



IBM Security Verify

Integrating Zscaler application with IBM Security Verify

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 application.

For any comments/corrections, please contact Nilesch Atal (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

Introduction.....	4
1 Zscaler Configuration	5
2 Configure Zscaler application in Verify	8
2.1 Create / Update Zscaler Application	8
2.2 Configure Sign-on	8
2.3 Configure Account Lifecycle	9
2.4 Define adoption policy for account synchronization	10
2.5 Define entitlements for application	11
3 Zscaler Provisioning Use Cases	13
3.1 Account Synchronization with Zscaler	13
3.2 New User Provisioning to Zscaler	15
3.2.1 Test the New User Can Login.....	16
3.3 Provisioning Use Case	17
3.3.1 Check User has been provisioned to Zscaler	18
3.3.2 Check new user can access Zscaler via SSO	19
3.4 De-Provisioning Use Case	20
4 Zscaler App Role Management Use Cases.....	22
4.1 Assign User to the Zscaler group through Permissions.....	22
4.1.1 Check the User has been added to the Zscaler group from Zscaler	23
4.2 Remove User from the Zscaler group through Permissions	24
4.2.1 Check the User has been removed to the Zscaler group from Zscaler	25
4.3 Provision a new user and assign to a Zscaler group through Permission.....	26
4.3.1 Check the User has been added to the Zscaler group from Zscaler	27
4.4 Add User to the Zscaler group through Roles.....	28

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 as an application leveraging these capabilities.

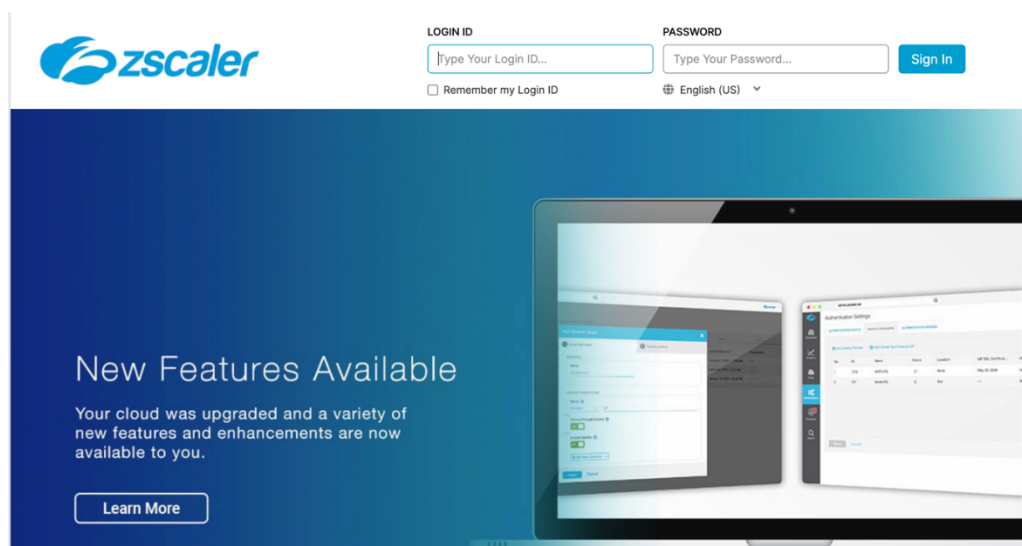
Before you begin

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

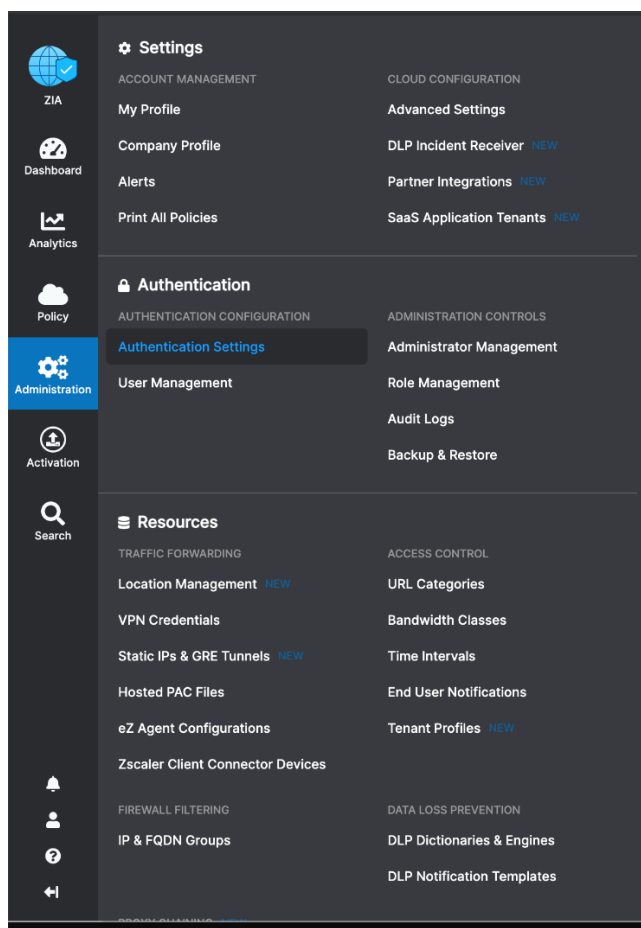
1 Zscaler Configuration

To allow user provisioning in IBM® Security Verify, follow the below mentioned steps to generate the SCIM url and token.

1. Log in as an admin user to your Zscaler Internet Access account using the following URL:
<https://admin.zscalerbeta.net>



2. Navigate to **Administration > Authentication > Authentication settings**.



3. For the **Authentication Type** field, select the **SAML** option.
4. Click **Open Identity Providers**.
5. **Identity Providers** ^{NEW} tab is displayed.
6. Click **Add IdP** (or Select the identity provider that you want to modify and click the edit icon)
7. Provide the following details in the **Open Identity Providers** window:
8. For the GENERAL INFO section, specify the following settings:

Name: Provide a name for your identity provider configuration.

Status: Select **Enabled**.

SAML Portal URL: `https://xxxxx.verify.ibm.com/saml/sps/saml20ip/saml20/login`

Login Name Attribute: Provide the login name attribute as NameID.

Entity ID: `<Zscaler Cloud>`

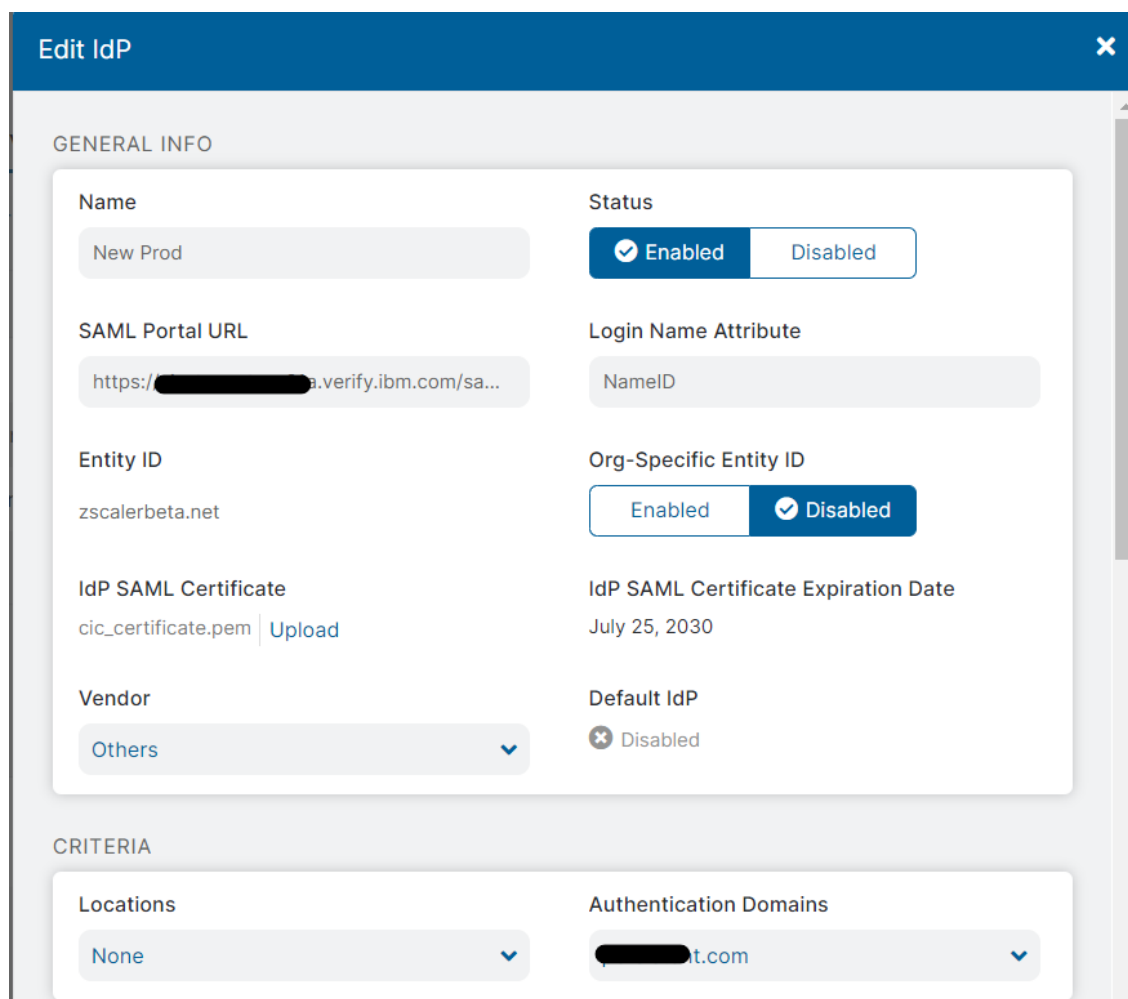
Org-Specific Entity ID: Enable if you have more than one organization instance on the same Zscaler cloud.

IdP SAML Certificate: Upload the certificate which can be downloaded from the Verify

Vendor: Select **Others**.
9. For the CRITERIA section, specify the following settings:

Locations: Select a value from the drop-down based on your requirements.

Authentication Domains: Select a value from the drop-down based on your requirements.



The screenshot shows the 'Edit IdP' window with the following details:

GENERAL INFO

Name New Prod	Status <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SAML Portal URL <code>https://[redacted].verify.ibm.com/sa...</code>	Login Name Attribute NameID
Entity ID zscalerbeta.net	Org-Specific Entity ID <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
IdP SAML Certificate cic_certificate.pem Upload	IdP SAML Certificate Expiration Date July 25, 2030
Vendor Others	Default IdP <input checked="" type="radio"/> Disabled

CRITERIA

Locations None	Authentication Domains [redacted].com
--------------------------	---

10. In the **SERVICE PROVIDER (SP) OPTIONS** section, keep the option as Disable for now
11. In the **Provisioning Options** section, enable the **Enable SCIM Provisioning**.

PROVISIONING OPTIONS

Enable SAML Auto-Provisioning

☐

Enable SCIM Provisioning

☒

Base URL

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

Bearer Token

[REDACTED]TIEvT7JCCsM9OcSfCreQTMPEUAcksOyNQpxLQ==

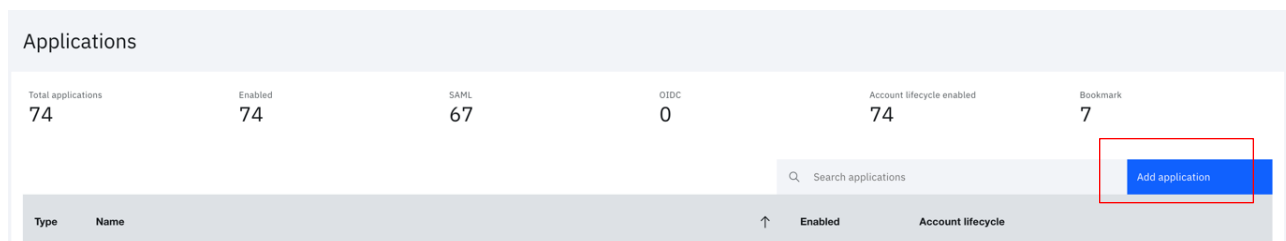
Generate Token

12. Copy **Base URL**.
13. Click **Generate Token** to create a bearer token and copy it as shown in the above image.
14. Click **Save**
15. In order to apply the new changes, logout from Zscaler admin console. Else changes will not come into effect.

2 Configure Zscaler application in Verify


2.1 Create / Update Zscaler Application

1. 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* into the search box.
4. When the Zscaler application is displayed, select it and then click the Add application button.
5. On the Add Application page leave Zscaler as the Company name.
6. If the Zscaler cloud portal URL is `https://admin.myCloudName`, use `myCloudName` as the value for 'Cloud name'.

Add application



Zscaler

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

No application owner

Add 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

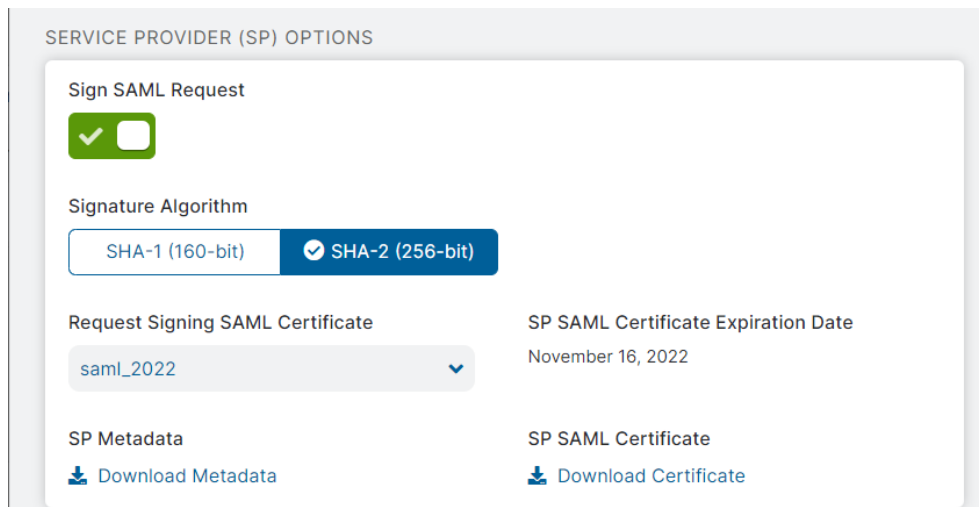
0.1

2.2 Configure Sign-on

1. Go to the **Sign-on** tab of Zscaler. Follow the instructions which are displayed in right pane
2. In another browser login to your Zscaler account as an admin user using the URL as: `https://admin.<Zscaler Cloud>`
3. For the **Authentication Type** field, Click **Open Identity Providers**.
4. **Identity Providers** ^{NEW} tab is displayed.
5. Select the previously created identity provider and click the edit icon
6. For the **SERVICE PROVIDER (SP) OPTIONS** section, specify the following settings:
 - Sign SAML Request:** Enable this option (If you want to sign the SAML request)
 - Signature Algorithm:** Select **SHA-2 (256-bit)**.
 - Request Signing SAML Certificate:** Select a certificate from the drop-down based on your requirements.

SP Metadata: Click this to download Zscaler metadata.

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](#)

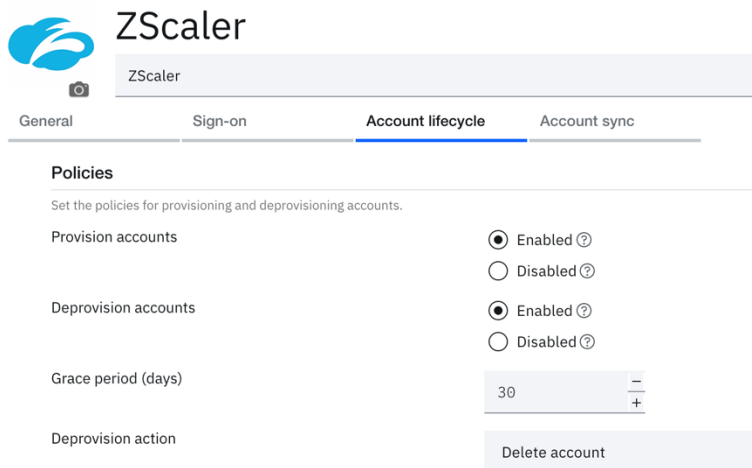
SP SAML Certificate
[Download Certificate](#)


7. In order to apply the new changes, logout from Zscaler admin console. Else changes will not come into effect.

2.3 Configure Account Lifecycle

1. Go to the **Account lifecycle** tab of Zscaler.
2. Enable the provisioning and deprovisioning. As Zscaler allows Suspend and Delete (With Grace Period) as a Deprovision action

Add application



 **Zscaler**

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

3. Scroll down to the **API Authentication** section.
4. In the SCIM base URL field, enter the SCIM url which you have generated before.
5. In the Bearer token, enter the token which you have generated before.

API authentication

API authentication information about the application.

SCIM base URL*

https://scim1.private.zscale

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.

- Click the **Test Connection** button to confirm the settings

Confirm that connection successful message is shown. If not, recheck if SCIM base URL and Bearer token is entered correctly.







- Scroll down to the **API Attribute Mappings** section and set the following:

- displayName** = *given_name*
- userName** = *preferred_username*
- name.givenName** = *given_name*
- name.familyName** = *family_name*
- 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
given_name × ▾	None × ▾	→ displayName × ▾	<input type="checkbox"/> 
preferred_username × ▾	None × ▾	→ userName × ▾	<input type="checkbox"/> 
department × ▾	None × ▾	→ department × ▾	<input type="checkbox"/> 
given_name × ▾	None × ▾	→ name.givenName × ▾	<input type="checkbox"/> 
family_name × ▾	None × ▾	→ name.familyName × ▾	<input type="checkbox"/> 
email × ▾	None × ▾	→ Email × ▾	<input type="checkbox"/> 


+ Add attribute mapping

- Click the **Save** button

2.4 Define adoption policy for account synchronization

As the Zscaler connection is successfully tested, let's define the adoption policy in order to synchronize the accounts with IBM® Security Verify. In order to define the adoption policy, click on **Account sync** tab from the details of 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

1. Click on **+ Attribute pairs** to add the attribute rule to be used to match the users from ZScaler with the existing users in Verify.

Define the rules as:

userName = preferred_username

 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

Target attributes		IBM Security Verify attributes	
userName	=	preferred_username	

 + Attribute pairs

2. Click the **Save** button


2.5 Define entitlements for application

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

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 "ZScaler 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)


 Zscaler User Group

Add

Remove

[Add new user](#)

Selected Items (1)


 Zscaler User Group

Cancel

OK

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

Applications / Details



ZScaler

ZScaler_demo_24thJune

General

Sign-on

Account lifecycle

Account sync

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

Add

Name ↑	Date Assigned	Automatic Access
 Zscaler User Group	6/24/2021	<input checked="" type="checkbox"/> On

3 Zscaler Provisioning Use Cases

After the **Zscaler application** is successfully configured as mentioned in above section, tenant admin can synchronize the **Zscaler account data** with Security Verify.

3.1 Account Synchronization with Zscaler

1. Login to ISV as tenant admin (**Scott**)
2. From the admin console navigate to **Applications**
3. Select **Accounts** from the three dot action menu against the Zscaler application



The screenshot shows the 'Applications' page with a table listing applications. The application 'Zscaler_demo_24thJune' is selected, and the 'Accounts' option is chosen from the action menu.

4. Click **Start account synchronization**

The screenshot shows the 'Accounts' page with a table listing accounts. The 'Start account synchronization' button is visible in the top right corner.

5. In order to monitor the account synchronization, navigate to the **Governance** menu and Click on **Account sync** tab

The screenshot shows the 'Account sync' page with a table listing synchronization results. The table has columns: Type, Application name, Status, Start time, and End time.



6. Click on the row for which details need to see seen. The account sync details will get open in right pane, which provides the summary of various accounts fetched from the Zscaler.

Governance

- Certification campaigns
- Operation results
- Account sync**

Filters

×
Refresh

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

Items per page 25
1-2 of 2 items
of 1 page

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

Account sync rule

The accounts will be matched on the basis on the attributes mapping defined in **Adoption policy** of Application. So, admin need to be careful while defining the attribute mapping.

3.2 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 = [zscaleruser01@ex.com](#) (*Use the Domain name which is registered or associated with Zscaler Identity Provider*)
- o Given name = *User01*
- o Surname = *Zscaler*
- o Email = *a valid real email address*

×

Add user

☒ On

Basic user profile

Given name

User01

Middle name (optional)

Surname

Zscaler

User name

zscaleruser01@~~ex.com~~

External ID (optional)

Preferred language (optional)

User information

Cancel
Save

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

Users & groups

Users Groups Settings

Search User01 Add user

User	Enabled	Linked identities	Date created	Last login
<input type="checkbox"/> User01 Zscaler shalesh.kathole@hcl.com zscaleruser01@genisistent.com@hcl	<input checked="" type="checkbox"/>		Jun 24, 2021	—

Items per page: 50 1-1 of 1 item of 1 page

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

3.2.1 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

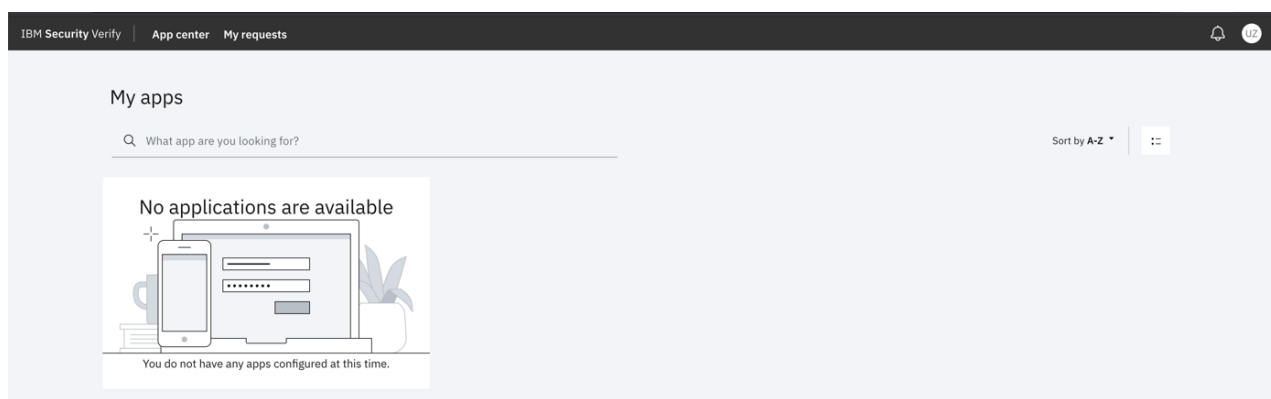
Your account was created.

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

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



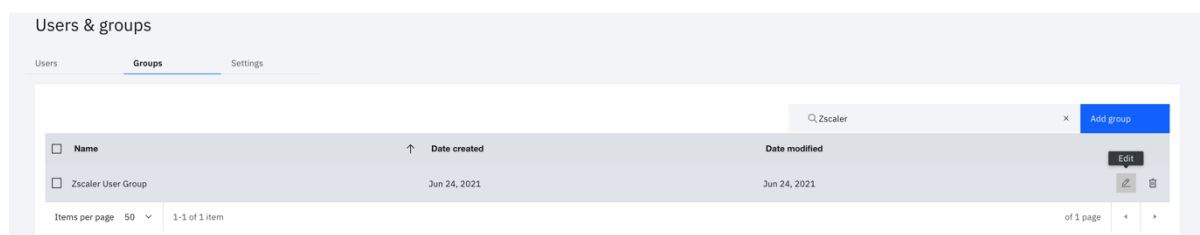
3.3 Provisioning Use Case

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

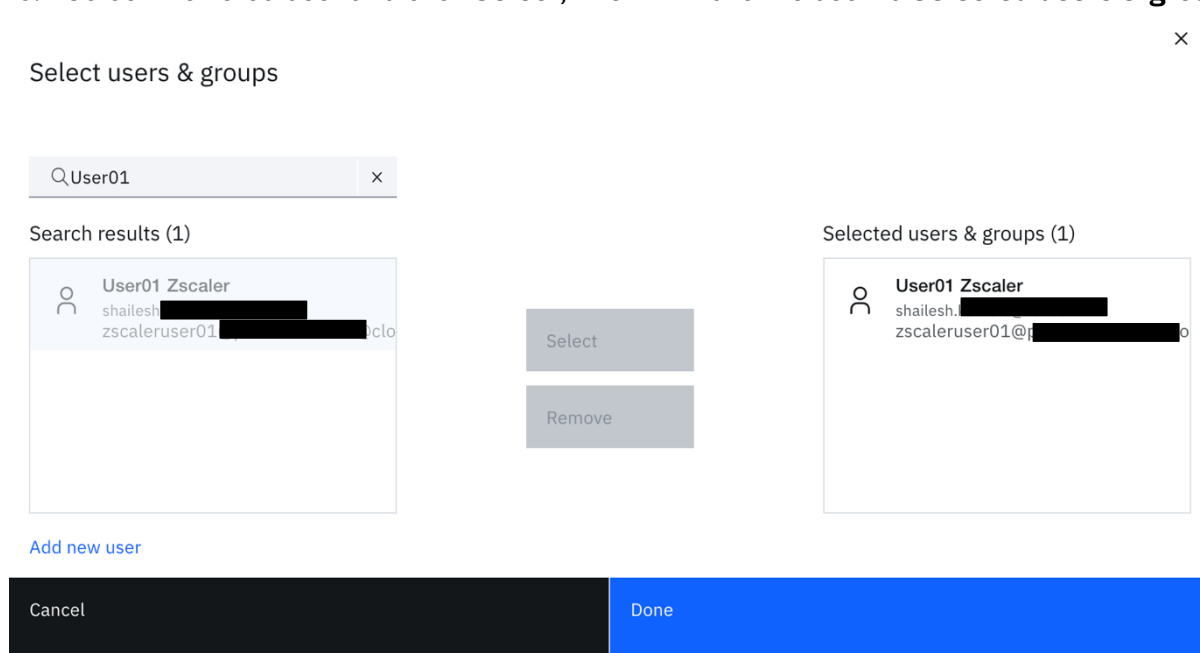
Add User to Group

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 “**Zscaler 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 **Zscaler User Group** group

Users & groups

User01 Zscaler

Profile MFA settings Activity

User information

Status Enabled

Expiration date —

Basic user profile

Full name User01 Zscaler

Given name User01

Middle name —

Surname Zscaler

User ID 617000AXZM

User name zscaleruser01@persistent.com

Realm cloudIdentityRealm

External ID —

Preferred language —

Email verified on —

Security settings

Password last changed on June 24, 2021

[Reset password](#)

Groups (1)

Zscaler User Group

Linked identities (0)

No linked identities

3.3.1 Check User has been provisioned to Zscaler

As the user has been added to **Zscaler 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_demo_24thJune	Provision account	persistent.com	Success	Jun 24, 2021 2:49 PM IST

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

1. Navigate to **Administration > Authentication > User Management**.

ZIA
 Dashboard
 Analytics
 Policy
 Administration
 Activation

Settings

ACCOUNT MANAGEMENT

My Profile

Company Profile

Alerts

Print All Policies

Authentication

AUTHENTICATION CONFIGURATION

Authentication Settings

User Management

CLOUD CONFIGURATION

Advanced Settings

DLP Incident Receiver **NEW**

Partner Integrations **NEW**

SaaS Application Tenants **NEW**

ADMINISTRATION CONTROLS

Administrator Management

Role Management

Audit Logs

Backup & Restore

2. Look for newly provisioned user


User Management						
<div> Users Groups Departments </div>						
<div> Add User Download Import Sample Import CSV file </div>						
<div> <div>User ID or Name</div> <div>User01</div> <div>✕</div> <div>🔍</div> </div>						
No.	User ID or Name	User Display Name	Groups	Department	Comments	
1	zscaleruser01@persistent.com	User01	---	---	---	

Validate the user details such as:

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

3.3.2 Check new user can access Zscaler via SSO

1. Access the SP init URL to Zscaler as (<http://gateway.your.domain/test>)
2. Provide the username



Sign In

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

User Name

[Sign In](#)

Need help? Contact your IT support.

3. Validate that user gets redirected to Verify for SSO
4. Provide the username and password

IBM **Security** Verify

Sign in with Cloud Directory

User name

Password

[Forgot password?](#)

[Sign in](#)

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

Users & groups

User01 Zscaler

Profile MFA settings Activity

User information

Status Enabled

Expiration date —

Basic user profile

Full name User01 Zscaler

Given name User01

Middle name —

Surname Zscaler

User ID 617000AXZM

User name [REDACTED]@persistent.com

Realm cloudIdentityRealm

Security settings

Password last changed on June 24, 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**)


- 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_demo_24thJune	Deprovision account	[REDACTED]@persistent.com	Success	Jun 24, 2021 3:14 PM IST

Check the User has been removed from Zscaler

- Return to the **Zscaler** and search with the username
- Check that no users get listed.

User Management

Users **Groups** Departments

[Add User](#) [Download](#) [Import](#) [Sample Import CSV file](#)

User ID or Name [x](#) [Q](#)

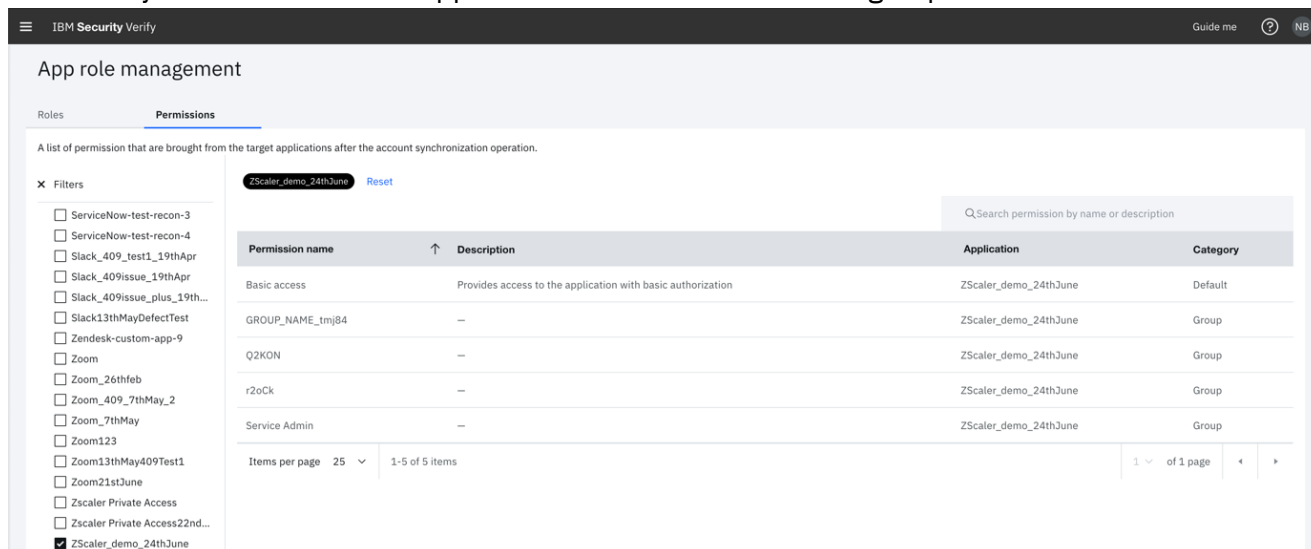
No.	User ID or Name	User Display Name	Groups	Department	Comments
No matching items found					

4 Zscaler App Role Management Use Cases

Permission can be managed through App Role Management where a user can be added to Zscaler groups. These groups are fetched during account synchronisation.

4.1 Assign User to the Zscaler group through Permissions

1. Login to ISV as tenant admin (Scott)
2. From the admin console navigate to **App Role Management > Permissions**
3. Filter your created Zscaler Application and check the Zscaler groups.



App role management

Roles **Permissions**

A list of permission that are brought from the target applications after the account synchronization operation.

Filters

- ☐ ServiceNow-test-recon-3
- ☐ ServiceNow-test-recon-4
- ☐ Slack_409_test1_19thApr
- ☐ Slack_409issue_19thApr
- ☐ Slack_409issue_plus_19th...
- ☐ Slack13thMayDefectTest
- ☐ Zendesk-custom-app-9
- ☐ Zoom
- ☐ Zoom_26thfeb
- ☐ Zoom_409_7thMay_2
- ☐ Zoom_7thMay
- ☐ Zoom123
- ☐ Zoom13thMay409Test1
- ☐ Zoom21stJune
- ☐ Zscaler Private Access
- ☐ Zscaler Private Access22nd...
- ☒ ZScaler_demo_24thJune

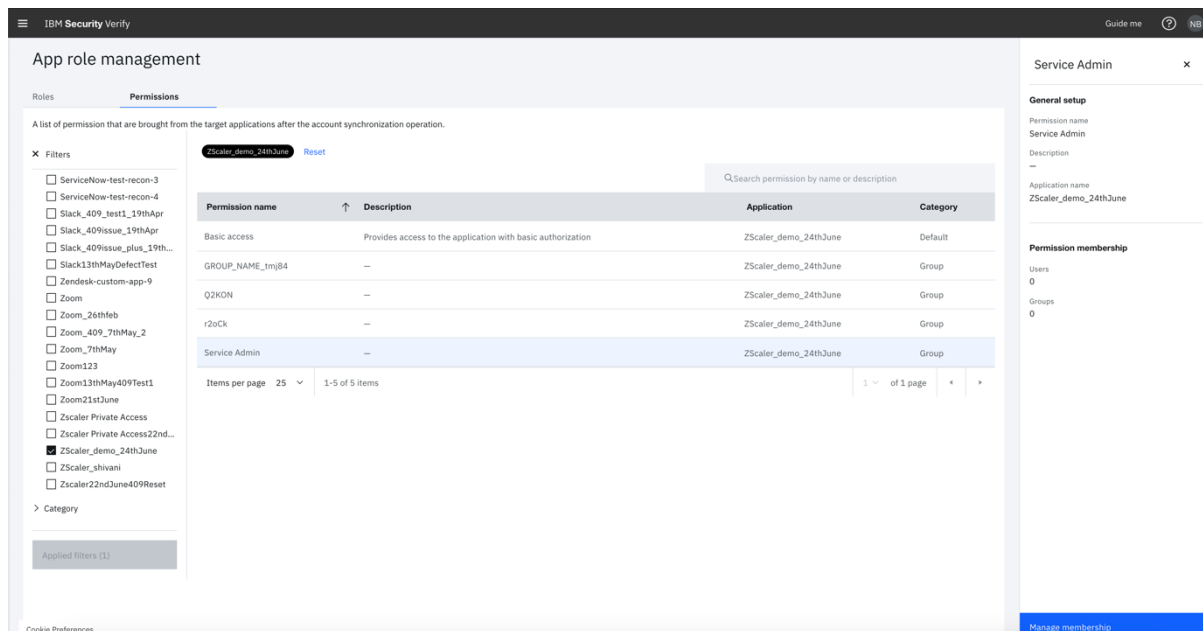
Permissions

Q Search permission by name or description

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

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

4. Click on any of the group (Service Admin) and click on **Manage membership**.



App role management

Roles **Permissions**

A list of permission that are brought from the target applications after the account synchronization operation.

Filters

- ☐ ServiceNow-test-recon-3
- ☐ ServiceNow-test-recon-4
- ☐ Slack_409_test1_19thApr
- ☐ Slack_409issue_19thApr
- ☐ Slack_409issue_plus_19th...
- ☐ Slack13thMayDefectTest
- ☐ Zendesk-custom-app-9
- ☐ Zoom
- ☐ Zoom_26thfeb
- ☐ Zoom_409_7thMay_2
- ☐ Zoom_7thMay
- ☐ Zoom123
- ☐ Zoom13thMay409Test1
- ☐ Zoom21stJune
- ☐ Zscaler Private Access
- ☐ Zscaler Private Access22nd...
- ☒ ZScaler_demo_24thJune
- ☐ Zscaler_shivani
- ☐ Zscaler22ndJune409Reset

Permissions

Q Search permission by name or description

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

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

Service Admin

General setup

Permission name
Service Admin

Description
—

Application name
ZScaler_demo_24thJune

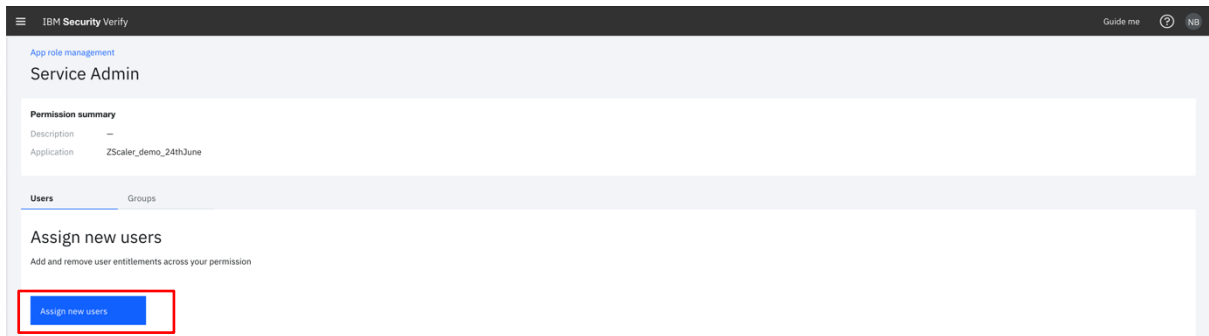
Permission membership

Users
0

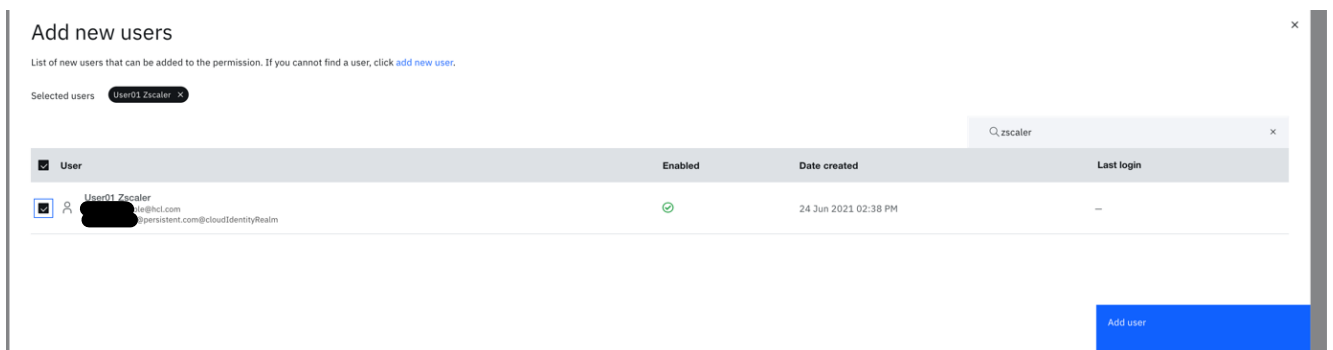
Groups
0

Manage membership

5. Click on **Assign new users**.

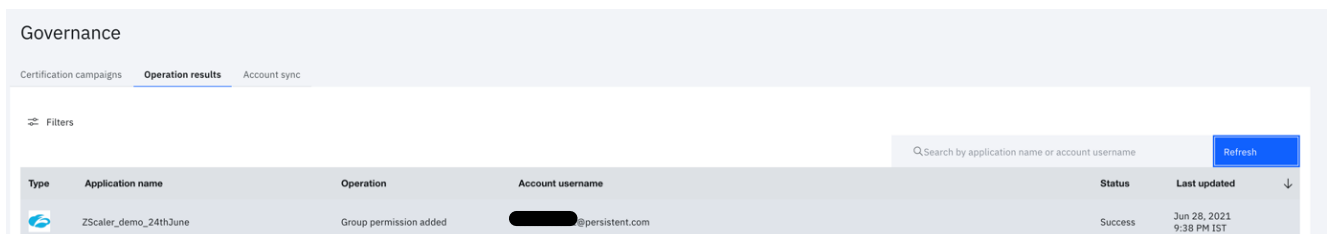


6. Search with the userName (zscaleruser01) , select the user and click on **Add User**



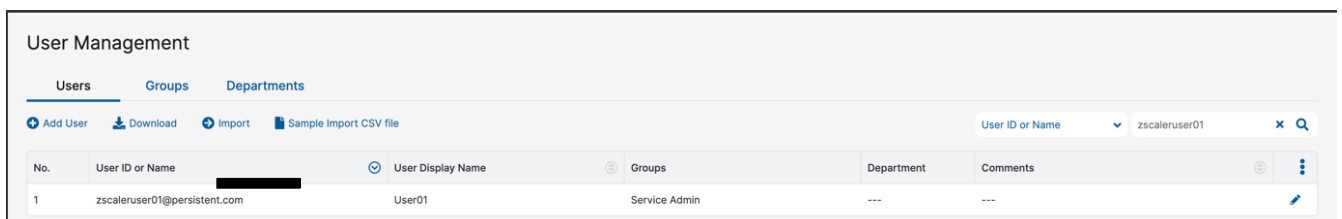
The group permission added task can be monitored by the admin (**Scott**)

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



4.1.1 Check the User has been added to the Zscaler group from Zscaler

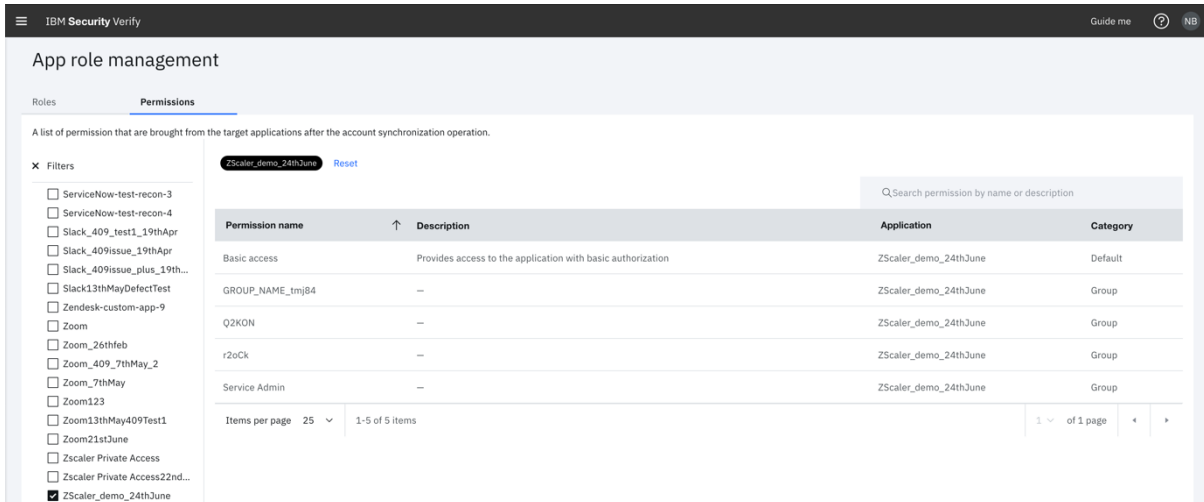
1. Return to the **Zscaler** and search with the username (zscaleruser01) .
2. check the Groups column.



4.2 Remove User from the Zscaler group through Permissions

When user is revoked from Zscaler group, then it also gets deprovisioned from the Zscaler.

1. Login to ISV as tenant admin (Scott)
2. From the admin console navigate to **App Role Management > Permissions**
3. Filter your created Zscaler Application and check the Zscaler groups.



App role management

Roles Permissions

A list of permission that are brought from the target applications after the account synchronization operation.

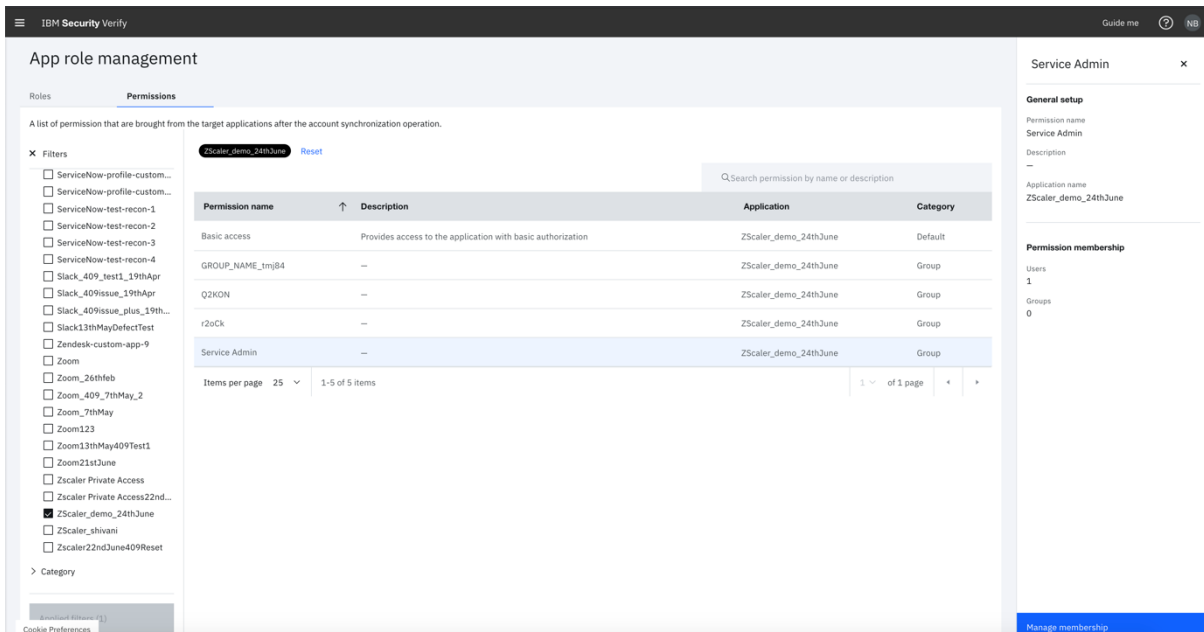
Filters: ZScaler_demo_24thJune Reset

Search permission by name or description

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

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

4. Click on any of the group (Service Admin) and click on **Manage membership**



App role management

Roles Permissions

A list of permission that are brought from the target applications after the account synchronization operation.

Filters: ZScaler_demo_24thJune Reset

Search permission by name or description

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

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

Service Admin

General setup

Permission name: Service Admin

Description: —

Application name: ZScaler_demo_24thJune

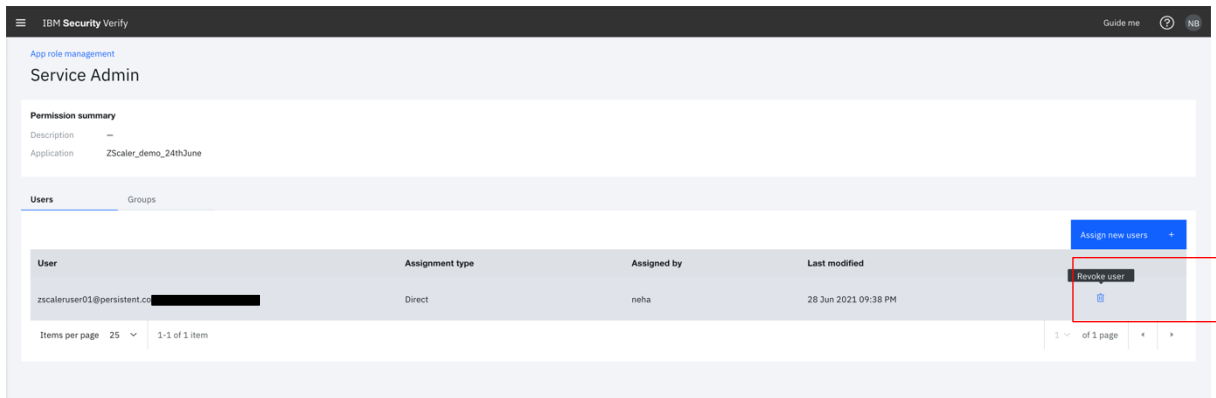
Permission membership

Users: 1

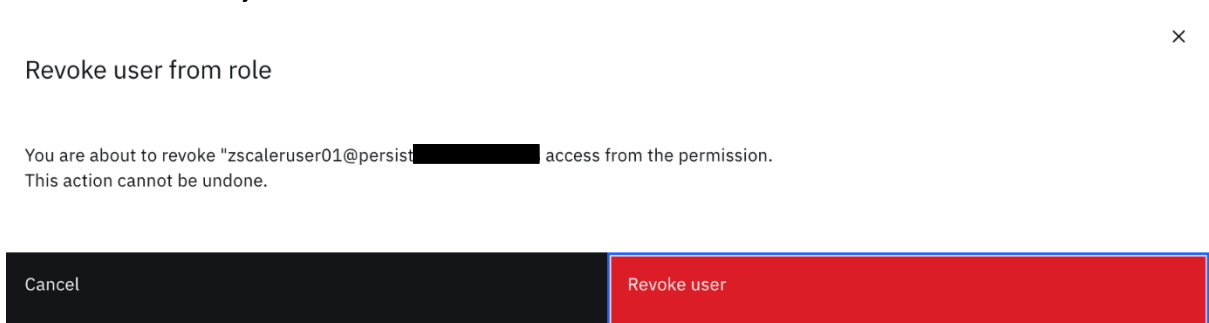
Groups: 0

Manage membership

5. Hover over the user whose permission you want to remove and click on the delete icon (**Revoke User**).

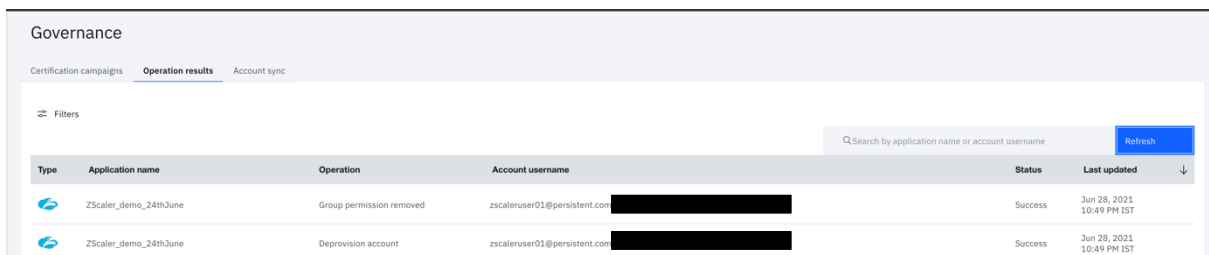


6. It will ask for you confirmation. Click on **Revoke User**.



The group permission removed task can be monitored by the admin (**Scott**)

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

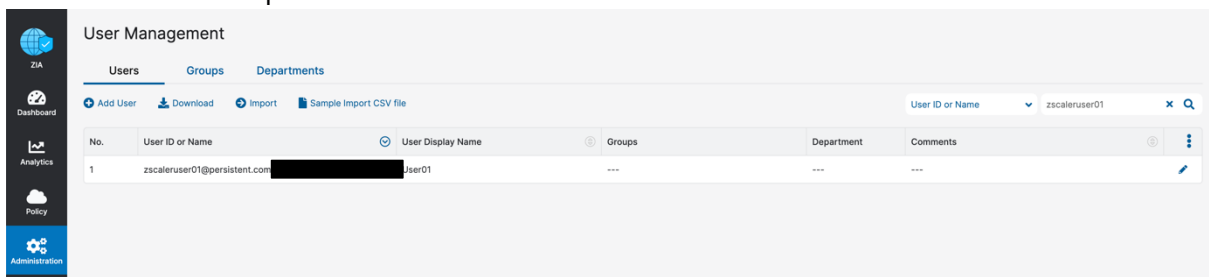


Important Note

If your Zscaler application deprovision action is set to **“Delete”**, then user gets delete from the Zscaler.

4.2.1 Check the User has been removed to the Zscaler group from Zscaler

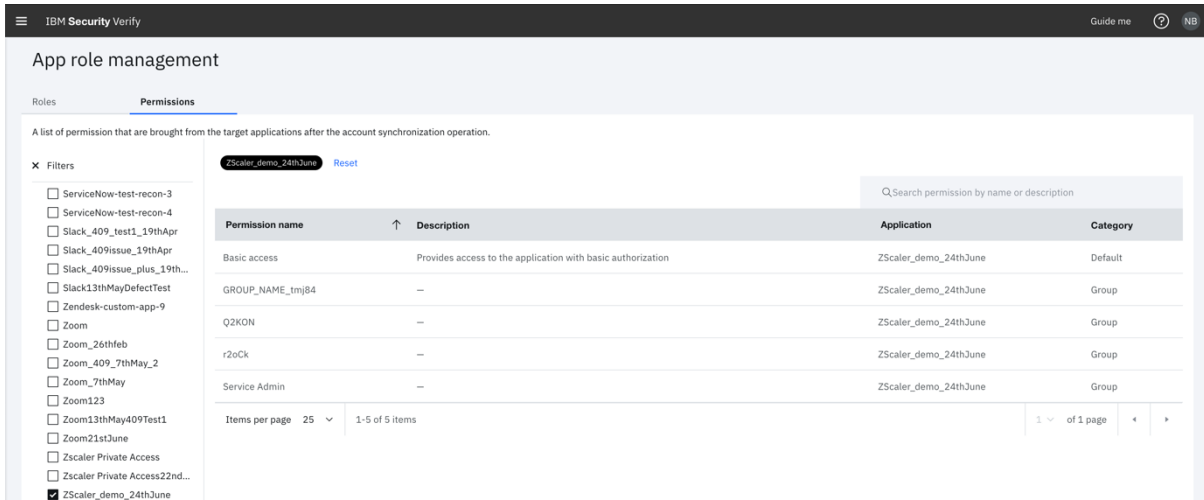
1. Return to the **Zscaler** and search with the username (zscaleruser01) .
2. Check the Groups column.



4.3 Provision a new user and assign to a Zscaler group through Permission.

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

1. Login to ISV as tenant admin (Scott)
2. From the admin console navigate to **App Role Management > Permissions**
3. Filter your created Zscaler Application and check the Zscaler groups.



App role management

Roles Permissions

A list of permission that are brought from the target applications after the account synchronization operation.

Filters: ZScaler_demo_24thJune Reset

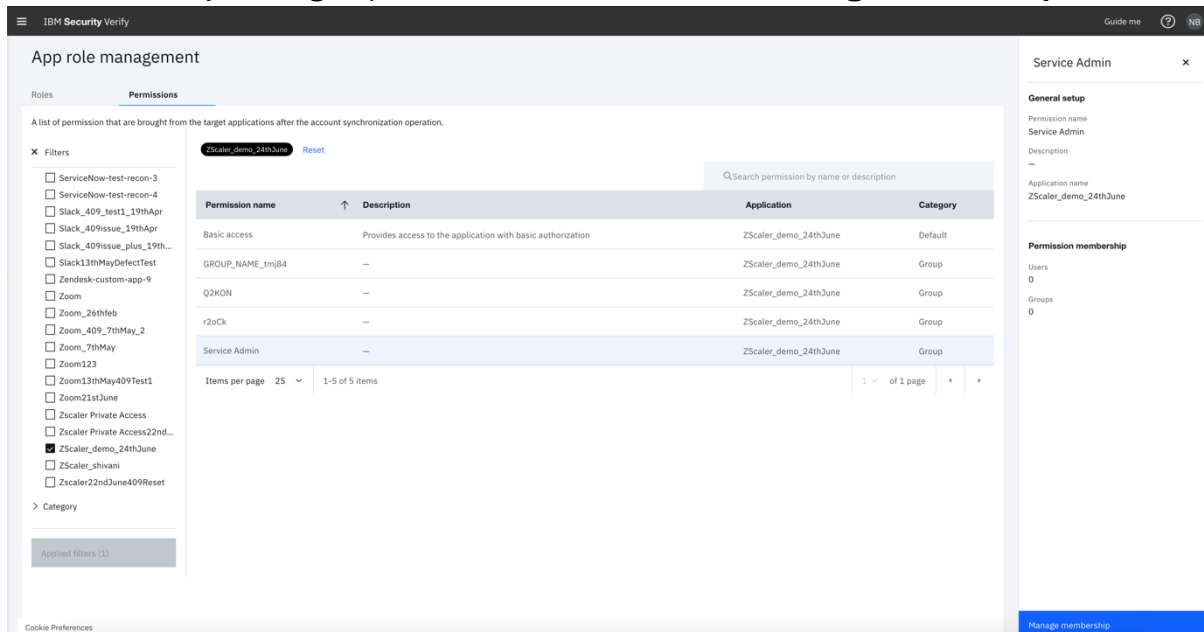
Search permission by name or description

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

Items per page: 25 1-5 of 5 items

1 of 1 page

4. Click on any of the group (Service Admin) and click on **Manage membership**



App role management

Roles Permissions

A list of permission that are brought from the target applications after the account synchronization operation.

Filters: ZScaler_demo_24thJune Reset

Search permission by name or description

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

Items per page: 25 1-5 of 5 items

1 of 1 page

Service Admin

General setup

Permission name: Service Admin

Description: —

Application name: ZScaler_demo_24thJune

Permission membership

Users: 0

Groups: 0

Manage membership

5. Click on **Assign new user**.



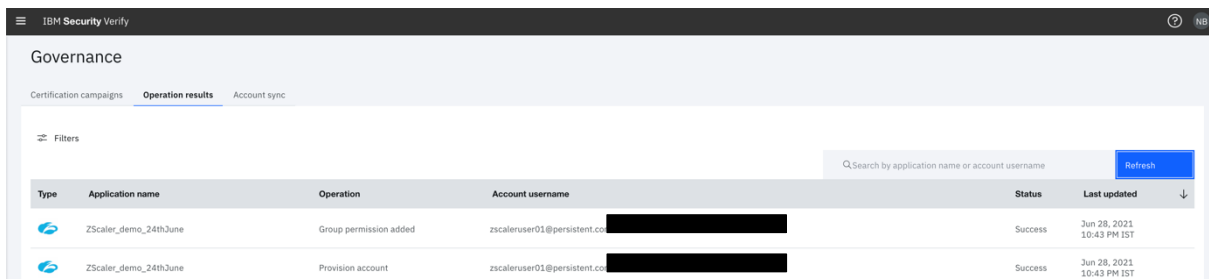
6. Click on the **add new user** link.



7. This will navigate to the **Users & Groups**.
8. Add a new user. Refer **New User Provisioning to Zscaler** section.
9. Once user is created , follow the same steps under **Add User to the Zscaler group** section.

The group permission added task can be monitored by the admin (**Scott**)

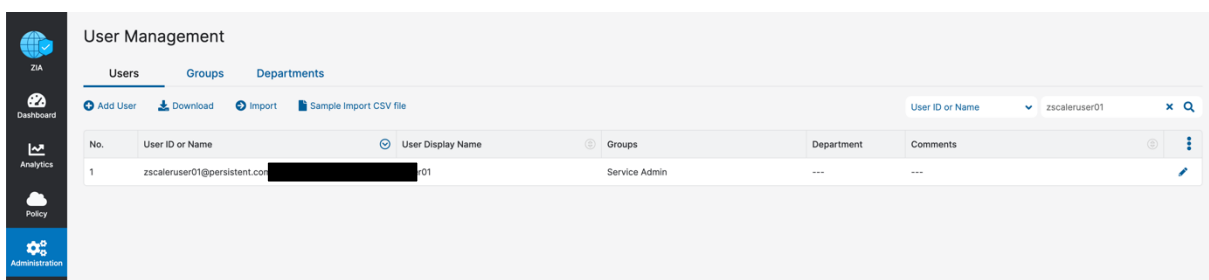
1. Navigate to **Governance > Operation results** tab



2. As can be seen in the above image, user account gets provision before group permission add when we create a new user and then assign it to a group through App Role Management.

4.3.1 Check the User has been added to the Zscaler group from Zscaler

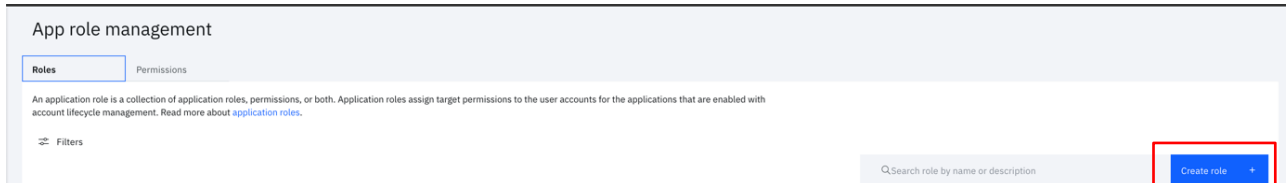
1. Return to the **Zscaler** and search with the username (zscaleruser01) .
2. Check the Groups column.



4.4 Add User to the Zscaler group through Roles

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

1. Login to ISV as tenant admin (Scott)
2. From the admin console navigate to **App Role Management > Roles**
3. Click on the **Create role**.



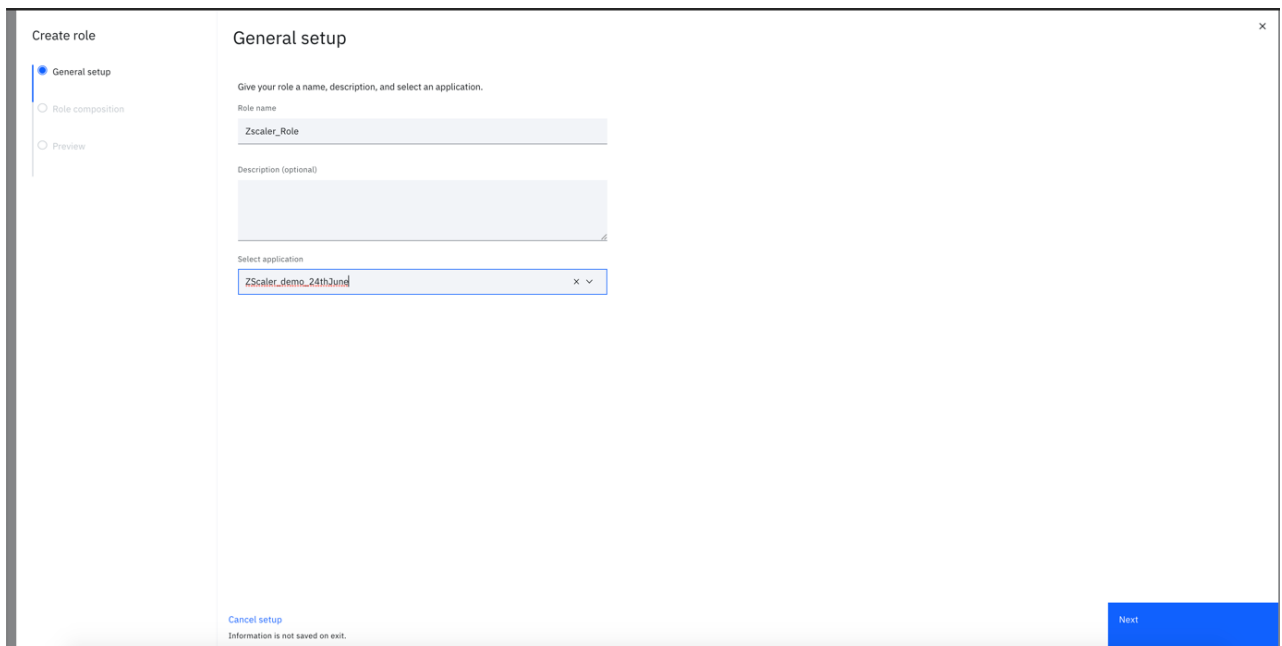
4. Add the following details :-

Role name: *Zscaler_Role*

Description: Add a meaningful description. This is an optional field

Select application: *Your Zscaler application*

Click Next.



5. Navigate to **Permissions** tab ,select the group (Service Admin) and click on Next.

Create role

General setup

Role composition

Preview

Role composition

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

Roles

Permissions

Selected permissions

Service Admin

Q 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_tmj84	—	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

6. Click Next.

Create role

General setup

Role composition

Preview

Preview

Here's a preview of the hierarchy that is formed by the selected permissions and roles.

Role name

Zscaler_Role

Description

—

Application name

Zscaler_demo_24thJune

Role hierarchy

Zscaler_Role (1)

Service Admin

Cancel setup

Information is not saved on exit.

Back

Create role

7. Click on Create Role.

8. Search with Role Name (Zscaler_Role).

App role management

Roles

Permissions

An application role is a collection of application roles, permissions, or both. Application roles assign target permissions to the user accounts for the applications that are enabled with account lifecycle management. Read more about [application roles](#).

Filters

Q Zscaler_Role

Create role

Role name	Application name	Description
Zscaler_Role	Zscaler_demo_24thJune	This is Zscaler role

Items per page 25

1-1 of 1 item

1 of 1 page

Page 29 of 30

9. In order to Manage membership, click on the above created Role (Zscaler_Role) and follow the same steps as mentioned under **Assign User to the Zscaler group through Permissions** section or **Provision a new user and assign to a Zscaler group through Permission** section.