

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.

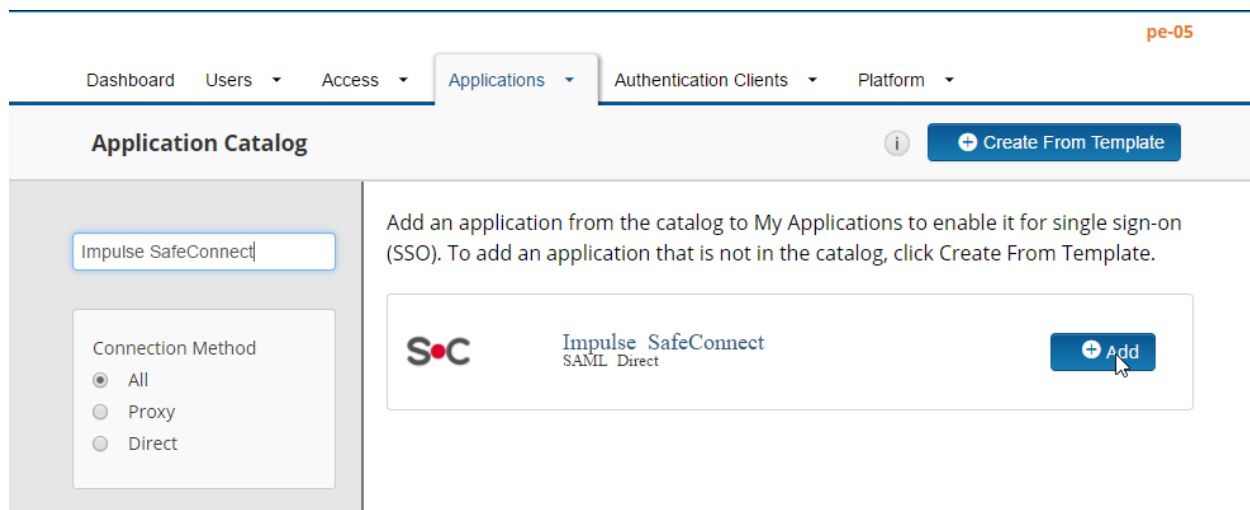
Procedure

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**.

The screenshot shows the 'Basic Information' configuration page in the Impulse SafeConnect interface. The breadcrumb navigation includes 'Dashboard', 'Users', 'Access', 'Applications', 'Authentication Clients', and 'Platform'. The page title is 'Impulse SafeConnect'. A sidebar on the left lists the steps: '1. Basic Information', '2. Connection Profile', '3. User Access', and '4. Portal Display'. The main content area contains the following fields and options:

- A note: 'All fields are required (except where noted)'
- Section: 'Basic Information'
- Field: 'Name' with the value 'Impulse SafeConnect'
- Field: 'Description (optional)' (empty)
- Checkbox: 'Disabled' (unchecked)

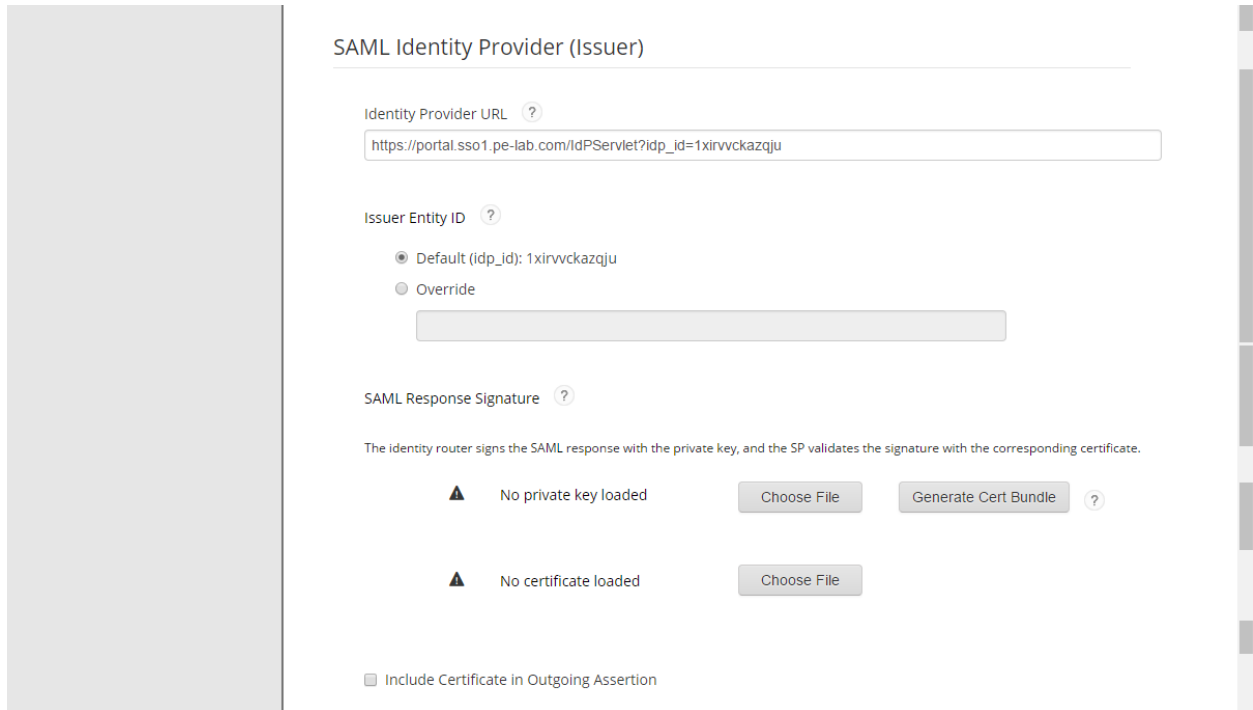
At the bottom right, there are 'Cancel' and 'Next Step' buttons. A mouse cursor is pointing at the 'Next Step' button.

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

The screenshot shows the 'Initiate SAML Workflow' configuration page. The sidebar on the left shows steps '3. User Access' and '4. Portal Display'. The main content area includes:

- Section: 'Initiate SAML Workflow'
- Field: 'Connection URL' with the value 'http://www.example.com'
- Radio buttons: 'IDP-initiated' (selected) and 'SP-initiated'
- Section: 'Binding Method for SAML Request' with radio buttons for 'Redirect', 'POST', and a checked 'Signed' checkbox.
- Section: 'Binding Method for SAML Request' with radio buttons for 'Redirect', 'POST', and a checked 'Signed' checkbox.
- Status: 'No certificate loaded' with a warning triangle icon.
- Buttons: 'Choose File' and 'Generate Cert Bundle'.

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.



SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?
 Default (idp_id): 1xirvckazqju
 Override

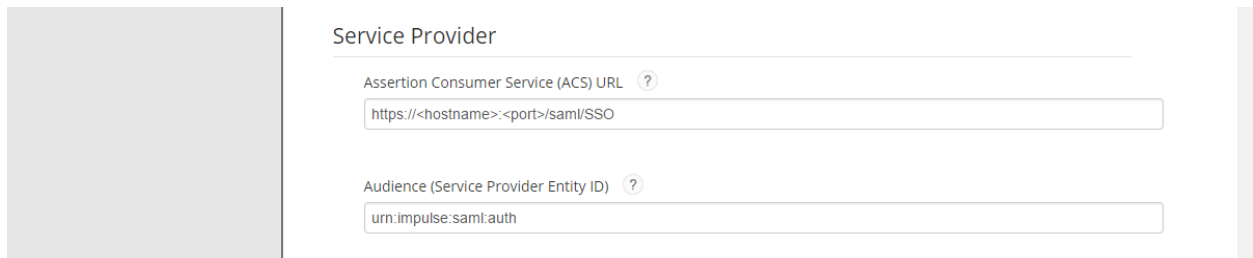
SAML Response Signature ?
The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

▲ No private key loaded ?

▲ No certificate loaded

Include Certificate in Outgoing Assertion

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



Service Provider

Assertion Consumer Service (ACS) URL ?

Audience (Service Provider Entity ID) ?

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**.

User Identity ?

NameID

Identifier Type Identity Source Property ?

unspecified AD20 USNinterste

Attribute Hunting ? NameID Attribute Hunting

Show Advanced Configuration

Cancel Next Step →

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

All fields are required (except where noted)

User Access

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy

No Access Allowed

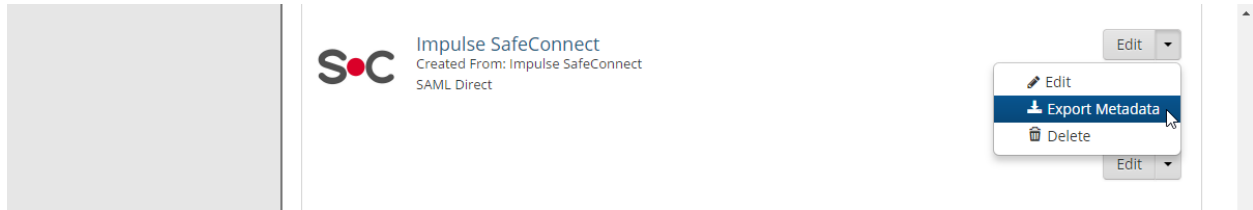
Cancel Next Step →

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")