RSA SecurID Access SAML Configuration for NetSuite

Last Modified: April 15, 2015

NetSuite offer a cloud base business management solution. NetSuite combines complete customer-facing CRM and Ecommerce capabilities with back-office Accounting/ERP and self-service portals for partners.

Before You Begin

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

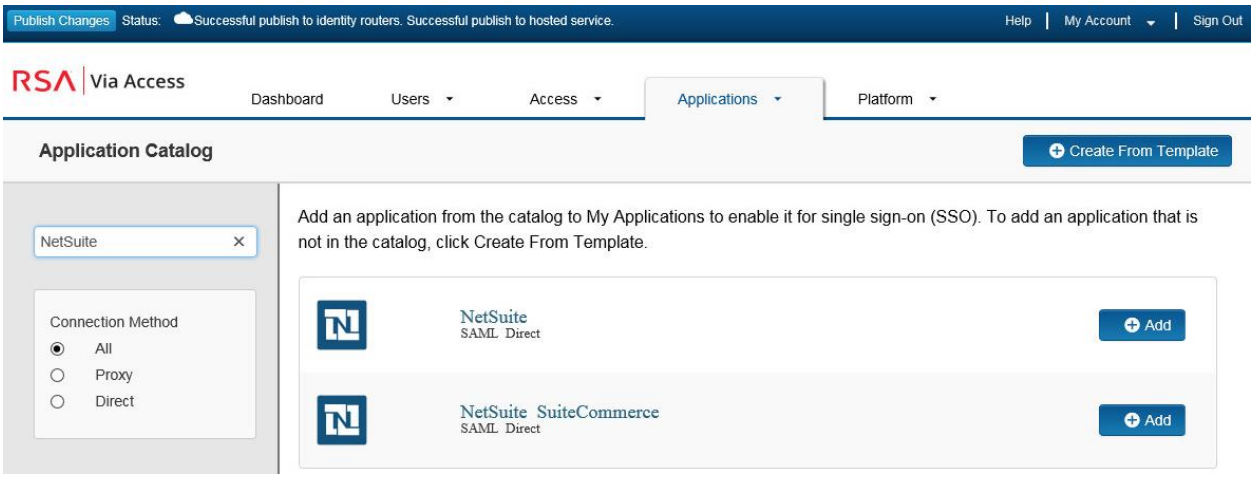
Procedure

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

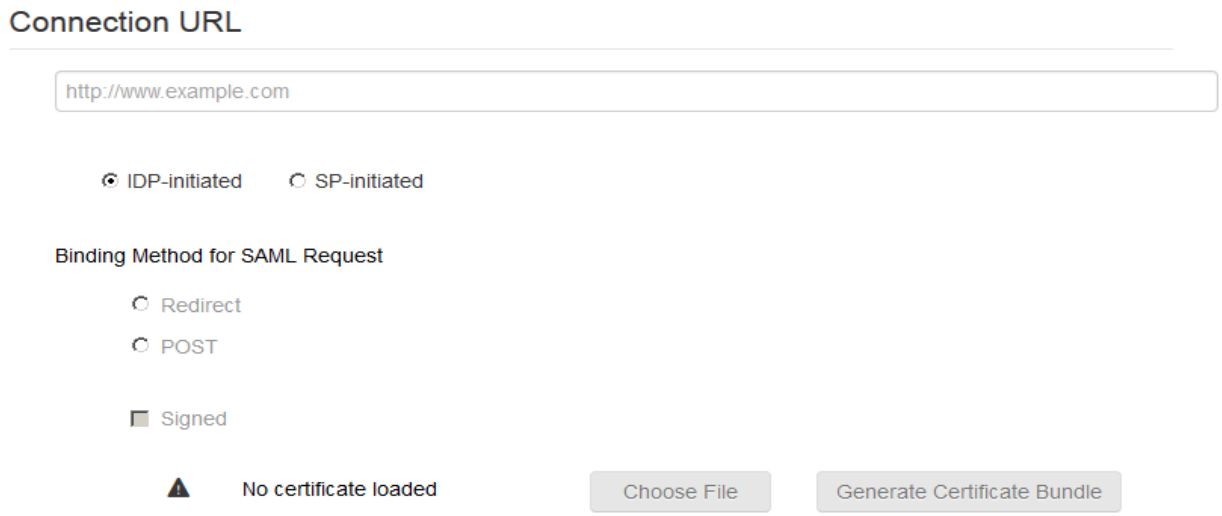
Add the Application in RSA SecurID Access

Procedure

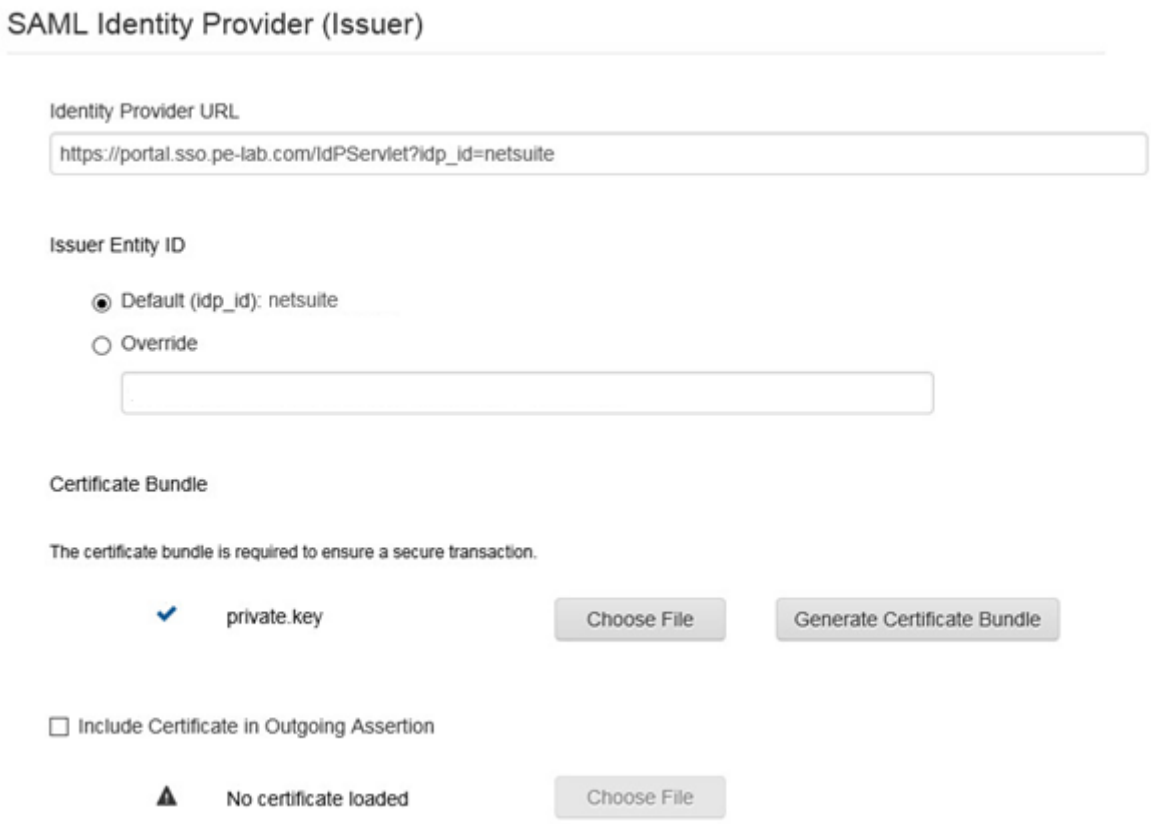
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** for the SAML application that you wish to add.



3. On the Basic Information page, specify the application name and click **Next Step**.
4. On the Connection Profile page, choose **IDP –initiated** and leave the URL blank.



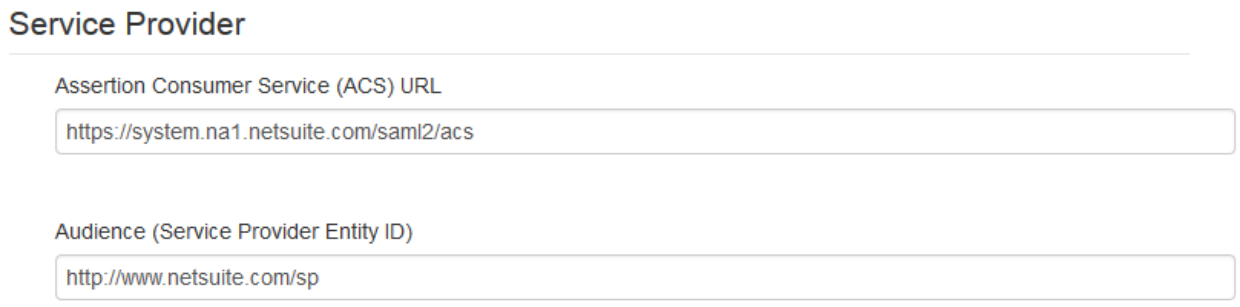
5. Scroll down to the **SAML Identity Provider (Issuer)** section.



   a. In the **Identity Provider URL** field, copy the URL which will be needed later to configure the NetSuite.
   b. Select **Choose File** and upload the private key.

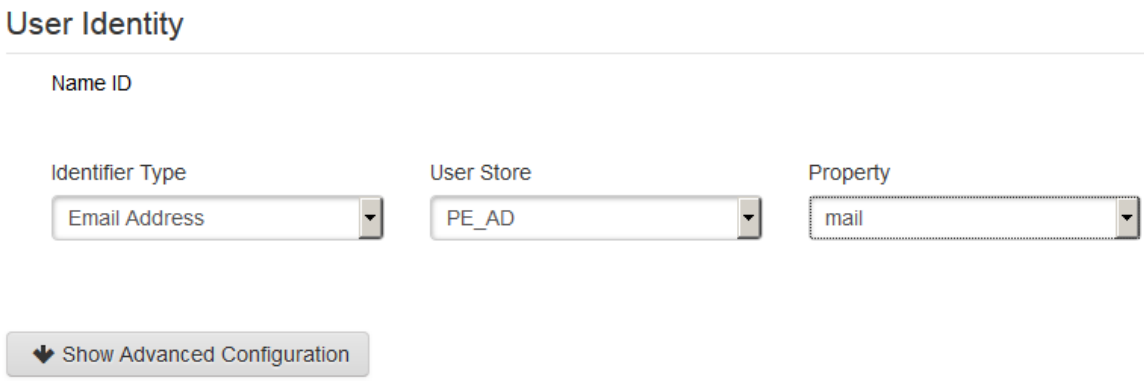
6. Scroll down to the **Service Provider** section.

> **Note: Refer to your NetSuite metadata file for your specific ACS URL and Service Provider Entity ID for these values may vary if you are hosted in a different data center.**

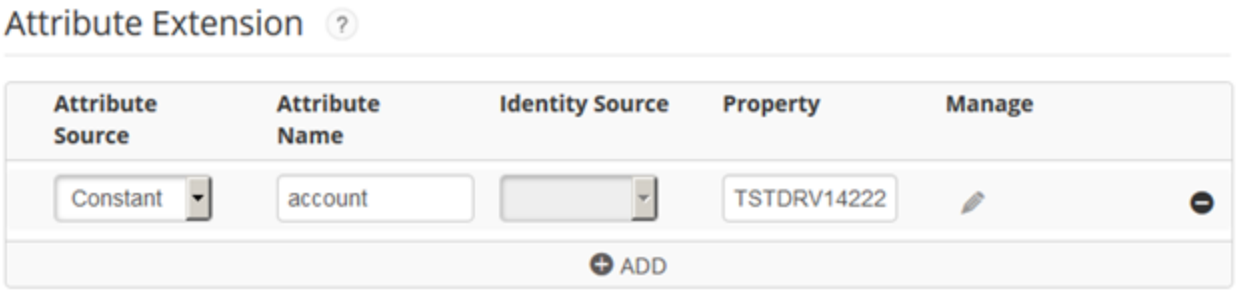


   a. In the **Assertion Consumer Service (ACS) URL** field, enter https://system.na1.netsuite.com/saml2/acs
   b. In the **Audience (Service Provider Entity ID)** field, enter http://www.netsuite.com/sp

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

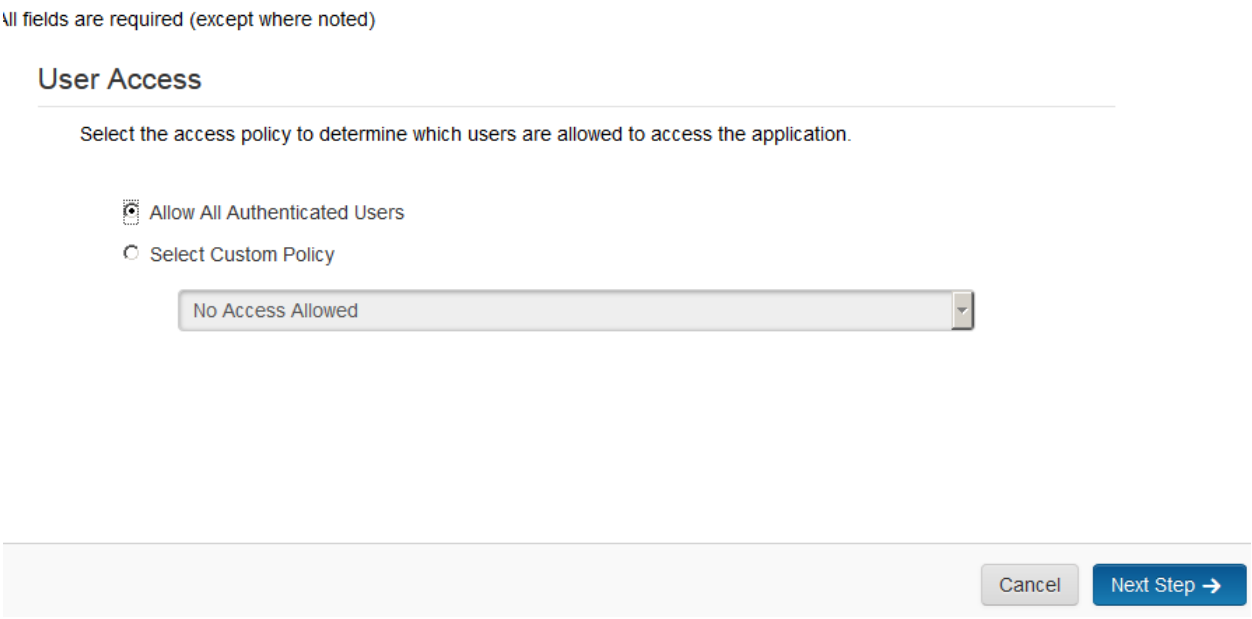


8. Click **Show Advanced Configuration** and scroll down to **Attribute Extension.**
9. Select **User Store** from the **Attribute Source** pulldown list.
10. Enter the attribute name **account** mapped to your account ID found on page 6 step 2.

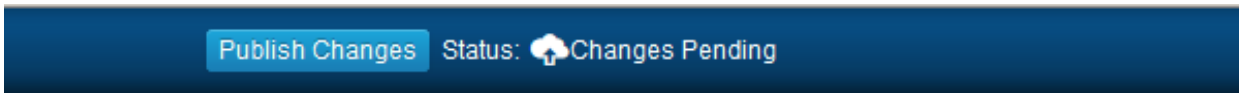


11. Click **Next Step**.

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



13. Click **Next Step**.
14. On the **Portal Display** page, select **Display in Portal**.
15. Click **Save and Finish**.
16. 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="CHANGE_ME_TO_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>CHANGE_ME_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="CHANGE_ME_TO_IDP_URL"/>

   <!-- Extended Attributes -->
     <Attribute
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      account="telephoneNumber">
      </Attribute>

 </IDPSSODescriptor>
</EntityDescriptor>
```

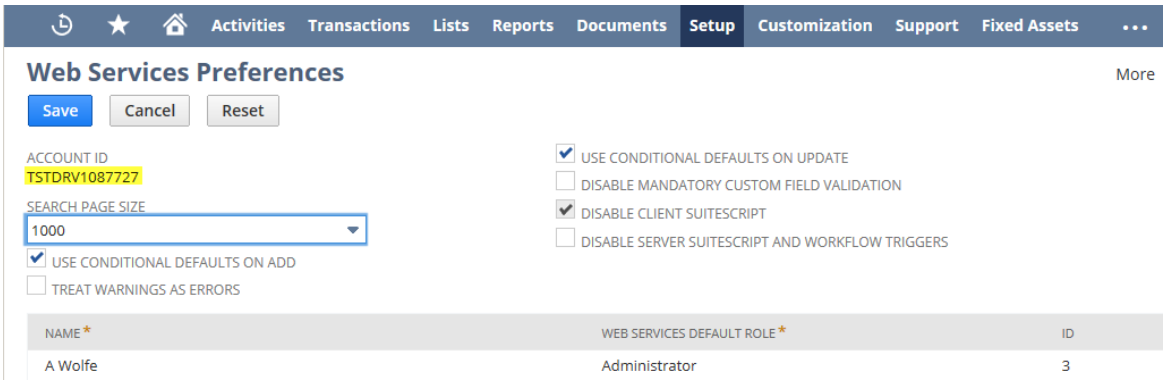
Next Steps

Configure NetSuite to Use RSA SecurID Access as an Identity Provider

Configure NetSuite to Use RSA SecurID Access as an Identity Provider

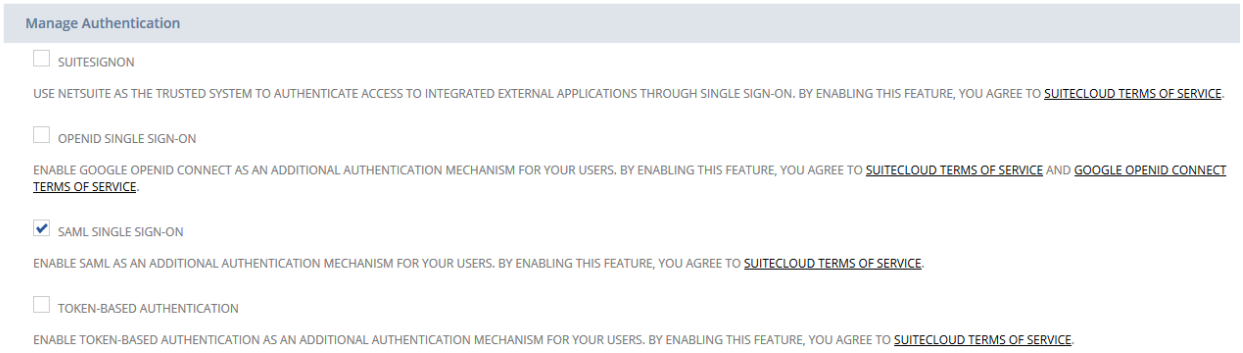
Procedure

1. Login into the NetSuite administration console; https://system.NetSuite.com/pages/login.jsp
2. Locate your Account ID by navigating to **Setup > Integration > Web Services Preferences**.



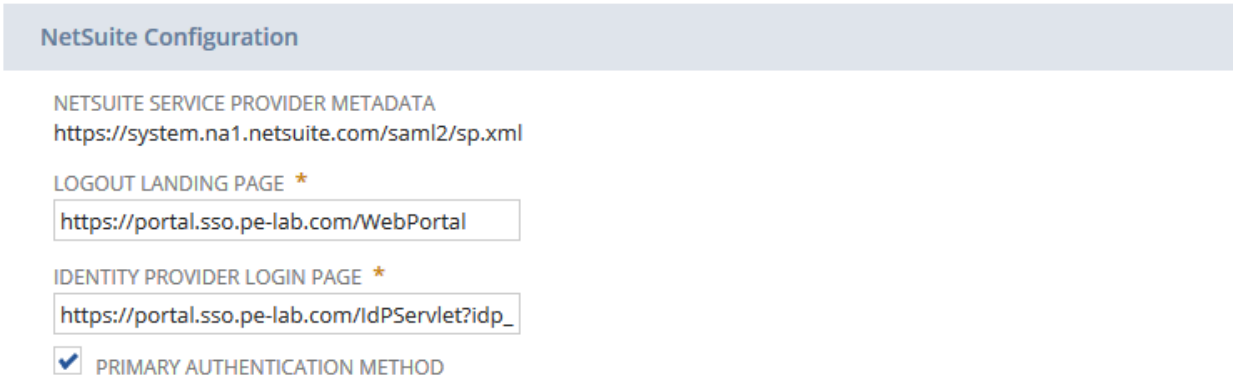
3. To enable SAML single sign-on, navigate to **Setup > Company > Enable Features**.
4. Select the **SuiteCloud** tab.

5. Scroll down to Manage Authentication section and check **SAML SINGLE SIGN-ON**.

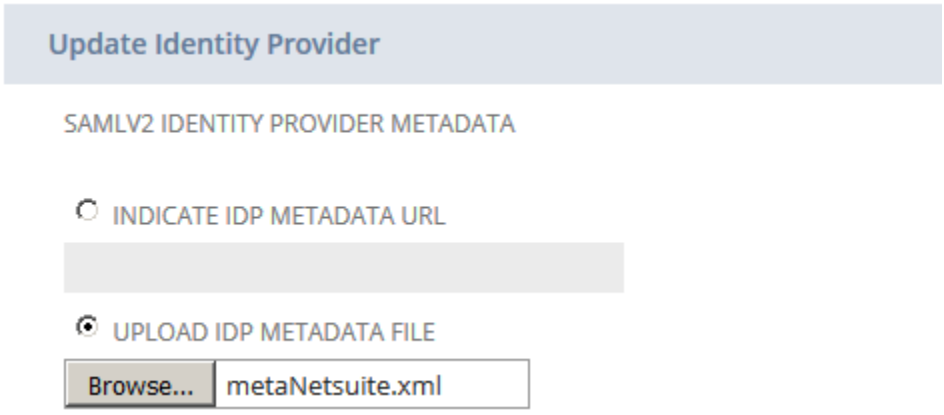


6. Click **Save**.

7. Navigate to **Setup >Integration > SAML Single Sign-on**.
8. Under the NetSuite Configuration section, enter the **LOGOUT LANDING PAGE** and the **IDENTITY PROVIDER LOGIN PAGE** urls.
9. Check the **PRIMARY AUTHENTICATION METHOD** box.



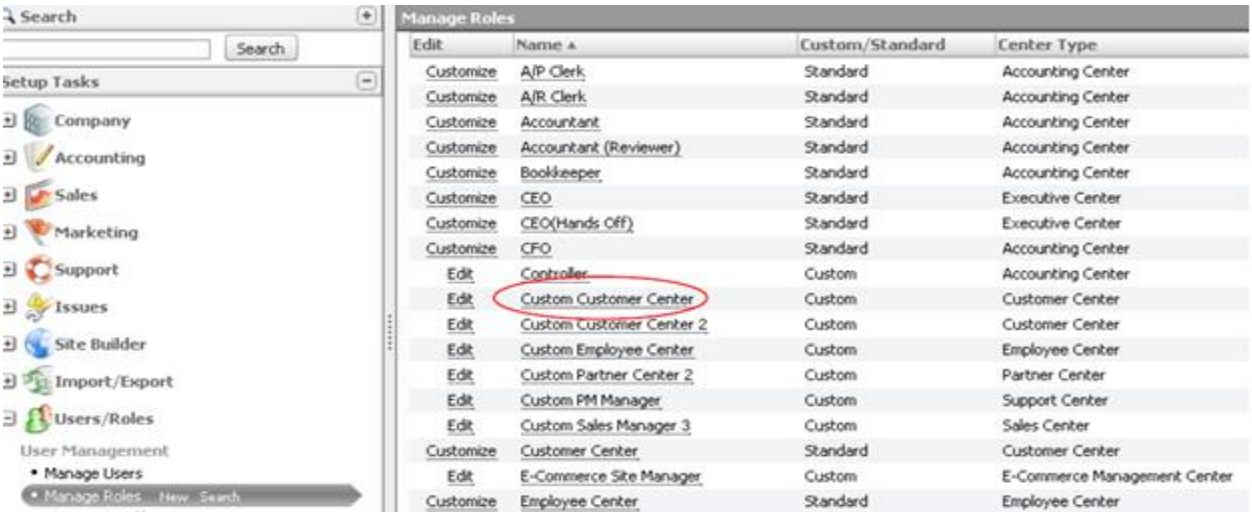
10. Under the Update Identity Provider section, upload the RSA SecurID Access metadata file.



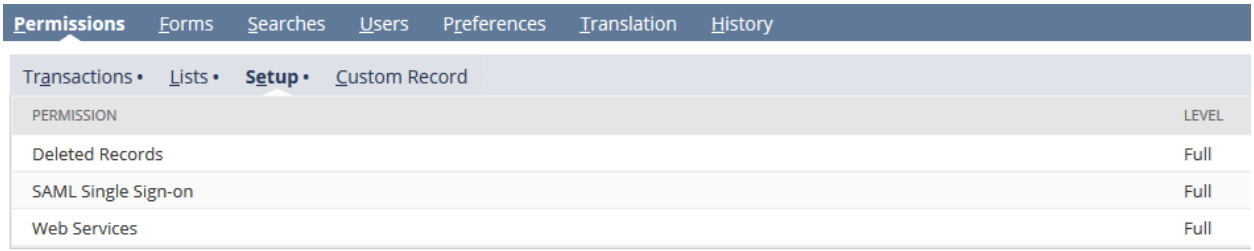
11. Click **Submit**.

Add SAML Permissions to Role

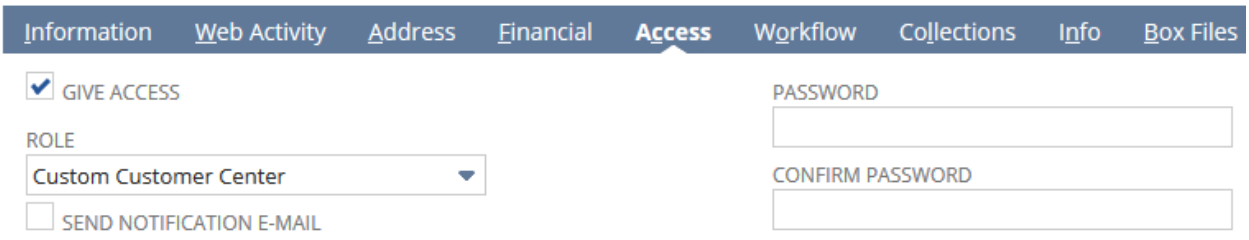
1. Navigate to **Setup > Users/Roles > Manage Roles**.
2. Edit the user's roles you wish to enable single sign-on for.



3. Under Permissions click **Setup**.
4. Set the level of **SAML Single Sign-on** to **Full**.



5. Navigate to **Setup > Users/Roles > Manage Users**.
6. Select the *User* and click **Edit**.
7. Under the **Access** tab, click **Roles**.
8. Add the role to the user.



9. Click **SAVE**.

GLS