

**Last Modified:** December 21, 2015

Daptiv provides a powerful, integrated suite of PPM applications that include portfolio management, project management, resource management, time & expense, document management and more.

## Before You Begin

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

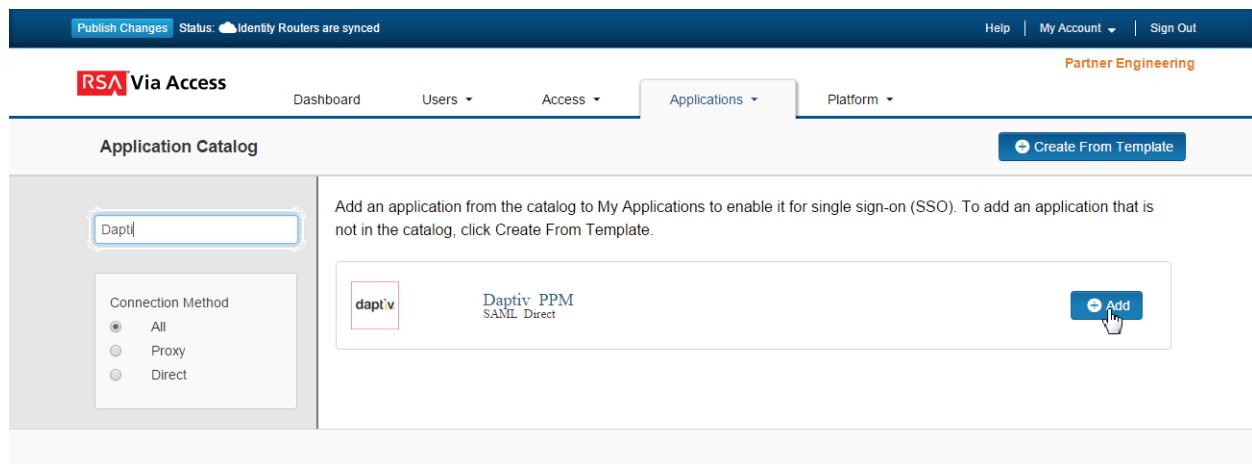
## Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Daptiv PPM 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** for the application that you wish to add.



3. On the Basic Information page, specify the application name and click **Next Step**.
4. On the Connection Profile page choose **IDP –initiated**, and scroll down to the SAML Identity Provider (Issuer) section.

## SAML Identity Provider (Issuer)

---

Identity Provider URL


Issuer Entity ID

Default (idp\_id): ugrfcswiyc5h

Override

Certificate Bundle


The certificate bundle is required to ensure a secure transaction.

 No private key loaded

Choose File

Generate Certificate Bundle

Include Certificate in Outgoing Assertion

 No certificate loaded

Choose File

- a. In the **Identity Provider URL** field, copy the URL which will be needed later to configure the Service Provider configuration.
- b. Take note of the **Issuer Entity ID**.
- c. Select **Choose File** and upload the private key. Select **Choose File** to locate and import a private key to sign the SAML assertion. The private key must correspond to the public signing certificate loaded in the SP application. If a private/public key pair is not readily available, you can click **Generate Certificate Bundle**.

5. Scroll down to the Service Provider section.

### Service Provider

---

Assertion Consumer Service (ACS) URL

https://ppm.daptiv.com/SamlLogin.aspx

Audience (Service Provider Entity ID)

https://ppm.daptiv.com

- a. In the **Assertion Consumer Service (ACS) URL** field, enter the URL you obtained from the application administrator.
  - b. In the **Audience (Service Provider Entity ID)** field, enter the Entity ID to match the configured value from the Service Provider.
6. Scroll down to the User Identity section. Verify the settings are correct for your environment. In this example the username to be in presented in email format and the user account will be validated again the User Store selected.

### User Identity

---

Name ID

Identifier Type

transient

User Store

nga2012dc

Property

mail

Attribute Hunting

NameID Attribute Hunting

7. Click **Next Step**.

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.

Publish Changes

Status:  Changes Pending

## Next Steps

[Configure Daptiv PPM to Use RSA SecurID Access as an Identity Provider](#)

## **Configure SaaS to Use RSA SecurID Access as an Identity Provider**

Open a support ticket with Daptiv to enable your instance with SSO via SAML 2.0. Daptiv will require the following information (at a minimum) in order to integrate with RSA SecurID Access IdP:

- Identity Provider URL
- Issuer Entity ID
- Signing Certificate