RSA SecurID Access SAML Configuration for Impulse SafeConnect

Last Modified: June 26th, 2017

SafeConnect is an essential network security solution for protecting your critical data and intellectual property, combining the real-time visibility, security and orchestration required to address regulatory compliance and security policy automation. SafeConnect automates your security policies, from assessing compliance with security policies to determining if a specific application is running on a device while it is on the network. SafeConnect is delivered as a Cloud-Managed Service that relieves the organization of costly technical support related to on-going proactive monitoring, maintenance, and upgrades.

Before You Begin

- Acquire an administrator account to RSA SecurID Access.
- Obtain the ACS URL from Impulse.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

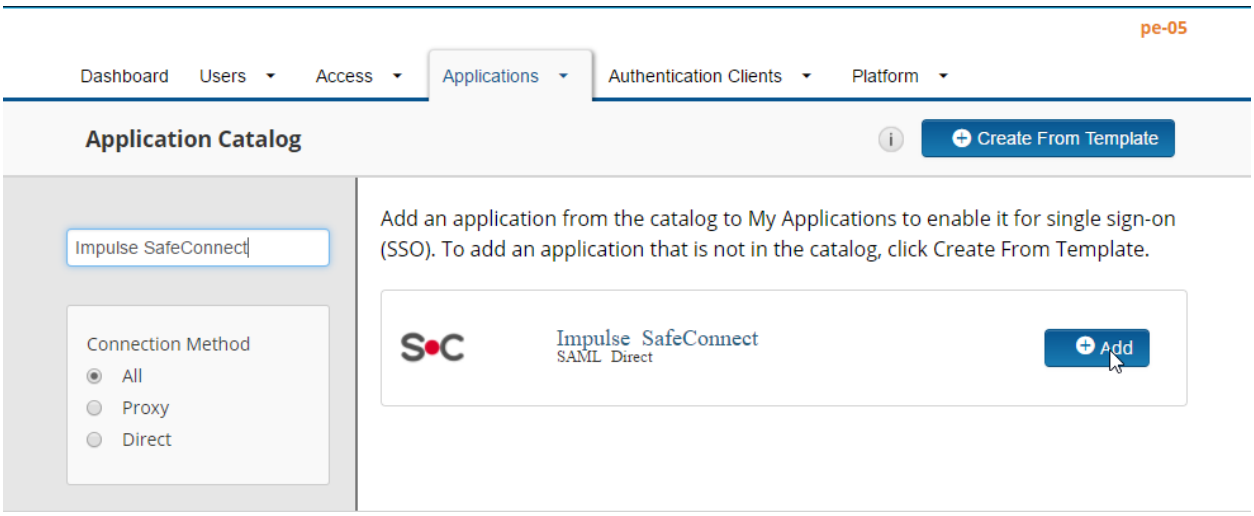
Procedure

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

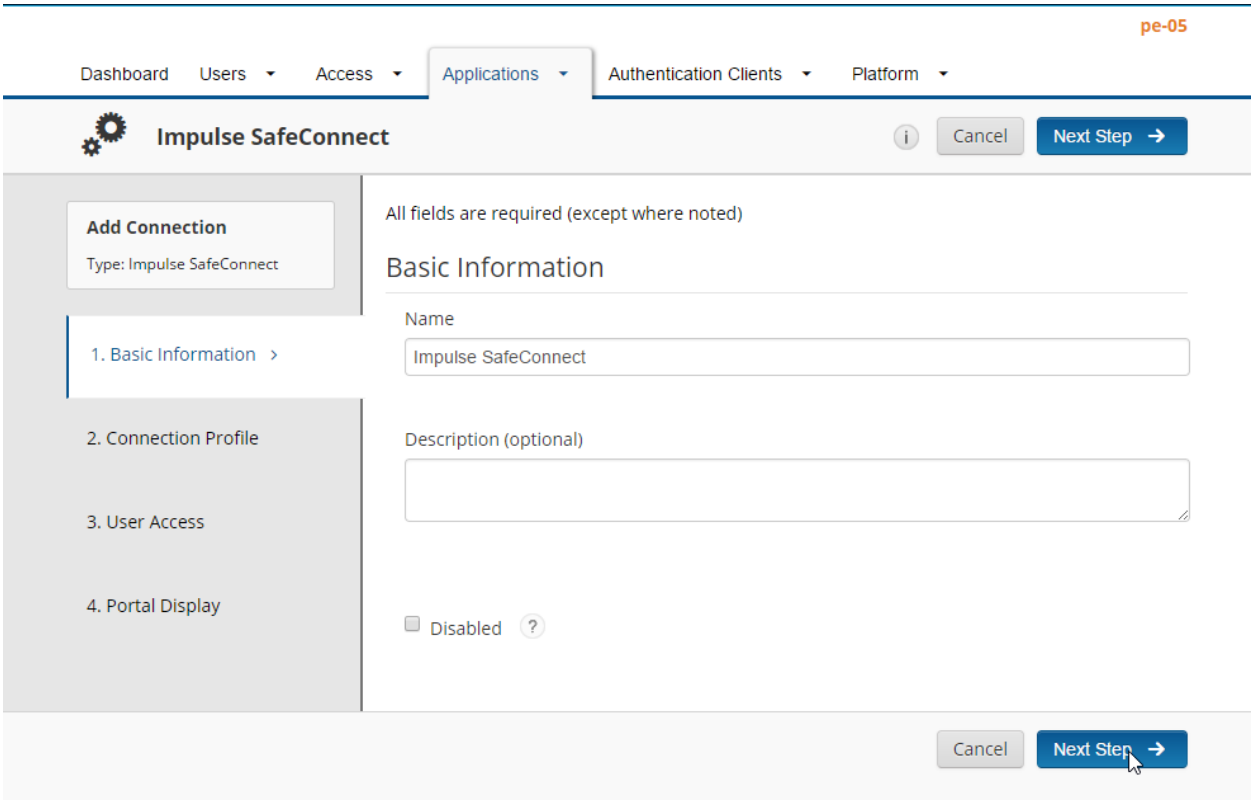
Add the Application in RSA SecurID Access

Procedure

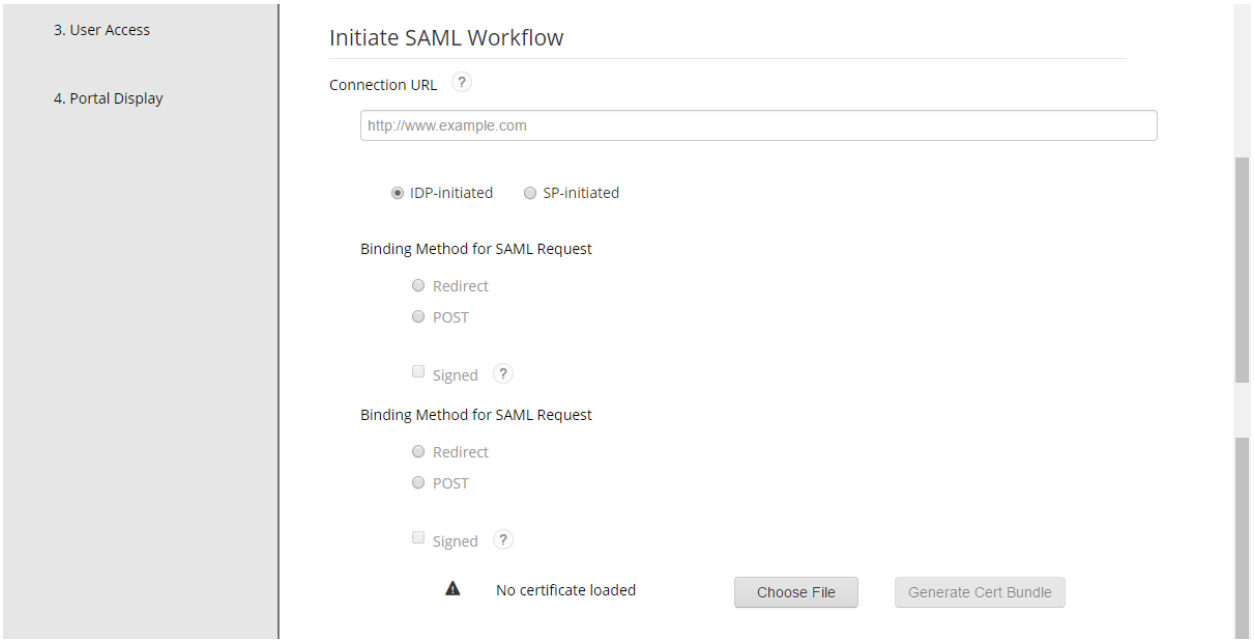
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, locate Impulse SafeConnect and click **+Add**.



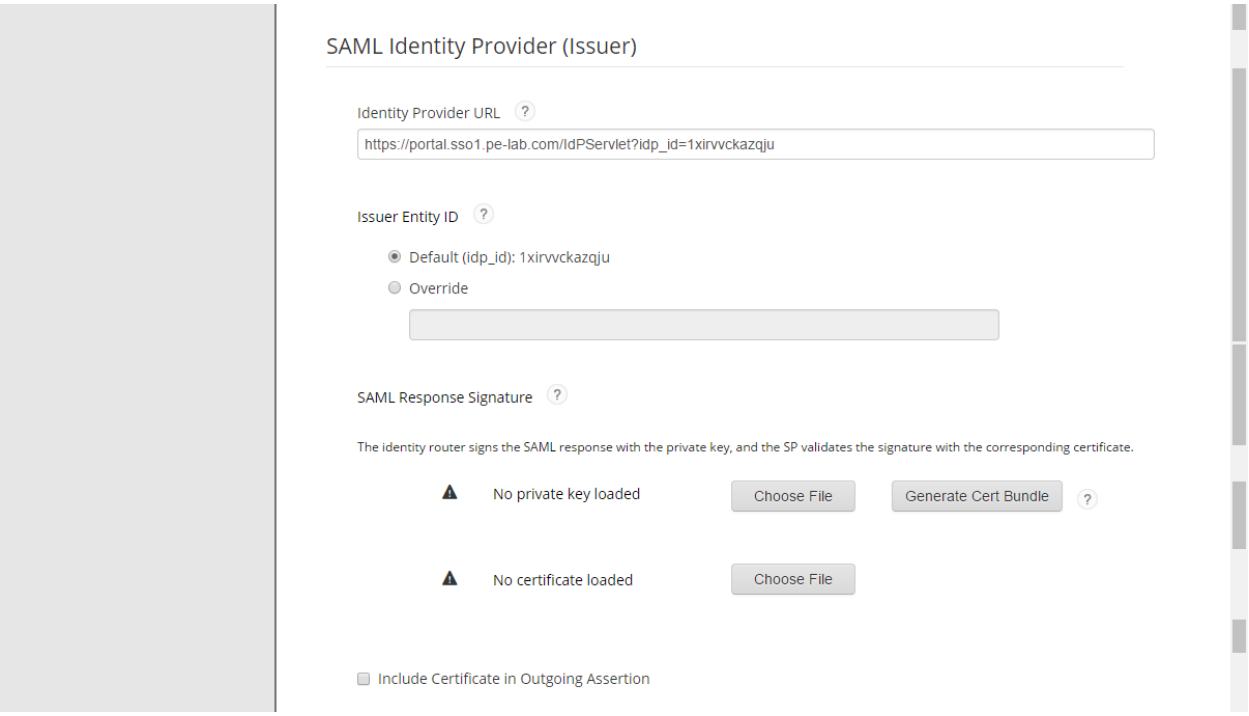
3. On the Basic Information page, specify the application name and click **Next Step**.



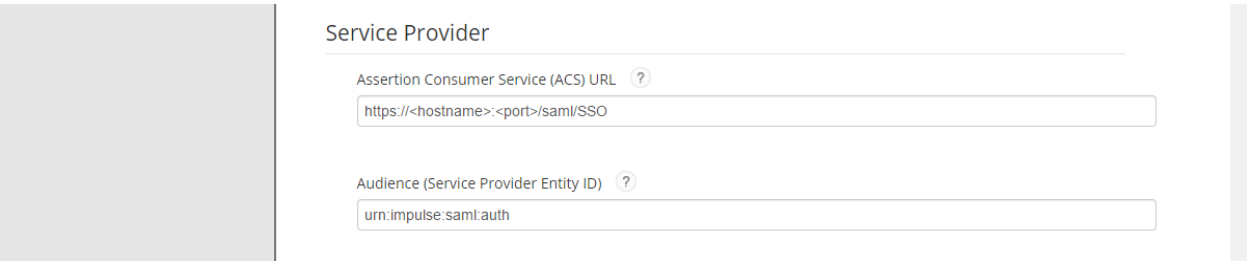
4. Scroll down to the **Initiate SAML Workflow** section, select **IDP-Initiated** and then scroll down to the **SAML Identity Provider (Issuer)** section.



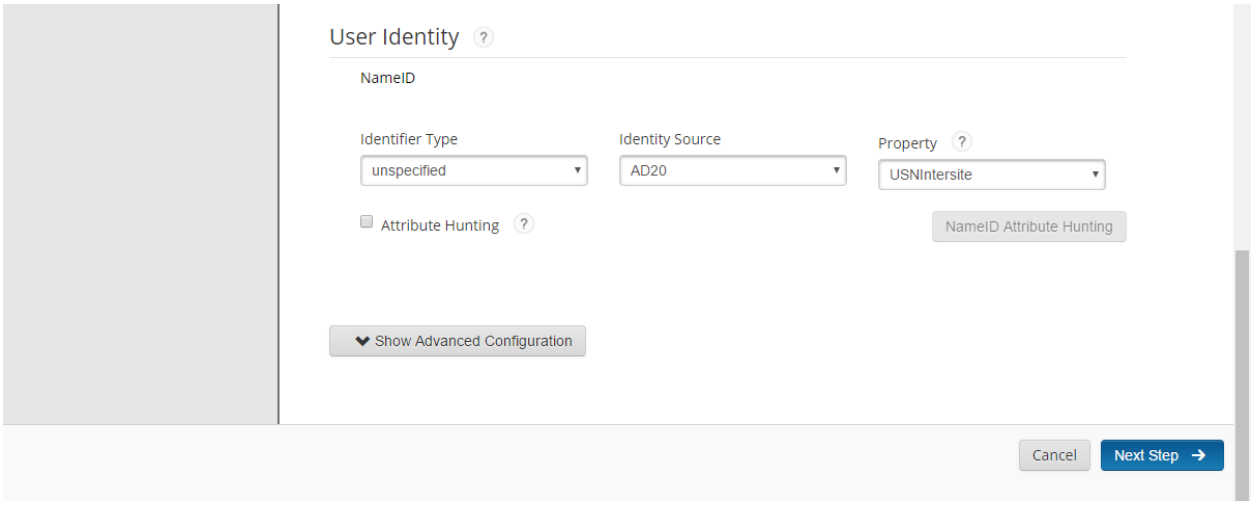
5. Set the **Identity Provider URL**, **Issuer Entity ID**, **SAML Response Signature** private key and certificate and scroll down to the **Service Provider** section. The default Identity Provider URL and Issuer Entity ID will work fine if you do not wish to make changes.



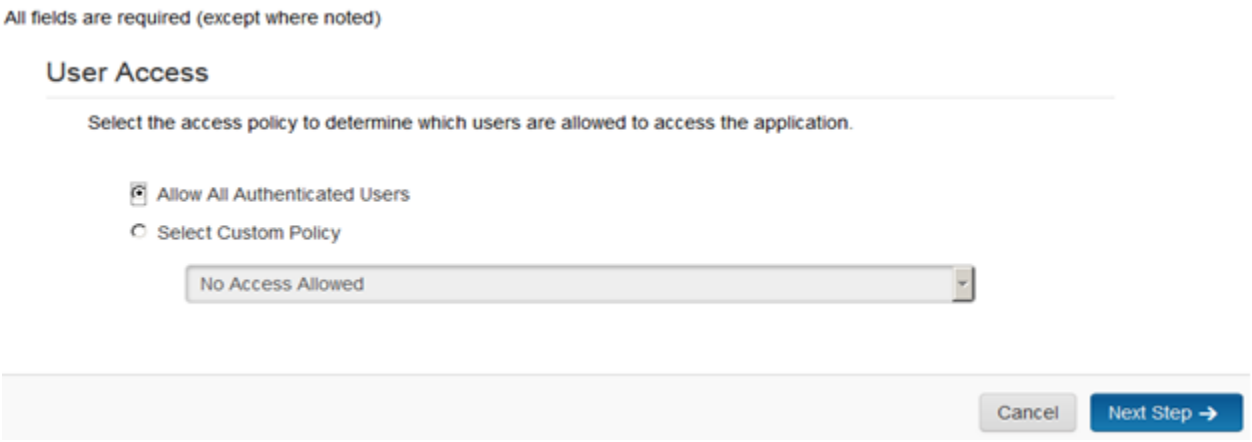
6. Enter the **Assertion Consumer Service (ACS) URL** and **Audience (Service Provider Entity ID)** and scroll down to the **User Identity** section.



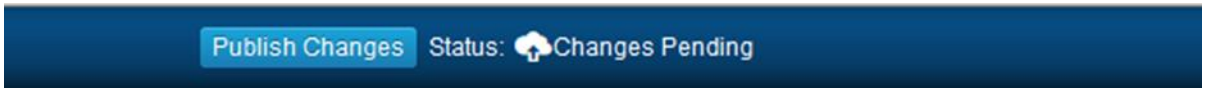
7. Select **unspecified** from the **Identifier Type** drop-down menu, the directory attribute which contains your **SafeConnect** username from the **Property** drop-down menu and click **Next Step**.



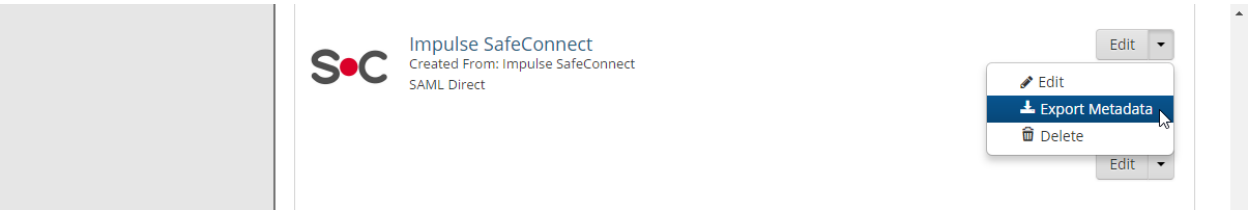
8. On the **User Access** page, select the desired user policy from the drop down list.



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



13. Navigate to **Applications > My Applications**.
14. Locate the application in the list and from the **Edit** pulldown select **Export Metadata**.



Next Steps

Configure Impulse SafeConnect to Use RSA SecurID Access as an Identity Provider

Configure Impulse SafeConnect to Use RSA SecurID Access as an Identity Provider

Email the following information to Impulse Support (support@impulse.com):

- IdP EntityId
- Metadata XML file
- Name and format of the attribute used for the username (format is usually: "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified")

PEW