

**Last Modified:** July 19, 2016

Samanage, an enterprise service-desk and IT asset-management provider, has its headquarters in Cary, North Carolina. The company's flagship product, Samanage, operates as a multi-tenant, Software-as-a-Service (SaaS) system for IT and enterprise service management.

## Before You Begin

- Acquire an administrator account for both RSA SecurID Access and Samanage.
- Obtain the Samanage [login URL](#), [ACS URL](#) and [Service Provider Issuer ID](#) from your Samanage service provider.

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

<b>Login URL</b>	<a href="https://gslab32.samanage.com/saml_login/gslab32">https://gslab32.samanage.com/saml_login/gslab32</a>
<b>ACS URL</b>	<a href="https://gslab32.samanage.com/saml/gslab32">https://gslab32.samanage.com/saml/gslab32</a>
<b>Service Provider Issuer ID</b>	<i>SAManage.com</i>

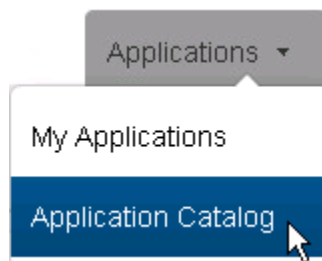
## Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Samanage to Use RSA SecurID Access as an Identity Provider](#)

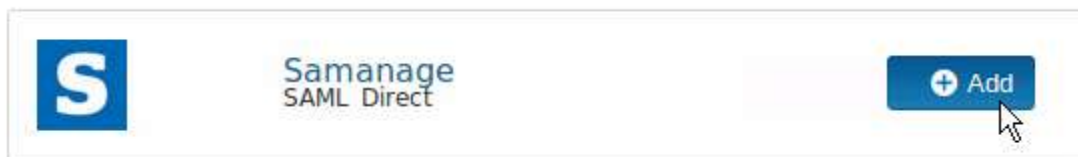
## Add the Application in RSA SecurID Access

### 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 *Samanage* 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 **IdP-initiated** radio button in the **Initiate SAML Workflow** section.

---

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

---

5. Enter the Samanage landing page URL in the **Connection URL** field. Portal users will be redirected to this page when they click the Samanage icon. The URL is formatted as follows: *https://<ACCOUNT\_NAME>.samanage.com/saml\_login/<ACCOUNT\_NAME>*, where *<ACCOUNT\_NAME>* is the name of your Samanage account. The connection URL in this example is *https://gslab32.samanage.com/saml\_login/gslab32*.

## Initiate SAML Workflow

Connection URL 

https://gslab32.samanage.com/saml\_login/gslab32

IDP-initiated  SP-initiated

6. Scroll to **SAML Identity Provider (Issuer)** section, copy the value in the **Identity Provider URL** field and paste it into a temporary file. You will need the URL when you [configure your Samanage service provider](#).

## SAML Identity Provider (Issuer)

Identity Provider URL 

https://portal.sso4.pe-lab.com/IdPServlet?idp\_id=10366rs5lrxxs

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 Samanage 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.

8. 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.
9. Click the **Choose File** button underneath the **Generate Certificate Bundle** button, locate and select your public certificate and click the **Open** button.
10. Select the **Include Certificate in Outgoing Assertion** checkbox.
11. Scroll to the **Service Provider** section and enter your [Samanage ACS URL](#) in the **Assertion Consumer Service (ACS) URL** field. The URL should be formatted as follows:  
`https://<ACCOUNT_NAME>.samanage.com/saml/<ACCOUNT_NAME>`.  
 The ACS URL in this example is `https://gslab32.samanage.com/saml/gslab32`.
12. Enter `SAManage.com` in the **Audience (Service Provider Entity ID)** field. This value is case sensitive, and it must match your [Samanage SP Issuer ID](#).

## Service Provider

Assertion Consumer Service (ACS) URL ?

`https://gslab32.samanage.com/saml/gslab32`

Audience (Service Provider Entity ID) ?

`SAManage.com`

13. 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*.
14. 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.

## User Identity

Name ID

Identifier Type      User Store      Property

Email Address      PE\_AD      mail

15. Click the **Next Step** button.

- On the **User Access** page, select the access policy the identity router will use to determine which users can access the Samanage 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.

Allow All Authenticated Users  
 Select Custom Policy ?

No Access Allowed ▼

- Click the **Next Step** button.
- Select the **Display in Portal** checkbox on the **Portal Display** page.
- 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.
- Click the **Save and Finish** button.

## Portal Display

Specify how the application appears in the application portal.

Display in Portal ?

Application Icon

Image file must be JPG or PNG format,  
and no larger than 50 KB.  
The recommended size is 75x75 pixels.



Change Icon

Application Tooltip ?

Samanage

Portal URL

https://portal.sso4.pe-lab.com/IdPServlet?idp\_id=10366rs5lrxxs

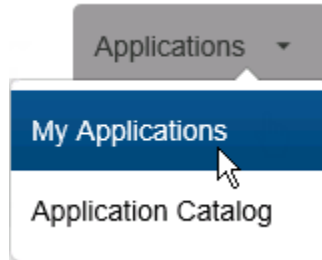
Cancel

Save and Finish

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



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



23. Search for *Samanage* 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. You will need the X509Certificate contained in this file [when you configure Samanage](#).

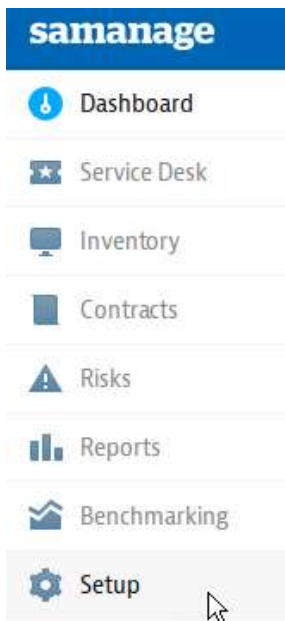


## Configure Samanage to Use RSA SecurID Access as an Identity Provider

Follow below steps to configure Samanage as service provider.

### Create an Identity Provider

1. Log in to your Samanage account and select *Setup* from the **Dashboard** dropdown list in the upper left corner of the page.



2. Check **Enable Single Sign On with SAML** checkbox in the **Login using SAML** section.
3. Enter your [RSA SecurID Access Identity Provider URL](#) in the **Identity Provider URL** field.
4. Enter your Samanage login URL in the **Login URL** field. The URL should be formatted as follows: *https://<ACCOUNT\_NAME>.samanage.com/saml\_login/<ACCOUNT\_NAME>*, where *<ACCOUNT\_NAME>* is the name of your Samanage account. The login URL in this example is *https://gslab32.samanage.com/saml\_login/gslab32*.

**Login using SAML**

Enable Single Sign-On with SAML

**Identity Provider URL.** Specify the URL used by your identity provider to authenticate sign-on requests.

**Login URL.** Use this address to point your users to.

5. (Optional) If you want Samanage to redirect users to a custom URL after they log out, enter the URL in the **Logout URL** field.
6. (Optional) If you want Samanage to redirect users to a custom error URL when an error occurs during the login process, enter the URL in the **Error URL** field.
7. Enter *SAManage.com* in the **SAML Issuer** field (default). This value is case sensitive, and it must match the [SP Entity ID in your RSA SecurID Access configuration](#).

**Logout URL.** URL to redirect users after logout.

**Error URL.** Specify the page users should be redirected to if there's an error during SAML login.

**SAML Issuer.** Specify the APP ID URI set in your identity provider (leave 'SAManage.com' if unknown).

8. Copy **X509Certificate** from the IdP metadata file [you exported](#) from RSA SecurID Access and paste in **Certificate** textbox.

Paste your Identity Provider x.509 Certificate below

```
-----BEGIN CERTIFICATE-----
MIICpjCCAY6gAwIBAgIGAV01GPz2MA0GCSqGSIb3DQEBCwUAMBQxEjAQBgNVBAMT
CwdzbGF1LmNvbTAeFw0xNjAzMjMwNjEwNT1aFw0yMDAzMjMwNjEwNT1aMBQxEjAQ
BgNVBAMTCWdzbGF1LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMraYXqMGpvPa+J+r46Nf5xG1U7NyIe5DCzTNY7uCSAXGgNou7SAN4vA1j9ZGsD
UgVQ20m8QpMkV5cmCNThNUBAIbhIXpdkSVGcdvvhScB14GC25roNYaswGz10Qxus
F/jPypNMzZcJ6p0zCT0yuWgX1yMqb1/CKuFTo/XUFxU26S251Y11hhqqp8MMxpt0
hkShJExvZGH/XFj8LSt5T7rZwQGwqIuYZa80leyxbJSv7Qvfi0tNCJv8ZsGgG/qn
qpzwPq81rpd/NkwvyB/+piUnPbbmVhh/gK8eExqQPPr+62KifgRzigIpN6GJXJ4q
GgpcNUWYqfORMuJevx/cpRcCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAmE0+IrC
556Z8xqwZY2I8PwqHkCttdYudSk4pA1XAmYcREqM+Z75Gjz/o1N+GubdVFSX4uV1
m85wfkUhm8V6UPMHWFhtXBaZuDVC27oEmyMioyuJIETJGIX6mEUEnlhvBKYpam
bVtgb/fsqd4+ahG6R90S+REE40c9TJd0XP49ZELC0SWFmxyVcCUV/tw/V1U5K0/s
jnHH09Y6Xr1/zI8myY2nYuXmHZ+LBk2Qi8amQZp40Ioqd4ooQSBYqs2YziEgo5b+
8p1CSCoouXxhxBKh06atLzth9gS7v57tHCUKMAxvzgisRG8t11mwWZg2nnE4j1DF
KxykG5p+nQvjeQ==
-----END CERTIFICATE-----
```

Note: your certificate should contain '-----BEGIN CERTIFICATE-----' and '-----END CERTIFICATE-----' lines

9. If you want Samanage to automatically create a user id whenever it receives a SAML assertion for a user who doesn't have a Samanage account, check the **Create users if they do not exist in Samanage** checkbox.



10. If you want to force all Samanage users to authenticate with SAML, check the **Redirect to the saml login page when logging into Samanage by default** checkbox.

11. Click the **Update** button.

Users are created in Samanage after successfully authenticating with your SAML servers, and are assigned the 'portal user' role. These users can only access the end-user service portal. You can always modify their roles later in the [users setup](#) section.

Create users if they do not exist in Samanage

Redirect to the saml login page when logging into Samanage by default.

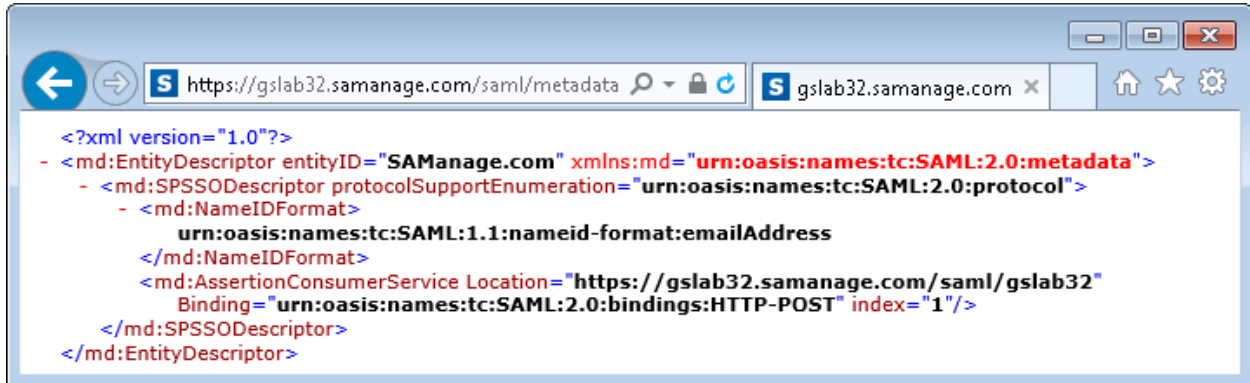




## Appendix

Your Samanage account's ACS URL is: [https://<ACCOUNT\\_NAME>.samanage.com/saml/metadata](https://<ACCOUNT_NAME>.samanage.com/saml/metadata). The ACS URL in this example is [https://gslab32.samanage.com/saml\\_login/gslab32](https://gslab32.samanage.com/saml_login/gslab32).

You can view the URL and other SAML metadata associated with your Samanage account at the following address: [https://<ACCOUNT\\_NAME>.samanage.com/saml/metadata](https://<ACCOUNT_NAME>.samanage.com/saml/metadata).



The screenshot shows a web browser window with the address bar containing <https://gslab32.samanage.com/saml/metadata>. The browser's developer tools are open, displaying the following XML content:

```
<?xml version="1.0"?>
- <md:EntityDescriptor entityID="SAManage.com" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  - <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    - <md:NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
    </md:NameIDFormat>
    <md:AssertionConsumerService Location="https://gslab32.samanage.com/saml/gslab32"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" index="1"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```