

RSA Via Access SAML Configuration for NetSuite SuiteCommerce



Last Modified: April 15, 2016

NetSuite SuiteCommerce supports the needs of both B2B and B2C commerce from a single cloud-based platform.

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.

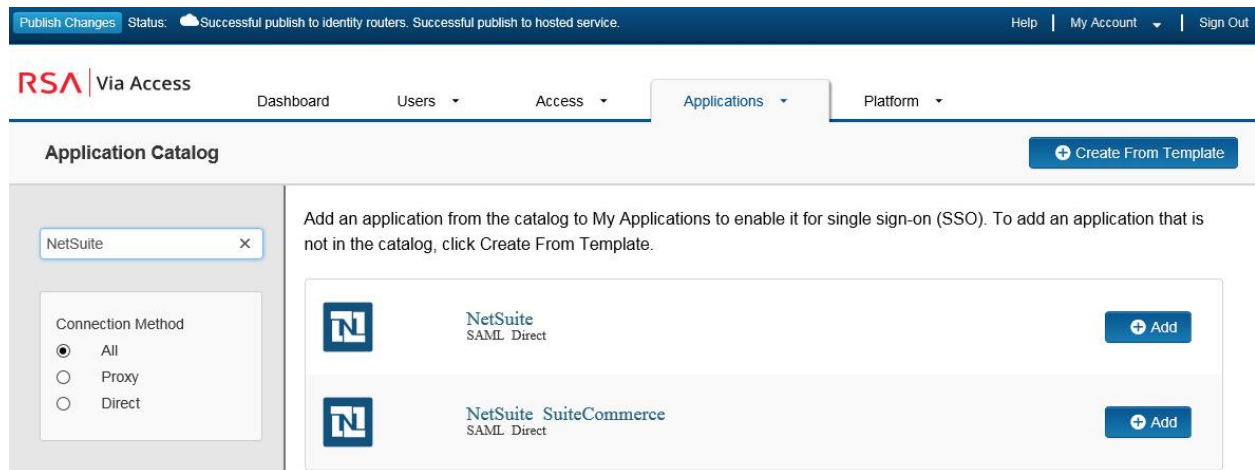
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure NetSuite SuiteCommerce 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**.

 **Note:** Netsuite SuiteCommerce currently only supports single sign-on for IDP initiated work flow. Accessing the shopping site directly does not redirect the user back to the IDP but will result in the user being prompted for their local Netsuite credentials.

To investigate a single sign-on solution for accessing the shopping web site directly consult the Netsuite documentation for Hosted HTML files and customized login pages.

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): shopping

Override

SAML Response Signature 

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

Private Key Loaded 


Certificate Loaded

CN= Valid
Until: 08/05/2017

Include Certificate in Outgoing Assertion

- 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 RSA SecurID Access private key.
- c. Select **Choose File** and upload the RSA SecurID Access public certificate.

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**.

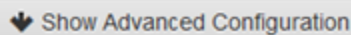
User Identity

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. Add attributes **email**, **account**, and **site**. The site number maps to the Site builder web site number, found on page 7 step 3. The account number can be found on page 6 step 2.

Attribute Extension

Attribute Source	Attribute Name	Identity Source	Property	Manage
<input type="text" value="User Store"/>	<input type="text" value="email"/>	<input type="text" value="DefaultIdel"/>	<input type="text" value="mail"/>	 
<input type="text" value="Constant"/>	<input type="text" value="account"/>	<input type="text" value=""/>	<input type="text" value="TSTDRV14222"/>	 
<input type="text" value="Constant"/>	<input type="text" value="site"/>	<input type="text" value=""/>	<input type="text" value="1"/>	 
 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>
```

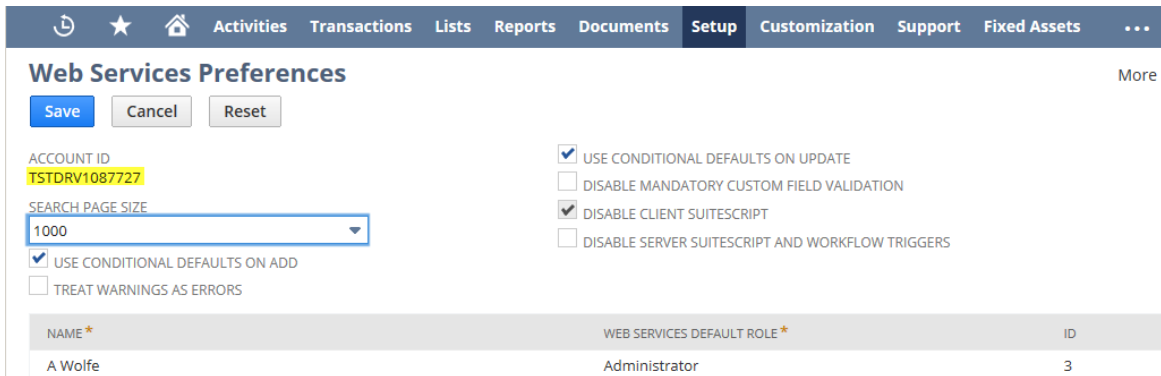
Next Steps

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

Configure NetSuite SuiteCommerce to Use RSA SecurID Access as an Identity Provider

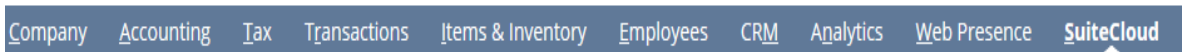
Procedure

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**.

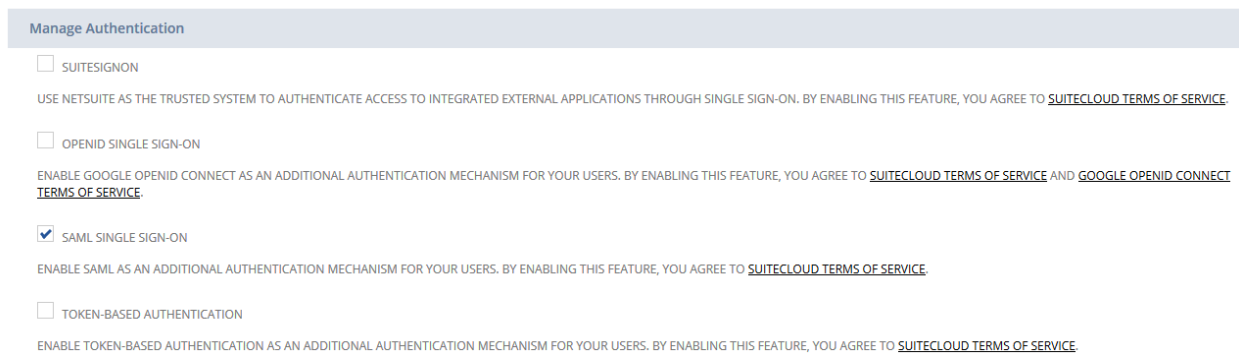


The screenshot shows the NetSuite 'Web Services Preferences' page. The top navigation bar includes 'Setup', 'Customization', 'Support', and 'Fixed Assets'. The page title is 'Web Services Preferences' with a 'More' link. Below the title are 'Save', 'Cancel', and 'Reset' buttons. The 'ACCOUNT ID' field is highlighted in yellow and contains 'TSTDREV1087727'. The 'SEARCH PAGE SIZE' dropdown menu 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 three 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 authentication options, each with a checkbox and a description:

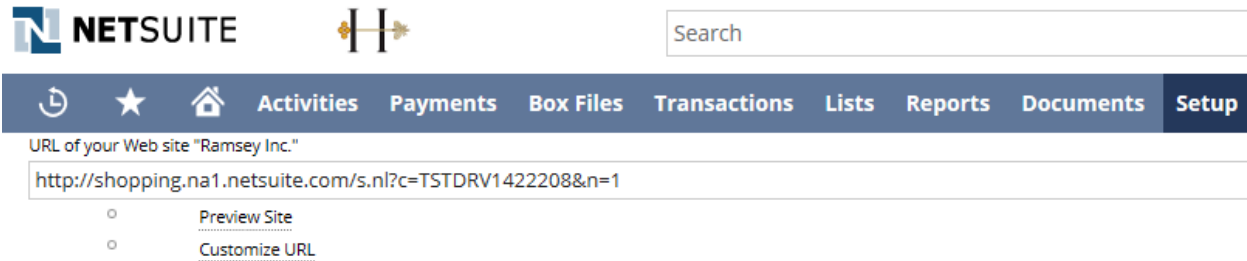
- SUITESIGNON
USE NETSUITE AS THE TRUSTED SYSTEM TO AUTHENTICATE ACCESS TO INTEGRATED EXTERNAL APPLICATIONS THROUGH SINGLE SIGN-ON. BY ENABLING THIS FEATURE, YOU AGREE TO [SUITECLOUD TERMS OF SERVICE](#).
- OPENID SINGLE SIGN-ON
ENABLE GOOGLE OPENID CONNECT AS AN ADDITIONAL AUTHENTICATION MECHANISM FOR YOUR USERS. BY ENABLING THIS FEATURE, YOU AGREE TO [SUITECLOUD TERMS OF SERVICE](#) AND [GOOGLE OPENID CONNECT TERMS OF SERVICE](#).
- SAML SINGLE SIGN-ON
ENABLE SAML AS AN ADDITIONAL AUTHENTICATION MECHANISM FOR YOUR USERS. BY ENABLING THIS FEATURE, YOU AGREE TO [SUITECLOUD TERMS OF SERVICE](#).
- TOKEN-BASED AUTHENTICATION
ENABLE TOKEN-BASED AUTHENTICATION AS AN ADDITIONAL AUTHENTICATION MECHANISM FOR YOUR USERS. BY ENABLING THIS FEATURE, YOU AGREE TO [SUITECLOUD TERMS OF SERVICE](#).


6. Click **Save**.

Create the Website

1. Navigate to **Setup > Site Builder > Web Site Assistant**.
2. Complete the 4 steps in the Web Site Assistant wizard to configure your site's URL and appearance.
3. Navigate to **Setup > Site Builder > Preview Website**.

 **Note:** If you have more than one web site configured, the n=1 in the URL will change to match the site number.



NETSUITE 

Search

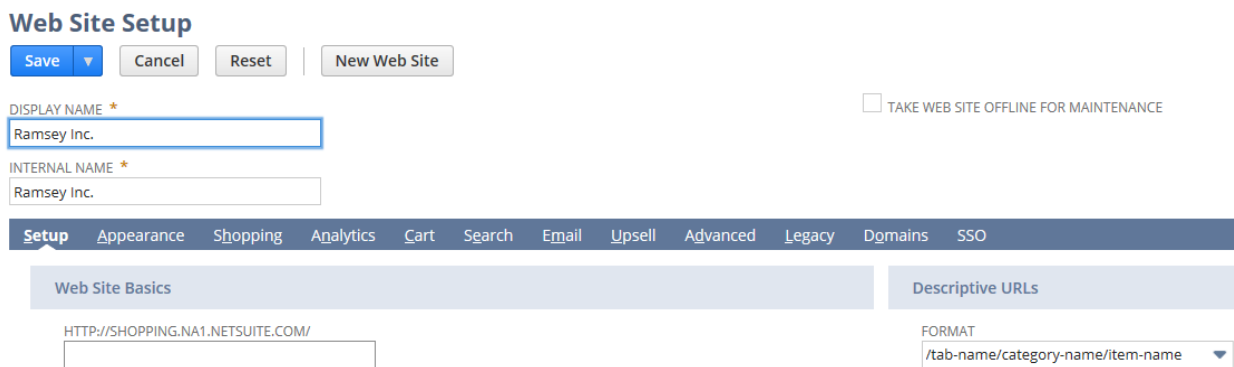
Activities Payments Box Files Transactions Lists Reports Documents Setup

URL of your Web site "Ramsey Inc."

- Preview Site
- Customize URL

Add SAML on the Shopping Site

1. Select **Customize URL**.
2. On the Web Site Setup page, select the **SSO** tab.



Web Site Setup

Save Cancel Reset New Web Site

DISPLAY NAME * TAKE WEB SITE OFFLINE FOR MAINTENANCE

INTERNAL NAME *

Setup Appearance Shopping Analytics Cart Search Email Upsell Advanced Legacy Domains SSO

Web Site Basics Descriptive URLs


HTTP://SHOPPING.NA1.NETSUITE.COM/

FORMAT

3. Enter a **LOGOUT LANDING PAGE** URL.
4. Enter the Identity Provider URL from page 2 step 5 into the **IDENTITY PROVIDER LOGIN PAGE** field.

Setup Appearance Shopping Analytics Cart Search Email Upsell Advanced Legacy Domains SSO

SAML •

**SAML Access Warning**

By enabling the SAML Single Sign-on feature, you allow users to access and use your NetSuite account directly from a third party service that may not have the same authentication and security features as NetSuite. This feature also extends NetSuite administration of user access to the administrators of the identity management system. You need to ensure that NetSuite account use through SAML meets all of your security, regulatory, and other compliance obligations, including Payment Card Industry (PCI) Data Security Standards.

NetSuite Configuration

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

LOGOUT LANDING PAGE *

IDENTITY PROVIDER LOGIN PAGE *

LANDING PAGE AFTER LOGIN

Current Identity Provider

ENTITY ID

Delete IDP Configuration
Current Identity Provider Metadata

Update Identity Provider

SAMLV2 IDENTITY PROVIDER METADATA

INDICATE IDP METADATA URL

UPLOAD IDP METADATA FILE
 No file chosen

|

5. Select **Browse**, and upload the RSA SecurID Access metadata file.
6. Click **Save**.

Register the User on the Shopping Site

1. Browse to the shopping site, and click **Login**.
2. Select the **New customer?** link.
3. Register a user with their single sign-on email address.

The screenshot shows a web page with a red header bar. On the left, there is a 'Login >' link and two buttons: 'Your Cart is Empty' (with a 'View Cart' link) and 'Login'. The main content area is titled 'New Customer Registration'. It contains several input fields: 'Name' (filled with 'alici'), 'Company Name', 'Email Address' (filled with 'alicia@pe-lab.com'), 'Password' (masked with dots), 'Re-enter Password' (masked with dots), and 'Password Hint'. Below these is a dropdown menu for 'How did you hear of us?' and a 'Partner Code' field. A checkbox is checked for 'Please notify me of upcoming specials and offers'. A yellow 'Continue' button is at the bottom. A link 'Returning customer? Click here' is at the bottom of the form area.

4. Once an account is created for the user, the user can access the Shopping site via the RSA SecurID Access portal using their single sign-on credentials.

