RSA SecurID Access SAML Configuration for Weekdone

Last Modified: August 29, 2016

Weekdone is an internal communication service for teams founded in 2012 that is based in Tartu, Estonia. It enables the OKR goal-setting and Progress, plans, problems weekly reporting methodologies.

Before You Begin

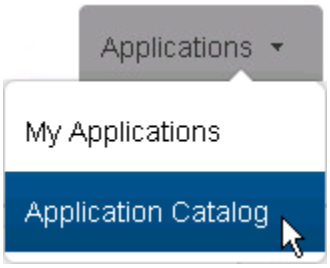
- Acquire an administrator account to both RSA SecurID Access and Weekdone.
- Configure a target application for your Weekdone service provider.
  Note: The ACL URL is configurable at the end point and the steps to configure it is explained in the document further.

Procedure

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

Add the Application in RSA SecurID Access

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 *Weekdone* in the list of applications and click the **+Add** button.

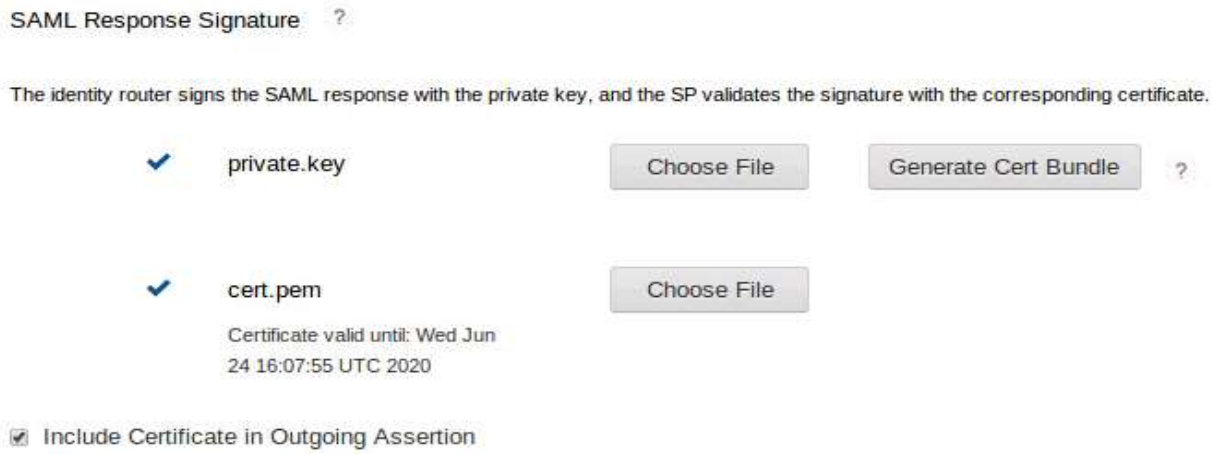
3. Enter a name for the application in the **Name** field on the **Basic Information** page and click the **Next Step** button.

4. In the **Initiate SAML Workflow** section, add the **Connection URL** as shown.

5. Scroll to the **SAML Identity Provider (Issuer)** section on the **Connection Profile** page and copy the auto-generated URL from the **Identity Provider URL** field.

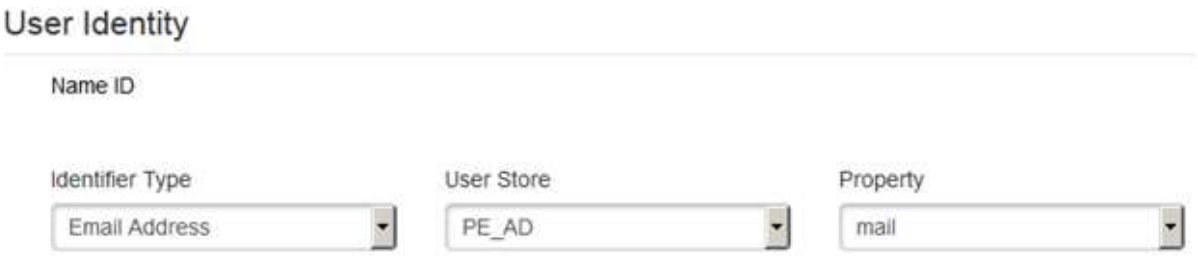
6. You will need to import a private/public key pair to sign and validate SAML assertions. If you don't have one readily available, follow the steps to generate a certificate bundle. Otherwise, continue to step 6.

    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 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.
7. Click the **Choose File** button 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.



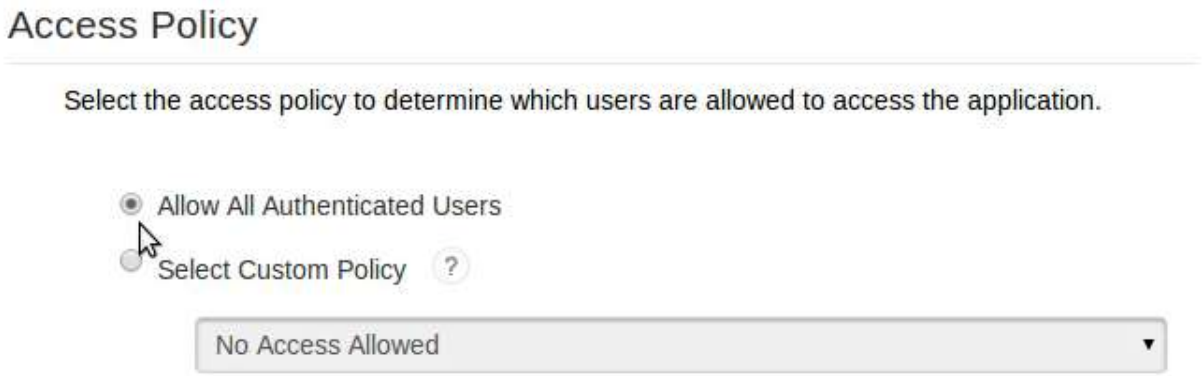
10. Scroll to the **Service Provider** section and enter your SAML name in the **Assertion Consumer Service (ACS) URL** field. If you haven't configured the service provider and do not know your SAML name then, you can give any name of your choice that would represent your company.
11. Do not change the **Audience (Service Provider Entity ID)** field.

12. Scroll to the **User Identity** section and select the format of the SAML assertion NameID from the **Identifier Type** dropdown list. In this example, a SAML assertion will present a NameID value in the form of an email.
13. 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.



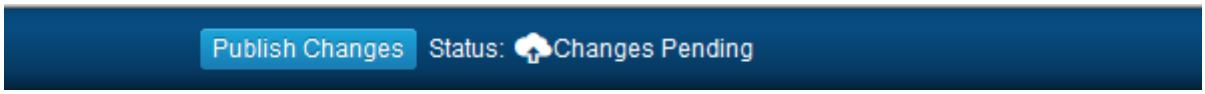
15. Click the **Next Step** button.

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



17. Click the **Next Step** button.
18. Select the **Display in Portal** checkbox on the **Portal Display** page.
19. 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.
20. Click the **Save and Finish** button.

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

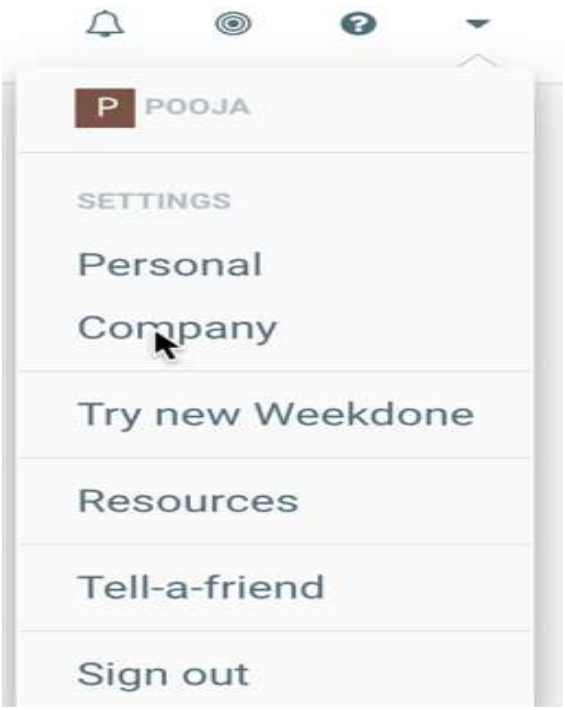


Configure Weekdone to Use RSA SecurID Access as an Identity Provider

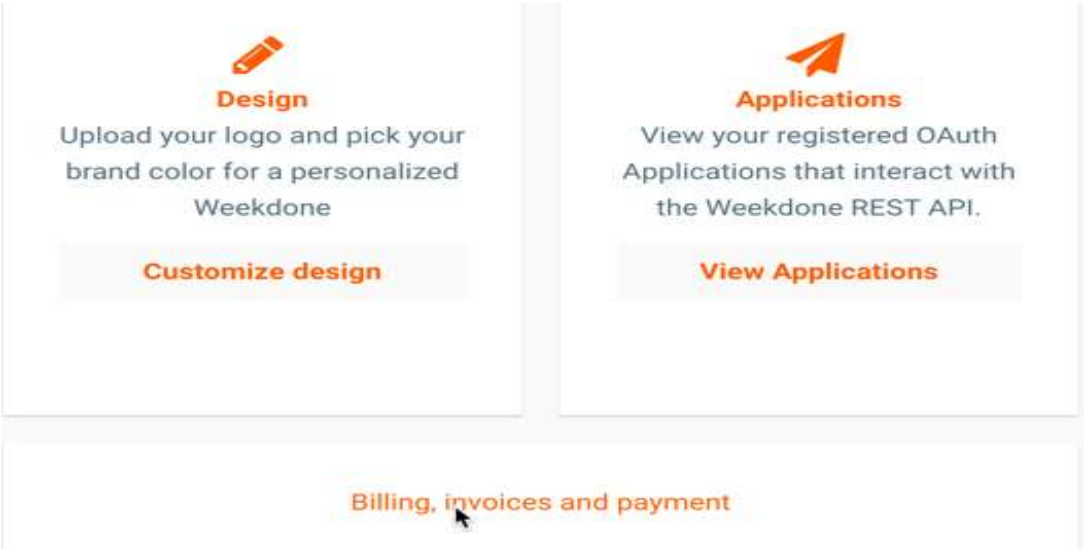
Follow below steps to configure Weekdone to accept SAML assertions.

1. Log in to the Weekdone console on the Domain (https://weekdone.com/).
2. Select the dropdown option in right extreme for more options and click it.

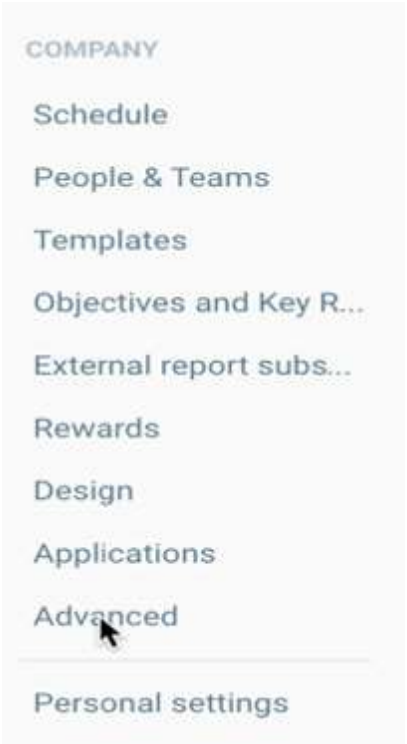
3. Choose the **Company** option.



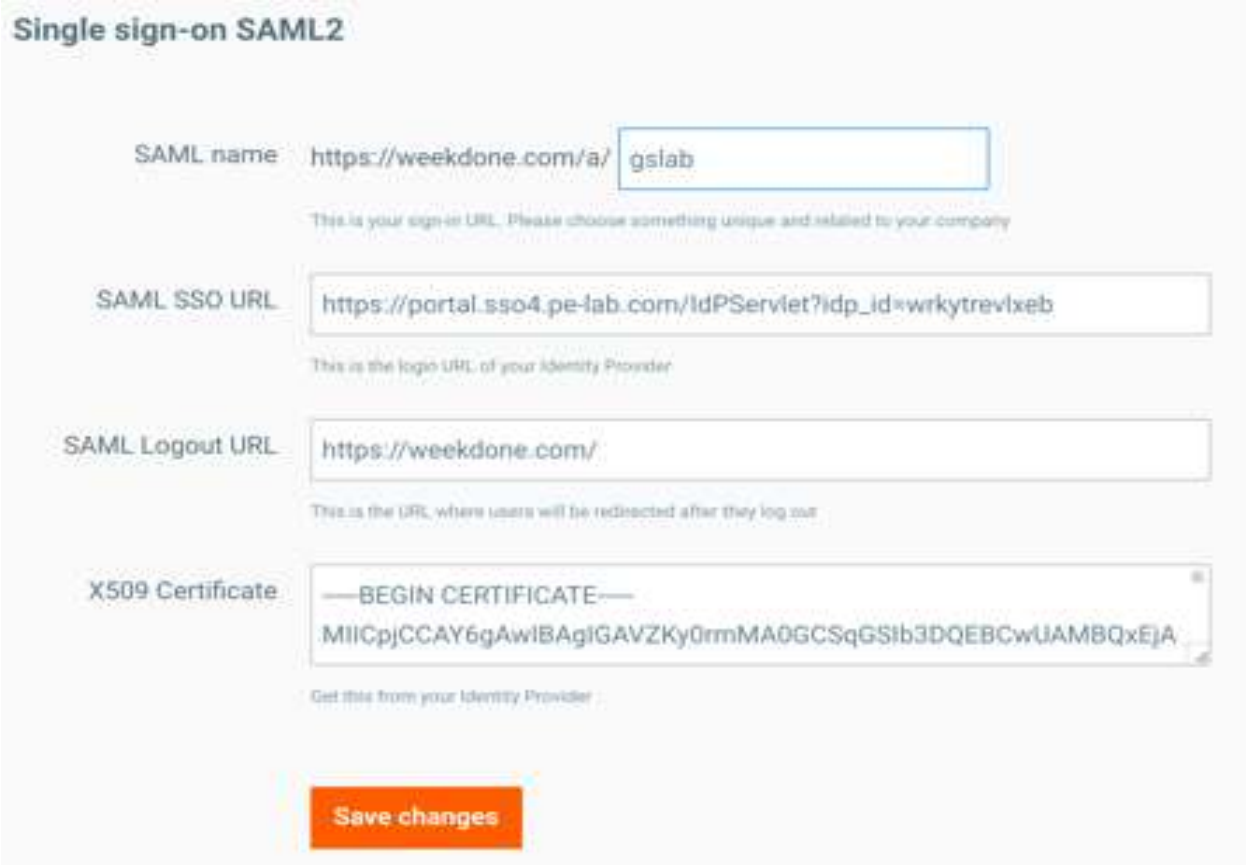
4. Select **Billing, invoices and payment** option at the right bottom.



5. Select the **Advanced** options from the left panel.



6. After following step 5, you will land on the page that looks like this.



On this page you need to enter the following details:

- The SAML name is the name that you mentioned in the Admin Configuration in Step 8. In our example we have SAML name as "gslab".
- SAML SSO URL is the IDP URL that was self generated by the admin and you copied it in step 4.
- The SAML Logout URL will be the URL that you want to land on when the user clicks logout. Preferably this URL should be logout page of endpoint. Hence we have configured it https://weekdone.com.
- X509 Certificate is the same certificate that was loaded into the Admin when we configured Weekdone.

7. Click on save Changes and exit the portal.