

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.

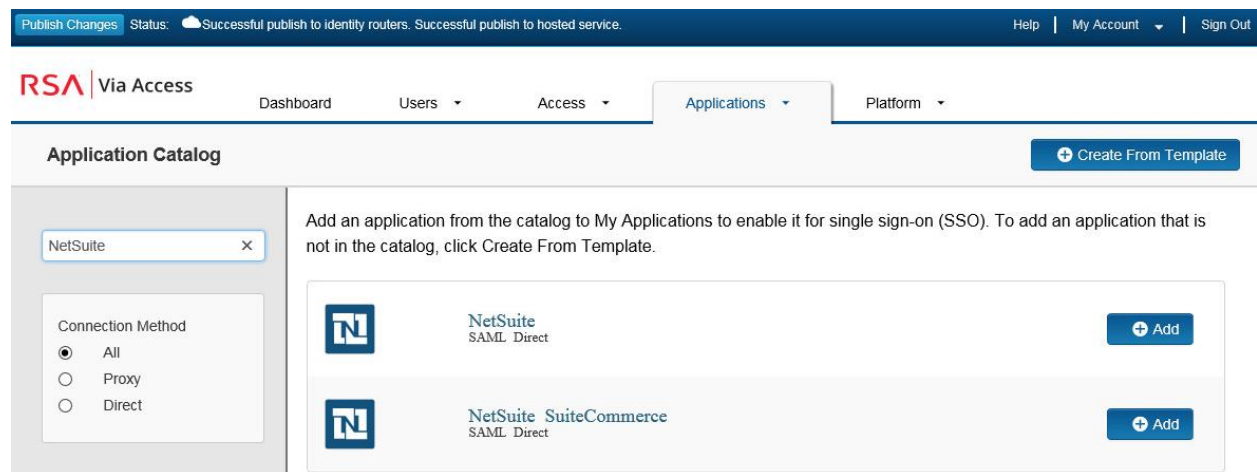
Procedure

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.

Connection URL


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed

 No certificate loaded

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

SAML Identity Provider (Issuer)

Identity Provider URL

Issuer Entity ID

Default (idp_id): netsuite


Override

Certificate Bundle

The certificate bundle is required to ensure a secure transaction.


private.key

Include Certificate in Outgoing Assertion

 No certificate loaded

- 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.

Service Provider

Assertion Consumer Service (ACS) URL

Audience (Service Provider Entity ID)

- 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**.

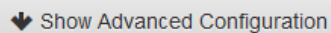
User Identity

Name ID

Identifier Type




User Store

Property



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.

Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
<input type="text" value="Constant"/>	<input type="text" value="account"/>	<input type="text"/>	<input type="text" value="TSTDRV14222"/>	 
 ADD				

11. Click **Next Step**.

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

All fields are required (except where noted)

User Access

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy

No Access Allowed

Cancel

Next Step →


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.

Publish Changes

Status:  Changes Pending

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>
```

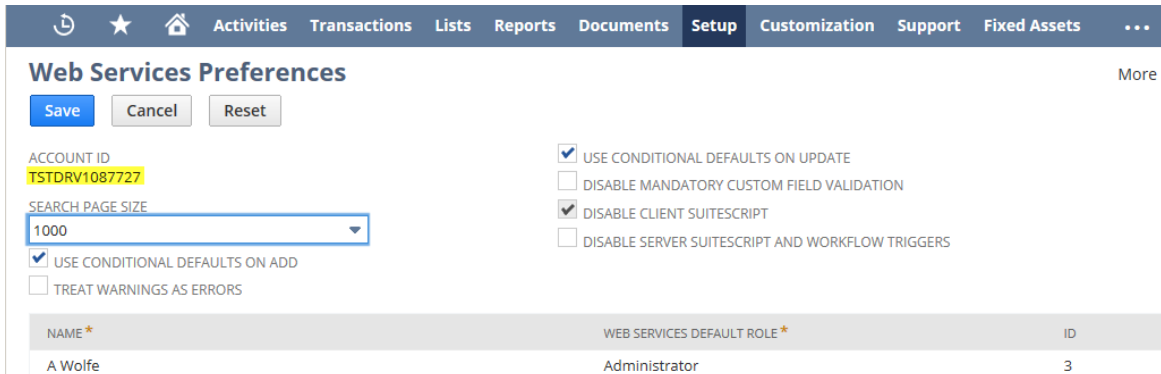
Next Steps

[Configure NetSuite to Use RSA SecurID Access as an Identity Provider](#)

Configure NetSuite to Use RSA SecurID Access as an Identity Provider

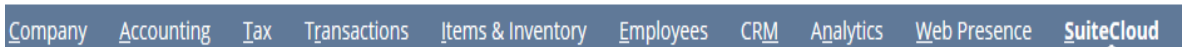
Procedure

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**.

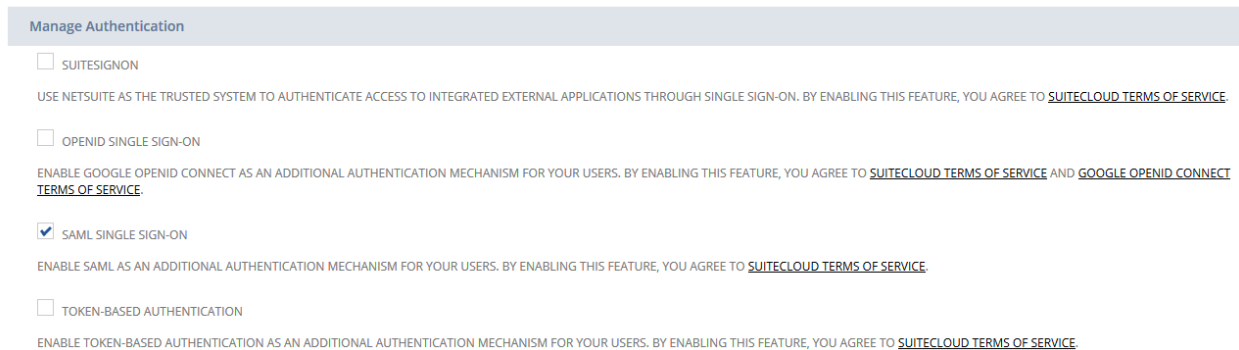


The screenshot shows the NetSuite 'Web Services Preferences' page. The top navigation bar includes 'Activities', 'Transactions', 'Lists', 'Reports', 'Documents', 'Setup', 'Customization', 'Support', and 'Fixed Assets'. The 'Setup' tab is active. Below the navigation bar, there are buttons for 'Save', 'Cancel', and 'Reset'. The 'ACCOUNT ID' is 'TSTDRV1087727'. The 'SEARCH PAGE SIZE' is set to '1000'. There are several checkboxes: 'USE CONDITIONAL DEFAULTS ON UPDATE' (checked), 'DISABLE MANDATORY CUSTOM FIELD VALIDATION' (unchecked), 'DISABLE CLIENT SUITESCRIPT' (checked), and 'DISABLE SERVER SUITESCRIPT AND WORKFLOW TRIGGERS' (unchecked). Below these are 'USE CONDITIONAL DEFAULTS ON ADD' (checked) and 'TREAT WARNINGS AS ERRORS' (unchecked). At the bottom, there is a table with columns 'NAME *', 'WEB SERVICES DEFAULT ROLE *', and 'ID'. The table contains one row: 'A Wolfe', 'Administrator', and '3'.

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**.



The screenshot shows the 'Manage Authentication' section in NetSuite. It contains four checkboxes: 'SUITESIGNON', 'OPENID SINGLE SIGN-ON', 'SAML SINGLE SIGN-ON', and 'TOKEN-BASED AUTHENTICATION'. The 'SAML SINGLE SIGN-ON' checkbox is checked. Below each checkbox is a brief description and a link to the 'SUITECLOUD TERMS OF SERVICE'.

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.

NetSuite Configuration

NETSUITE SERVICE PROVIDER METADATA
<https://system.na1.netsuite.com/saml2/sp.xml>

LOGOUT LANDING PAGE *

IDENTITY PROVIDER LOGIN PAGE *

PRIMARY AUTHENTICATION METHOD

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

Update Identity Provider

SAMLV2 IDENTITY PROVIDER METADATA

INDICATE IDP METADATA URL

UPLOAD IDP METADATA FILE

metaNetsuite.xml

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.

Edit	Name	Custom/Standard	Center Type
Customize	A/P Clerk	Standard	Accounting Center
Customize	A/R Clerk	Standard	Accounting Center
Customize	Accountant	Standard	Accounting Center
Customize	Accountant (Reviewer)	Standard	Accounting Center
Customize	Bookkeeper	Standard	Accounting Center
Customize	CEO	Standard	Executive Center
Customize	CEO(Hands Off)	Standard	Executive Center
Customize	CFO	Standard	Accounting Center
Edit	Controller	Custom	Accounting Center
Edit	Custom Customer Center	Custom	Customer Center
Edit	Custom Customer Center 2	Custom	Customer Center
Edit	Custom Employee Center	Custom	Employee Center
Edit	Custom Partner Center 2	Custom	Partner Center
Edit	Custom PM Manager	Custom	Support Center
Edit	Custom Sales Manager 3	Custom	Sales Center
Customize	Customer Center	Standard	Customer Center
Edit	E-Commerce Site Manager	Custom	E-Commerce Management Center
Customize	Employee Center	Standard	Employee Center

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

PERMISSION	LEVEL
Deleted Records	Full
SAML Single Sign-on	Full
Web Services	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.

GIVE ACCESS

ROLE: Custom Customer Center

SEND NOTIFICATION E-MAIL

PASSWORD:

CONFIRM PASSWORD:

9. Click **SAVE.**