialog.
- Return to the **Users** tab, hover over your new user, and click the **User Details** icon on the right side.
- Confirm the new user is in the **ZPA User Group**.

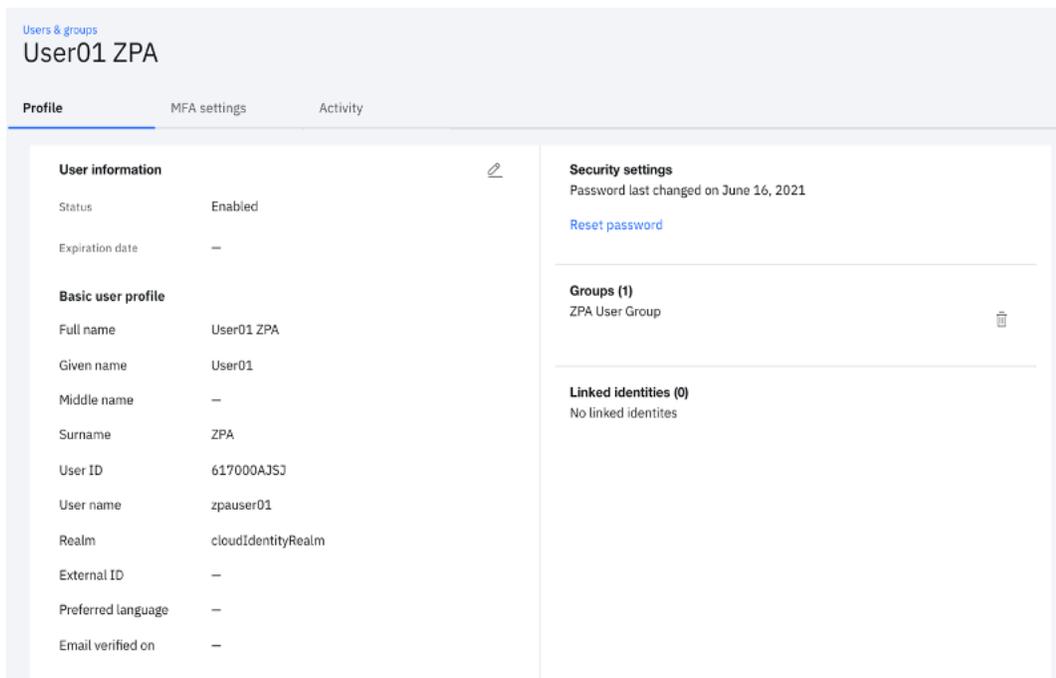


Figure 80. Users & groups

Check that the User is Provisioned to ZPA

Adding the user to the **ZPA User Group** automatically triggers Zscaler user provisioning by IBM Security Verify.

1. From the admin console, go to **Governance > Operation** results tab.

Type	Application Name	Operation	Account Username	Status	Last Updated
	Zscaler Private Access	Provision account	zpauser01	Success	Jun 16, 2021 9:45 PM IST

Figure 81. Governance

2. Also validate the new user provisioning by logging in the ZPA Admin Portal. Go to **Authentication > User Authentication > SCIM Users**.

Last Updated	Internal User ID	SCIM User Name	IdP SCIM User ID
No Items Found			

Figure 82. SCIM Users in the ZPA Admin Portal

3. Look for newly provisioned user.

Last Updated	Internal User ID	SCIM User Name	IdP SCIM User ID
Jun 16th, 2021, 21:45 (IST)	2961792	zpauser01	None

Figure 83. SCIM Users tab

4. Validate the user details such as:
 - The new user is listed in ZPA and the user name is correct.
 - Other user attributes are created per attribute mapping rules.

Check that the New User Can Access Zscaler via SSO

For service provider-initiated SSO, use the Zscaler Client Connector.



ZPA does not support identity provider-initiated SSO.

Deprovisioning Use Case

Test deprovisioning the user from ZPA.

Remove User from ZPA User Group

1. Return to the IBM Security Verify admin console as a user.
2. Go to **Users & groups** and click the **Groups** tab.
3. Edit the **ZPA User Group**.
4. Select the newly added user and click **Remove**.

Edit group ×

Name*

Description

Date created Jun 16, 2021

Date modified Jun 16, 2021

Group members

Add
Remove

User01 ZPA

zpauser@xyz.com

zpauser01@cloudIdentityRealm

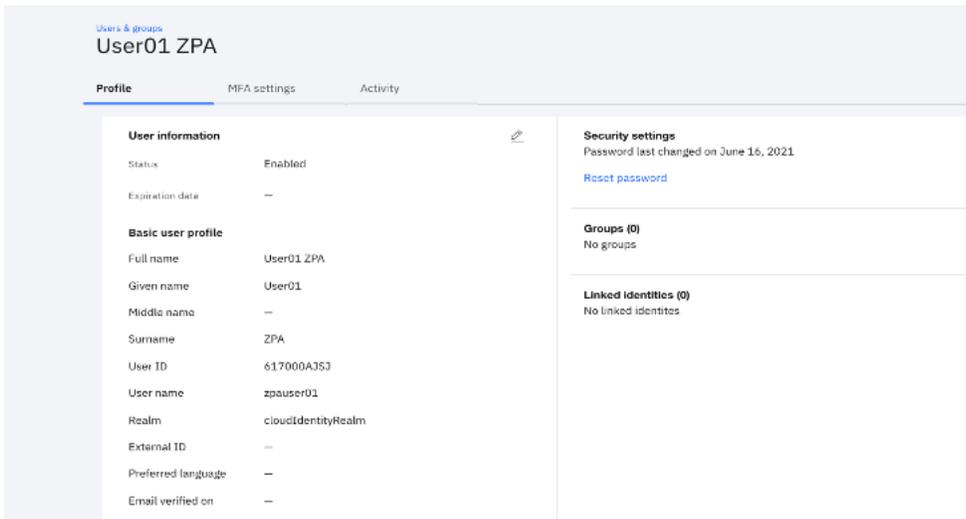
Send the end-user an email notification regarding this change.

Note: Notification applies when the group's user membership is modified. Notification is not sent to nested group members.

Cancel
Save

Figure 84. Edit group

- Click **Save**.
- As before, check the details of the user in the **Users** tab. Ensure no groups are listed in **Groups** section.



User01 ZPA

Profile | MFA settings | Activity

User information

Status	Enabled
Expiration date	—

Basic user profile

Full name	User01 ZPA
Given name	User01
Middle name	—
Surname	ZPA
User ID	617000A353
User name	zpauser01
Realm	cloudIdentityRealm
External ID	—
Preferred language	—
Email verified on	—

Security settings

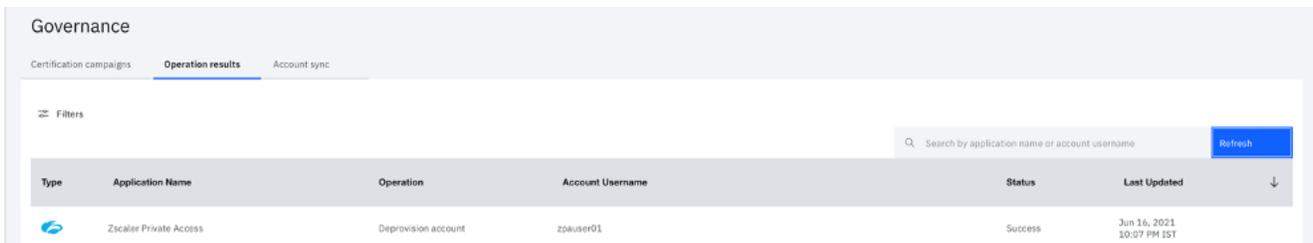
Password last changed on June 16, 2021
[Reset password](#)

Groups (0)
No groups

Linked Identities (0)
No linked identities

Figure 85. Users & groups

- Monitor the user deprovisioning task by going to **Governance > Operation results**.



Governance

Certification campaigns | **Operation results** | Account sync

Filters

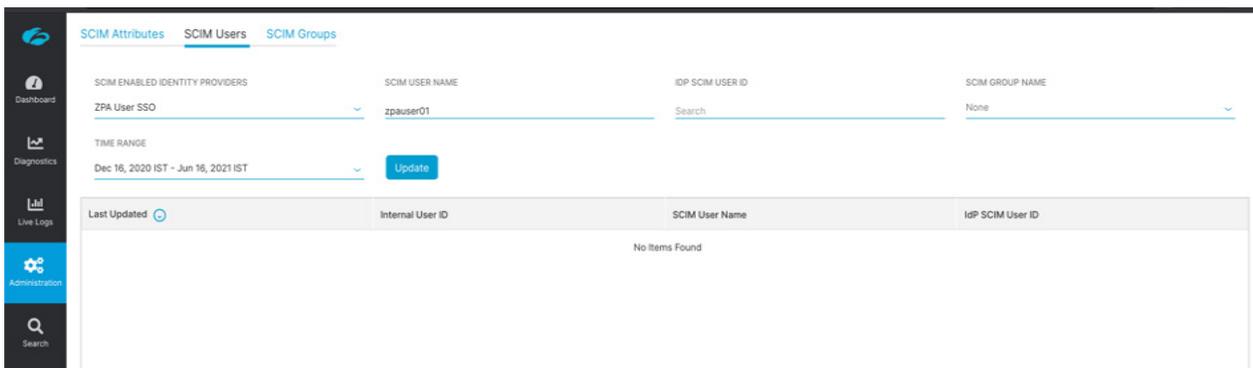
Search by application name or account username [Refresh](#)

Type	Application Name	Operation	Account Username	Status	Last Updated
	Zscaler Private Access	Deprovision account	zpauser01	Success	Jun 16, 2021 10:07 PM IST

Figure 86. Governance

Check that the User is Removed from ZPA

- Return to ZPA Admin Portal and search for the **SCIM User Name**.
- Check that no users are listed.



SCIM Attributes | **SCIM Users** | SCIM Groups

SCIM ENABLED IDENTITY PROVIDERS: ZPA User SSO

SCIM USER NAME: zpauser01

IDP SCIM USER ID: Search

SCIM GROUP NAME: None

TIME RANGE: Dec 16, 2020 IST - Jun 16, 2021 IST [Update](#)

Last Updated	Internal User ID	SCIM User Name	IDP SCIM User ID
No Items Found			

Figure 87. SCIM Users tab

Appendix A: Requesting Zscaler Support

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

To contact Zscaler Support, go to **Administration > Settings >** and then click **Company Profile**.

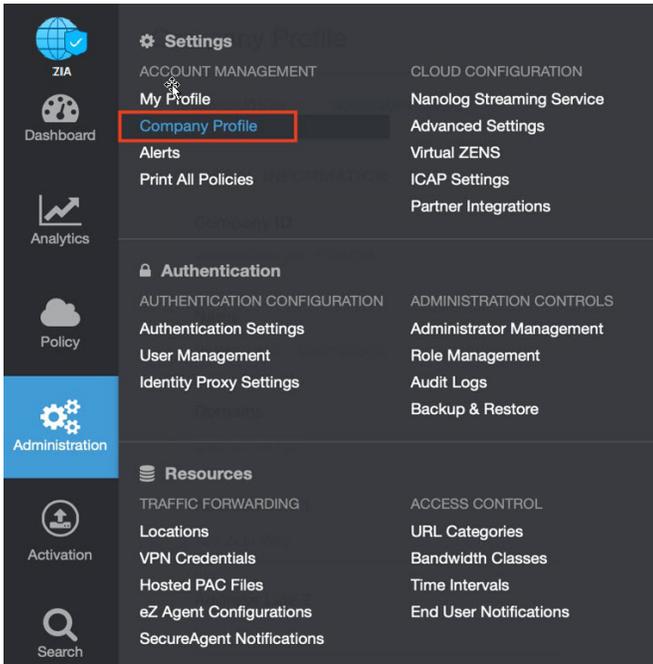


Figure 88. Collecting details to open support case with Zscaler TAC

Save Company ID

Copy the Company ID.

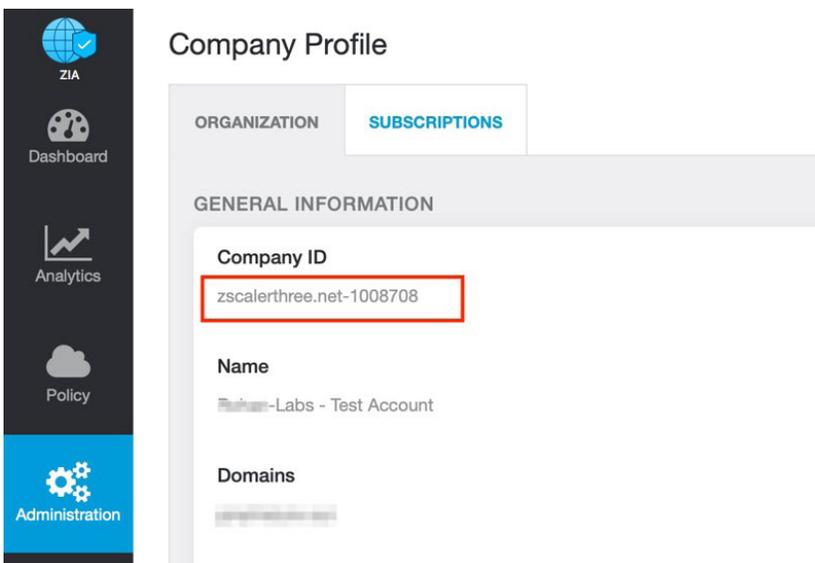


Figure 89. Company ID

Enter Support Section

Now that you have your company ID, you can open a support ticket. Go to **Dashboard > Support > Submit a Ticket**.

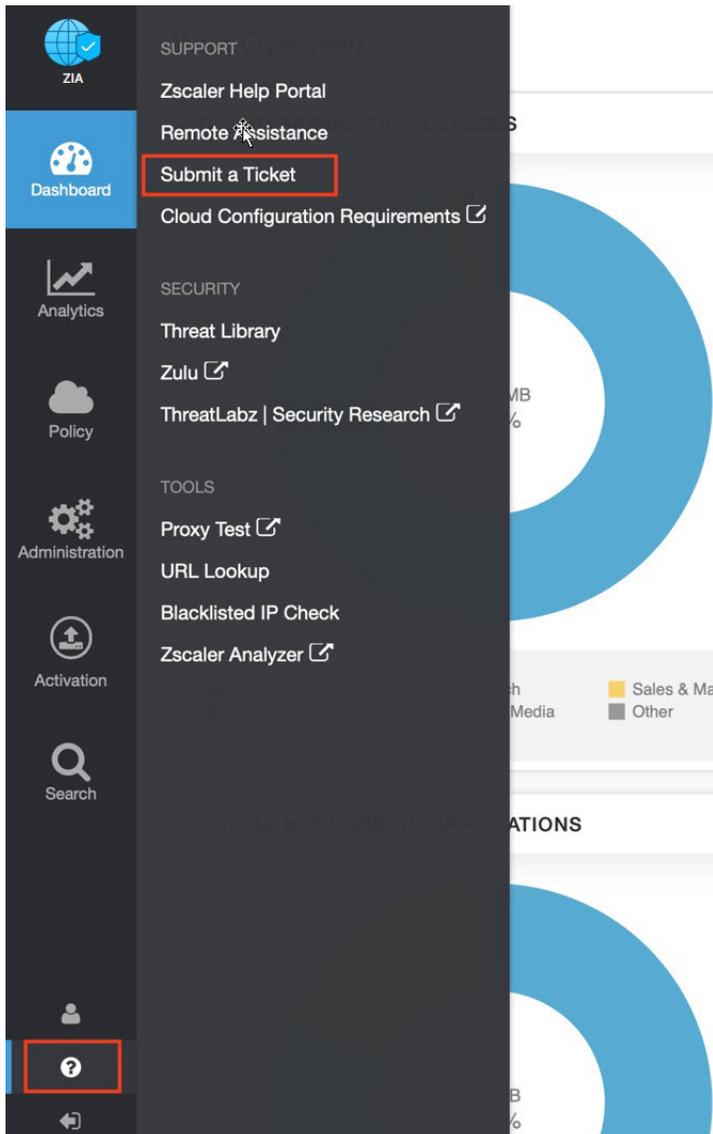


Figure 90. Submit the ticket

