RSA SecurID Access SAML Configuration for Concur

Last Modified: March 26, 2015

Concur is a leading provider of integrated travel and expense management solutions.

Before You Begin

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

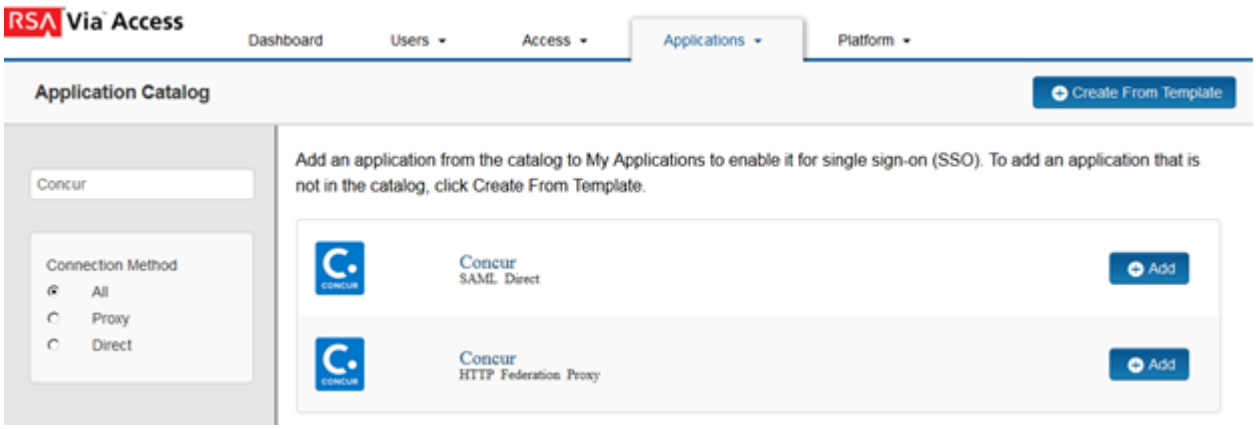
Procedure

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

Add the Application in RSA SecurID Access

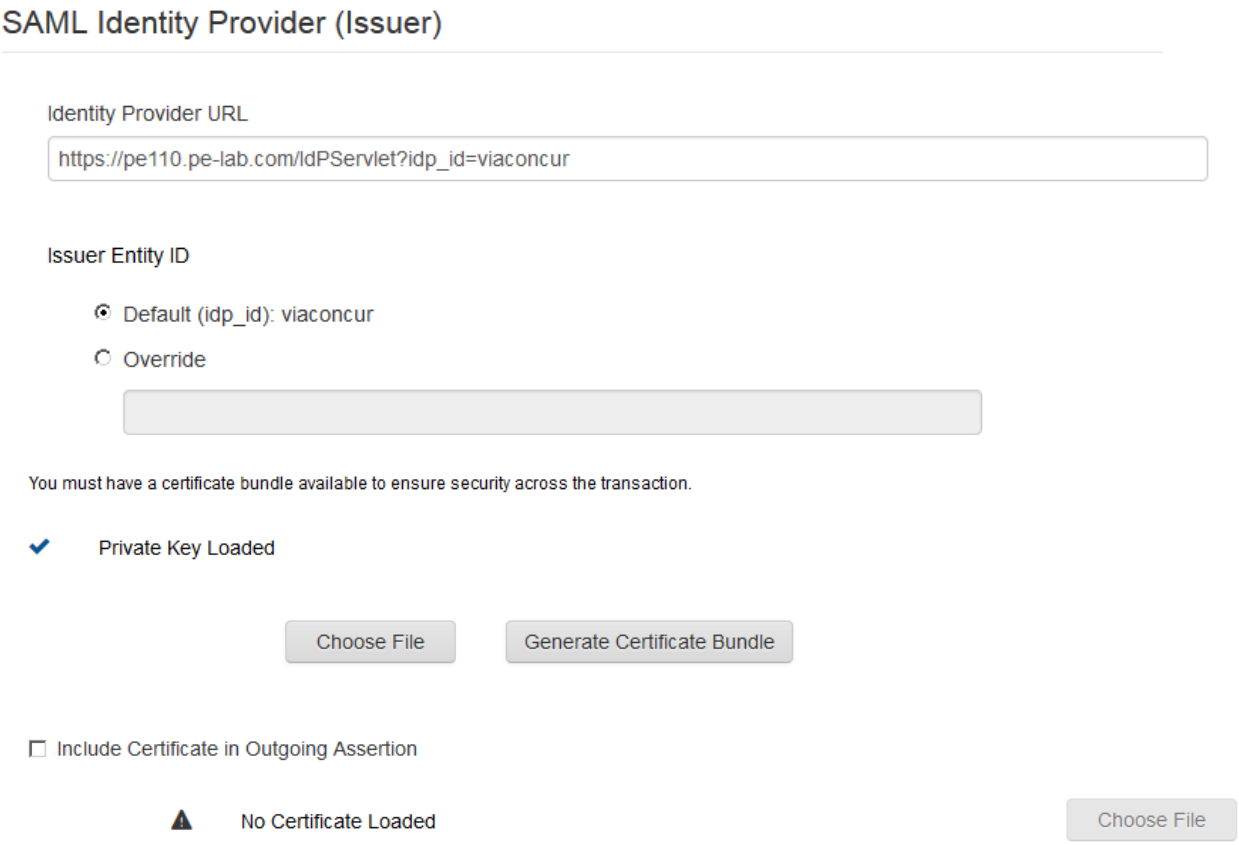
Procedure

1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, select Concur SAML Direct and click **+Add**.

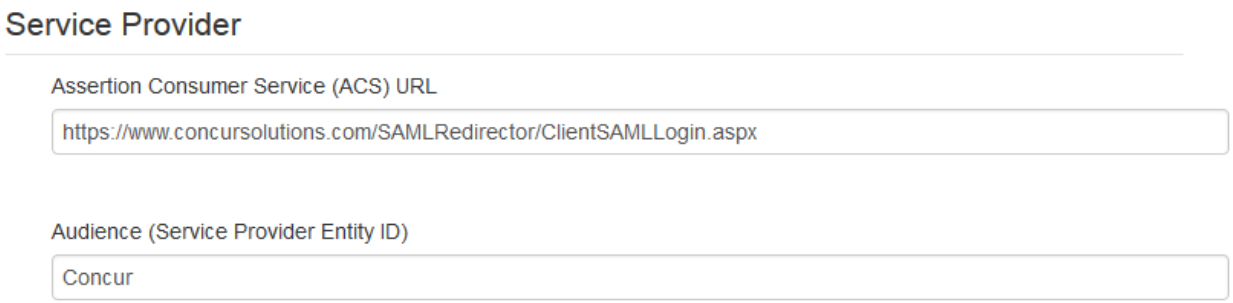


3. On the Basic Information page, specify the application name and click **Next Step**.
4. In the Connection URL section, select **IDP -initiated**.

5. Scroll down to the **SAML Identity Provider (Issuer)** section.
6. Click **Choose File** and upload the private key.

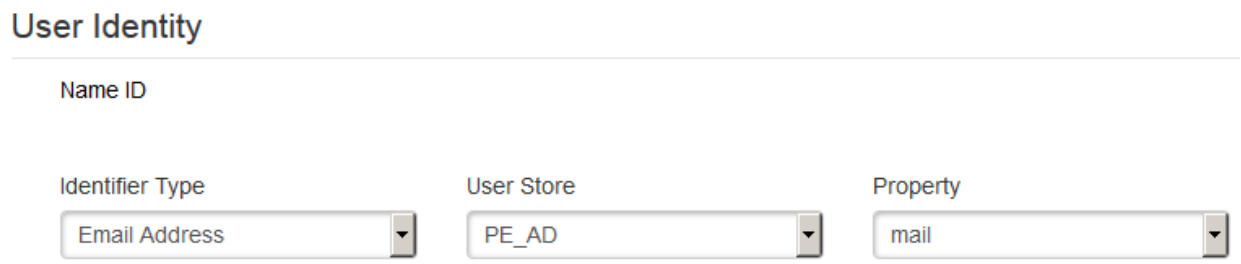


7. Scroll down to the **Service Provider** section.



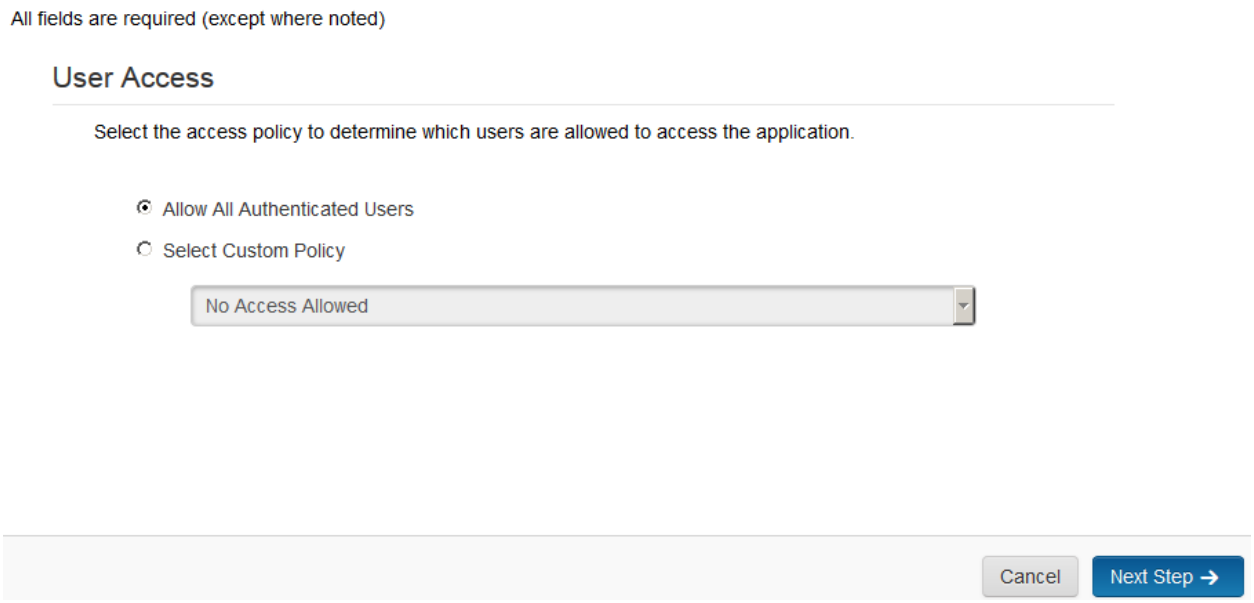
   a. In the **Assertion Consumer Service (ACS) URL** field, enter https://www.concursolutions.com/SAMLRedirector/ClientSAMLLogin.aspx
   b. In the **Audience (Service Provider Entity ID)** field, enter Concur.

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

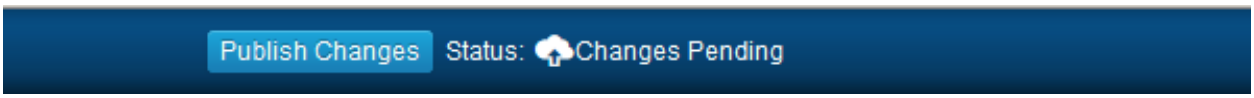


9. Click **Next Step**.

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



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



Create the RSA SecurID Access Metadata file

1. Modify the XML file below with your environment information.
2. Make changes to the sections in yellow.
3. 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>
```

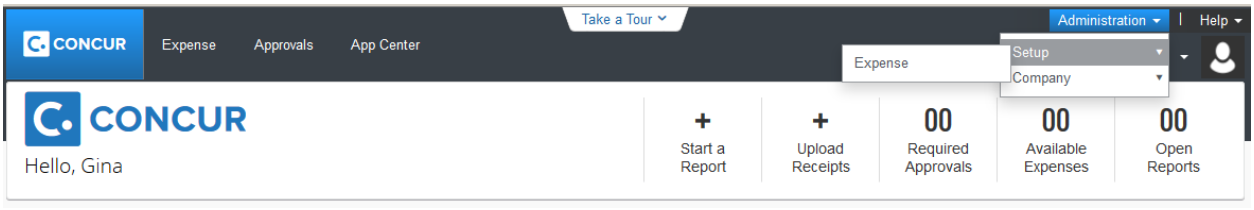
Next Steps

Configure Concur to Use RSA SecurID Access as an Identity Provider

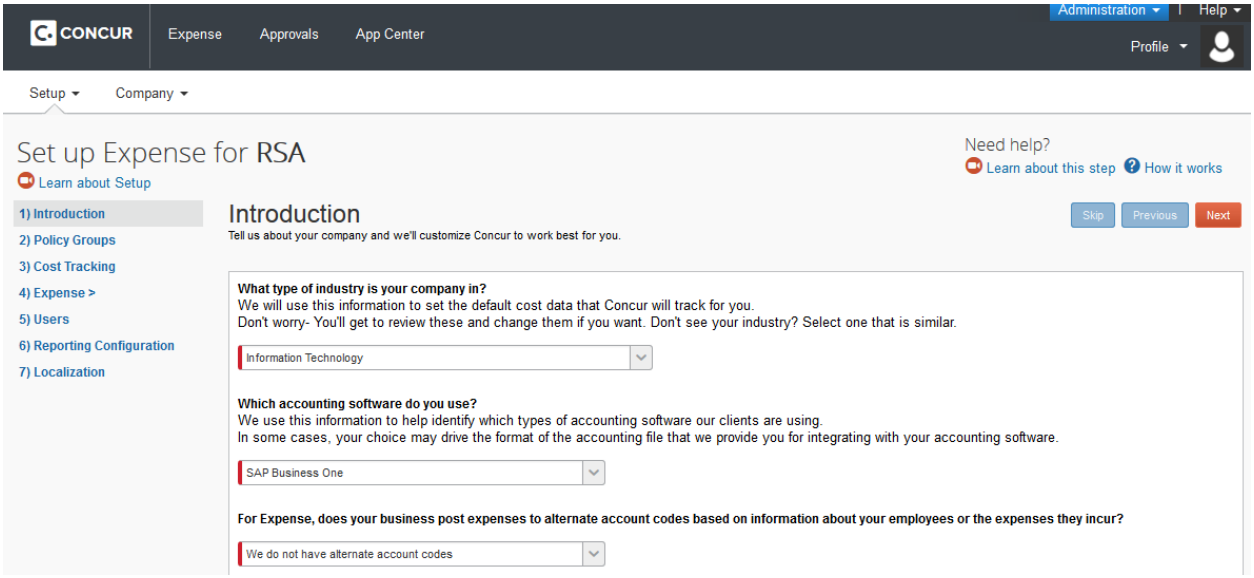
Configure Concur to Use RSA SecurID Access as an Identity Provider

Procedure

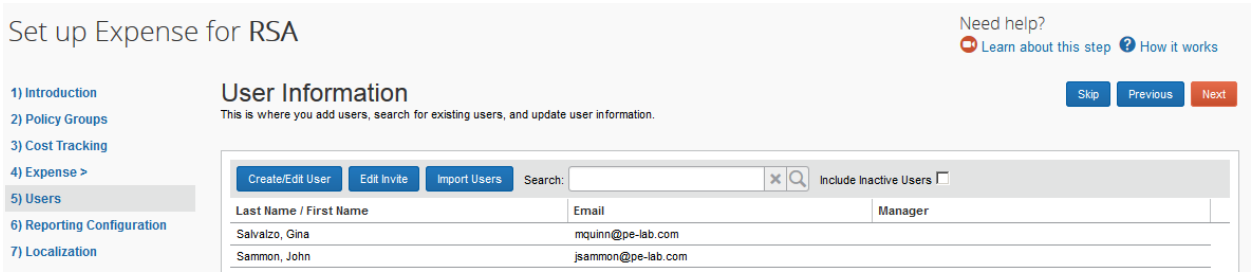
1. Contact Concur and provide them the RSA SecurID Access metadata file.
2. Once Concur has uploaded your metadata file login as an administrator and add your users.



3. Navigate to **Administration > Setup > Expense**.
4. Complete the setup steps to configure your Expense configuration.



5. On step 5, click **Create/Edit User** and add your users.



6. You are now configured for Single Sign-on.
7. Login to the RSA SecurID Access portal and select the Concur App.

GLS