RSA SecurID Access SAML Configuration for Cerner

Last Modified: February 21th, 2017

Cerner Corporation is an American supplier of health information technology (HIT) solutions, services, devices and hardware.

Before You Begin

- Acquire an administrator account to RSA SecurID Access.
- Obtain the ACS URL information from Cerner.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

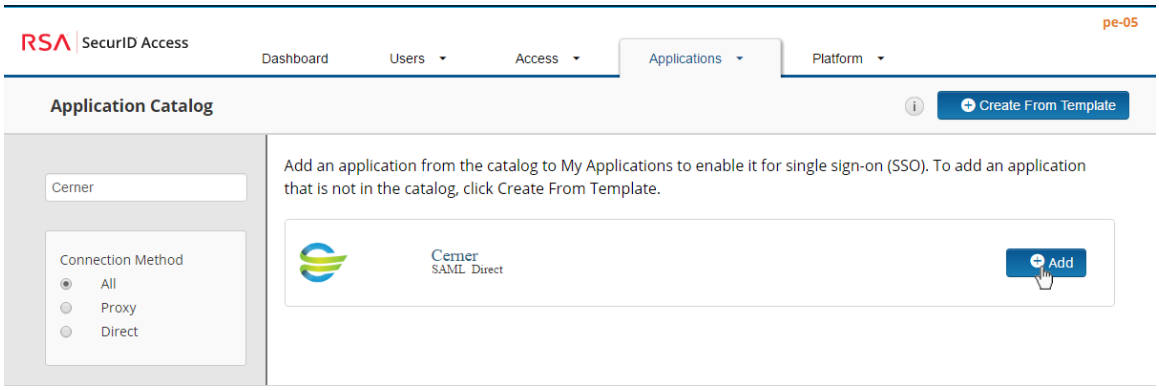
Procedure

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

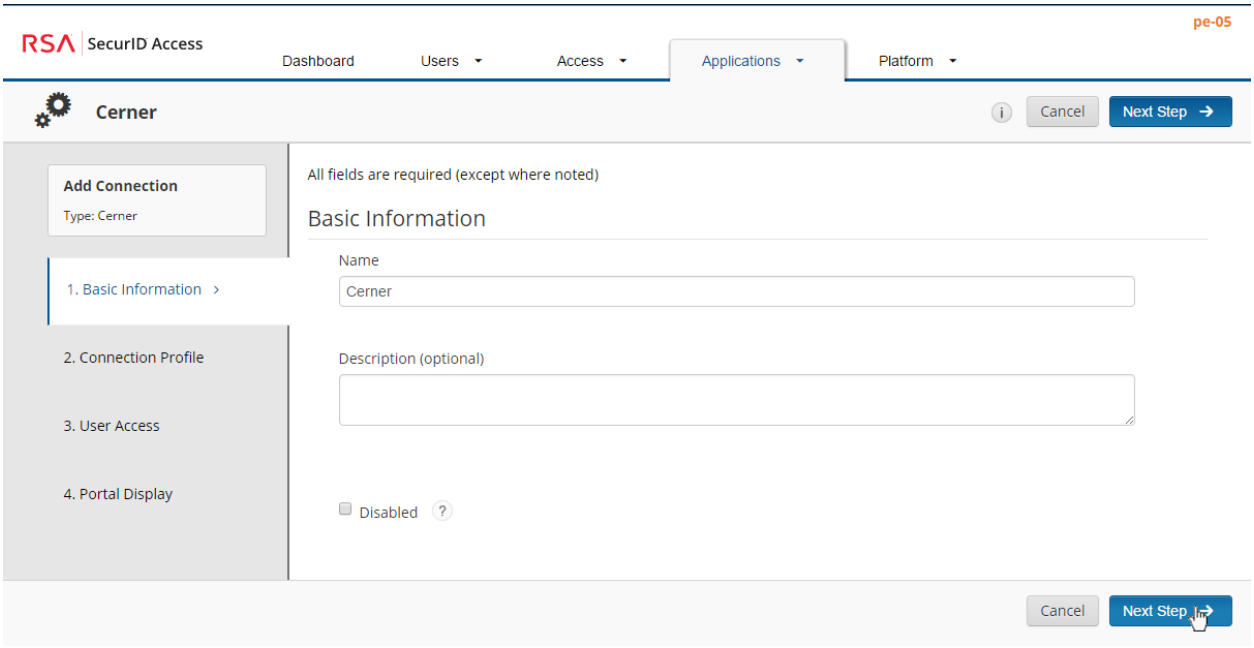
Add the Application in RSA SecurID Access

Procedure

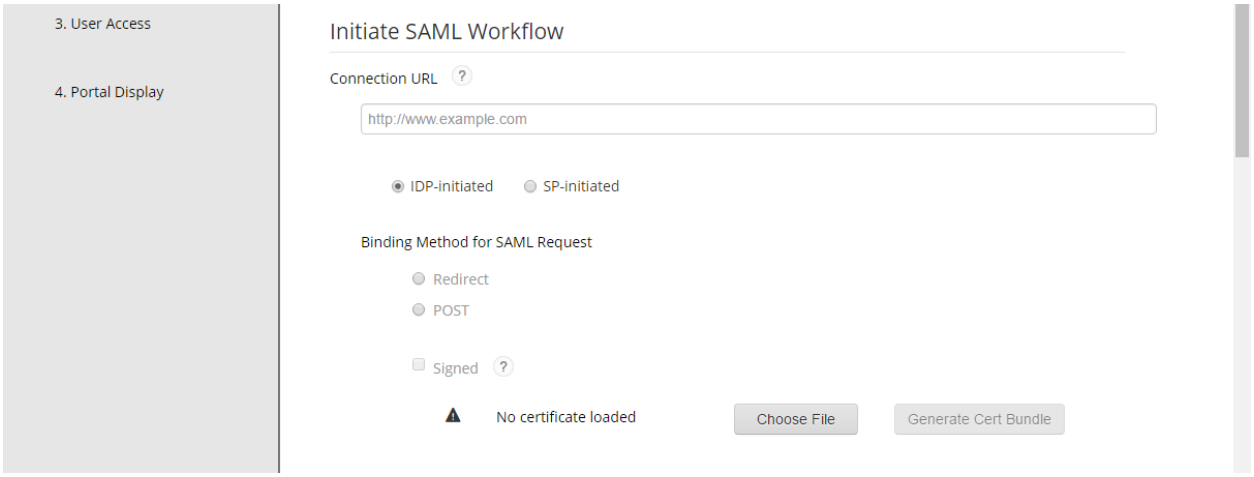
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, locate **Cerner** and click **+Add**.



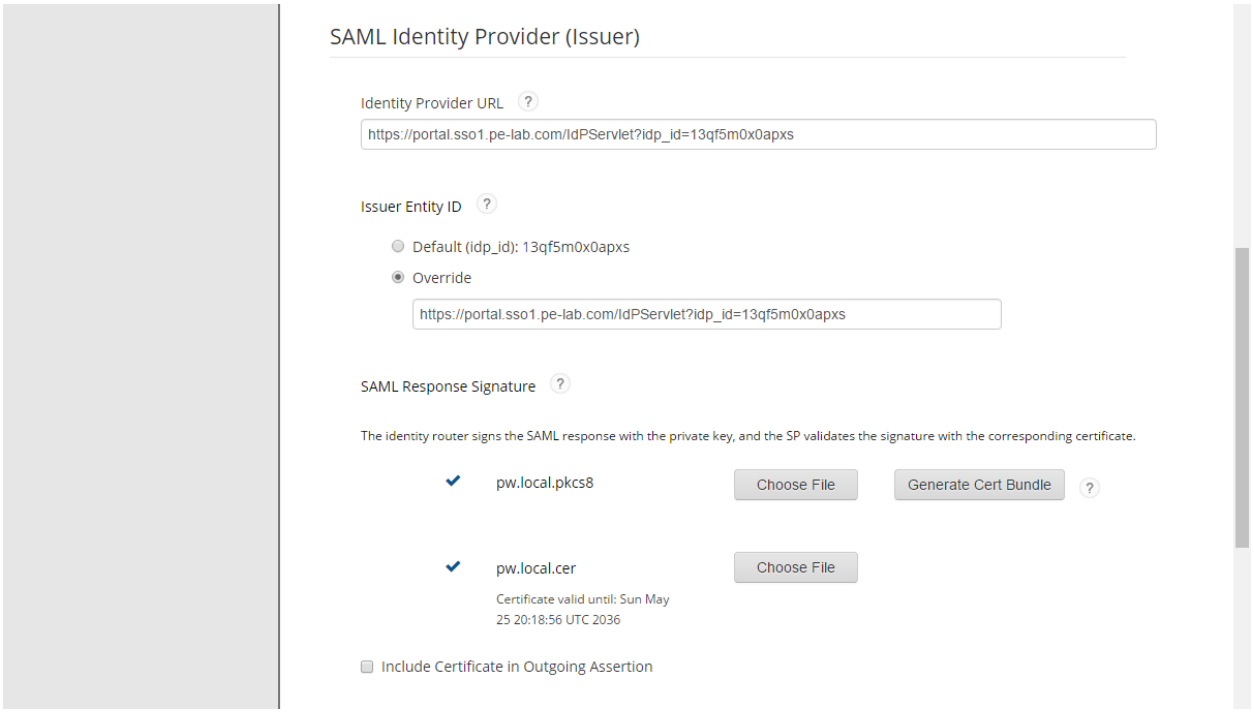
3. On the Basic Information page, specify the application name and click **Next Step**.



4. Configure the Initiate SAML Workflow settings and then scroll down to the **SAML Identity Provider (Issuer)** section.

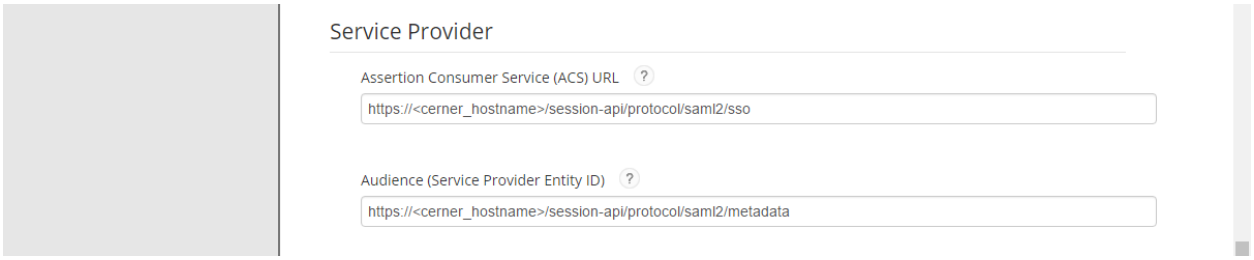


5. Configure the SAML Identity Provider settings and scroll down to the **Service Provider** section.



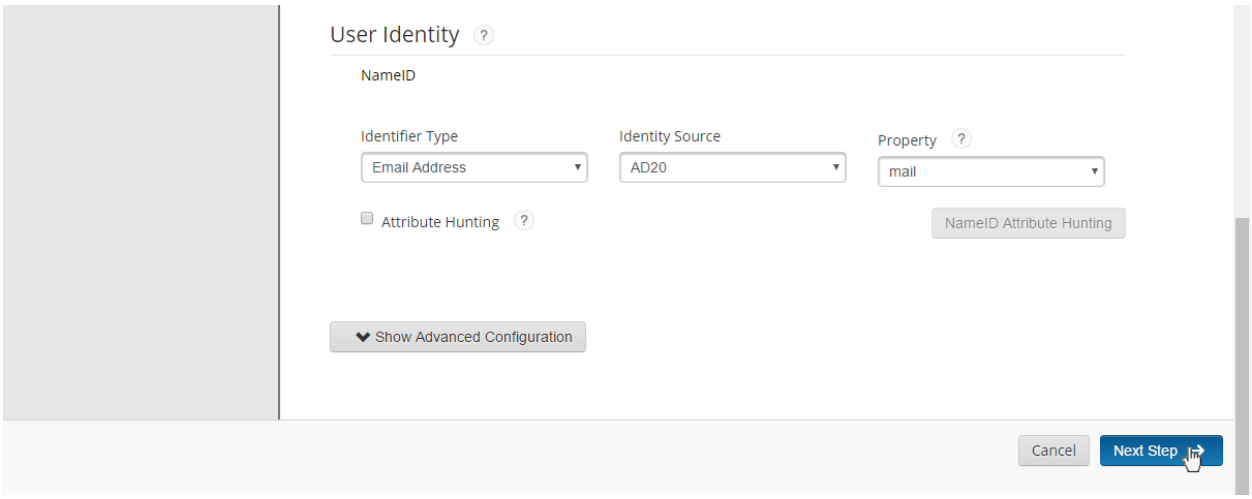
- Keep the default value in the **Identity Provider URL**.
- Set the **Issuer Entity ID** to **Override** and then enter the value from the Identity Provider URL.
- Upload the SAML response signing private key and corresponding certificate.

6. Configure the Service Provider settings and scroll down to the **User Identity** section.



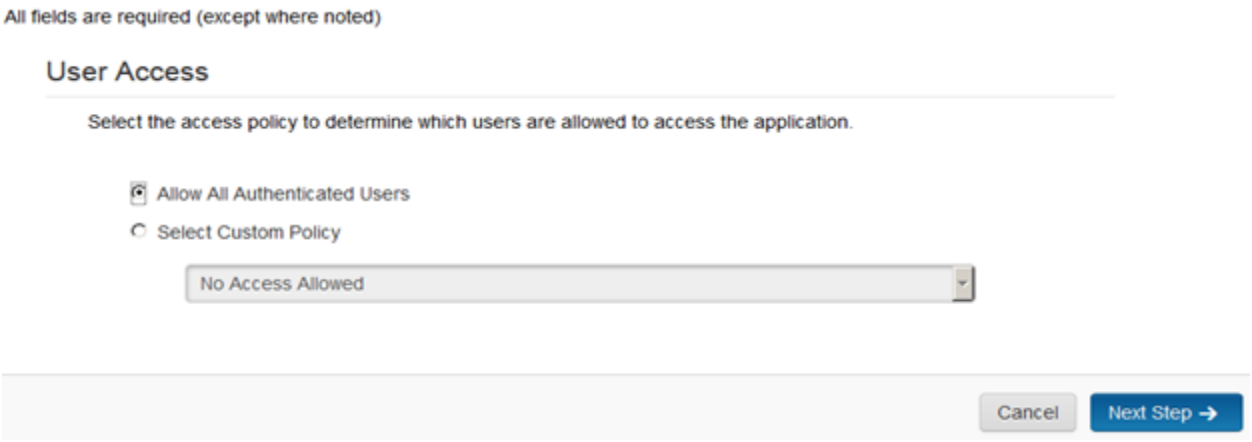
- In the **Assertion Consumer Service (ACS) URL** field, change the <cerner_hostname> to match the hostname of your Cerner instance.
- In the **Audience (Service Provider Entity ID)** field, change the <cerner_hostname> to match the hostname of your Cerner instance.

7. Configure the User Identity settings and click **Next Step**.

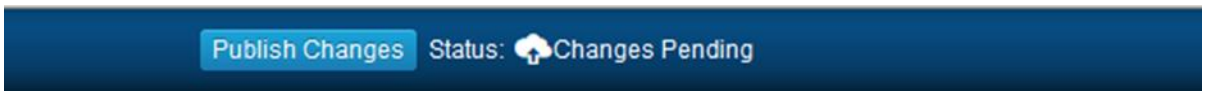


- Set the **Identifier type** to **Email Address**.
- Set the **Property** to **mail**.

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



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.



Next Steps

[Configure Cerner to Use RSA SecurID Access as an Identity Provider]

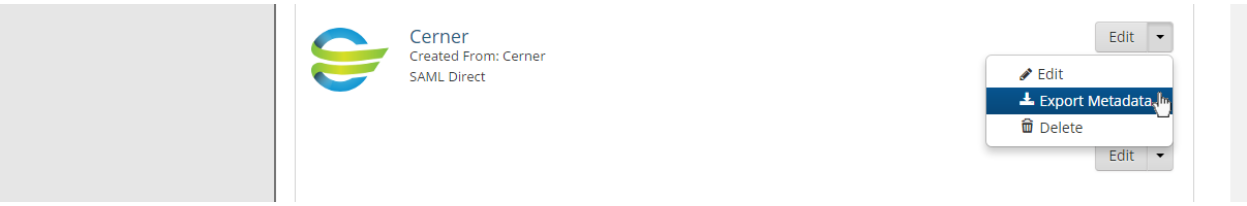
Configure Cerner to Use RSA SecurID Access as an Identity Provider

The Cerner SAML service provider application requires that the SAML IdP has its metadata file hosted and reachable via public Web server. At this time, SecurID Access does not have this capability built in. You will have to download the metadata file from the SecurID Access Console and host it on your own Web server.

Once the metadata file has been hosted on a Web server you can engage with Cerner ops personnel to implement the necessary configuration changes needed for SAML SSO.

To download the metadata file from SecurID Access:

1. Logon to the SecurID Access Console and navigate to **Applications > My Applications**.
2. Locate the application in the list and from the **Edit** pulldown select **Export Metadata**.



PEW