

**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:

<b>SP Login URL</b>	<a href="https://data3.rev.vbrick.com/#/login">https://data3.rev.vbrick.com/#/login</a>
<b>ACS URL</b>	<a href="https://data3.rev.vbrick.com:443/sso/consume">https://data3.rev.vbrick.com:443/sso/consume</a>
<b>Service Provider Issuer ID</b>	<a href="https://data3.rev.vbrick.com:443/">https://data3.rev.vbrick.com:443/</a>

## 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.



Cisco vBrick  
SAML Direct



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

The screenshot shows the 'Edit Connection' page for a Cisco vBrick. The page title is 'Cisco vBrick' with a gear icon. In the top right corner, there are 'Cancel' and 'Next Step' buttons. A sidebar on the left contains a list of steps: '1. Basic Information' (selected), '2. Connection Profile', '3. User Access', and '4. Portal Display'. The main content area is titled 'Basic Information' and includes a note: 'All fields are required (except where noted)'. There are two input fields: 'Name' (containing 'Cisco vBrick') and 'Description (optional)'. At the bottom of the main area, there is a 'Disabled' checkbox with a help icon. At the bottom right of the page, there are 'Cancel' and 'Next Step' buttons.

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.

All fields are required (except where noted)

## Connection Profile

Configure the relationship between the identity router, acting as the SAML identity provider (IdP), and the application, acting as the SAML service provider (SP). You can upload a SAML metadata file to automatically configure the SP options. You can edit these values if necessary.


No metadata loaded

Import Metadata



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.

---

## Initiate SAML Workflow

---

Connection URL 


IDP-initiated     SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed 

 No certificate loaded

Choose File

Generate Cert Bundle

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

## SAML Identity Provider (Issuer)

---

Identity Provider URL ?

Issuer Entity ID ?

Default (idp\_id): 6imt198ktjjq

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.com, Valid Until:  
08/09/2020

Include Certificate in Outgoing Assertion

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

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

## Service Provider

---

Assertion Consumer Service (ACS) URL ?

<ACS\_URL>

Audience (Service Provider Entity ID) ?

<SP\_ENTITY\_ID>

- 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.

## User Identity ?

---

NameID

Identifier Type

unspecified

Identity Source

AD20

Property ?

name

Attribute Hunting ?

NameID Attribute Hunting

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

## 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

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.



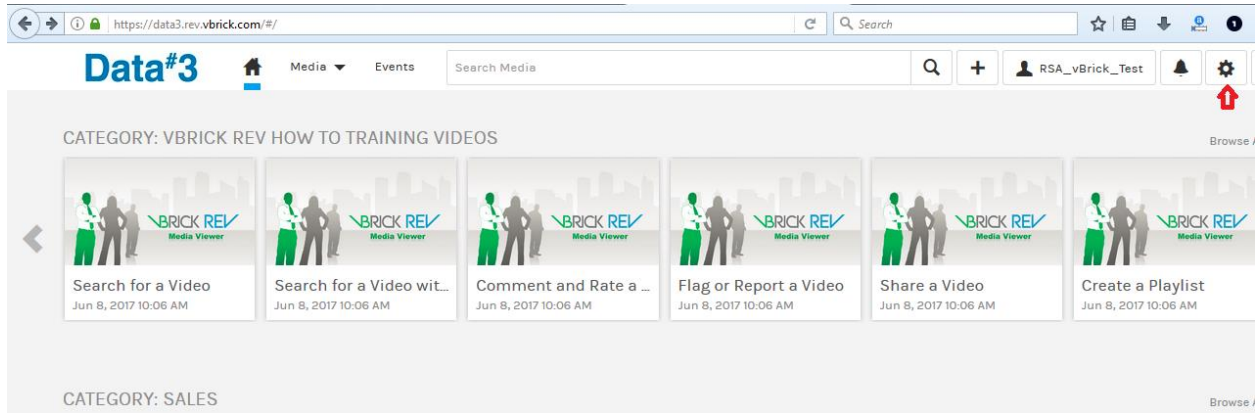
15. Navigate to **Applications > My Applications**.
16. Locate Cisco vBrick in the list and from the **Edit** option, select **Export Metadata**.



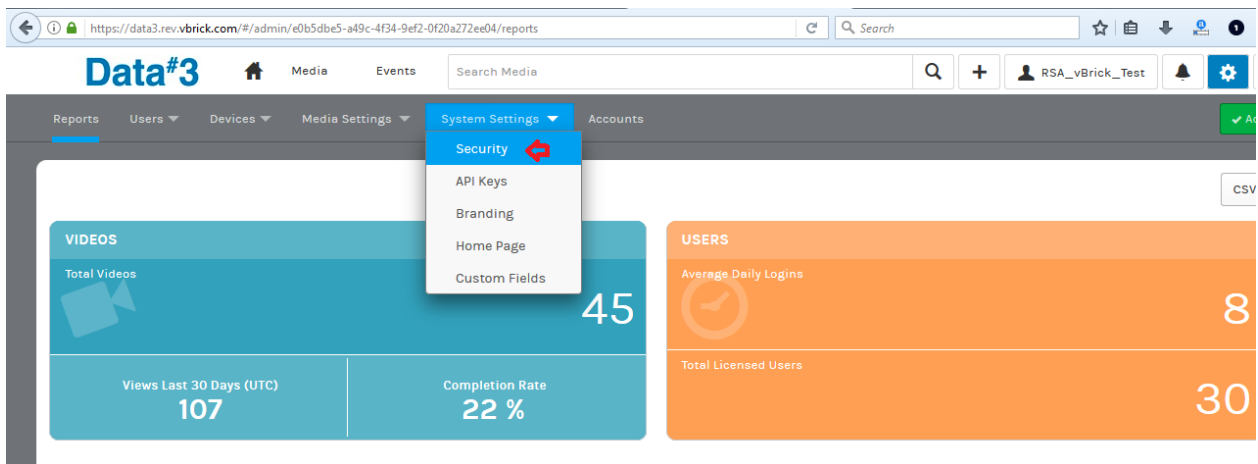
# Configure Cisco vBrick to Use RSA SecurID Access as an Identity Provider

## 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* (gearing 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.

**SINGLE SIGN ON**

Enable Single Sign On  Enabled

User Provisioning  Enabled

SAML Identity Location  NameIdentifier Element  
 Attribute Element

Identity Provider Metadata

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="u6ujdkabb5uz">
  <md:IDPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
```

Signature Algorithm SHA256withRSA \*

Sign SAML Request  Enabled

Download Service Provider MetaData

Regenerate Cert

- Click on **Enabled** checkbox in front of **Enable Single Sign On** option.
- Keep the **User Provisioning** field to its default value.
- Select **NameIdentifier Element** for **SAML Identity Location** field.
- 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.
- Select **SHA256with RSA** value from dropdowns for the **Signature Algorithm** field.
- Keep the **Sign SAML Request** field to its default value.
- 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.
- Once sure of settings, click on **Save** button which is available at bottom-right corner of the page to complete configuration changes.

Cancel Save

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