RSA SecurID Access SAML Configuration for VictorOps

Last Modified: March 23rd, 2017

VictorOps is a real-time incident management platform that combines the power of people and data to embolden DevOps pros to handle incidents as they occur.

Before You Begin

- Acquire an administrator account for both RSA SecurID Access and VictorOps.
- Obtain the VictorOps Login URL, ACS URL and Service Provider Entity ID from your VictorOps service provider.

The instructions in this guide use the following Login URL, ACS URL and issuer ID (entity ID) values:

Login URL	*https://core.futuresimple.com/users/login*
ACS URL	*https://sso.victorops.com/sp/ACS.saml2*
Service Provider Entity ID	*victorops.com*

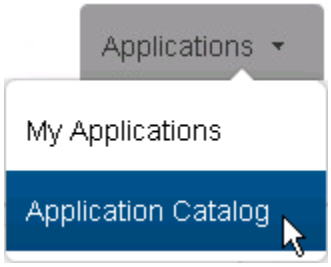
Procedure

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

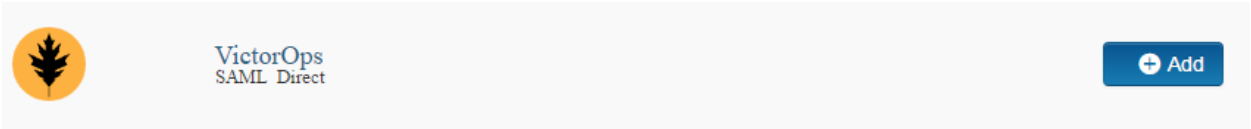
Add the Application in RSA SecurID Access

Procedure

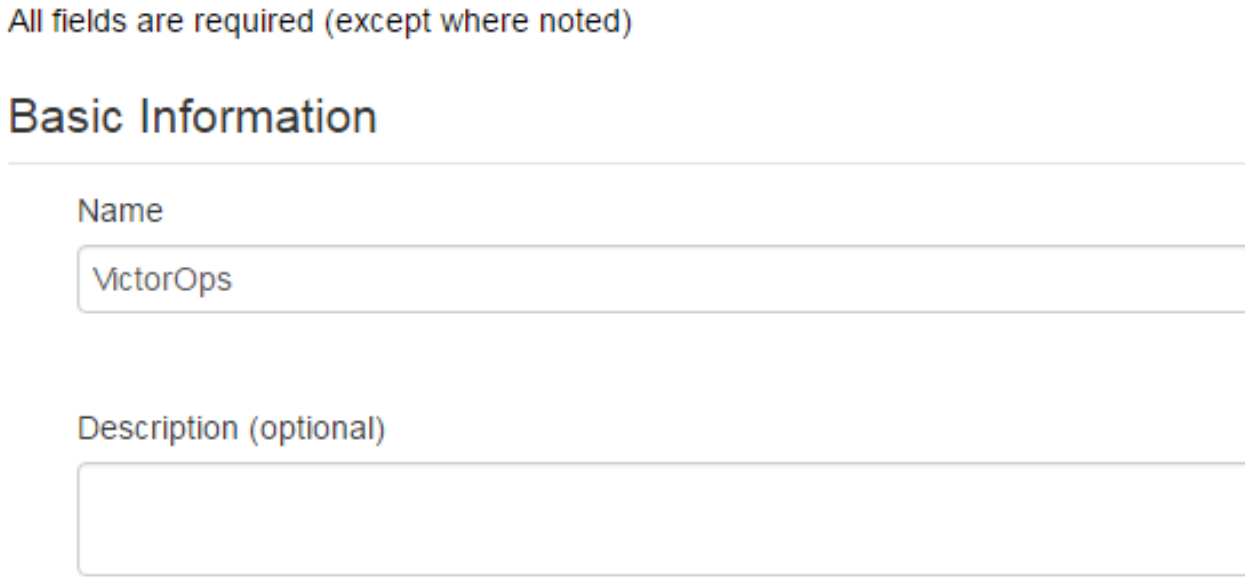
1. Log in to the RSA SecurID Access Administration Console, click the **Applications** tab and select *Application Catalog* from the **Application** tab dropdown list.



2. Search for *VictorOps* in the list of applications and click the **+Add** button.



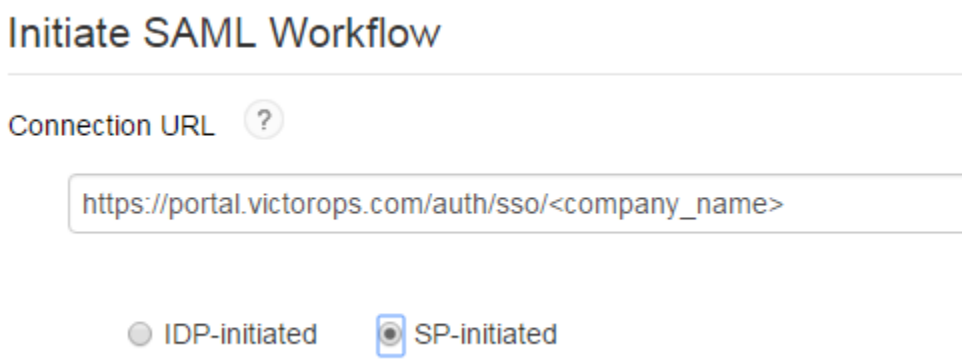
3. Enter a name for the application in the **Name** field on the **Basic Information** page and click the **Next Step** button.



4. Select the **SP-initiated** radio button in the **Initiate SAML Workflow** section.

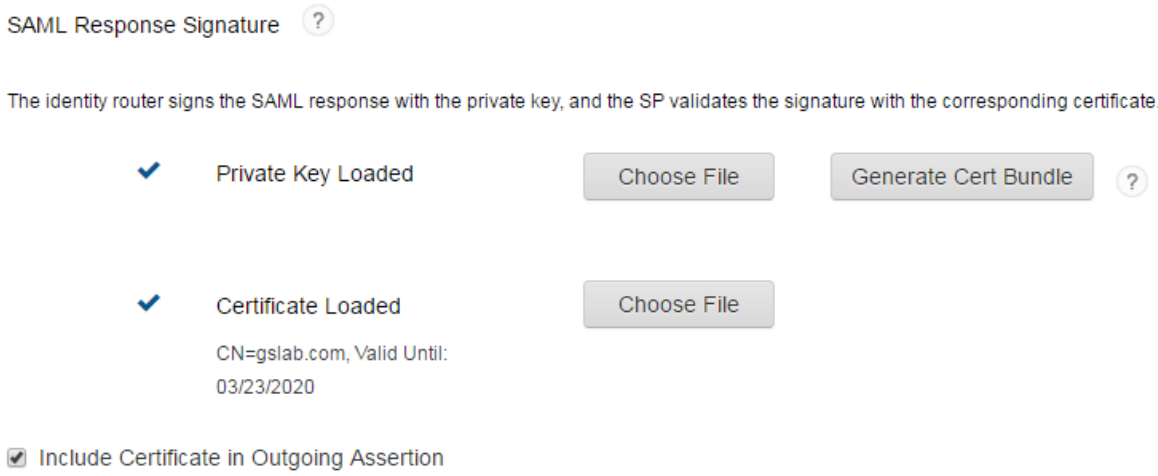
Note: The following IdP-initiated configuration works for SP-initiated VictorOps connections as well.

5. Enter the VictorOps landing page URL in the **Connection URL** field. Portal users will be redirected to this page when they click the VictorOps icon.
The URL is formatted as follows: https://portal.victorops.com/auth/sso/<comapany_name>

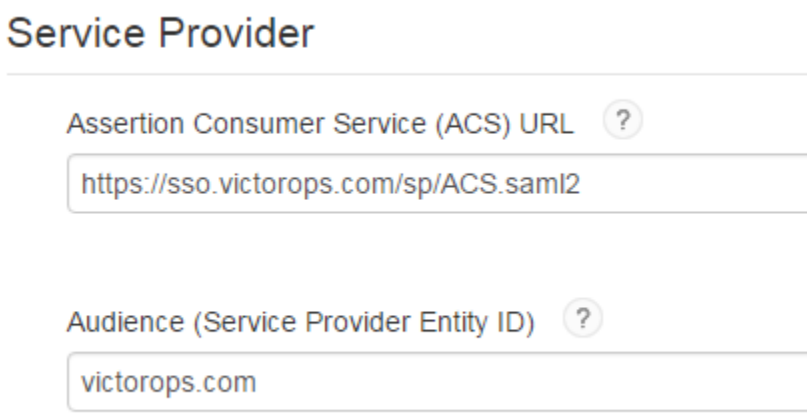


6. In SAML Identity Provider (Issuer) section keep the configuration as default.

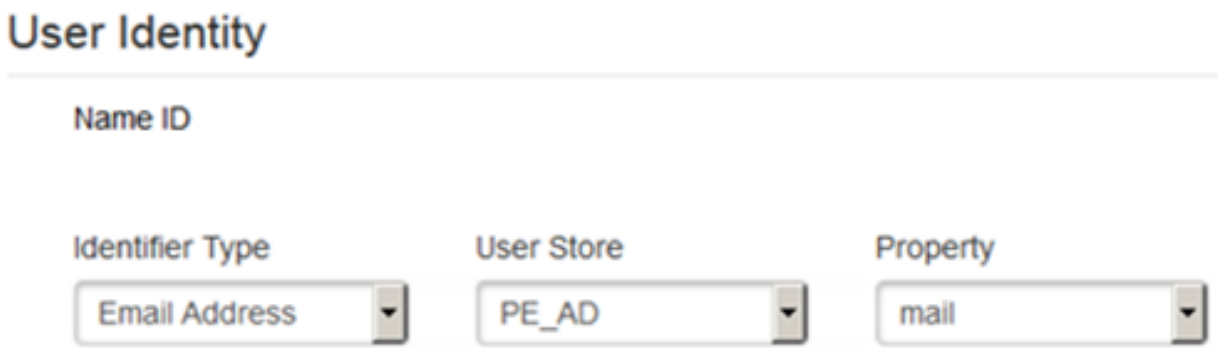
7. You must import a private/public key pair to sign and validate SAML assertions. If you don't have one readily available, follow the steps to generate a certificate bundle. Otherwise, continue to step 8.
    a. Click the **Generate Certificate Bundle** button in the **SAML Response Signature** section.
    b. In the **Common Name (CN)** field, enter the hostname of the VictorOps service provider's HTTPS server that will be sending authentication requests.
    c. Click the **Generate and Download** button, save the certificate bundle ZIP file to a secure location and extract its contents. The ZIP file will contain a private key, a public certificate and a certificate signing request. Click the **Choose File** button on the left of the **Generate Certificate Bundle** button, locate and select a private key for signing the SAML assertions and click the **Open** button.
8. Click the **Choose File** button underneath the **Generate Certificate Bundle** button, locate and select your public certificate and click the **Open** button.
9. Select the **Include Certificate in Outgoing Assertion** checkbox.



10. Scroll to the **Service Provider** section and enter your VictorOps ACS URL in the **Assertion Consumer Service (ACS) URL** field. The URL should be formatted as follows: https://sso.victorops.com/sp/ACS.saml2
11. Enter *victorops.com* in the **Audience (Service Provider Entity ID)** field. This value is case sensitive, and it must match your VictorOps SP Entity ID.

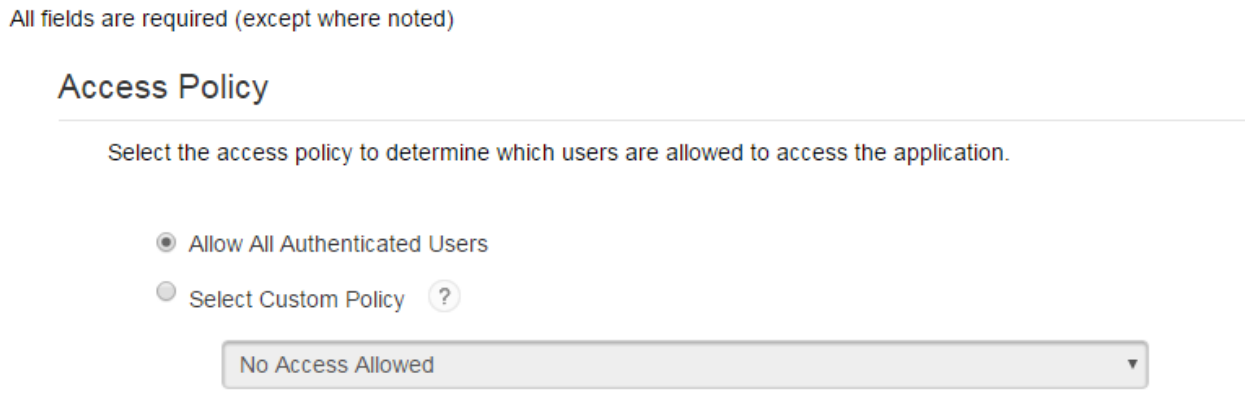


12. Scroll to the **User Identity** section, select *Email Address* from the **Identifier Type** dropdown list and select the name of your user identity source from the **User Store** dropdown list. In this example, user accounts are stored in an identity source named *PE_AD*.
13. Select the identity source's attribute that will be used as the NameID from the **Property** dropdown list. In this example, the identity source's *mail* attribute will be used to uniquely identify a user in SAML assertions.

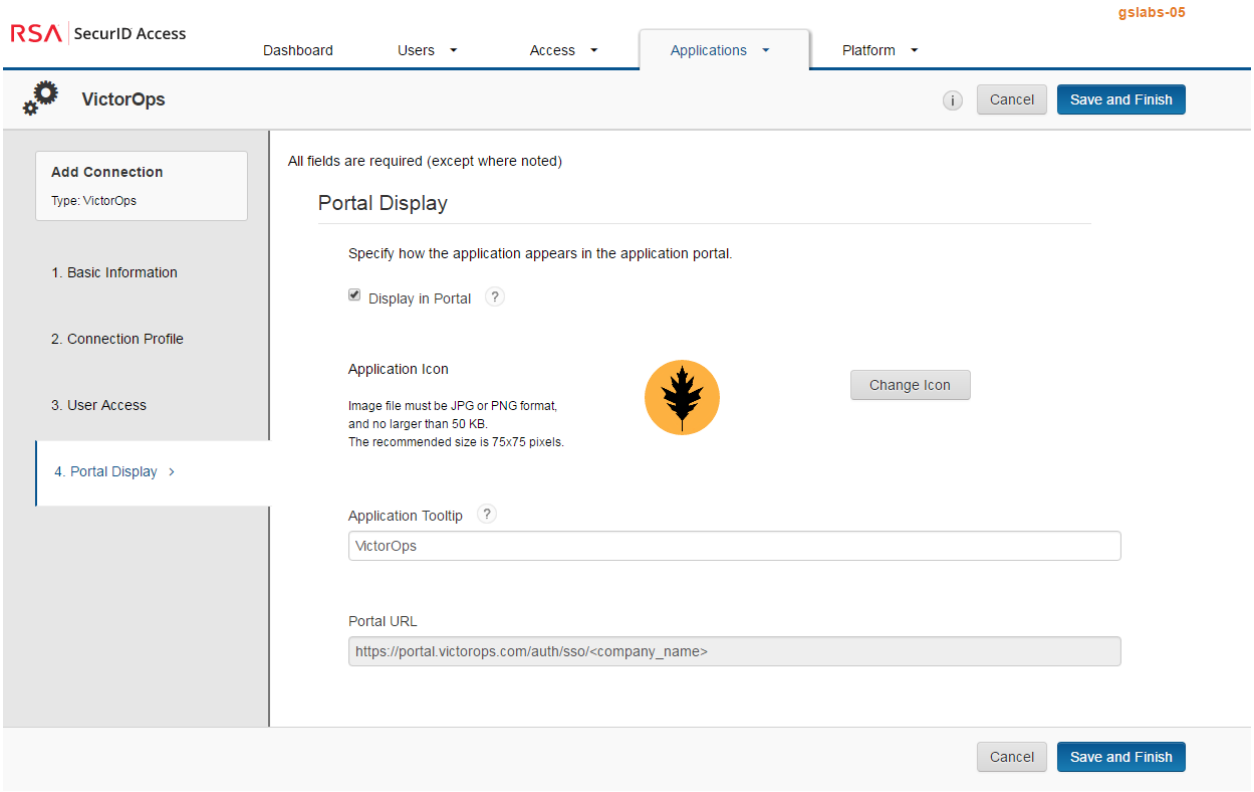


14. Click the **Next Step** button.

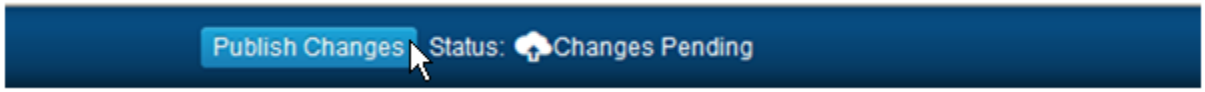
15. On the **User Access** page, select the access policy the identity router will use to determine which users can access the VictorOps service provider from the portal. If you want to allow access to all users who are signed in to the portal, select the **Allow All Authenticated Users** radio button. Otherwise, select the **Select Custom Policy** radio button and select the policy you want to use from the dropdown list.



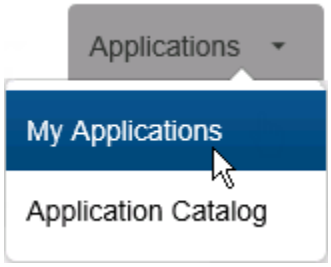
16. Click the **Next Step** button.
17. Select the **Display in Portal** checkbox on the **Portal Display** page.
18. Enter descriptive text about the application in the **Application Tooltip** field. The portal will display this text when a user passes the cursor over the application's icon.
19. Click the **Save and Finish** button.



20. Click the **Publish Changes** button in the top left corner of the page.



21. Click the **Applications** tab and select *My Applications* from the dropdown list.



22. Search for *VictorOps* in the list of applications and select *Export Metadata* from the **Edit** dropdown list to download an *XML* file containing your RSA SecurID Access IdP's metadata.

Configure VictorOps to Use RSA SecurID Access as an Identity Provider

Follow below steps to configure VictorOps as service provider.

1. Send SAML Idp metadata file to support@victorops.com
2. Their support team will enable SAML integration for your account using metadata file.

MD