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 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 ......................................................................................... Error! Bookmark not defined.
   2.1 Create / Update Zscaler Application ...................................................................................... Error! Bookmark not defined.
   2.2 Configure Sign-on ....................................................................................................................... Error! Bookmark not defined.
   2.3 Configure Account Lifecycle ..................................................................................................... Error! Bookmark not defined.
   2.4 Define adoption policy for account synchronization .............................................................. Error! Bookmark not defined.
   2.5 Define entitlements for application ......................................................................................... Error! Bookmark not defined.

3 Zscaler Provisioning Use Cases ....................................................................................................... 13
   3.1 Account Synchronization with Zscaler ..................................................................................... Error! Bookmark not defined.
   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

4 Zscaler App Role Management Use Cases ......................................................................................... Error! Bookmark not defined.
   4.1 Assign User to the Zscaler group through Permissions ............................................................. Error! Bookmark not defined.
      4.1.1 Check the User has been added to the Zscaler group from Zscaler Error! Bookmark not defined.
   4.2 Remove User from the Zscaler group through Permissions ...................................................... Error! Bookmark not defined.
      4.2.1 Check the User has been removed to the Zscaler group from Zscaler Error! Bookmark not defined.
   4.3 Provision a new user and assign to a Zscaler group through Permission Error! Bookmark not defined.
      4.3.1 Check the User has been added to the Zscaler group from Zscaler Error! Bookmark not defined.
   4.4 Add User to the Zscaler group through Roles ............................................................................. Error! Bookmark not defined.
**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

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

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.
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
8. Update the **Assertion Consumer Service URL** text field with **Service Provider URL** copied from Zscaler.

9. Update the **Provider ID** text field with **Service Provider Entity ID** copied from Zscaler.

10. In the instructions pane, goto **SAML CONFIGURATION** section and download the **IdP Metadata** file.

11. Save the application configuration in Verify.

12. Now go back to the Zscaler admin console, upload the downloaded **IdP Metadata** at the **Create IdP** section.

13. Set **Status** as Enabled.

14. Set **SAML Attributes for Policy** as Enabled.

15. 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

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

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
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

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** = **user Name**
    b. **given_name** = **name.givenName**
    c. **family_name** = **name.familyName**
    d. **email** = **Email**
    Others can be left as it is.
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

5. Click the **Save** button to save application changes.
### Zscaler Private Access

#### General

**Access Type**
- [ ] Automatic access for all users and groups
- [ ] Approval required for all users and groups
- [x] Select users and groups, and assign individual accesses

**Approver**
- [ ] User's manager
- [ ] Application owner

#### Entitlements

<table>
<thead>
<tr>
<th>Name</th>
<th>Date Assigned</th>
<th>Automatic Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZPA User Group</td>
<td>6/23/2022</td>
<td>On</td>
</tr>
</tbody>
</table>
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:**
- Identity Source = Cloud Directory
- User name = zpauser01
- Given name = User01
- Surname = ZPA
- Email = a valid real email address

5. Click the Save button to create the user
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

![IBM Security Verify](image)

**Your account was created.**

**Your temporary password is:** kMD–7ScS

After you log in, you must change your password.

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

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
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

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

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

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 private access

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