RSA SecurID Access SAML Configuration for Panorama9

Last Modified: April 03, 2017

Panorama9 is a cloud-based service within enterprise Network management. The company sells a hosted Dashboard monitoring everything on the network ensuring that servers, PC, peripherals and external Internet related services are all running. Furthermore, Panorama9 offers a set of reports on inventory on both hardware, software and users.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Panorama9.
- Obtain SP metadata details from the Service Provider.
- Obtain IdP metadata from IDR portal.

The instructions in this guide use the following SP Login URL, ACS URL and Issuer ID (entity ID) values:

SP Login URL	*https://dashboard.panorama9.com/login*
ACS URL	*https://dashboard.panorama9.com/saml/consume/14121*
Service Provider Issuer ID	https://www.panorama9.com/saml20/14121

Procedure

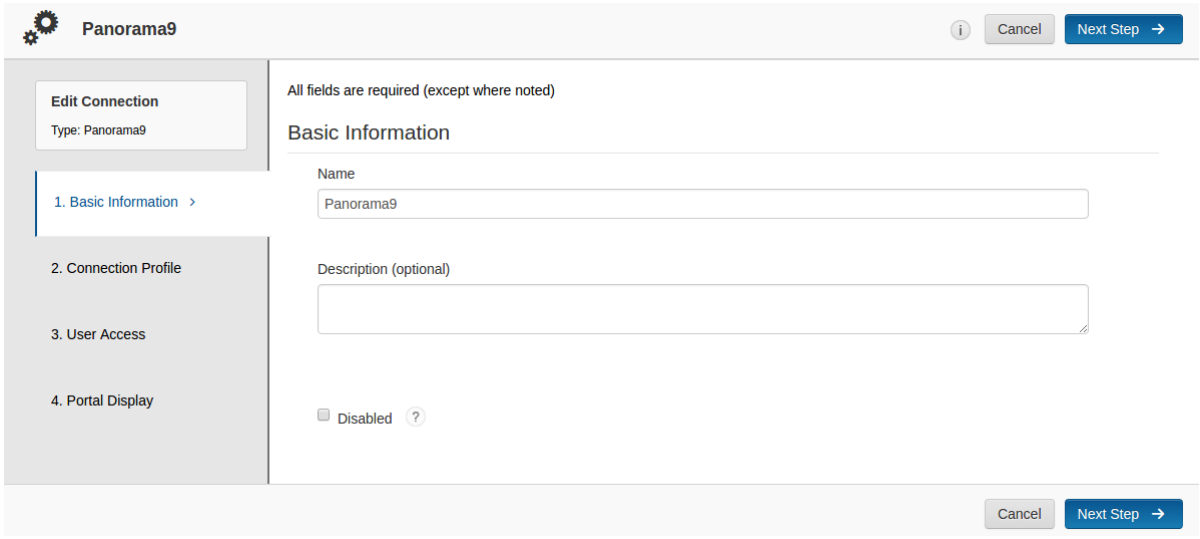
1. Add the Application in RSA SecurID Access
2. Configure Panorama9 to Use RSA SecurID Access as an Identity Provider

Add the Application in RSA SecurID Access

Procedure

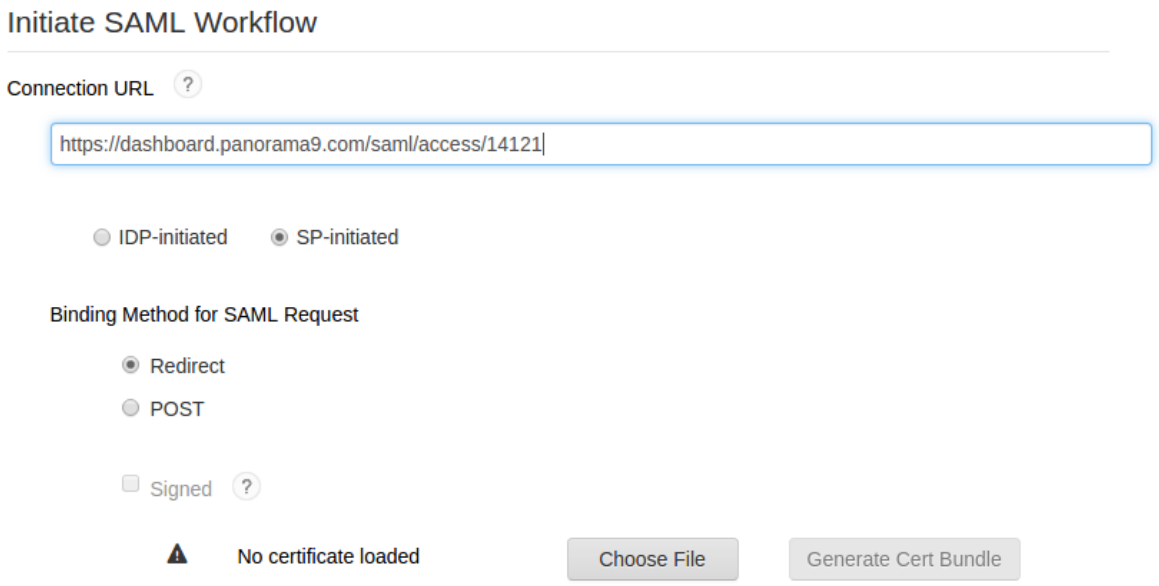
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** Panorama9.

3. On the Basic Information page, specify the application name and click **Next Step**.

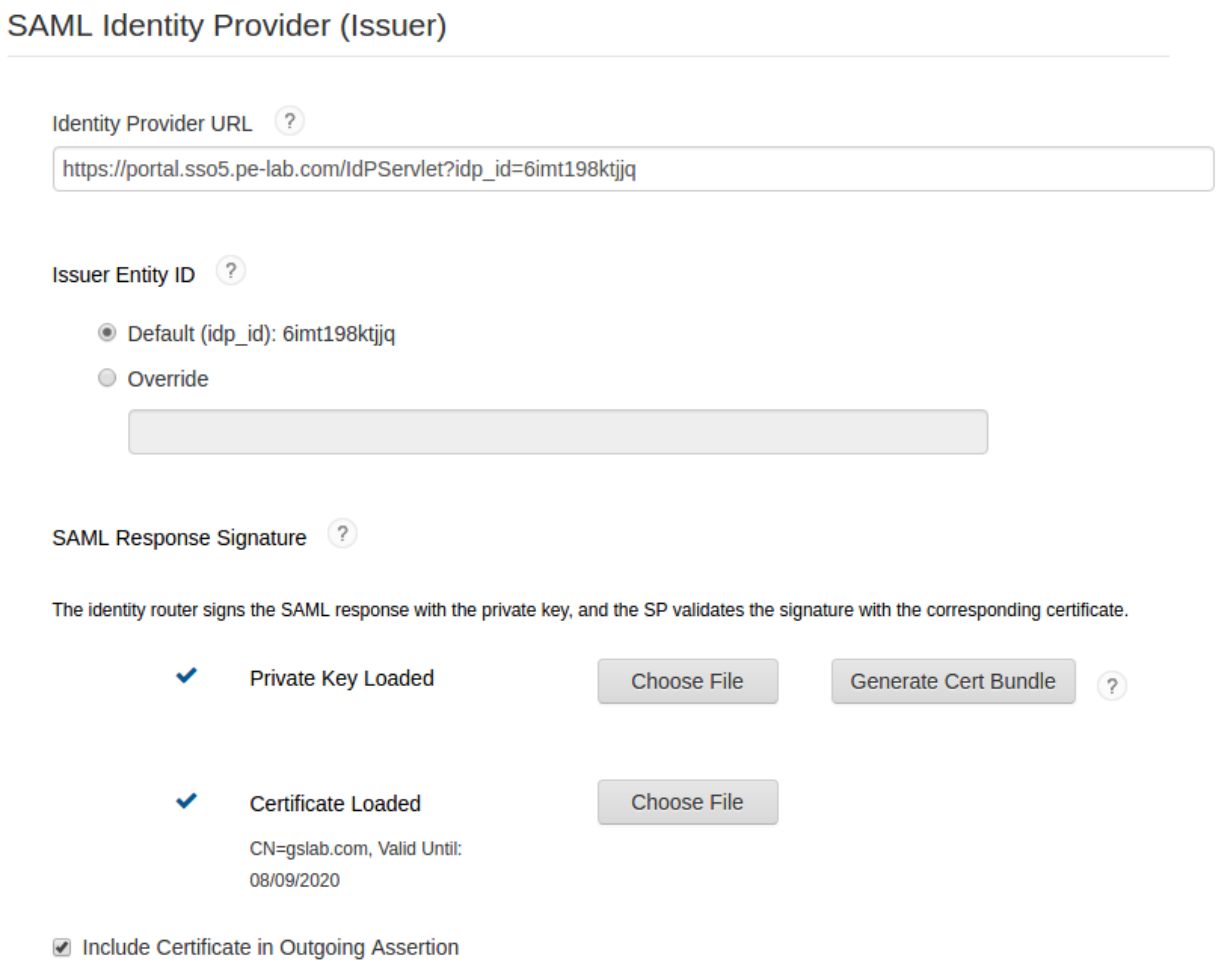


4. Navigate to **Initiate SAML Workflow** section.
   a. In the **Connection URL** field, Enter SP URL value received from service provider. For ex. https://dashboard.panorama9.com/saml/access/<UNIQUE_ACCOUNT_ID>
   b. Choose **SP–initiated**.
   c. Choose **Redirect** binding option for **Binding Method for SAML Request**.
   d. Keep rest of the option to their defaults.

Note: Panorama9 only supports SP-Init SSO scenario.

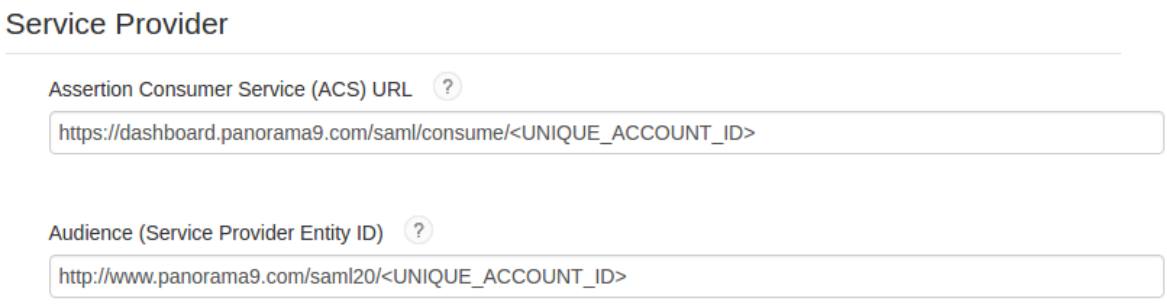


5. Scroll down to **SAML Identity Provider (Issuer)** section.

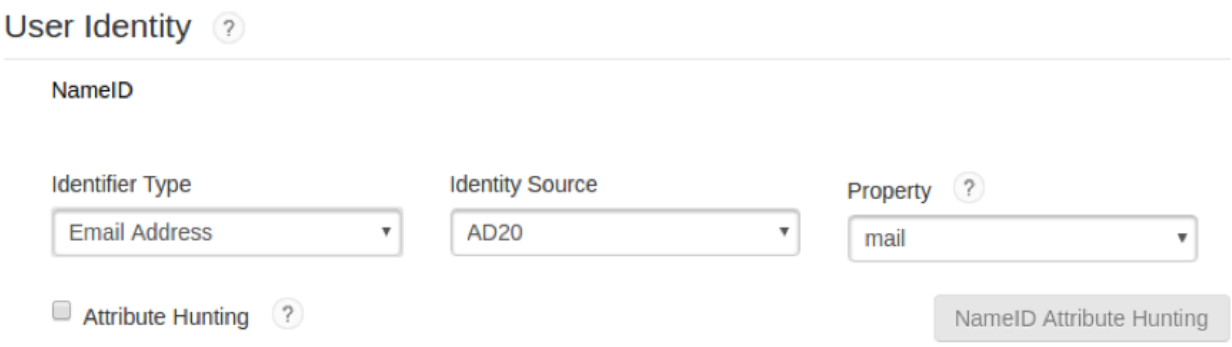


   a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
   b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
   c. Select **Choose File** and upload the private key.
   d. Select **Choose File** to import the public signing certificate.
   e. Select the checkbox for **Include Certificate in Outgoing Assertion**.

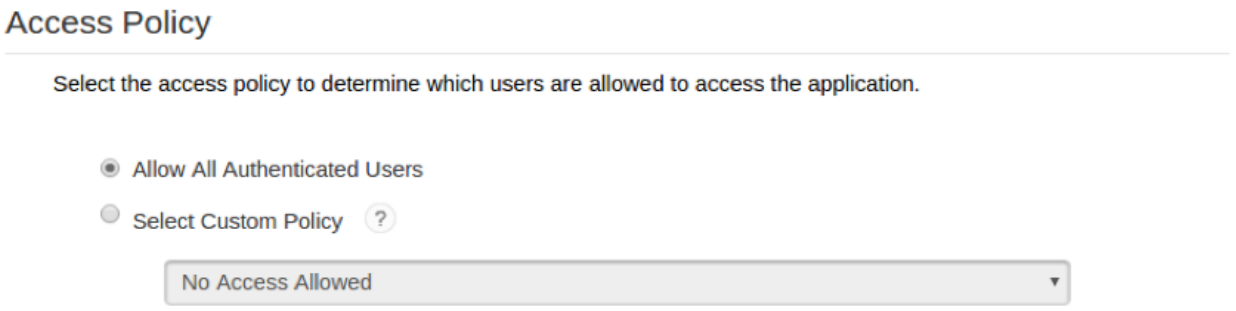
6. Scroll down to the **Service Provider** section.



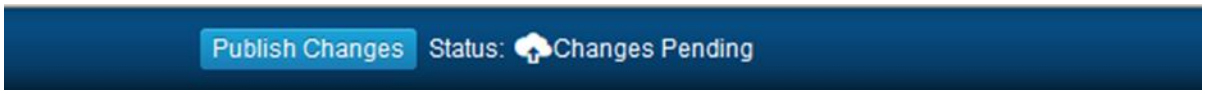
   a. In the **Assertion Consumer Service (ACS) URL** field, replace <UNIQUE_ACCOUNT_ID> value with your organization account value.
   b. In the **Audience (Service Provider Entity ID)** field, replace <UNIQUE_ACCOUNT_ID> value with your organization account value.
7. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.



8. Click **Next Step**.
9. On the **User Access** page, select **Allow All Authenticated Users** user policy from the available options.

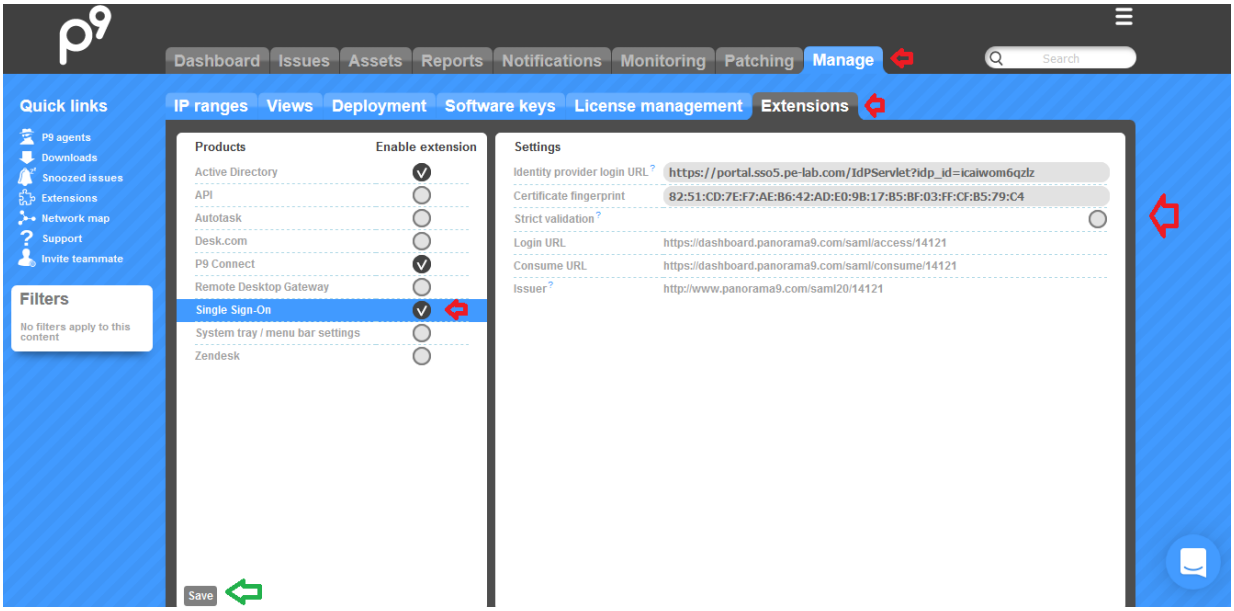


10. Click **Next Step**.
11. On the **Portal Display** page, select **Display in Portal**.
12. Click **Save and Finish**.
13. Click **Publish Changes**. Your application is now enabled for SSO.



Procedure

1. Login to your Panorama9 application web account. (https://dashboard.panorama9.com/login)
2. Following UI will be displayed. Go to *Manage -> Extensions -> Single Sign-On.* Click on the checkbox that appears in front to enable SSO.



   a. **Identity provider login URL** : Enter the Identity Provider URL found on page 3 step 5. It is of following format : https://<Your_Portal_URL>?idp_id=<Unique_IdP_ID>
   b. **Certificate fingerprint** : Provide fingerprint of the RSA SecurID Access IdP public certificate here.
   c. Keep the **Strict validation** option un-checked.
   d. Make note of the values – **Login URL**, **Consume URL**, **Issuer** as these will be handy during SAML configuration at identity provider end.
   e. Once sure of changes, click on the **Save** button at the left-bottom of the page.

3. Your Panorama9 account is now enabled for SAML authentication.

RJ

