

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.

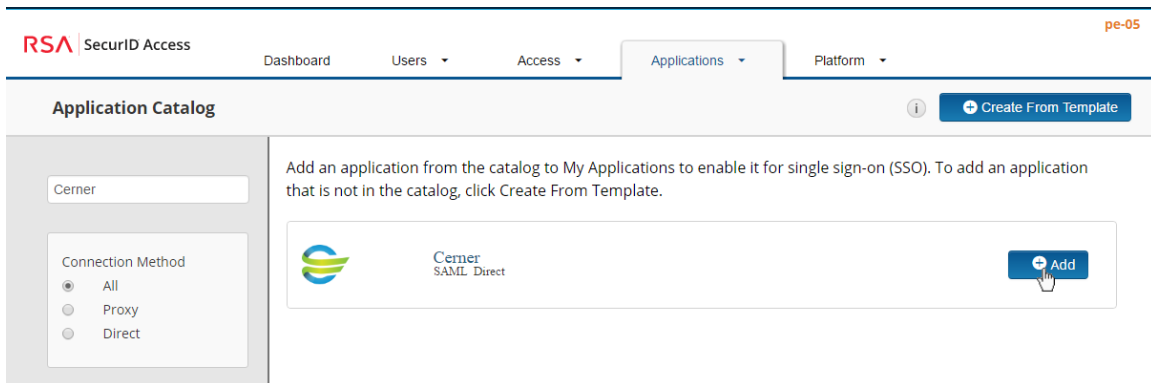
Procedure

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**.

The screenshot shows the RSA SecurID Access interface. At the top, there is a navigation bar with 'RSA SecurID Access' on the left and 'pe-05' on the right. Below this are tabs for 'Dashboard', 'Users', 'Access', 'Applications', and 'Platform'. The 'Applications' tab is active. On the left side, there is a sidebar with a gear icon and the word 'Cerner'. Below the sidebar, there is a list of steps: '1. Basic Information', '2. Connection Profile', '3. User Access', and '4. Portal Display'. The main content area is titled 'Basic Information' and contains the following fields: 'Name' (with the value 'Cerner'), 'Description (optional)', and a 'Disabled' checkbox. At the bottom right, there are 'Cancel' and 'Next Step' buttons.

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

The screenshot shows the 'Initiate SAML Workflow' page. On the left side, there is a sidebar with a list of steps: '3. User Access' and '4. Portal Display'. The main content area is titled 'Initiate SAML Workflow' and contains the following fields: 'Connection URL' (with the value 'http://www.example.com'), 'IDP-initiated' and 'SP-initiated' radio buttons, 'Binding Method for SAML Request' (with 'Redirect' and 'POST' radio buttons), and a 'Signed' checkbox. At the bottom, there is a warning icon and the text 'No certificate loaded', along with 'Choose File' and 'Generate Cert Bundle' buttons.

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

SAML Identity Provider (Issuer)

Identity Provider URL ?
https://portal.sso1.pe-lab.com/IdPServlet?idp_id=13qf5m0x0apxs

Issuer Entity ID ?
 Default (idp_id): 13qf5m0x0apxs
 Override
https://portal.sso1.pe-lab.com/IdPServlet?idp_id=13qf5m0x0apxs

SAML Response Signature ?
The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

pw.local.pkcs8

pw.local.cer
Certificate valid until: Sun May 25 20:18:56 UTC 2036

Include Certificate in Outgoing Assertion

- 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.

Service Provider

Assertion Consumer Service (ACS) URL ?
https://<cerner_hostname>/session-api/protocol/saml2/sso

Audience (Service Provider Entity ID) ?
https://<cerner_hostname>/session-api/protocol/saml2/metadata

- 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**.

User Identity ?

NameID

Identifier Type: Email Address

Identity Source: AD20

Property: mail

Attribute Hunting ?

NameID Attribute Hunting

Show Advanced Configuration

Cancel 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.

All fields are required (except where noted)

User Access

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

Allow All Authenticated Users

Select Custom Policy

No Access Allowed

Cancel Next Step

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**.

