

Last Modified: July, 25, 2016

Shibboleth is an open-source project that provides Single Sign-On capabilities and allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner.

In this guide Shibboleth is configured as the service provider and is listed in the RSA catalog as ShibbolethSP.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Application which is to be protected by Shibboleth.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

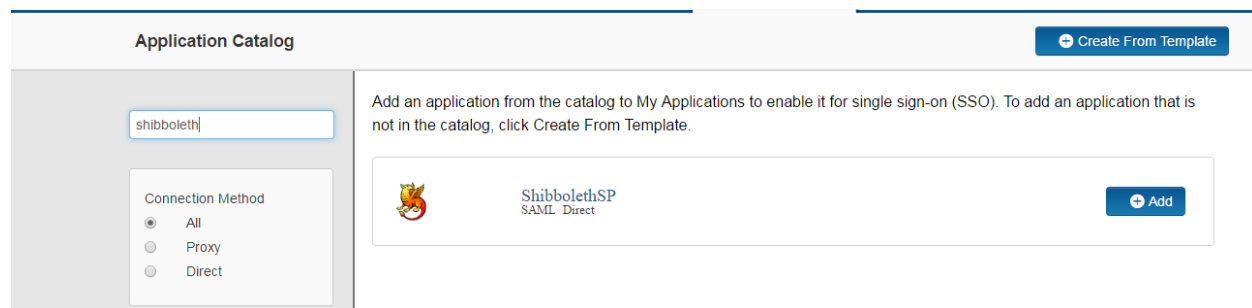
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure ShibbolethSP 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** for ShibbolethSP.



3. On the Basic Information page, specify the application name and click **Next Step**.
4. On the Connection Profile page, specify Connection URL as per your application.
For ex: for Default index.html application, specify Connection URL as **https://hostname:port /index.html**.
5. Select workflow **SP-initiated**.

Initiate SAML Workflow

Connection URL 

IDP-initiated SP-initiated

6. Select binding method **POST**.

Binding Method for SAML Request

Redirect

POST

Signed 

 No certificate loaded

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

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp_id): o7lxbqeani2w

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.

Private Key Loaded

?

Certificate Loaded


CN=gslab, Valid Until:
07/25/2020

Include Certificate in Outgoing Assertion

- Take note of the **Issuer Entity ID**.
- Select **Choose File** to import a private key to sign the SAML assertion.
- Select **Choose File** to import the public certificate file.
- Check the **Include Certificate in Outgoing Assertion** check box.

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

Service Provider

Assertion Consumer Service (ACS) URL 

https://<yourhostname>/Shibboleth.sso/SAML2/POST

Audience (Service Provider Entity ID) 

https://<yourhostname>:444/shibboleth

- a. In the **Assertion Consumer Service (ACS) URL** field, enter the URL you obtained from the application administrator.

For Shibboleth 2.0, ACS URL will be

https://<yourhostname>/Shibboleth.sso/SAML2/POST

- b. In the **Audience (Service Provider Entity ID)** field, enter the Entity ID to match the configured value from the Service Provider i.e value from Shibboleth2.xml.

```
<ApplicationDefaults entityID="https://yourhostname:444/shibboleth"
REMOTE_USER="eppn persistent-id targeted-id">
```

9. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be in presented in email format and the user account will be validated again the User Store selected.

User Identity

Name ID

Identifier Type


Email Address

User Store

PE_AD

Property

USNIntersite

 Show Advanced Configuration

10. Click **Show Advanced Configuration**.

11. Select **Assertion within response** below

Sign Outgoing Assertion in the Uncommon Formatting SAML Response Options section.

Sign Outgoing Assertion

Entire SAML response Assertion within response

Signature Algorithm

rsa-sha1

Digest Algorithm

sha1

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

All fields are required (except where noted)

Access Policy

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

Allow All Authenticated Users

Select Custom Policy ?

No Access Allowed

13. Click **Next Step**.

14. On the **Portal Display** page, select **Display in Portal**.

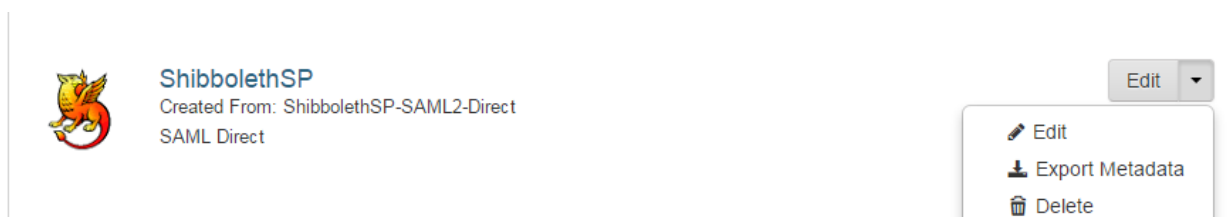
15. Click **Save and Finish**.

16. Click **Publish Changes**. Your application is now enabled for SSO.



17. Navigate to **Applications > My Applications**.

18. Locate ShibbolethSP in the list and from the **Edit** pulldown, select **Export Metadata**.



Next Steps

[Configure ShibbolethSP to Use RSA SecurID Access as an Identity Provider](#)

Configure ShibbolethSP to Use RSA SecurID Access as an Identity Provider

Follow below steps to configure ShibbolethSP as service provider.

Create Identity Provider

1. Open Shibboleth2.xml file from shibboleth installation.
2. Change the entity ID with the Entity ID obtained from IDP metadata which you downloaded in step 18 page 4.

```
<SSO entityID="1q37rpeqemvvd" >  
  SAML2 SAML1  
</SSO>
```

3. Placed the IDP metadata file at the same level of Shibboleth2.xml in Shibboleth, make the changes to the file name in Shibboleth2.xml file

```
<MetadataProvider type="XML" file="ShibbolethSP-idp-metadata.xml"/>
```

4. Save the file and restart Shibboleth and Web Server service.