Cookbook for Ivanti Connect Secure

Ivanti Connect Secure can work as SAML service provider. Use Okta or any appropriate IDP and configure a Customer SP federation pair on Access using Ivanti Connect Secure SP and IDP.

This cookbook considers Okta as the identity provider.

NOTE: If the user tries to configure Request Header rule with Header Name as "Referer", the configured header rule will not be evaluated by Access. This occurs as by default, Ivanti Connect Secure does not send Referer Header in the SAML request.

Complete the following procedure to configure Ivanti Connect Secure.

Before you begin

- Ensure your global SAML configuration is correct
  - Login to Ivanti Connect Secure admin portal.
  - Under **System** > **Configuration** > **SAML**, select **Settings**.
    Validate or populate Host FQDN for SAML with the FQDN of your Ivanti Connect Secure Appliance
  - Click **Save**.

Creating metadata file for Ivanti Connect Secure

1. Login to **Ivanti Connect** Ivanti Connect portal.
2. Under **System** > **Configuration** > **SAML**, select **New Metadata Provider**.
3. Enter a **Name** such as Access_ZSO.
4. Select **Remote** for location.
5. Enter the **Download URL** provided by Okta.
6. Verify the Identity Provider for roles.
7. Click **Save**.
   It takes a few moments for the values to populate from the Metadata Service. Refresh the page to see if download was successful or not.

Downloading metadata on Ivanti Connect Secure

1. Login to **Ivanti Connect Secure** admin portal.
2. Under **Authentication** > **Auth. Servers** choose new SAML Server and click **New Server**.

3. Enter a **Name** such as Access_ZSO.
4. Select **2.0** for SAML Version.
5. Select **Metadata** for Configuration Mode.
6. Select the **Identity Provider Entity Id** from your Okta SAML Metadata Provider (In Creating metadata file for Ivanti Connect Secure).
7. Select **POST** for SSO Method.
8. Select the **Okta SSO Certificate**.
9. Select a valid **Device Certificate for Signing**.
10. Click **Save**.
11. Edit the Authentication Server created and click **Download Metadata**.

Configuring Federated Pair on Access

1. Login to **Access admin portal**.
2. Click **Profile** > **Federation** > **Add Pair**.
3. Select **Pulse Secure** as the service provider.
4. Upload **Pulse SAML metadata.xml** saved in Downloading metadata on Ivanti Connect Secure.
5. Select **Use Tunnel Certificates for SSO**.
6. Click **Next**.
7. Select **Okta** as the identity provider in the catalog.
8. Upload the **Okta Metadata**.
9. Click **Done**.
10. Publish the profile.

Updating Ivanti Connect Secure configuration to federate with Access

1. Login to **Ivanti Connect Secure** admin portal.
2. Edit the metadata provider created in Creating metadata file for Ivanti Connect Secure.
3. Enter the **Access IDP Metadata (Upload to SP)** download URL.
4. Click **Save**.
   Refresh the page to ensure that the new metadata is downloaded successfully.
5. Edit the SAML Auth server created in Downloading metadata on Ivanti Connect Secure.

6. Edit and update the Identity Provider Entity ID to newly updated access url.
7. Select the **Access SSO Certificate**.
8. Click **Save**.

Updating Okta configuration to federate with Access

1. Login to **Okta admin portal** and edit the Metadata Provider.

Additional configurations on Pulse Secure required for end-end flow

The following configuration is for users with ZSO enabled on Access admin portal.

Enable ZSO for user portal

Configure Users Realm to use SAML Auth Server

1. Login to **Pulse admin portal** > **Users** > **User Realm** > **New User Realm**.
2. Enter a name for realm and select **SAML Auth server in Authentication**.
3. Click **Save**.
4. Under **Role mapping**, create a new rule with username * and select **Users** role from the list.
5. Click **Save**.

Configure Sign In Policy for ZSO

1. Login to **Pulse admin portal** > **Authentication** > **Sign In** > **Sign In Policies**.
2. Click **New URL**.
3. Select **User type** > **Users**.
4. Enter "***/zso**" as the Sign-in URL.
5. In Authentication realm, select **User Picks from a list of authentication realm** and select the User realm configured for ZSO.
6. Click **Save**.

Enable ZSO for Admin Portal

Configure Admin Realm to use SAML Auth Server

1. Login to **Pulse admin portal** > **Admin** > **Admin Realm** > **New Admin Realm**.
2. Enter a name for realm and select **SAML Auth server in Authentication**.
3. Click **Save**.
4. Under **Role mapping**, create a new rule with username * and select **Users** role from the list.
5. Click **Save**.

Configure Sign In Policy for ZSO

1. Login to **Pulse admin portal** > **Authentication** > **Sign In** > **Sign In Policies**.
2. Click **New URL**.
3. Select **User type** > **Administrators**.
4. Enter "***/zso**" as the Sign-in URL.
5. In Authentication realm, select **User Picks from a list of authentication realm** and select the **Admin realm configured for ZSO.**
6. Click **Save**.

Enable ZSO for Pulse Client

Configure VPN Profile for Pulse Client

1. Login to **Pulse admin portal** > **Users** > **Resource Policies** > **VPN Tunneling** > **Connection profile**.
2. Create a **New Profile**.
3. Enter a name for the profile.
4. In IPv4 address assignment, select **IPv4 address pool** and enter a pool of IP address. For example: 10.10.10.1-100
5. Click **Save**.