



# IBM Security Verify

## User provisioning and Single sign-on for Zscaler private access

Version 2.0  
July 2021

## Document Purpose

This document provides the instructions for running the IBM Security Verify User Lifecycle Management & SSO features for ZScaler private access application.

For any comments/corrections, please contact Nilesch Atal ([NileschAtal@in.ibm.com](mailto:NileschAtal@in.ibm.com)).

## Document Conventions

The following conventions are used in this document:

■ A note, some special information or warning.

```
A piece of code
```

Text – Some command/text to be entered

**Text** – Some selection to be made

**Text** – Highlighting a button or function

Normal paragraph font is used for general information.

## Document Control

Release Date	Ver	Authors	Comments
4 Jul 2021	1.0	Neha Bist	First draft with provisioning usecases
10 Jul 2021	2.0	Nilesch Atal	Added SSO configuration details

## Table of Contents

<b>Introduction.....</b>	<b>4</b>
<b>1 Zscaler Configuration .....</b>	<b>5</b>
<b>2 Configure Zscaler application in Verify .....</b>	<b>Error! Bookmark not defined.</b>
2.1 Create / Update Zscaler Application .....	<b>Error! Bookmark not defined.</b>
2.2 Configure Sign-on .....	<b>Error! Bookmark not defined.</b>
2.3 Configure Account Lifecycle .....	<b>Error! Bookmark not defined.</b>
2.4 Define adoption policy for account synchronization .....	<b>Error! Bookmark not defined.</b>
2.5 Define entitlements for application .....	<b>Error! Bookmark not defined.</b>
<b>3 Zscaler Provisioning Use Cases .....</b>	<b>13</b>
3.1 Account Synchronization with Zscaler .....	<b>Error! Bookmark not defined.</b>
3.2 New User Provisioning to Zscaler .....	13
3.2.1 Test the New User Can Login.....	14
3.3 Provisioning Use Case .....	15
3.3.1 Check User has been provisioned to Zscaler .....	16
3.3.2 Check new user can access Zscaler via SSO .....	18
3.4 De-Provisioning Use Case .....	18
<b>4 Zscaler App Role Management Use Cases.....</b>	<b>Error! Bookmark not defined.</b>
4.1 Assign User to the Zscaler group through Permissions.....	<b>Error! Bookmark not defined.</b>
4.1.1 Check the User has been added to the Zscaler group from Zscaler.....	<b>Error! Bookmark not defined.</b>
4.2 Remove User from the Zscaler group through Permissions .....	<b>Error! Bookmark not defined.</b>
4.2.1 Check the User has been removed to the Zscaler group from Zscaler.....	<b>Error! Bookmark not defined.</b>
4.3 Provision a new user and assign to a Zscaler group through Permission.....	<b>Error! Bookmark not defined.</b>
4.3.1 Check the User has been added to the Zscaler group from Zscaler.....	<b>Error! Bookmark not defined.</b>
4.4 Add User to the Zscaler group through Roles.....	<b>Error! Bookmark not defined.</b>

## Introduction

IBM® Security Verify provides support for Single Sign-on (SSO), Multifactor authentication (MFA), Adaptive Access as well as account lifecycle management for several applications out of the box. This document provides instructions for configuring IBM Security Verify with “Zscaler Private Access” as an application leveraging these capabilities.

## Before you begin

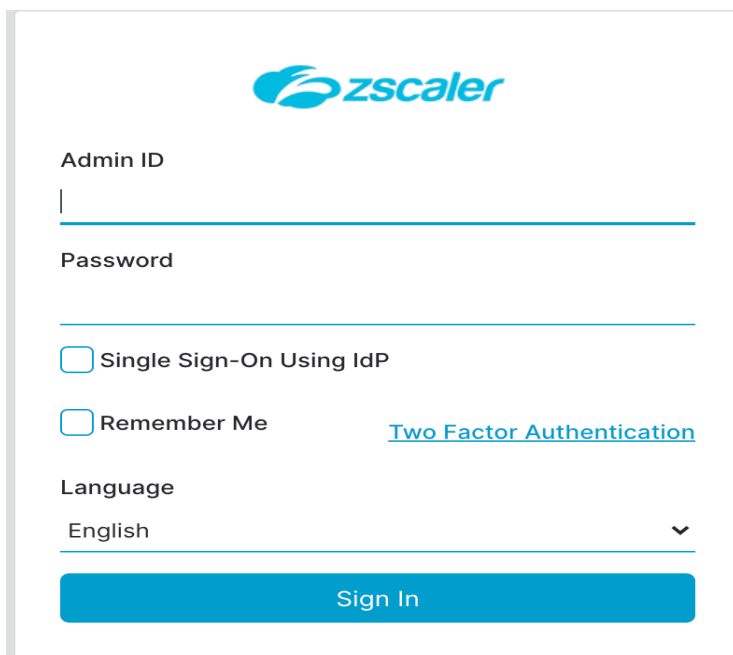
Make sure to have Zscaler Private Access account with administrator access.

# 1 Configuration

## 1.1 Zscaler configuration

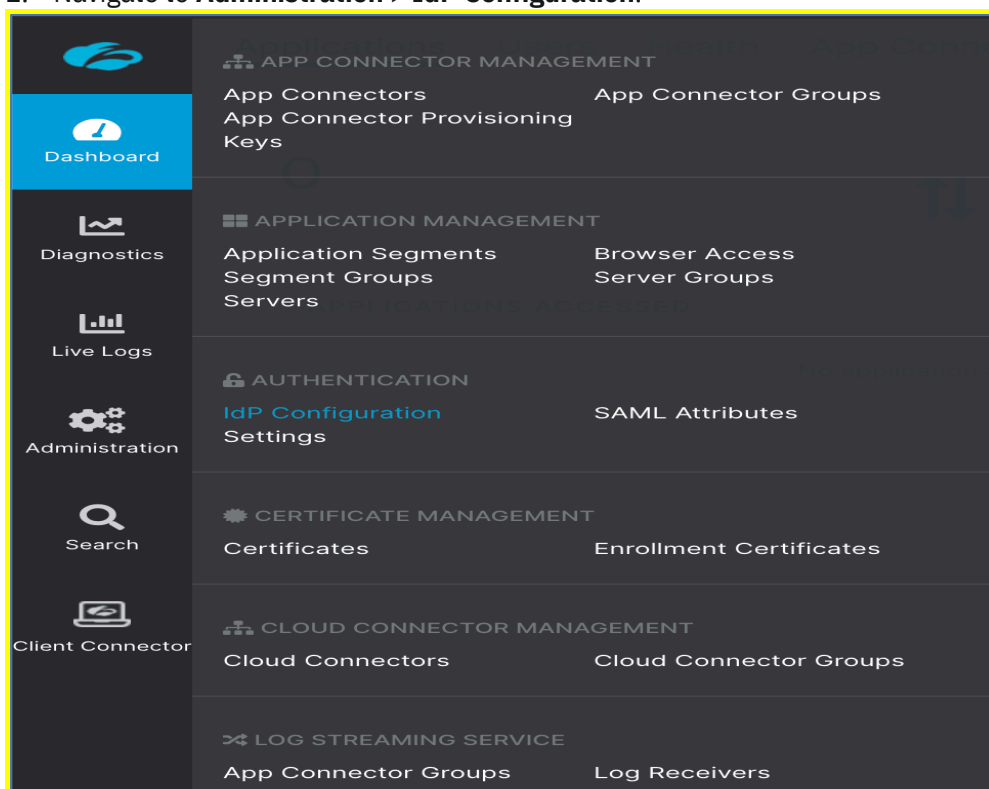
To allow **Single Sign-on** and **user provisioning** for **Zscaler private access** application, follow the below mentioned configuration.

1. Log in as an admin user to your Zscaler private Access account using the following URL:  
`https://admin.private.zscaler.com`



The image shows the Zscaler login page. At the top is the Zscaler logo. Below it are two input fields: 'Admin ID' and 'Password'. There are two checkboxes: 'Single Sign-On Using IdP' and 'Remember Me'. Below these is a link for 'Two Factor Authentication'. There is a 'Language' dropdown menu currently set to 'English'. At the bottom is a large blue 'Sign In' button.

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



3. Click **Add IdP Configuration**
4. Provide **Name** and select **Single Sign-on** as **User**
5. Select User **SP Certificate Rotation** from the available list
6. Select **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

7. Click **Next**
8. SP Metadata tab is displayed.
9. Download **Service Provider Metadata** and **Service Provider Certificate**.
10. Service Provider URL is displayed. Copy this URL which need to be copied to the **Assertion Consumer Service URL** text field of **Zscaler private access** application configuration in Verify.
11. Service Provider Entity ID is displayed. Copy this ID which need to be copied to the **Provider ID** text field of **Zscaler private access** application configuration in Verify.

Add IdP Configuration
✕

1 IdP Information
2 SP Metadata
3 Create IdP

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/144131012882858133/sso>

Service Provider Entity ID

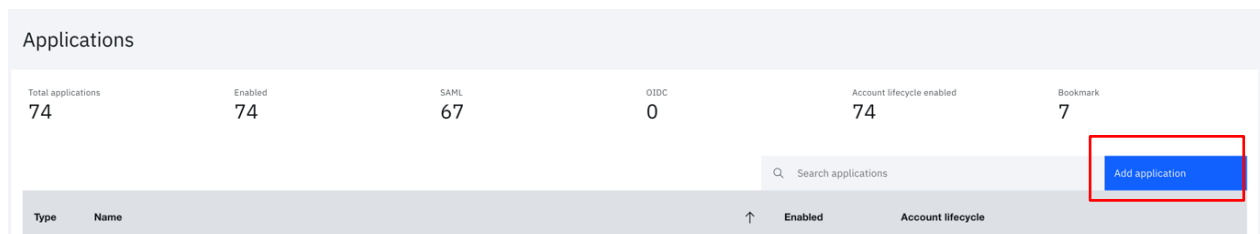
<https://samlsp.private.zscaler.com/auth/metadata/144131012882858133>

Next
Pause

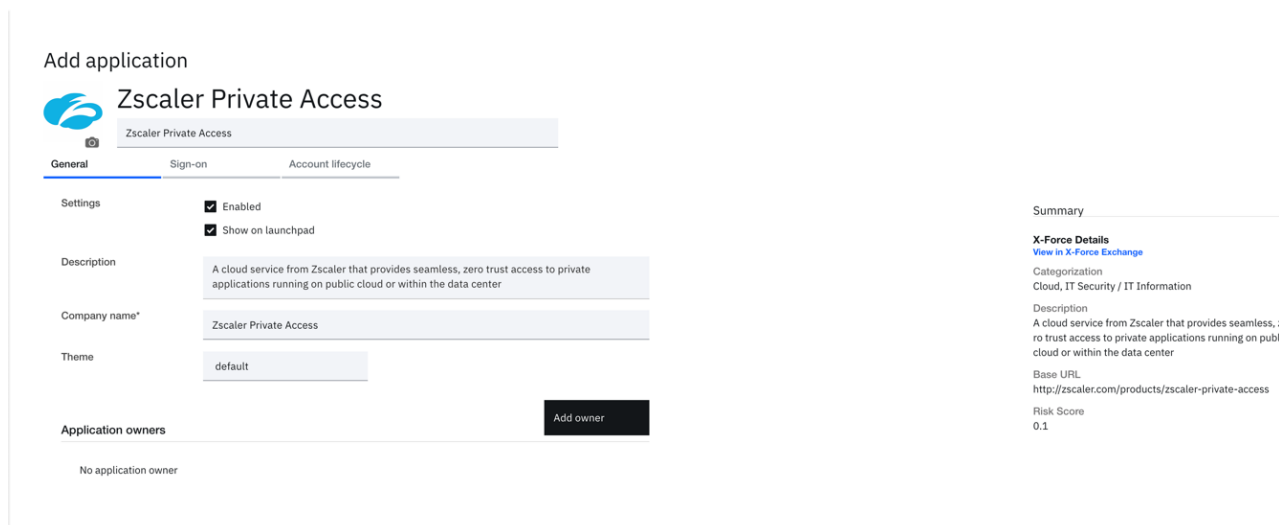
12. Click **Next**
13. **Create IdP** section gets displayed
14. We need few details from Verify to fill required information. Hence open a new browser.

## 1.2 Zscaler application configuration

1. In another browser, login to IBM® Security Verify as tenant admin (**Scott**)
2. Navigate to **Applications** page, click the **Add application** button.




3. On the **Select Application Type** dialog, enter **Zscaler Private Access** into the search box.
4. When the Zscaler Private Access application is displayed, select it and then click the **Add application** button.
5. On the Add Application page provide **Zscaler Private Access** as the **Company name**.



6. Click on **Sign-on** tab
7. Follow the instructions which are displayed in right pane

## Add application



### Zscaler Private Access

General
Sign-on
Account lifecycle

Provider ID\*

https://samlsp.private.zscaler.com/auth/metadata/144131012882858132

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://samlsp.private.zscaler.com/auth/144131012882858132/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 identity provider.

Click Next.

Create IdP 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?virtualId=0dc58f9b2c9

IdP Certificate

Download the certificate for uplo

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

MIDPjCCAiaGAWIBAgIERZV5vTANBgkqhkiG9w0BAQsFADBhMQkwBwYDVQQGEwAxCTA

HBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTA

HBgNVBAStADEoMCIYGA1UEAxMFY2lnLXRlbmFudC1ldTAxYS52ZXJpZnku

WJtLmNvbTAeFw0yMDA3Mjc0MjA3MThaFw0zMDA3MjUxMjA3MThaMGExCTA

HBgNVBAYTAD

EJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTA

HBgNVBAoTADEJMAcGA1UECzMAMSGwJgYDVQQDEx9ja

-----

Cancel
Save

- Update the **Assertion Consumer Service URL** text field with **Service Provider URL** copied from **Zscaler**.
- Update the **Provider ID** text field with **Service Provider Entity ID** copied from **Zscaler**
- In the instructions pane, goto **SAML CONFIGURATION** section and download the **IdP Metadata** file
- Save the application configuration in Verify
- Now go back to the Zscaler admin console, upload the downloaded **IdP Metadata** at **Create IdP** section

Edit IdP Configuration

IdP Metadata File

metadata.xml

Change Remove

IdP Certificate

Upload the Certificate File...

Select File

-----BEGIN CERTIFICATE-----
MIDPjCCAiaGAWIBAgIERZV5vTANBgkqhkiG9w0BAQsFADBhMQkwBwYDVQQGEwAxCTA
HBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTA
HBgNVBAStADEoMCIYGA1UEAxMFY2lnLXRlbmFudC1ldTAxYS52ZXJpZnku
WJtLmNvbTAeFw0yMDA3Mjc0MjA3MThaFw0zMDA3MjUxMjA3MThaMGExCTA
HBgNVBAYTAD
EJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTA
HBgNVBAoTADEJMAcGA1UECzMAMSGwJgYDVQQDEx9ja
-----

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

- Set **Status** as Enabled.
- Set **SAML Attributes for Policy** as Enabled.
- Save the configuration



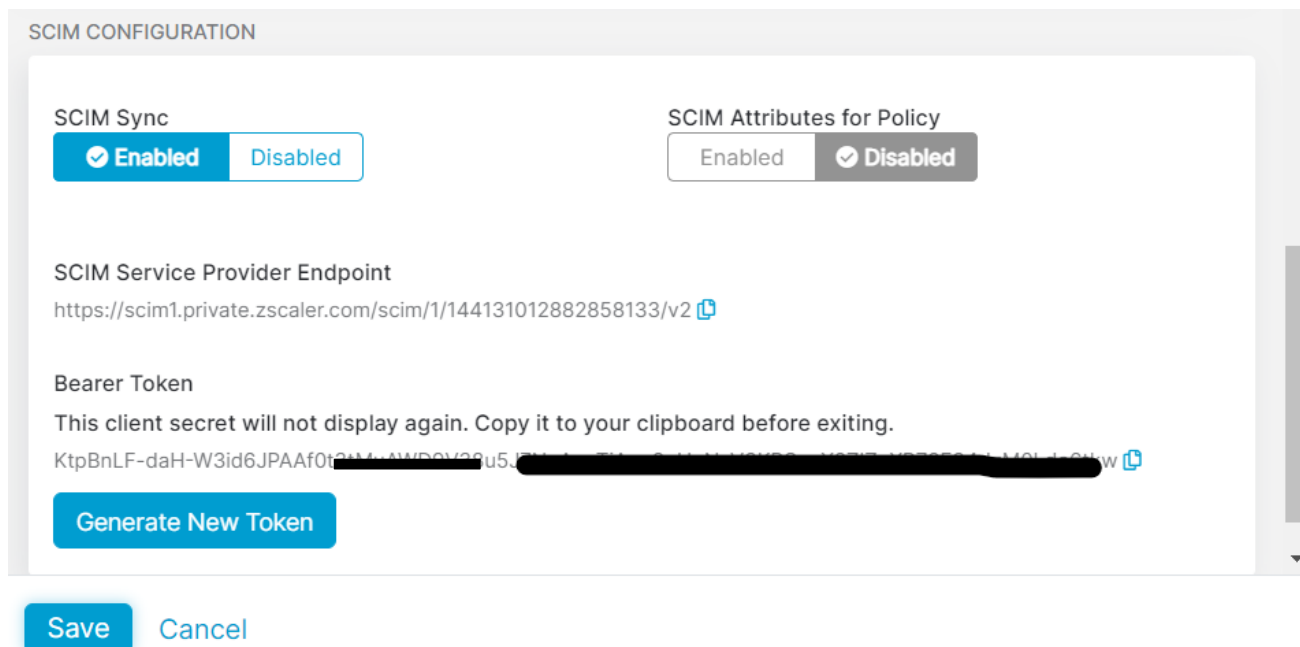
## 1.3 Enable SCIM configuration for Zscaler

1. Log in as an admin user to your Zscaler private Access account (Continue to use existing session if not logged out)
2. Navigate to **Administration > IdP Configuration**.
3. Edit the IdP configuration created above



Name	Status	IdP Entity ID	Single Sign-On	Actions
Admin	Enabled	https://scim1.private.zscaler.com/scim/1/144131012882858133/v2	Admin	Edit Delete
ZPA User SSO	Enabled	https://scim1.private.zscaler.com/scim/1/144131012882858133/v2	User	Edit Delete

4. In the **Edit IdP Configuration** window, select **Enabled** for **SCIM Sync**.



**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-W3id6JPAAf0t9M4-AWBOV22u5J...

5. Copy **SCIM Service Provider Endpoint** as shown in the above image.
6. Click **Generate New Token** to create a bearer token and copy it as shown in the above image.
7. Click **Save**

## 1.4 Enable lifecycle for Zscaler application

1. Login to IBM® Security Verify as tenant admin (**Scott**) (Continue to use existing session if not logged out)
2. Navigate 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**. As Zscaler Private Access allows Suspend and Delete (With 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

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 admin console
8. In the **Bearer token**, enter the token copied from Zscaler admin console
9. Click the **Test Connection** button to confirm the settings

#### API authentication

API authentication information about the application.

SCIM base URL\*

https://scim1.private.zscaler.com/scim/1/144131012882858133

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.

10. Confirm that connection successful message is shown. If not, recheck if SCIM base URL and Bearer token are entered correctly.
11. Scroll down to the **API Attribute Mappings** section and set the following:
  - a. *preferred\_username* = **userName**
  - b. *given\_name* = **name.givenName**
  - c. *family\_name* = **name.familyName**
  - d. *email* = **Email**
 Others can be left as it 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"/>	

12. Click the **Save** button


## 1.5 Define entitlements for application

Now, define the entitlement for users / groups who should get access to this application. When you saved application above, a new tab (**Entitlements**) gets exposed.


1. On the **Entitlements** make sure that **Select users and groups, and assign individual accesses** option is selected
2. Click the **Add** button
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 the **OK** to close the dialog

### Select User/Group

Matching Items (1)

 ZPA User Group

Selected Items (1)

 ZPA User Group

Add

Remove

[Add new user](#)

Cancel

OK

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



# Zscaler Private Access

Zscaler Private Access

GeneralSign-onAccount lifecycleEntitlements

- 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

Add

Name ↑	Date Assigned	Automatic Access
ZPA User Group	6/16/2021	<input checked="" type="checkbox"/> On

## 2 Zscaler Provisioning Use Cases

After the **Zscaler application** is successfully configured as mentioned in above section, tenant admin can provision user accounts with **Zscaler private access**.

**NOTE:** IBM Security Verify does not support account synchronization with Zscaler private access.

### 2.1 New User Provisioning to Zscaler

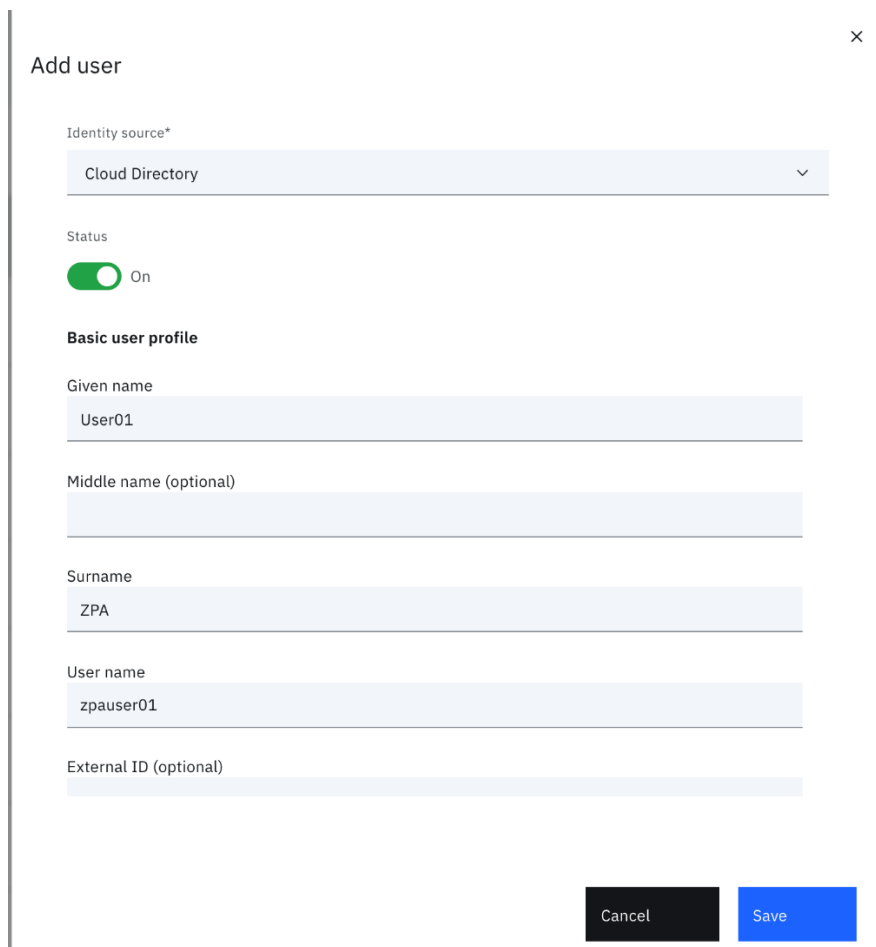
First, let's create a new user in Security Verify and make sure he / she can log in.

#### Create New User

1. Log to IBM® Security Verify tenant as your administrative user (**Scott**)
2. Go to **Users & groups**
3. Click the **Add user** button
4. Create a user. You can create any user you like (as long as it doesn't clash with existing ones).

#### For example:

- o Identity Source = *Cloud Directory*
- o User name = *zpauser01*
- o Given name = *User01*
- o Surname = *ZPA*
- o Email = *a valid real 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

5. Click the **Save** button to create the user

Users & groups					
<div> <div>Users</div> <div>Groups</div> <div>Settings</div> </div>					
<div> <input type="text" value="zpa"/> <span>×</span> <span>Add user</span> </div>					
<input type="checkbox"/>	User	Enabled	Linked identities	Date created	Last login
<input type="checkbox"/>	User01 ZPA zpauser@ibm.com zpauser01@cloudidentityRealm	<span>✓</span>		Jun 16, 2021	—
<div> <div>Items per page 50</div> <div>1-1 of 1 item</div> </div>					

The user should get created and listed in the **Users** table

### 2.1.1 Test the New User Can Login

New user will get the initial password via e-mail. Go to your email client of newly created user and look for an email indicating a user has been created

**Admin Prod EU01a** admin@prod-eu01a.com [via](#) iam.ibm.com  
to me ▾

## IBM Security Verify

Your account was created.

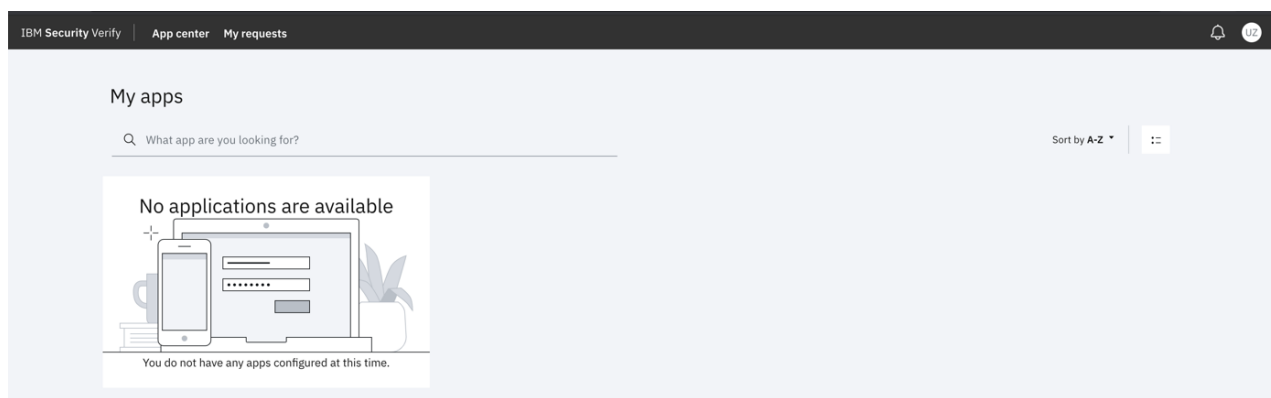
Your temporary password is: **kMD~7\$ScS**

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)

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** and click the **Change Password** button
3. Validate that user is able to access the Verify launchpad



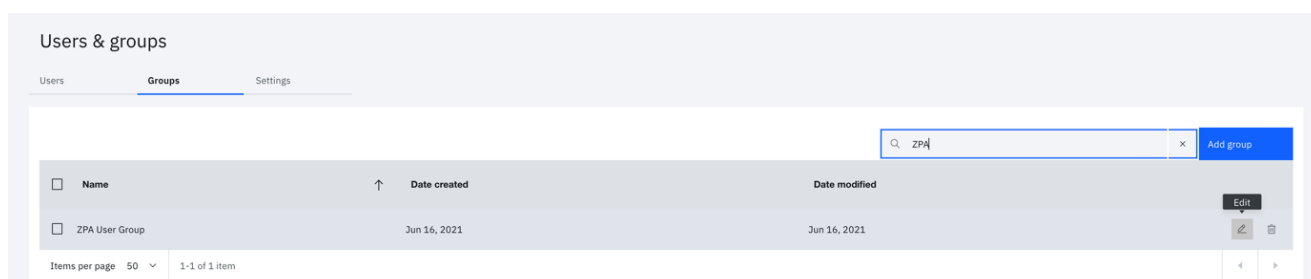
## 2.2 Provisioning Use Case

We have entitled the **Zscaler User Group** group with “Automatic access” for the **Zscaler Private access** application. Now in order to provision new Zscaler account for newly created user, let’s make the new user as a member of **ZPA User Group** group. This will trigger the automatic provisioning for the Zscaler private access account.

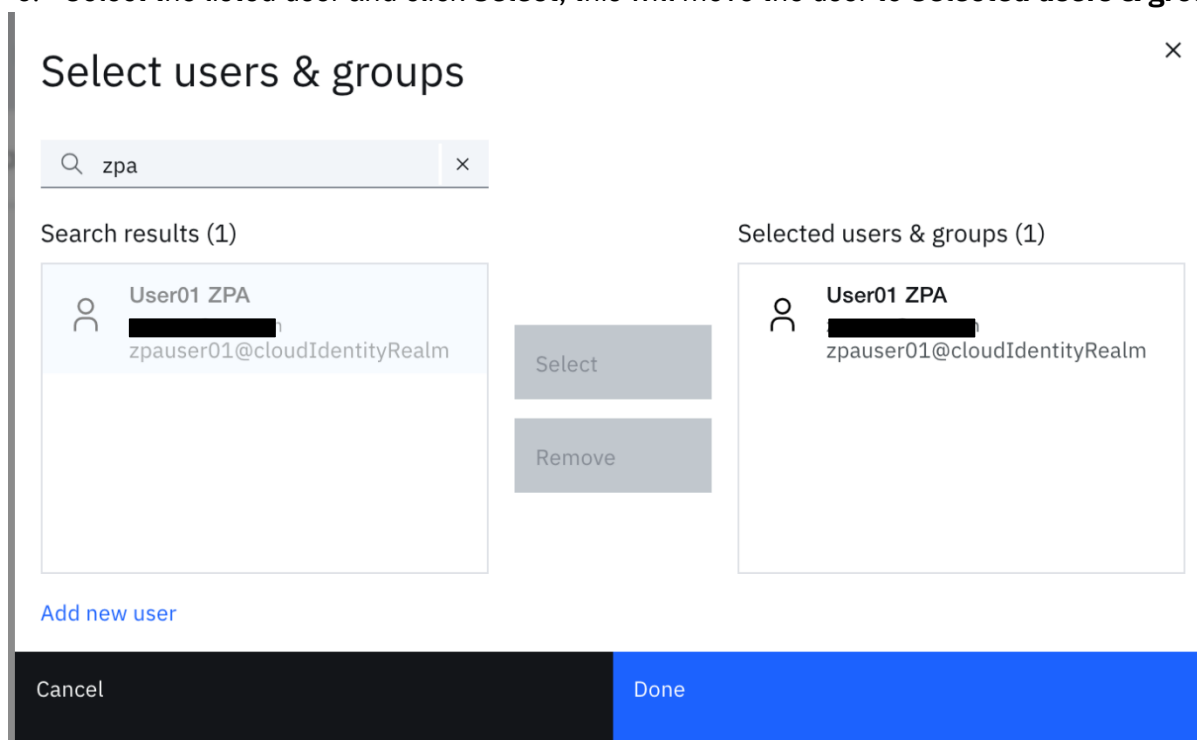
### Add User to Group

Return to the IBM® Security Verify admin interface as the admin user (**Scott**) – you should still have the window open from before steps

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



3. Click the **Add** button beside **Group Members**
4. Search for name of new user which will get listed in the **Search results**
5. Select the listed user and click **Select**, this will move the user to **Selected users & groups**



6. Click the **Done** button to add them, then **Save** on the *Edit Group* dialog
7. Go back to the **Users** tab, hover over your new user and click the **User Details** icon on the right
8. Confirm the new user is in the **ZPA User Group** group

Users & groups

## 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 617000AJSJ

User name zpauser01

Realm cloudIdentityRealm

External ID —

Preferred language —

Email verified on —

### Security settings

Password last changed on June 16, 2021

[Reset password](#)

### Groups (1)

ZPA User Group

### Linked identities (0)

No linked identities

### 2.2.1 Check User has been provisioned to Zscaler private access

As the user has been added to **ZPA User Group** group, automatic Zscaler user provisioning gets triggered by Security Verify at the backend. The user provisioning task can be monitored by the admin (**Scott**)


1. Navigate to **Governance > Operation results** tab

Governance

Certification campaigns **Operation results** Account sync

Filters

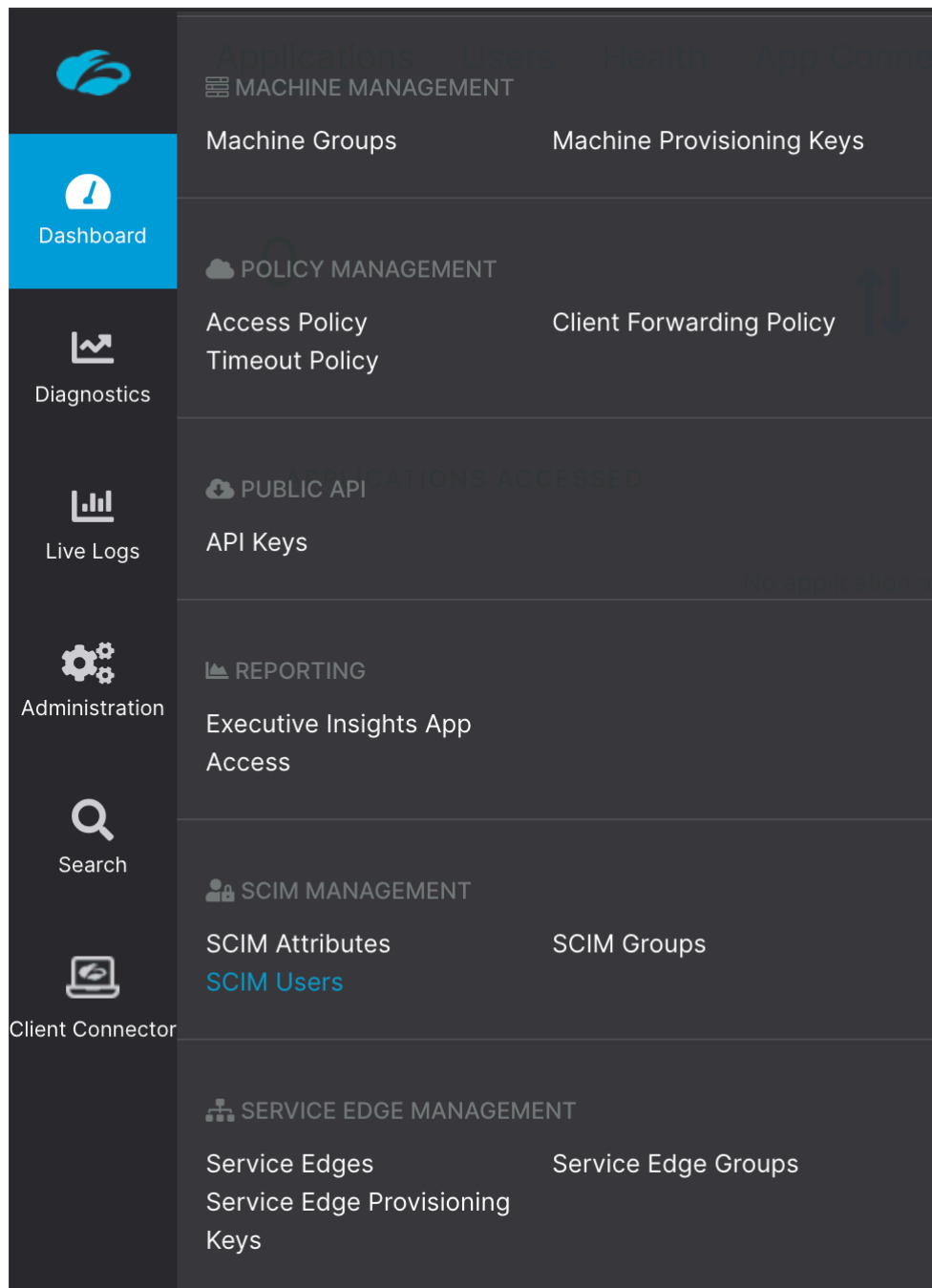
Search by application name or account username Refresh

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

Also validate the new user provisioning by log in to *Zscaler Private Access*

1. Navigate to **Administration > SCIM Users**.





## 2. Look for newly provisioned user

SCIM Attributes SCIM Users SCIM Groups			
SCIM ENABLED IDENTITY PROVIDERS	SCIM USER NAME	IDP SCIM USER ID	SCIM GROUP NAME
ZPA User SSO	Search	Search	None
TIME RANGE			
Dec 16, 2020 IST - Jun 16, 2021 IST	Update		
Last Updated	Internal User ID	SCIM User Name	IdP SCIM User ID
Jun 16th, 2021, 21:45 (IST)	2901792	zpauser01	None

Validate the user details such as:

1. New user is listed in Zscaler Private Access and the username is correct
2. Other user attributes are created as per attribute mapping rules

## 2.2.2 Check new user can access Zscaler via SSO

**NOTE:** Zscaler Private Access does not support identity provider-initiated SSO.

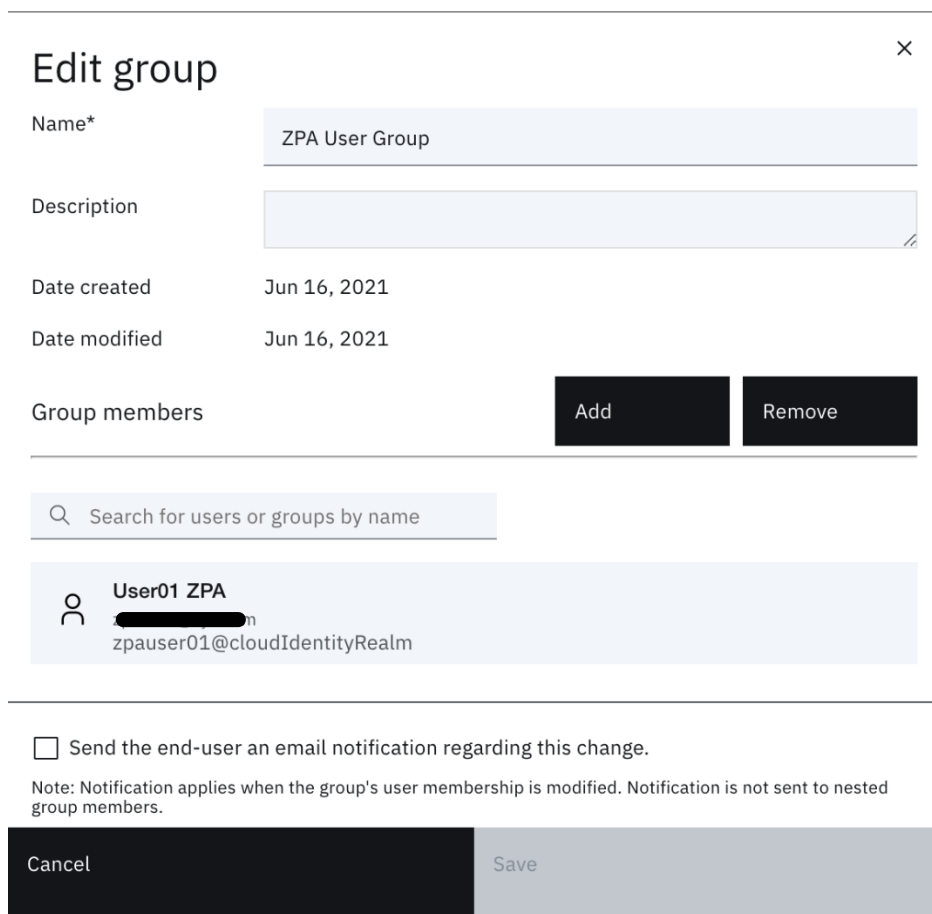
For Service provider-initiated SSO, use the Zscaler Client Connector (Z App) application.

## 2.3 De-Provisioning Use Case

Let's do the reverse operation to test de-provisioning user from Zscaler private access

### Remove User from ZPA User Group

1. Return to the IBM® Security Verify admin interface using admin user (**Scott**)
2. Go to **Users & groups** and click **Groups** tab
3. Edit the **ZPA User Group** group
4. Select newly added user and click the **Remove** button



### Edit group

Name\* ZPA User Group

Description

Date created Jun 16, 2021

Date modified Jun 16, 2021

Group members Add Remove

Search for users or groups by name

User01 ZPA  
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

5. Click the **Save** button
6. As before, check details of user in the **Users** tab. There should not be any groups listed in **Groups** section.

Users & groups

## 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 617000AJSJ

User name [REDACTED]

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

The user de-provisioning task can be monitored by the admin (**Scott**)

1. Navigate to **Governance > Operation results** tab

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

**Check the User has been removed from Zscaler private access**

1. Return to the **Zscaler private access** and search with the username
2. Check that no users get 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			