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 Nilesh Atal (NileshAtal@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**

<table>
<thead>
<tr>
<th>Release Date</th>
<th>Ver</th>
<th>Authors</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 Jul 2021</td>
<td>1.0</td>
<td>Neha Bist</td>
<td>First draft with provisioning usecases</td>
</tr>
<tr>
<td>10 Jul 2021</td>
<td>2.0</td>
<td>Nilesh Atal</td>
<td>Added SSO configuration details</td>
</tr>
</tbody>
</table>
# 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://xxxx.verify.ibm.com/saml/sps/saml20ip/saml20/login](https://xxxx.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.
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**.
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 Zcaler 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'.

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.
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.

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.
6. 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 in entered correctly.

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

Others can be left as it is.

8. 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.
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`

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. 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 “ZScaler User Group” (This group must have been already created by admin)
4. Click the **OK** to close the dialog
5. Click the **Save** button to save application changes.
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
4. Click Start account synchronization
5. In order to monitor the account synchronization, navigate to the Governance menu and Click on Account sync tab
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.
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:
- Identity Source = Cloud Directory
- User name = zscaleruser01@ex.com (Use the Domain name which is registered or associated with Zscaler Identity Provider)
- Given name = User01
- Surname = Zscaler
- Email = a valid real email address

5. Click the Save button to create the user
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.

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
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

Also validate the new user provisioning by log in to Zscaler
1. Navigate to Administration > Authentication > User Management.
2. Look for newly provisioned user

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

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

IBM Security Verify
Sign in with Cloud Directory
5. Validate that user gets access to Zscaler

3.4 De-Provisioning Use Case

Let’s do the reverse operation to test de-provisioning user from Zscaler

Remove User from Zscaler 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 Zscaler User Group group
4. Select newly added user and click the Remove button
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.

The user de-provisioning task can be monitored by the admin (**Scott**)
1. Navigate to **Governance > Operation results** tab

**Check the User has been removed from Zscaler**
1. Return to the **Zscaler** and search with the username
2. Check that no users get listed.
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.

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

5. Click on Assign new users.
6. Search with the userName (zscaleruser01), select the user and click on **Add User**

![Add User](image)

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

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

![Governance](image)

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.

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

Revoke user from role

You are about to revoke "zscaleruser01@person" access from the permission. This action cannot be undone.

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.

4. Click on any of the group (Service Admin) and click on 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.
6. Click Next.

7. Click on Create Role.

8. Search with Role Name (Zscaler_Role).
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.