RSA SecurID Access SAML Configuration for Replicon

Last Modified: April 23, 2015

Replicon offers the leading hassle-free web timesheet software to track employee time, project time and expenses, streamlining attendance, payroll and billing.

Before You Begin

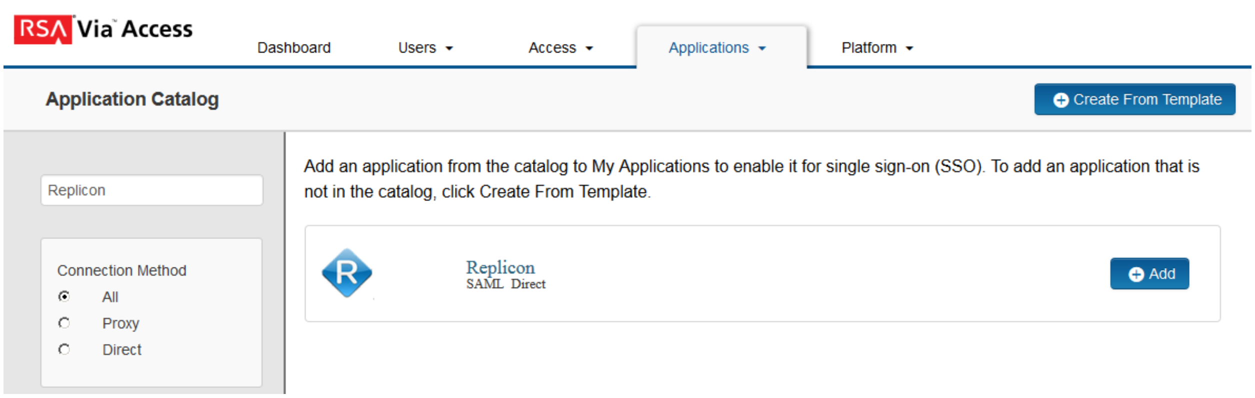
- Acquire an administrator account to both RSA SecurID Access and Replicon.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

Procedure

Add the Application in RSA SecurID Access

Procedure

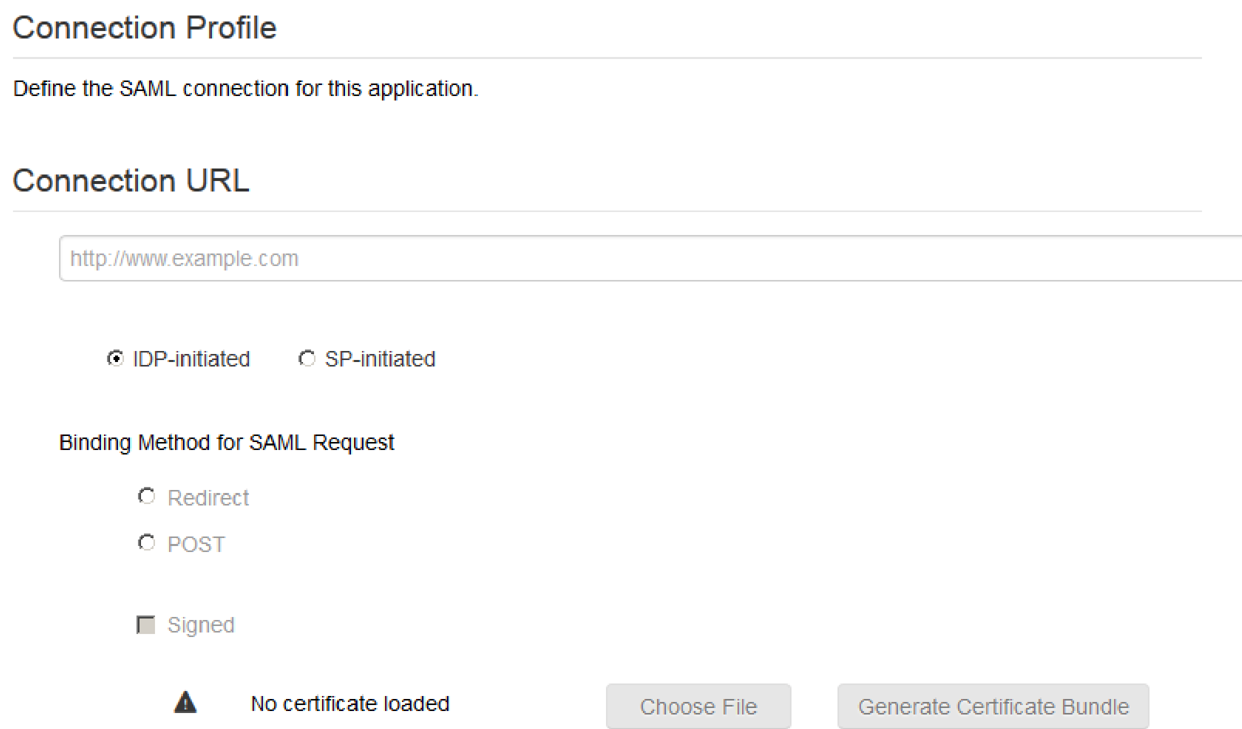
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, search for Replicon and click **+Add**.



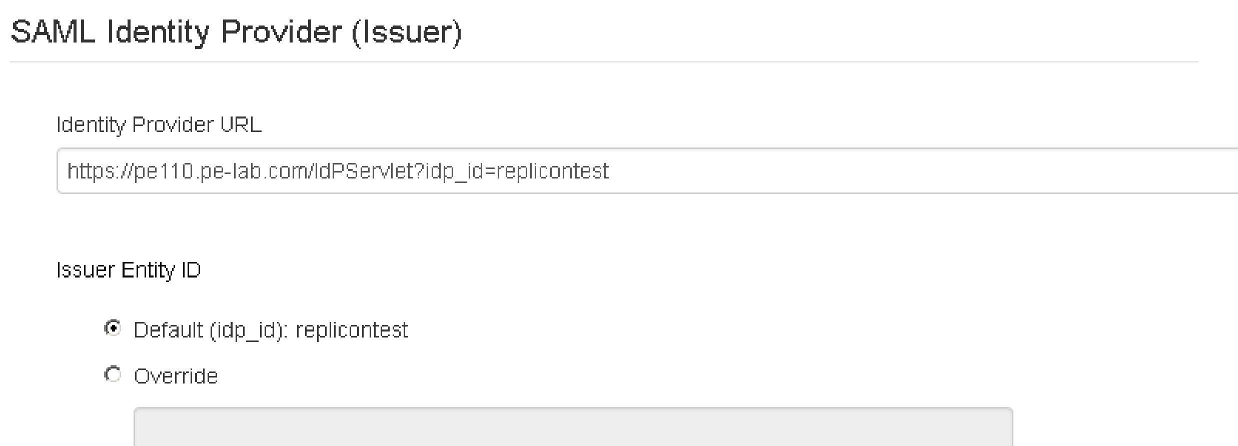
3. On the Basic Information page, specify the application name and click **Next Step**.

Note: Replicon only supports single sign-on IDP-initiated sessions.

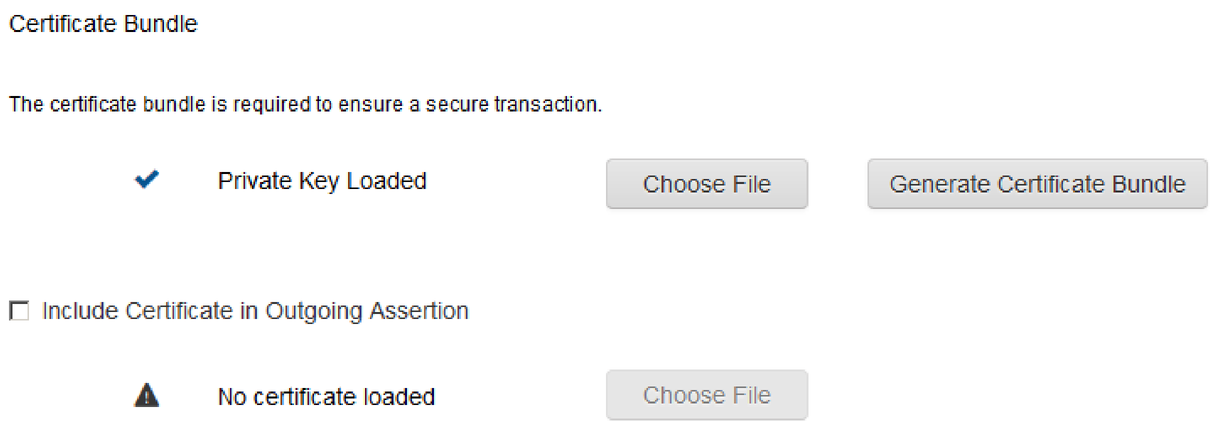
4. On the Connection Profile page, leave the URL blank and select **IDP -initiated**.



5. Scroll down to **SAML Identity Provider (Issuer)** section.
6. Take note of the Issuer Entity ID it will be needed to create the RSA SecurID Access metadata file.

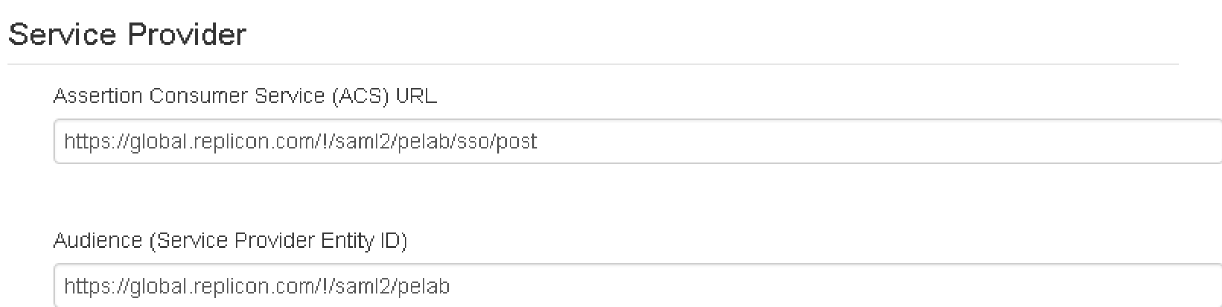


7. Click **Choose File** and upload the private key.



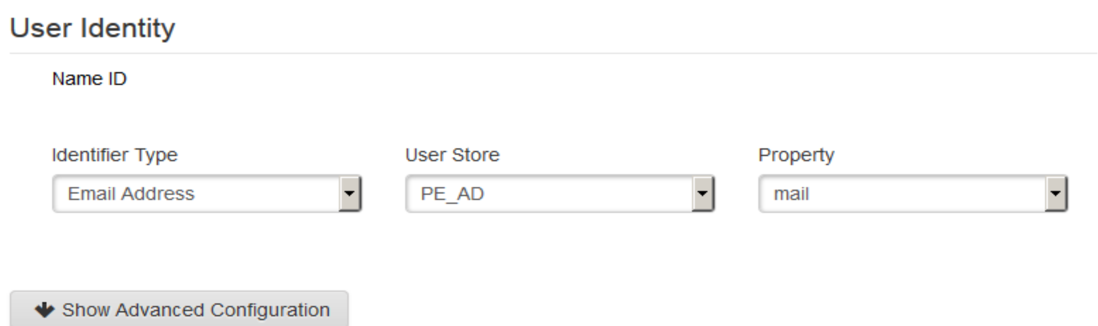
8. Scroll down to the **Service Provider** section.

> **Note: Obtain the ACS URL and the Service Provider Entity ID from the Replicon metadata file at https://global.replicon.com/!/saml2/<yourCompanyID>.**

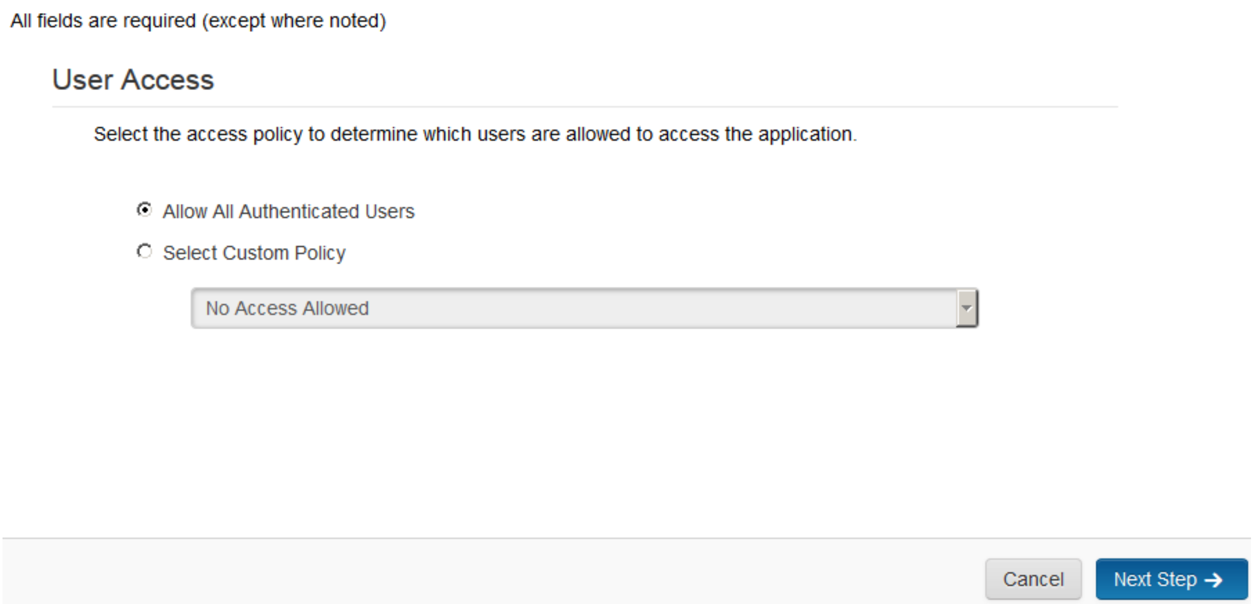


   a. In the **Assertion Consumer Service (ACS) URL** field, enter https://global.replicon.com/!/saml2/<your_companyID>/sso/post
   b. In the **Audience (Service Provider Entity ID)** field, enter https://global.replicon.com/!/saml2/<your_companyID>.

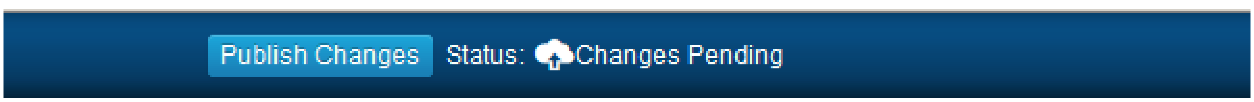
9. Scroll down to the **User Identity** section. Set the **Identifier Type** to **Email Address** and **Property** to **mail**.



10. Click **Next Step**.
11. On the **User Access** page, select the desired user policy from the drop down list.



12. Click **Next Step**.
13. On the Portal Display page, select **Display in Portal**.
14. Click **Save and Finish**.
15. Click **Publish Changes**. Your application is now enabled for SSO.



Create the RSA SecurID Access Metadata file

1. Modify the example below with your environment information.
2. When inserting the cert.pem file do not include the -----BEGIN CERTIFICATE---- and ----END CERTIFICATE----lines.

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<EntityDescriptor xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
    xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
    entityID="CHANGEME_TO_CONNECTOR_IDP_ENTITY_ID">
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <!-- public saml cert -->
          <ds:X509Certificate>CHANGEME_TO_PUBLIC_SAML_CERT_CONTENT</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>

    <!-- Supported Name Identifier Formats -->
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</NameIDFormat>

    <!-- POST binding and location=idp url -->
    <SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="CHANGEME_TO_IDP_URL" />

  </IDPSSODescriptor>
</EntityDescriptor>
```

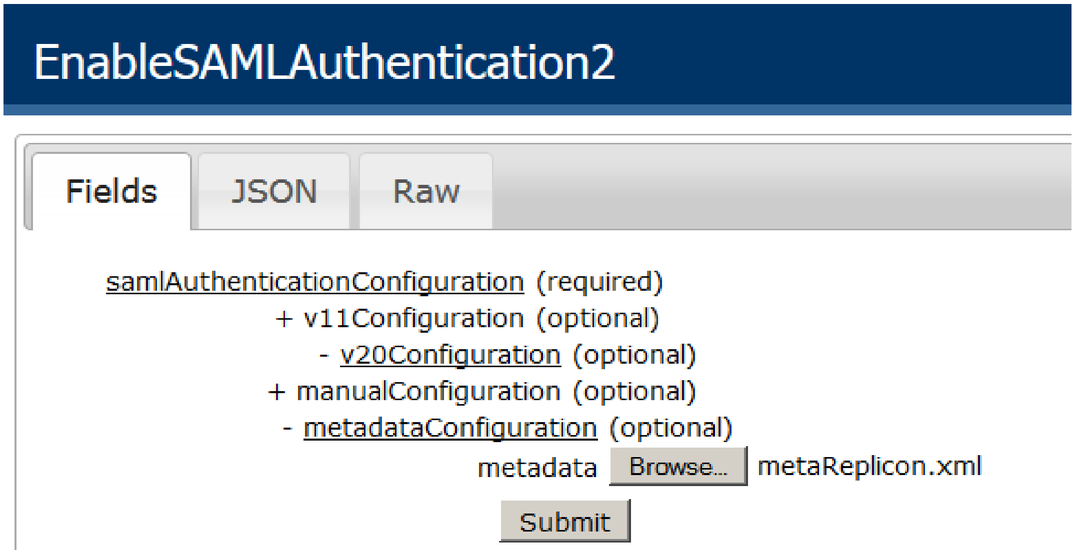
Next Steps

Configure Replicon to Use RSA SecurID Access as an Identity Provider

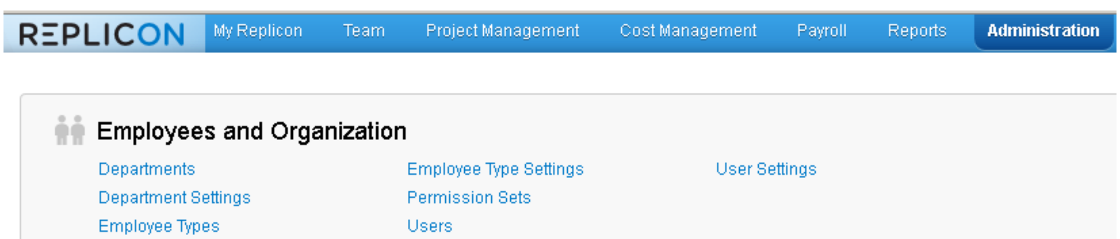
Configure Replicon to Use RSA SecurID Access as an Identity Provider

Procedure

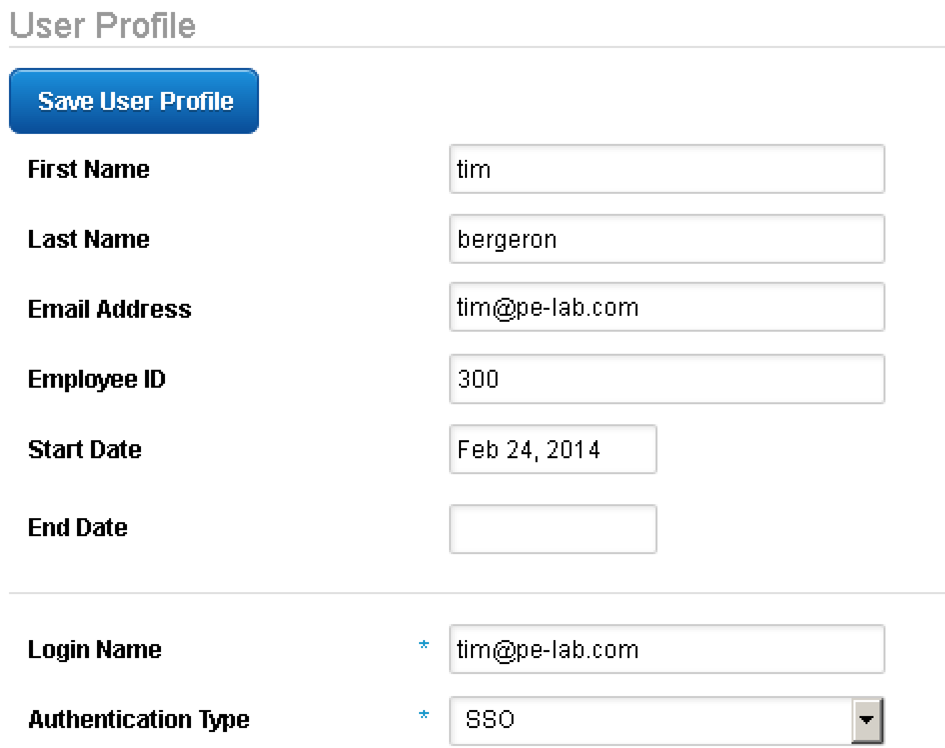
1. Browse to https://na2.replicon.com/<your_company_ID>/services/SecurityService1.svc/help/test/EnableSAMLAuthentication2



2. Expand **+v20Configuration**.
3. Expand **+metadataConfiguration**.
4. Select **Browse** and choice the RSA SecurID Access metadata file.
5. Click **Submit**.
6. Login to Replicon with your administrator account. https://na2.replicon.com
7. Go to **Administration** > **Employees and Organization** > **Users**.



8. Select a user to edit.
9. Enter user's email address in the Login Name field.
10. From the **Authentication Type** field pull down, select **SSO**.



11. Click **Save User Profile.**

GLS