MobileIron Access Cookbook

Access with ServiceNow and PingOne

September 26, 2017

Contents

Overview 3
Prerequisites 3
Configuring ServiceNow and Pingone with MobileIron Access 4
Configure Access to create a Federated Pair 4
Configure the ServiceNow environment 5
Configure PingOne environment 6
Register Sentry to Access 7
Verification 7

Overview

SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as ServiceNow is federated with an identity provider such as PingOne for authentication. Users get authenticated from PingOne and obtain a SAML token for accessing applications in a cloud environment, such as ServiceNow.
This guide serves as step-by-step configuration manual for users using PingOne as an authentication provider with ServiceNow in a cloud environment.

Prerequisites

- Verify that you have the metadata for ServiceNow (SP).

    1. Login to ServiceNow with admin credentials.
    2. Navigate to **Multi Provider SSO** > **Identity Providers** > **PingOne identity provider** and note the below attributes:

        - EntityID = https://<domain_name>.service-now.com
        - ServiceNow HomePage: https://<domain_name>.service-now.com/navpage.do

- Verify that you have the metadata for PingOne (IdP):

    1. Login to PingOne with admin credentials.
    2. Navigate to **Applications** > **ServiceNow**.
    3. Click the *SAML Metadata* download link to download the IdP metadata file.

Configuring ServiceNow and PingOne with MobileIron Access

You must perform the following tasks to configure ServiceNow and PingOne with MobileIron Access:

- Configure Access to create a Federated Pair
- Configure the ServiceNow environment
- Configure the PingOne environment
- Register Sentry to Access

Configure Access to create a Federated Pair

You must configure Access to create a Federated Pair. For this, you must create a service provider and then associate the identity provider with Access.

Procedure

1. Log in to **Access**.
2. Click **Profiles** > **Get Started**.
3. Enter Access host information and upload the **ACCESS SSL certificate**. All other fields are set to default. Click **Save**.
4. On the **Federated Pairs** tab, click **Add** and select **ServiceNow** as the service provider.
5. Enter the following details:
    a. Name
    b. Description
    c. Upload the Access Signing Certificate.
    d. Add the metadata. See Prerequisites.
    e. (Optional): Select **Use Tunnel Certificates for SSO** for users to be authenticated automatically. This leverages the user's authentication in the MobileIron Tunnel VPN. See *Appendix* in the *MobileIron Access Guide* at https://support.mobileiron.com/docs/curent/accs.
6. Click **Next**.
7. Select **Ping Identity** as the Identity Provider. Click **Next**.
8. Upload the **IdP metadata file** that you downloaded. See Prerequisites.
9. Click **Done**.
10. Download the **ACCESS SP Metadata** file and upload to PingOne.
11. Download the **ACCESS IDP Metadata** file and upload to ServiceNow.
12. On the **Profile** tab, click **Publish** to publish the profile.

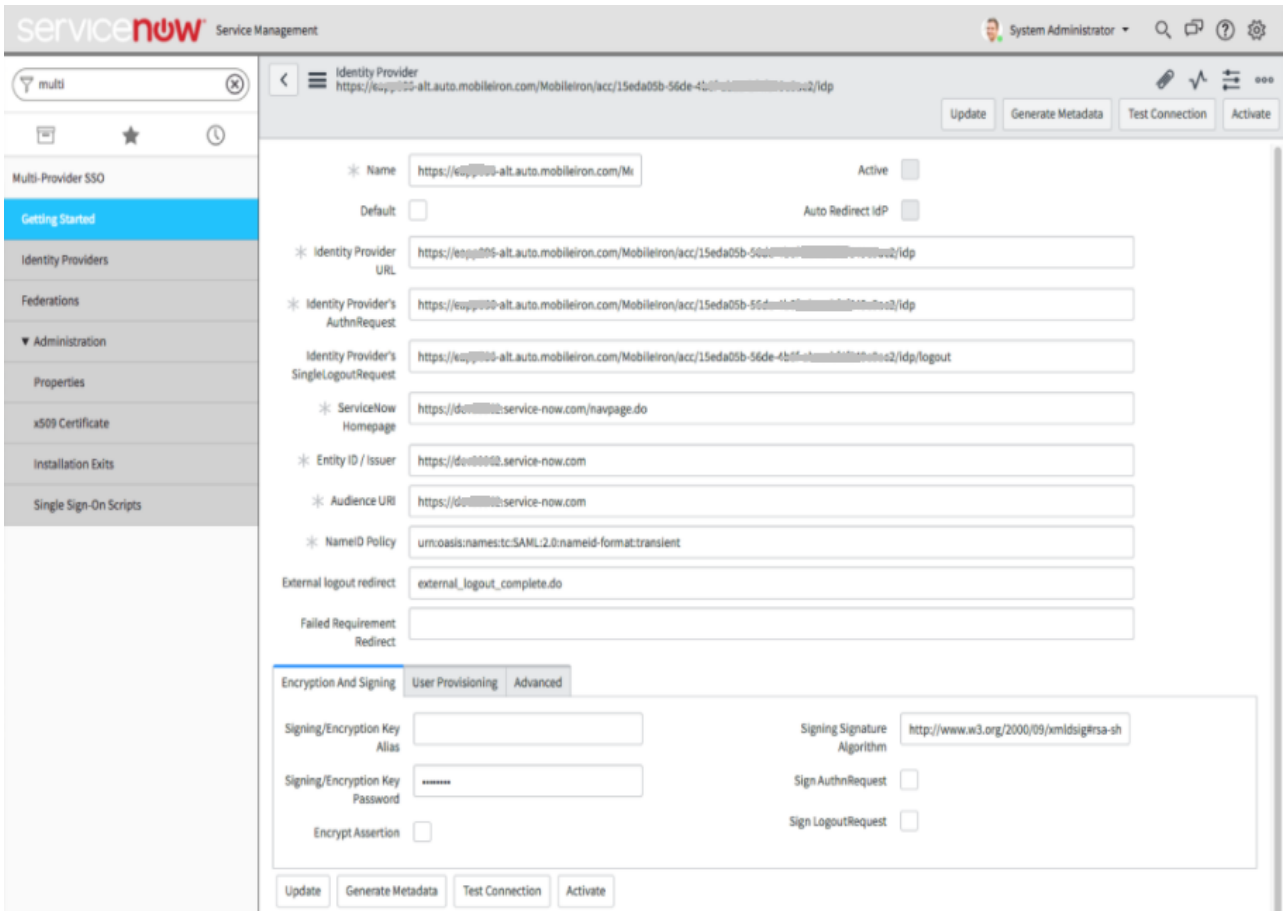
Task Result

The Federated Pair is created.

Configure the ServiceNow environment

You must configure the ServiceNow with Access natively.

1. Login to ServiceNow with admin credentials.
2. Navigate to **Multi-Provider SSO > Identity Providers** > **New** > **SAML** > **Import Access IdP Metadata** using XML that you downloaded at **Step 11** of Configuring ServiceNow and PingOne with MobileIron Access**.** The following details populate when you upload the metadata file.

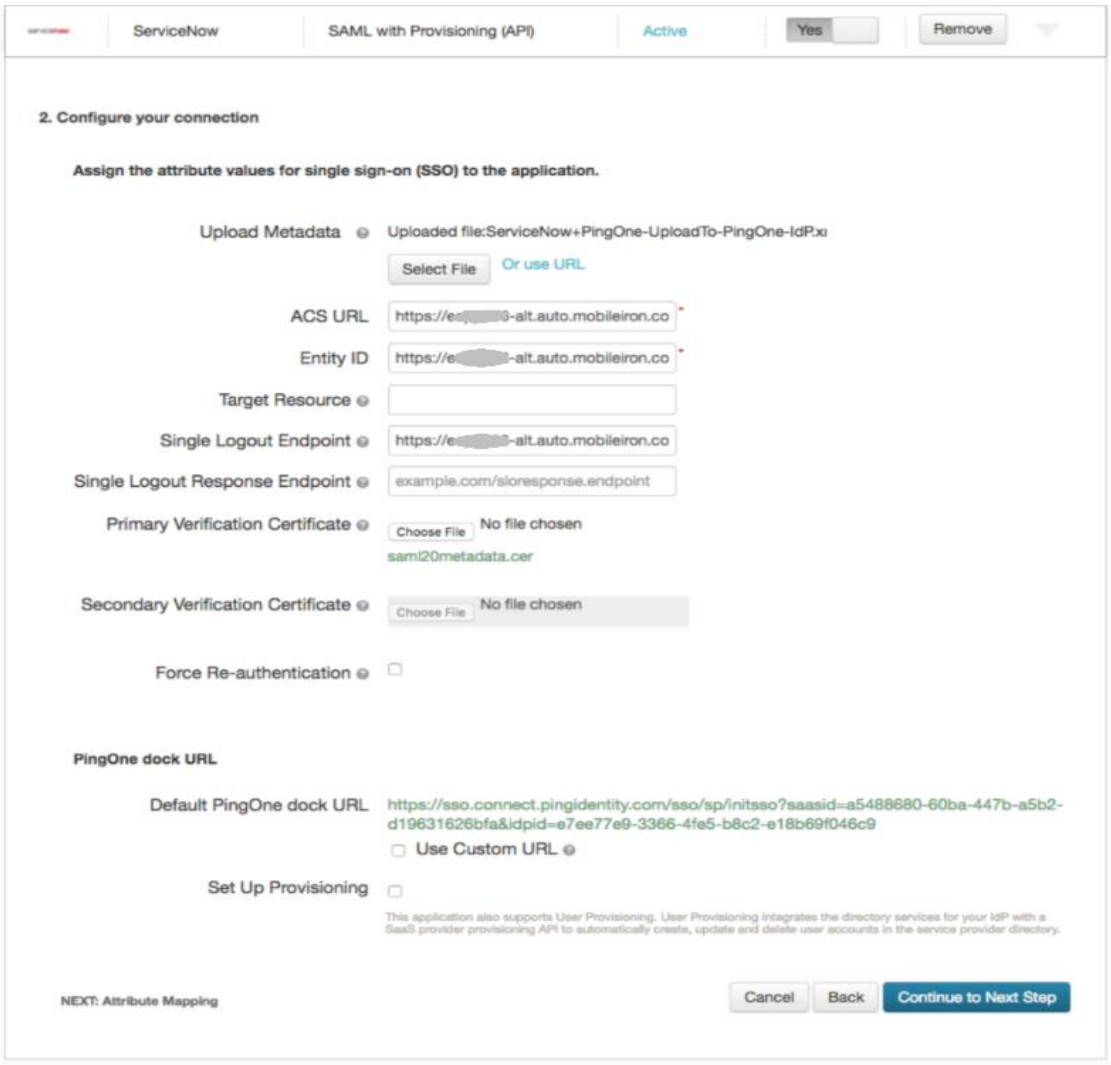


3. Click **Test Connection** and enter the **username** and **password**. Click **Sign On**.
   The test connection must be successful.
   The Activate button is available after the connection is tested.
4. Click **Activate** to activate the rule.
5. Select **Auto Redirect IdP** to set the redirect option.

Configure the PingOne environment

You must configure PingOne with Access for the setup to complete.

1. Login to PingOne with admin credentials.
2. Navigate to **Applications** > **ServiceNow** > **Edit**. Click **Continue to Next Step**.
3. Upload the Access metadata file that you downloaded at **Step 10** of Configuring ServiceNow and PingOne with MobileIron Access**.** The following details populate when you upload the metadata file.



4. Click **Continue to Next Step**.
5. Click **Save** and **Publish**.
6. Click **Finish**.

Register Sentry to Access

You must register Sentry to Access to fetch the latest configuration from Access.

Prerequisite

Verify that you have registered Sentry earlier using the below command. If so, then do not perform this step.
show accs registration

Procedure

1. Run **clish** Sentry. In the configuration mode, execute the following command for registration.
   (config)#accs registration https://<FQDN of Access server><Admin Username of Access Server>
2. Enter the **Tenant password** and complete the registration.
3. In **Access**, click the **Sentry** tab.
4. Select the appropriate Sentry instance, then click **Action** > **Assign**.
5. Click **OK**.
6. **Clish** Sentry and execute the following command in configuration mode to fetch the latest configuration from Access immediately:

   (config)# accs config-fetch update

   Note: All the published configuration changes are fetched by Sentry assigned to the profile in fifteen minutes. However, if you want to see the changes immediately, then perform Step 6.

Task Result

Single sign-on service is now configured using SAML with ServiceNow and PingOne. This configuration lets you fetch the latest configuration from Access.

Verification

1. Log into ServiceNow domain with your instance. Redirection occurs through Access and PingOne login page displays.
2. Enter valid user credentials and register the mobile device with Core.
3. Verify that you are redirected to ServiceNow through Access.