RSA SecurID Access SAML Configuration for StatusDashboard

Last Modified: Mar 28, 2017

StatusDashboard provides an enterprise service that allows your teams to easily manage and communicate system status to your customers. StatusDashboard also provide the ability to create custom, automated digital signs on large displays in lobbies or network operations centers.

Before You Begin

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

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

Login URL	*https://www.statusdashboard.com/accounts/login/*
ACS URL	*https://emc21.statusdashboard.com/acs*
Service Provider Issuer ID	*emc21.statusdashboard.com*

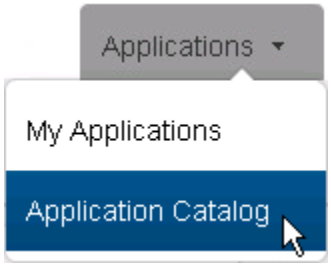
Procedure

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

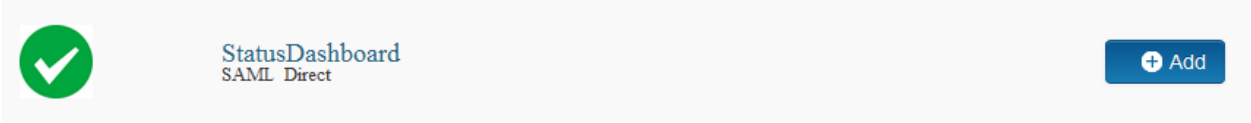
Add the Application in RSA SecurID Access

Procedure

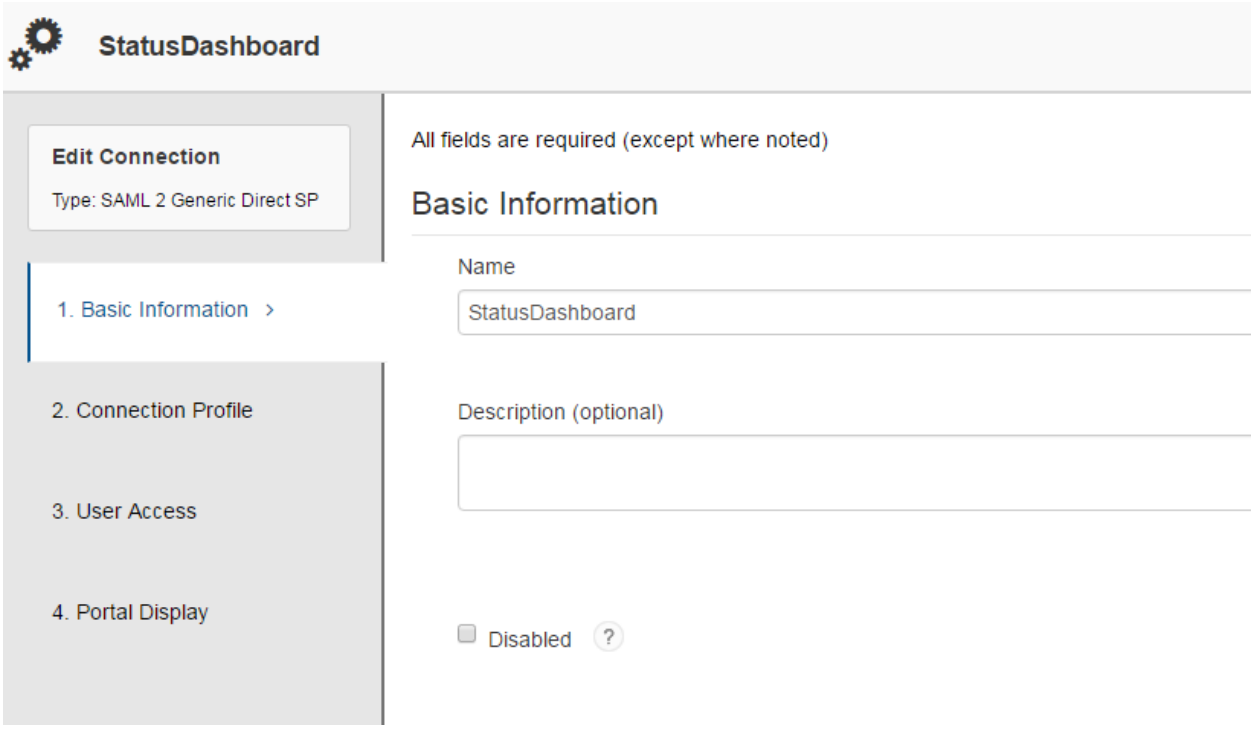
1. Log in to the RSA SecurID Access Administration Console, click the **Applications** tab and select *Application Catalog* from the **Application** tab dropdown list.



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



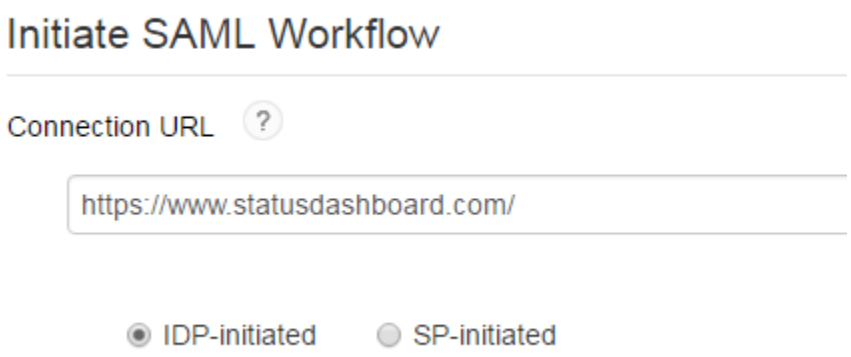
3. Enter a name for the application in the **Name** field on the **Basic Information** page and click the **Next Step** button.



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

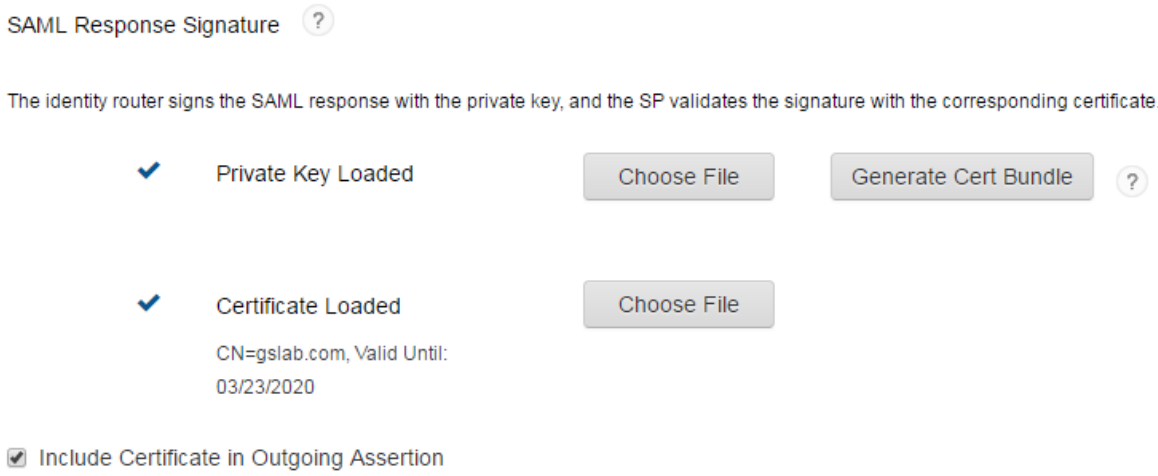
Note: The following Idp-initiated configuration works for SP-initiated StatusDashboard connections as well.

5. Enter the StatusDashboard landing page URL in the **Connection URL** field. Portal users will be redirected to this page when they click the StatusDashboard icon.
The URL is formatted as follows: https://www.statusdashboard.com/



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

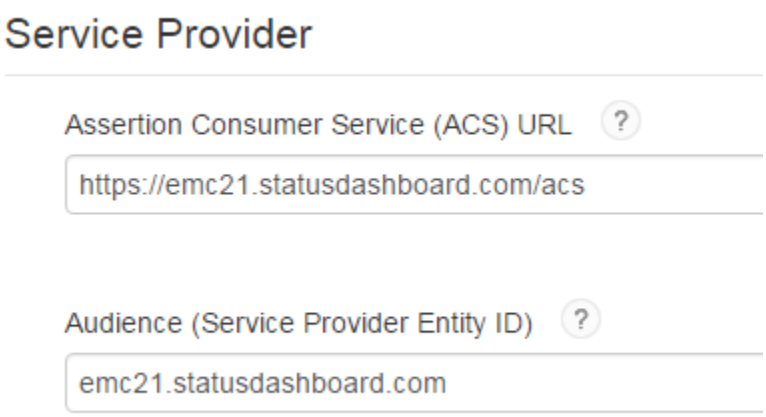
7. Under SAML Response Signature you must import a private/public key pair to sign and validate SAML assertions. If you don't have one readily available, follow the steps to generate a certificate bundle. Otherwise, continue to step 8.
    a. Click the **Generate Certificate Bundle** button in the **SAML Response Signature** section.
    b. In the **Common Name (CN)** field, enter the hostname of the StatusDashboard 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.



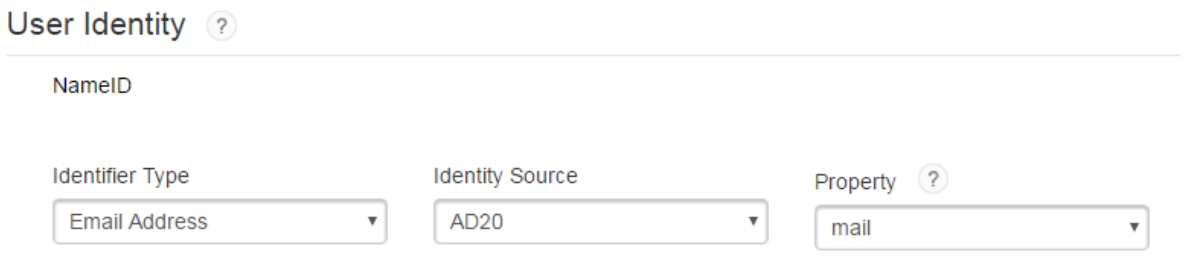
10. Scroll to the **Service Provider** section and enter your StatusDashboard ACS URL in the **Assertion Consumer Service (ACS) URL** field. The URL should be formatted as follows: *https://<Domain_Alias>.statusdashboard.com/acs*

    The ACS URL in this example is *https://emc21.statusdashboard.com/acs*

11. Enter *StatusDashboard.com* in the **Audience (Service Provider Entity ID)** field. This value is case sensitive, and it must match your StatusDashboard SP Issuer ID.

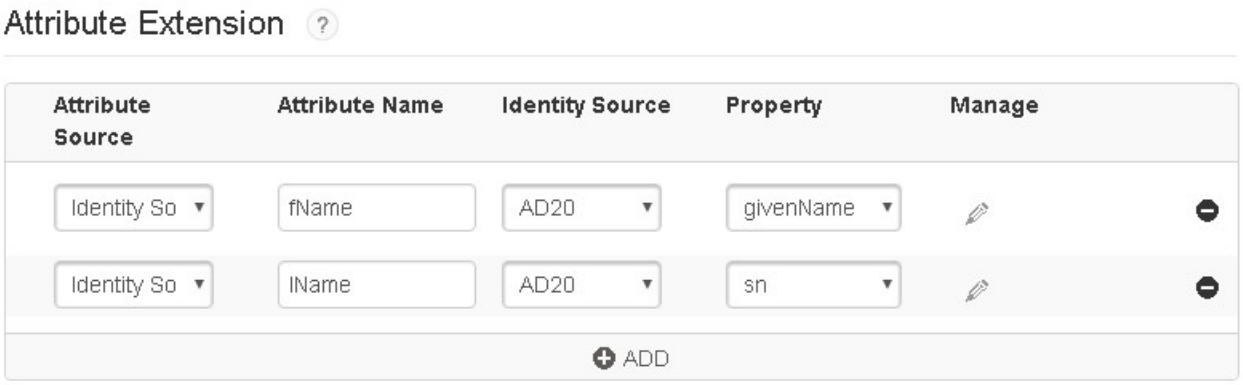


12. Scroll to the **User Identity** section, select *Email Address* from the **Identifier Type** dropdown list and select the name of your user identity source from the **User Store** dropdown list. In this example, user accounts are stored in an identity source named *AD20*.
13. Select the identity 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.

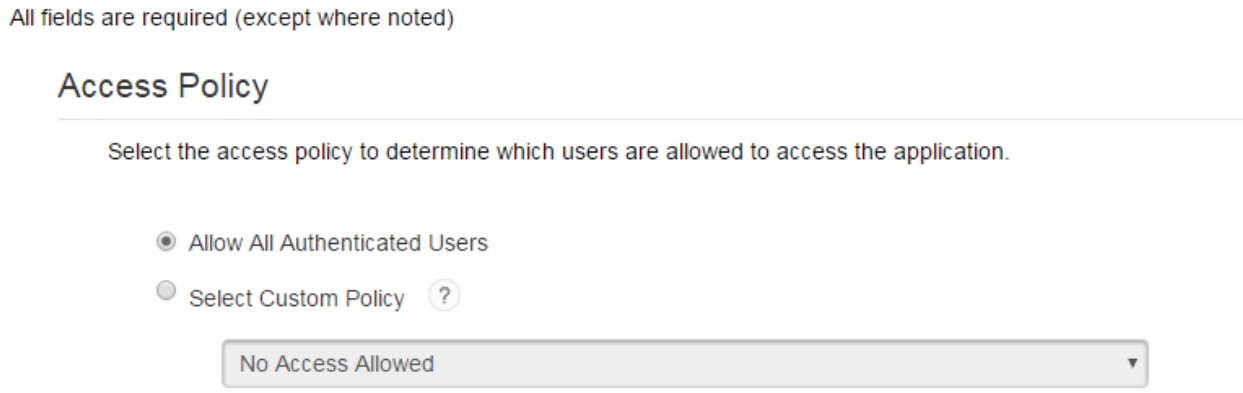


14. Select **Show Advanced Configuration.**

15. In the **Attribute Extension** section, add **fName**, **lName**. These are mandatory provisioning attributes which need to be forwarded at the time of SSO.

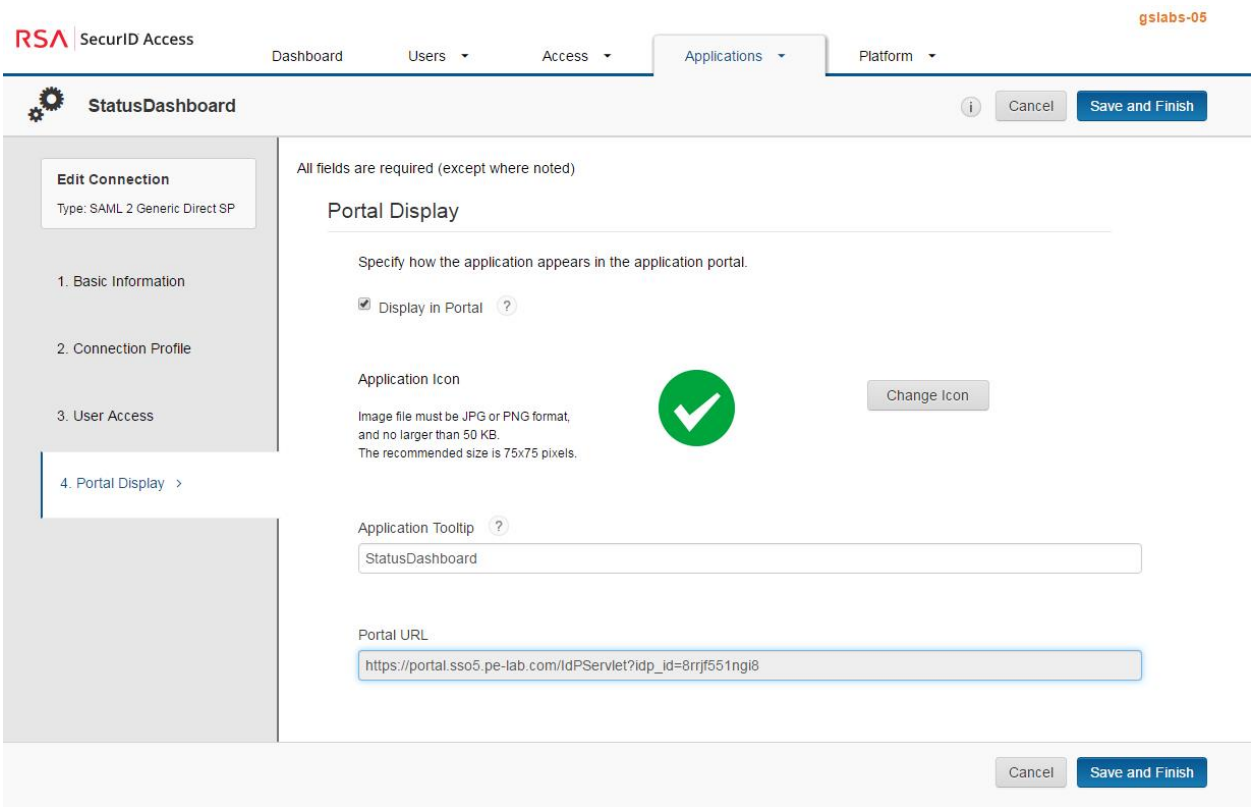


16. Click the **Next Step** button.
17. On the **User Access** page, select the access policy the identity router will use to determine which users can access the StatusDashboard service provider from the portal. If you want to allow access to all users who are signed in to the portal, select the **Allow 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.

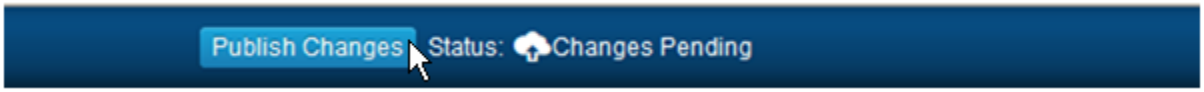


18. Click the **Next Step** button.

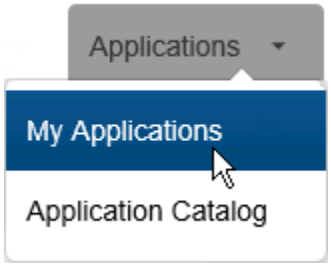
19. Select the **Display in Portal** checkbox on the **Portal Display** page.
20. Enter descriptive text about the application in the **Application Tooltip** field. The portal will display this text when a user passes the cursor over the application's icon.
21. Click the **Save and Finish** button.



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



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



24. Search for *StatusDashboard* 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 StatusDashboard to Use RSA SecurID Access as an Identity Provider

Follow below steps to configure StatusDashboard as service provider.

1. Send RSA SecurID IdP metadata file to support@statusdashboard.com.
2. Their support team will enable SAML integration for your account using the metadata file.

MD