RSA SecurID Access SAML Configuration for Cisco vBrick

Last Modified: June 22, 2017

Cisco vBrick Rev enables companies to deliver video across a variety of platforms and devices, making enterprise video easier and more manageable with the widest range of deployment options. It helps transform business processes with a secure enterprise video platform supported across both mobile and desktop devices. vBrick does not support auto-provisioning of the user feature.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Cisco vBrick.
- 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://data3.rev.vbrick.com/#/login*
ACS URL	*https://data3.rev.vbrick.com:443/sso/consume*
Service Provider Issuer ID	*https://data3.rev.vbrick.com:443/*

Procedure

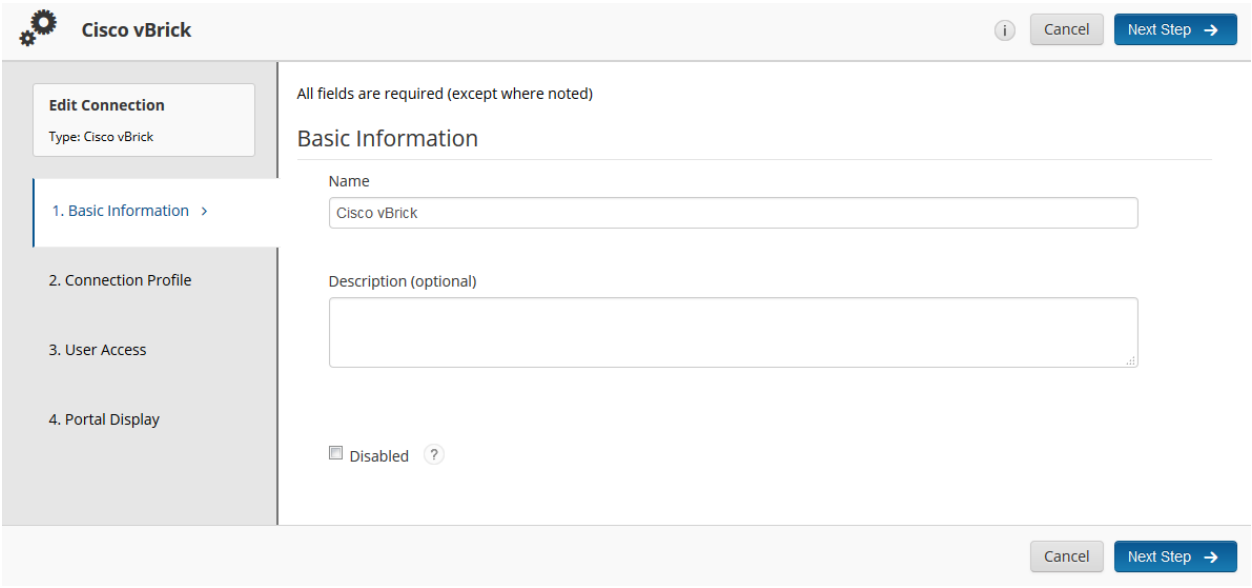
1. Add the Application in RSA SecurID Access
2. Configure Cisco vBrick to Use RSA SecurID Access as an Identity Provider

Add the Application in RSA SecurID Access

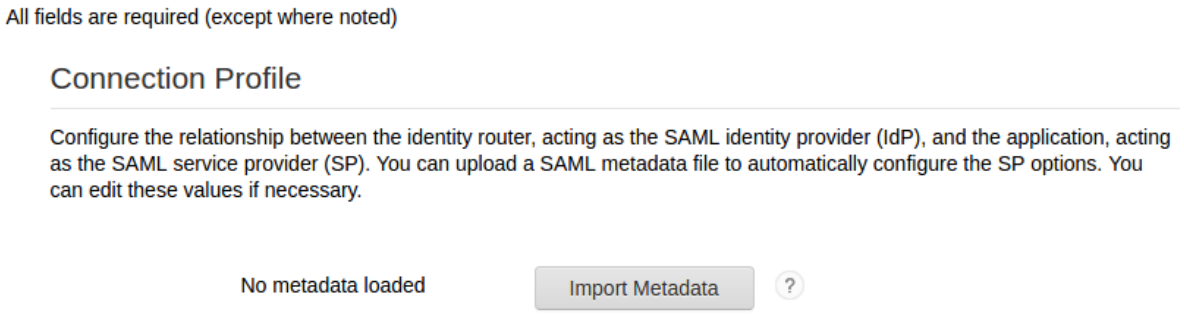
Procedure

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

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

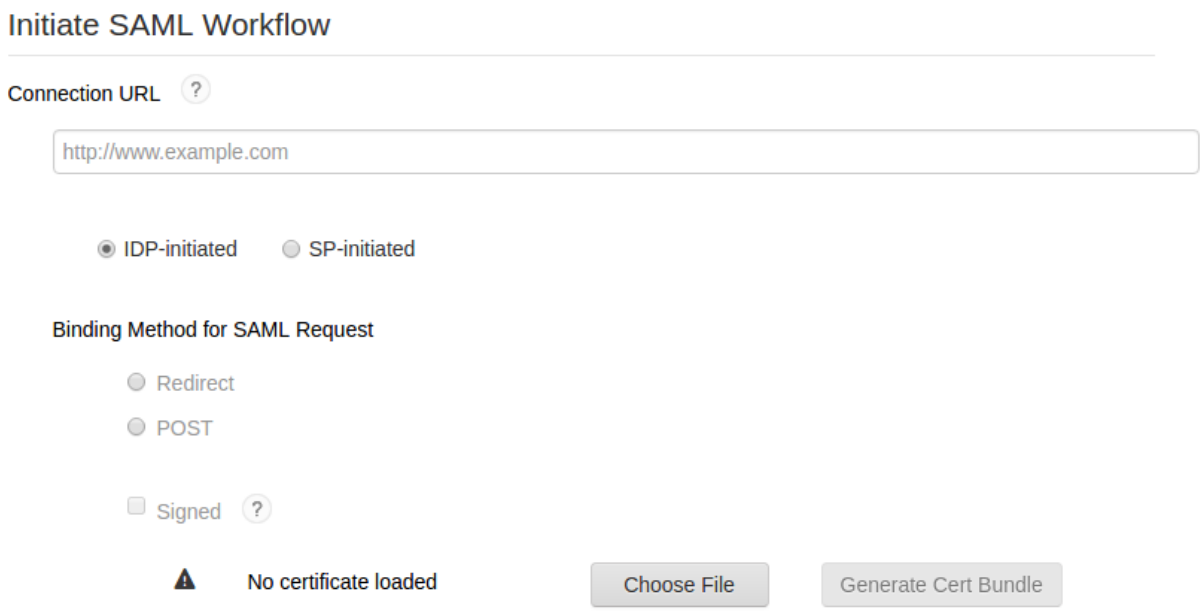


4. Navigate to **Connection Profile** section. Click on **Import Metadata** button to configure SAML settings by providing path to the service provider's metadata file you downloaded. Refer to page 8 step 4g.

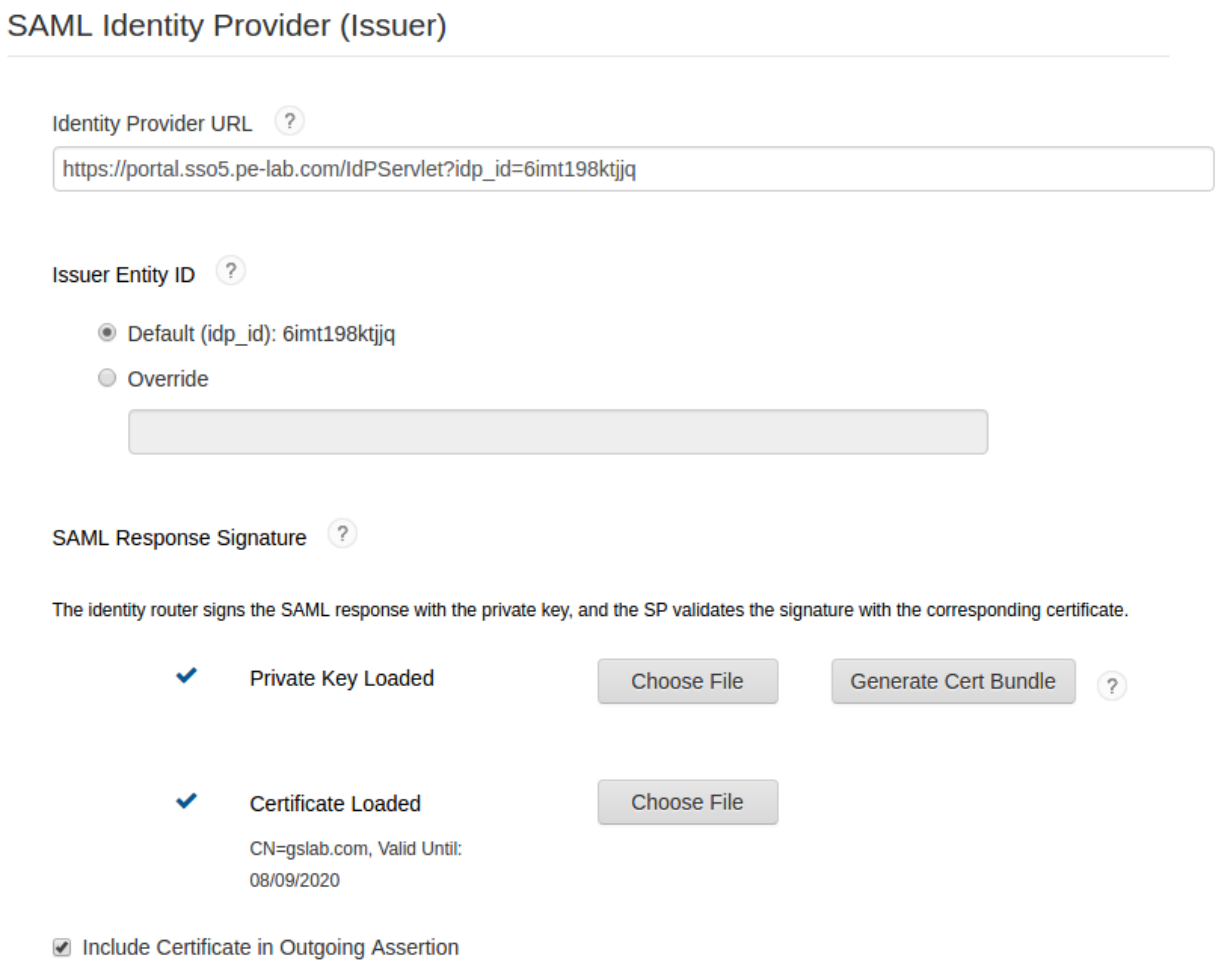


5. Navigate to **Initiate SAML Workflow** section.
   a. In the **Connection URL** field, verify the field is blank as the value is not required.
   b. Verify that **IDP-initiated** is selected.

Note: Cisco vBrick application only supports IdP-initiated SSO scenario as of now.



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

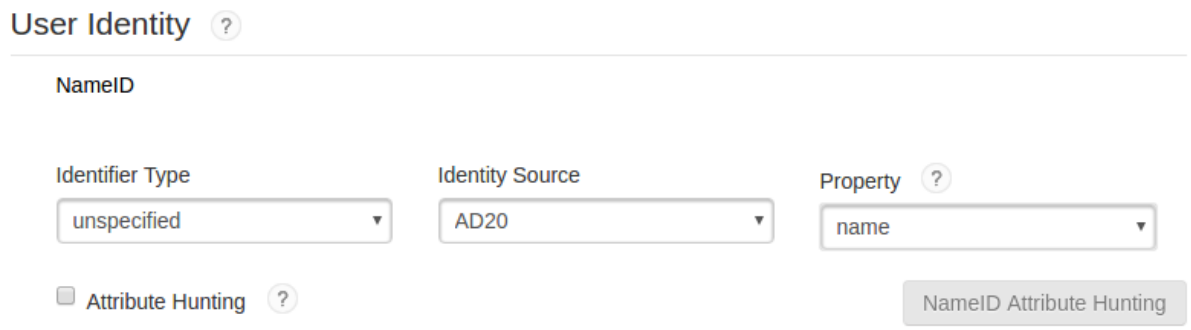


a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File** 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**.

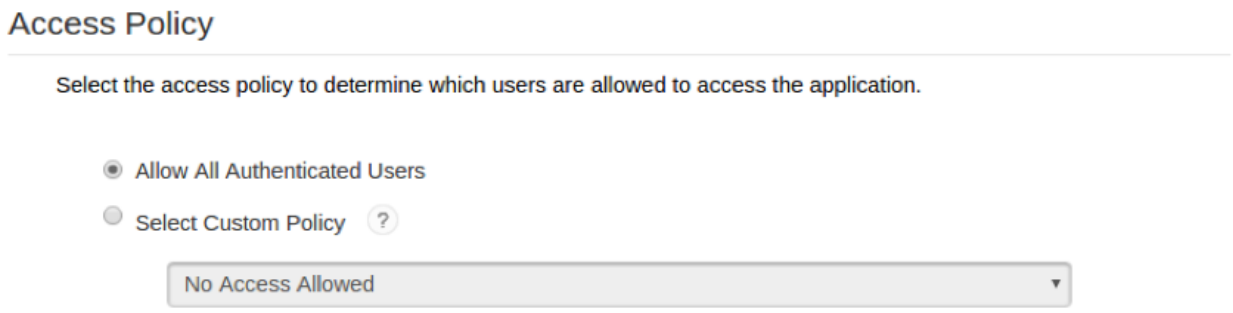
7. Scroll down to the **Service Provider** section.

   a. In the **Assertion Consumer Service (ACS) URL** field, replace <ACS_URL> value with your organization unique ACS URL value.
   b. In the **Audience (Service Provider Issuer ID)** field, replace <SP_ENTITY_ID> value with your organization unique SP ENTITY ID value.

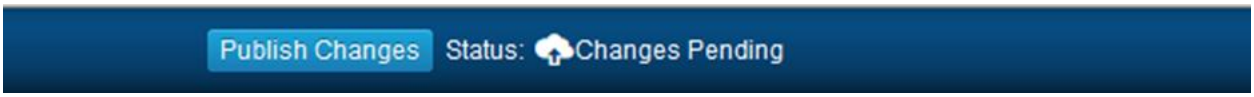
8. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in username format and the user account will be validated against the User Store selected.



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



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



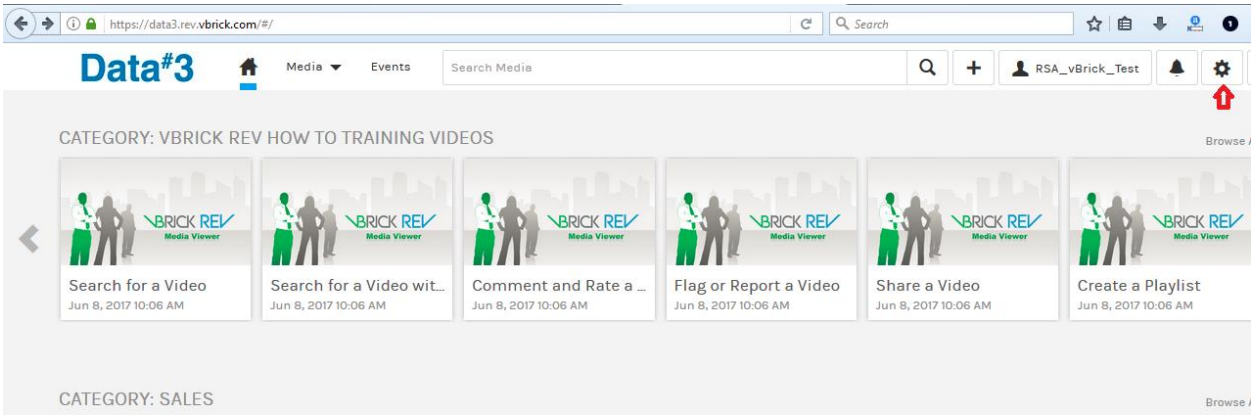
15. Navigate to **Applications > My Applications**.
16. Locate Cisco vBrick in the list and from the **Edit** option, select **Export Metadata**.

Configure Cisco vBrick to Use RSA SecurID Access as an Identity Provider

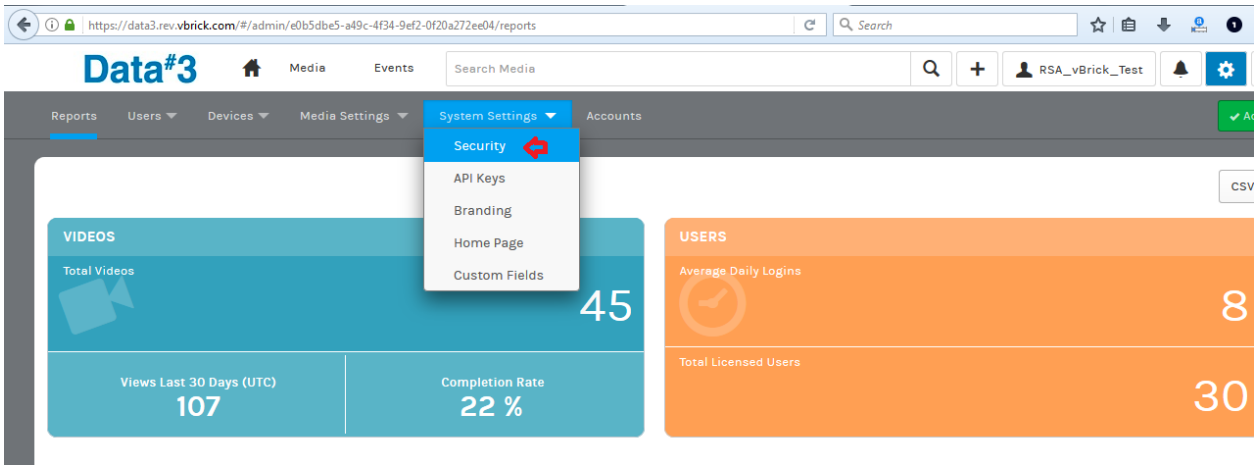
Procedure

1. Login to your Cisco vBrick application web account. (https://<DOMAIN>.rev.vbrick.com/#/login)

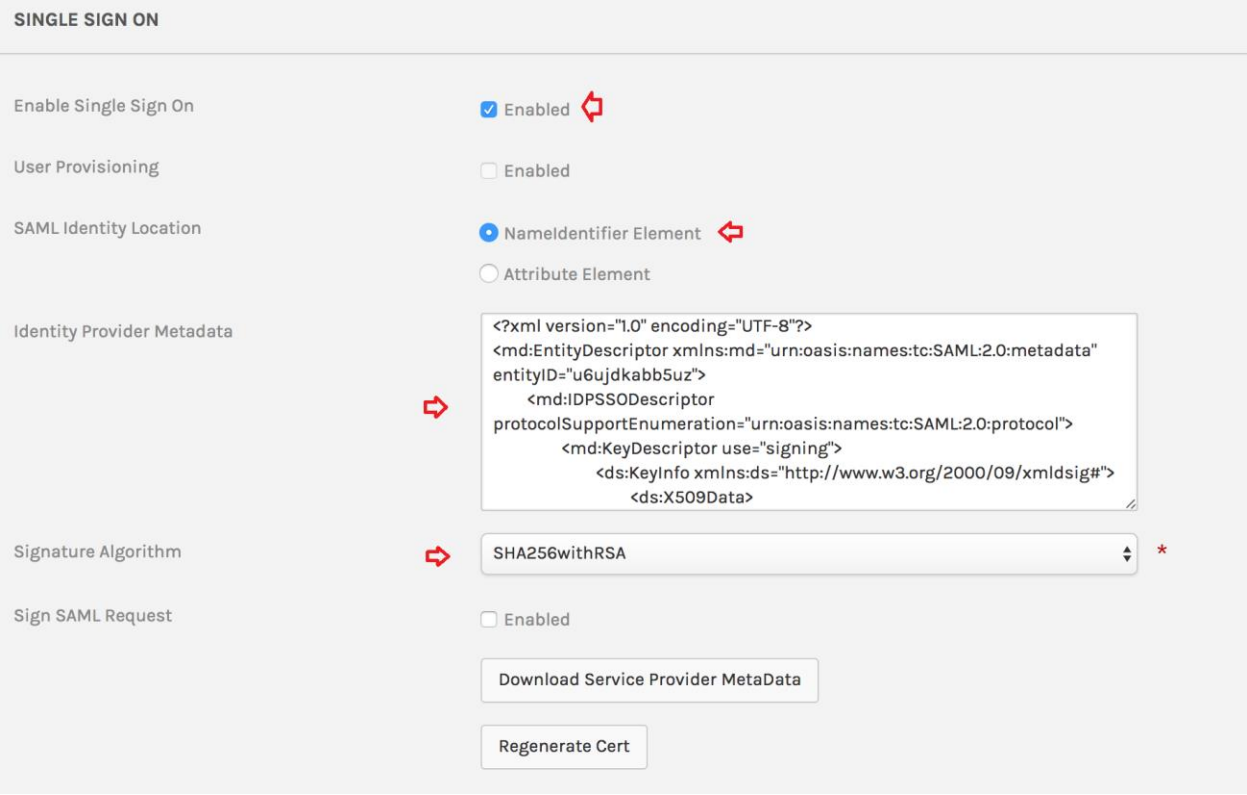
2. Following UI will be displayed. Go to *Settings (geared icon)* available at top-right corner of the page.



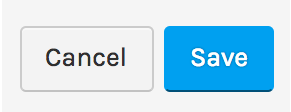
3. Following UI will be displayed. Navigate to *System Settings → Security.*



4. Navigate to *SINGLE SIGN ON* tab. Following UI will be displayed.



a. Click on **Enabled** checkbox in front of **Enable Single Sign On** option.
b. Keep the **User Provisioning** field to its default value.
c. Select **NameIdentifier Element** for **SAML Identity Location** field.
d. Under **Identity Provider Metadata** field, paste the contents of the metadata.xml file that you downloaded from RSA portal inside step – 15 on page – 5.
e. Select **SHA256with RSA** value from dropdowns for the **Signature Algorithm** field.
f. Keep the **Sign SAML Request** field to its default value.
g. **Download Service Provider MetaData** to get SP metadata details to configure IdP side settings. Download metadata file to the machine. This file can be directly imported to configure SAML settings at identity provider end in *step – 4* on *page – 2* above.
h. Once sure of settings, click on **Save** button which is available at bottom-right corner of the page to complete configuration changes.



5. Your Cisco vBrick account is now enabled for SAML SSO authentication.

RJ