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.

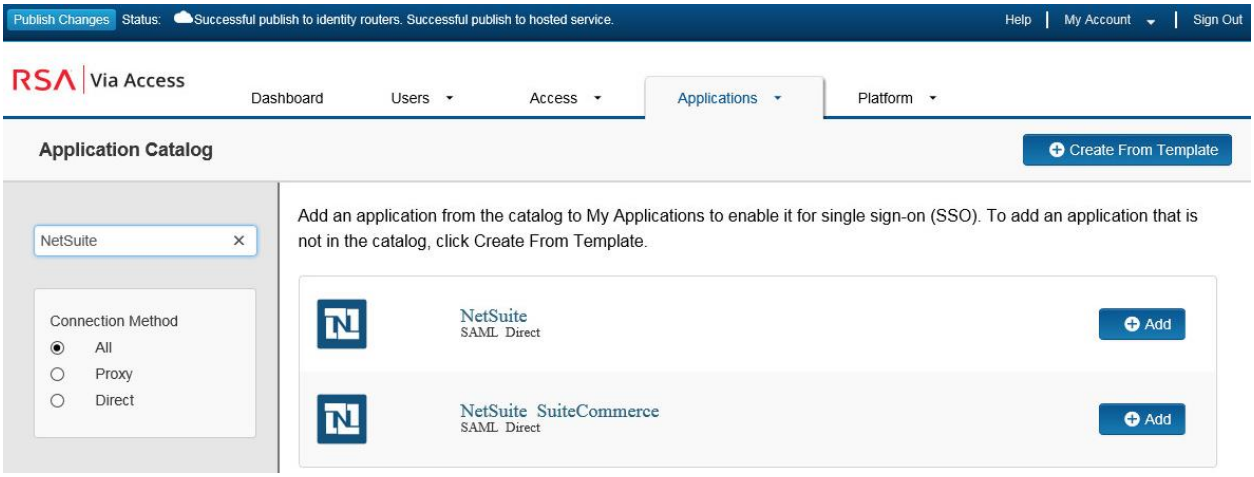
Procedure

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.

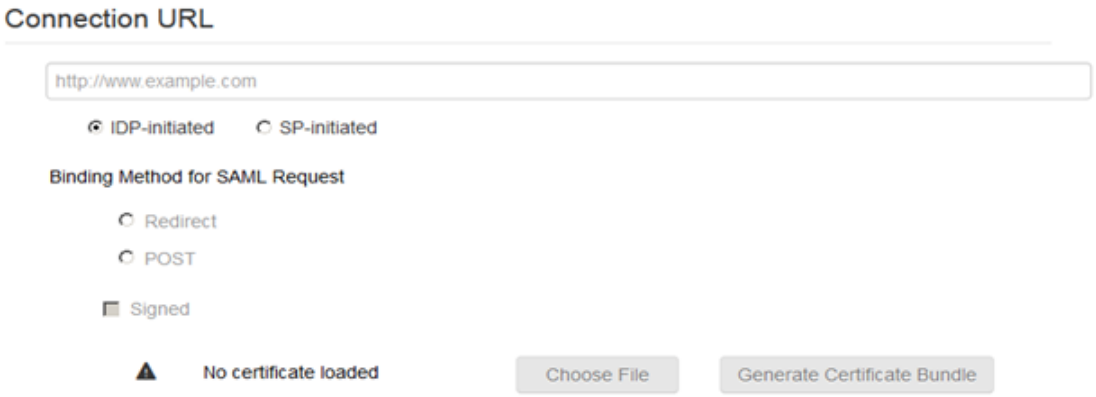


Copyright © 2016 EMC Corporation. All Rights Reserved.

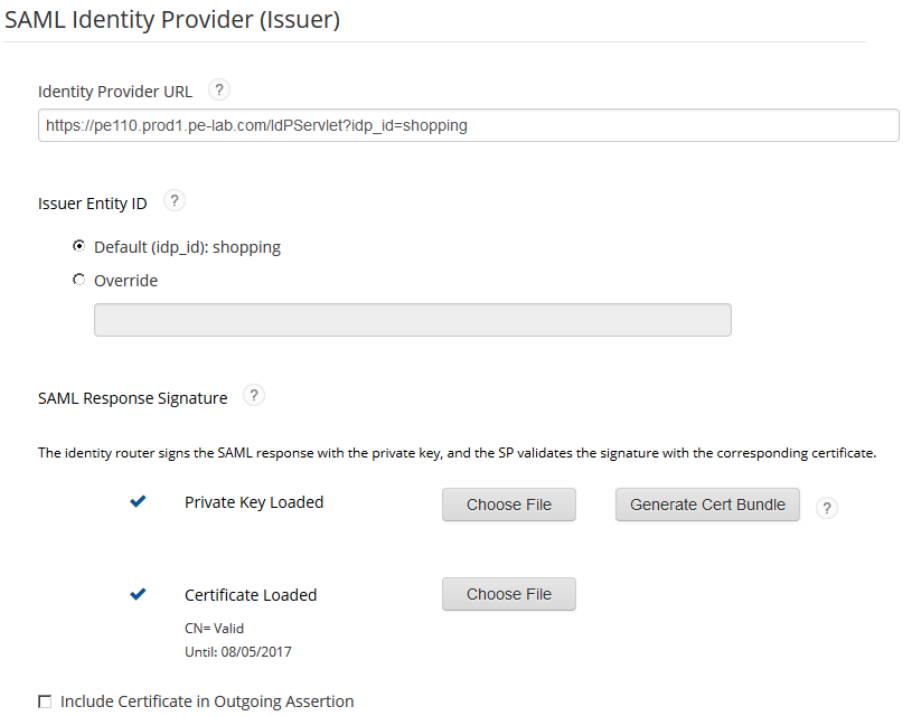
3. On the Basic Information page, specify the application name and click **Next Step**.

> **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.



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

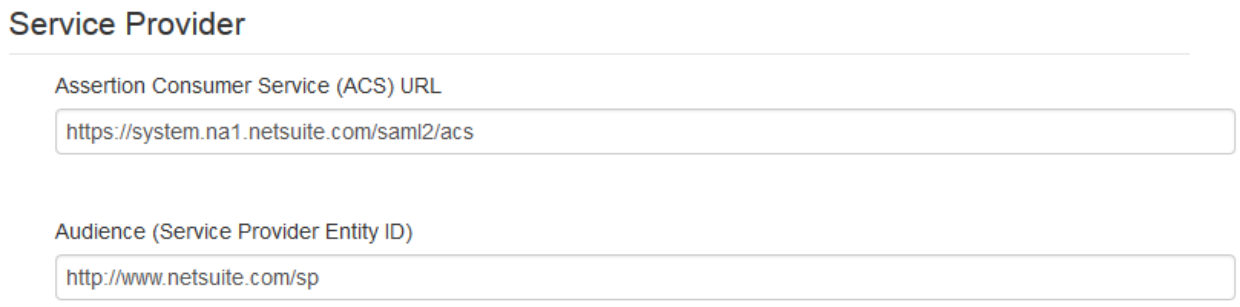


   a. In the **Identity Provider URL** field, copy the URL which will be needed later to configure the NetSuite.
   b. Select **Choose File** and upload the RSA SecurID Access private key.
   c. Select **Choose File** and upload the RSA SecurID Access public certificate.

Copyright © 2016 EMC Corporation. All Rights Reserved.

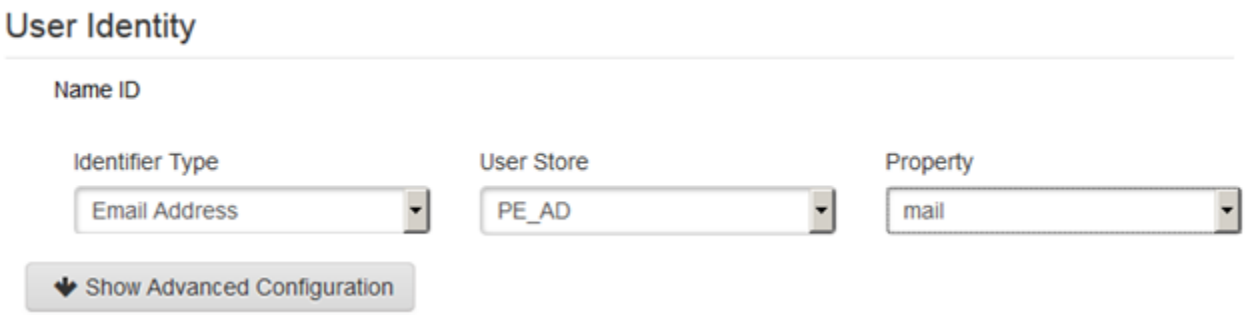
6. Scroll down to the **Service Provider** section.

> **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.**

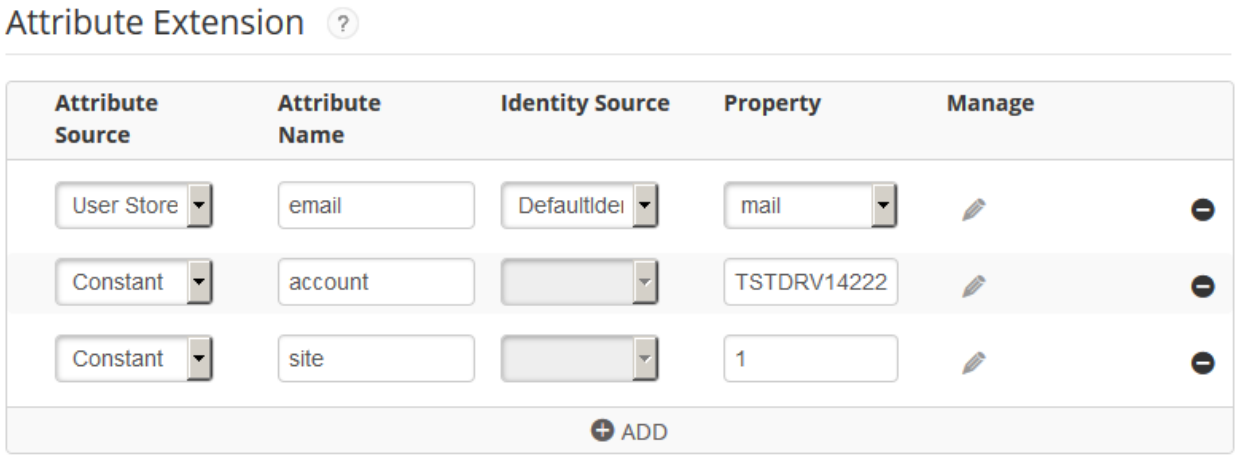


   a. In the **Assertion Consumer Service (ACS) URL** field, enter https://system.na1.netsuite.com/saml2/acs
   b. In the **Audience (Service Provider Entity ID)** field, enter http://www.netsuite.com/sp

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



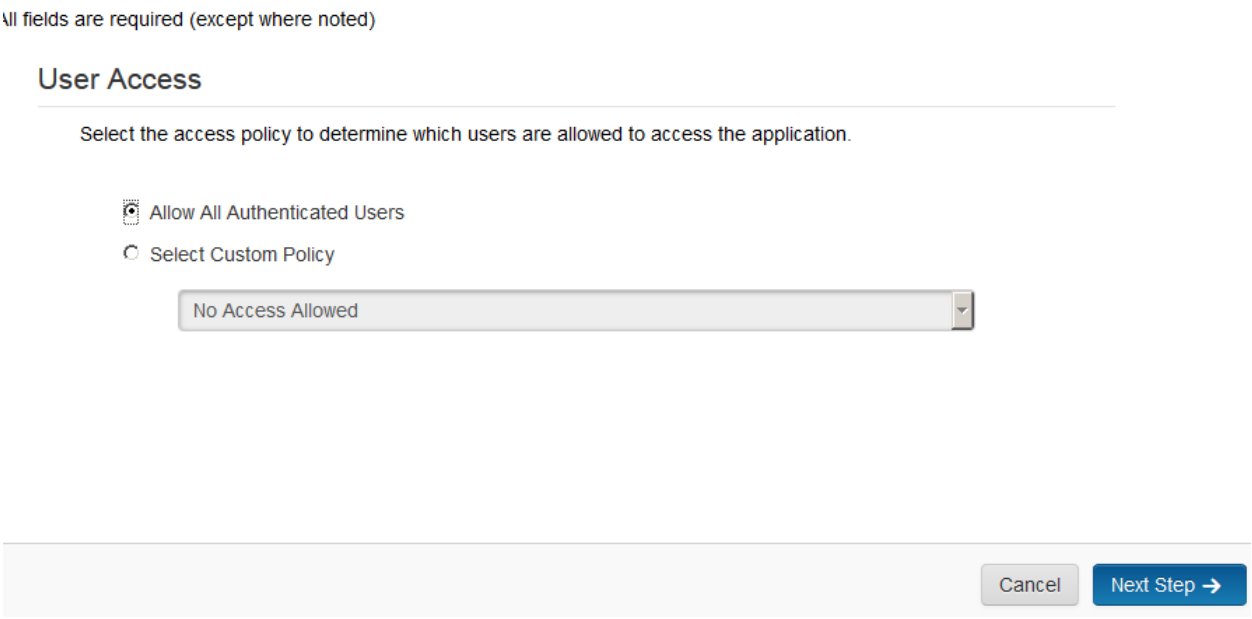
8. Click **Show Advanced Configuration** and scroll down to **Attribute Extension.**
9. Select **User Store** from the **Attribute Source** pulldown list.
10. Add attributes **email**, **account,** and **site**. The site number maps to the Site builder web site number, found on page 7 step 3. The account number can be found on page 6 step 2.



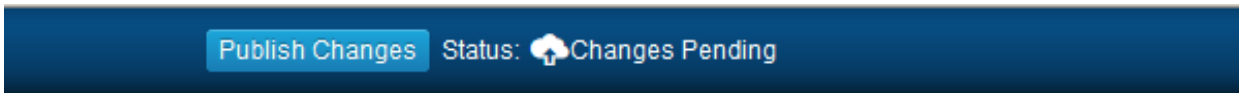
11. Click **Next Step**.

Copyright © 2016 EMC Corporation. All Rights Reserved.

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.



Copyright © 2016 EMC Corporation. All Rights Reserved.

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

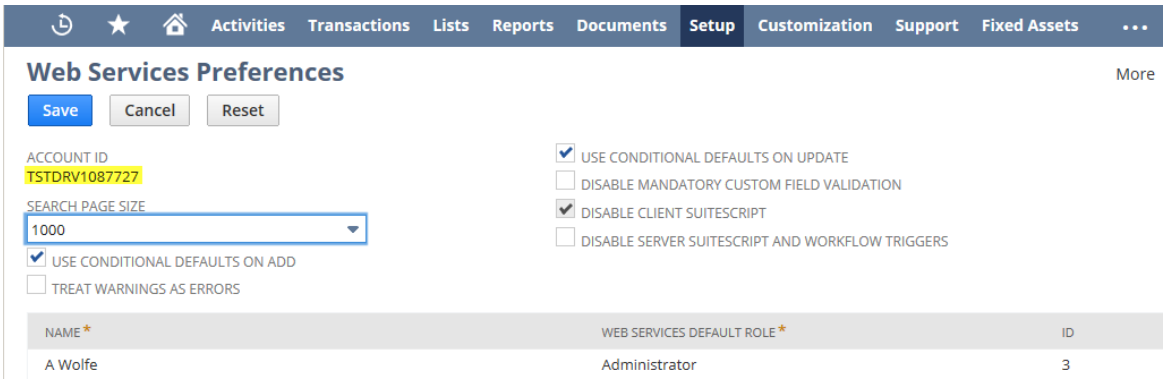
Configure NetSuite SuiteCommerce to Use RSA SecurID Access as an Identity Provider

Copyright © 2016 EMC Corporation. All Rights Reserved.

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

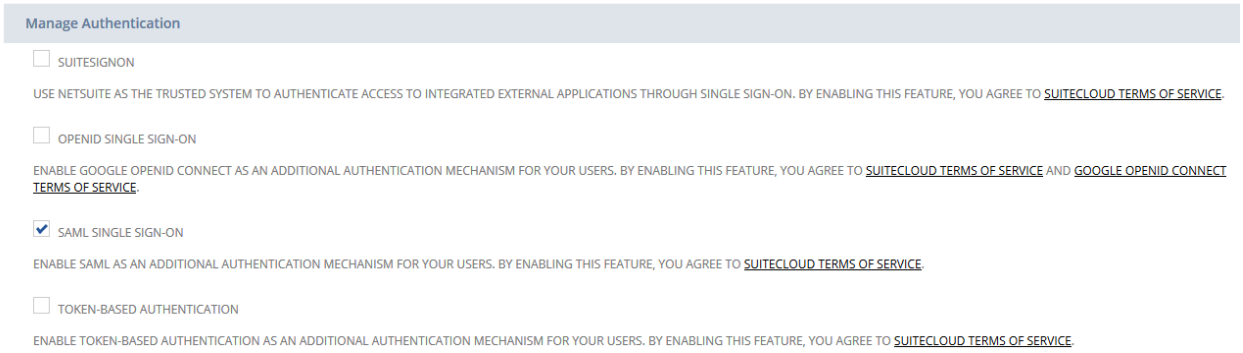
Procedure

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**.



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**.



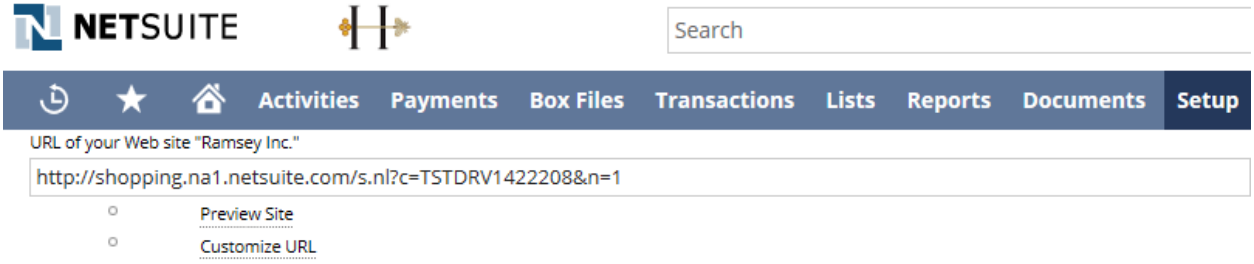
6. Click **Save**.

Copyright © 2016 EMC Corporation. All Rights Reserved.

Create the Website

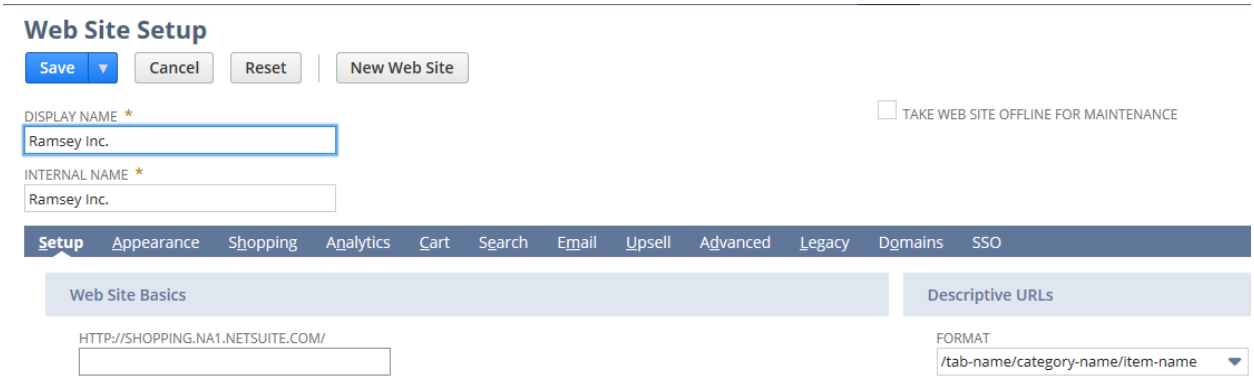
1. Navigate to **Setup > Site Builder > Web Site Assistant**.
2. Complete the 4 steps in the Web Site Assistant wizard to configure your site's URL and appearance.
3. Navigate to **Setup > Site Builder > Preview Website.**

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



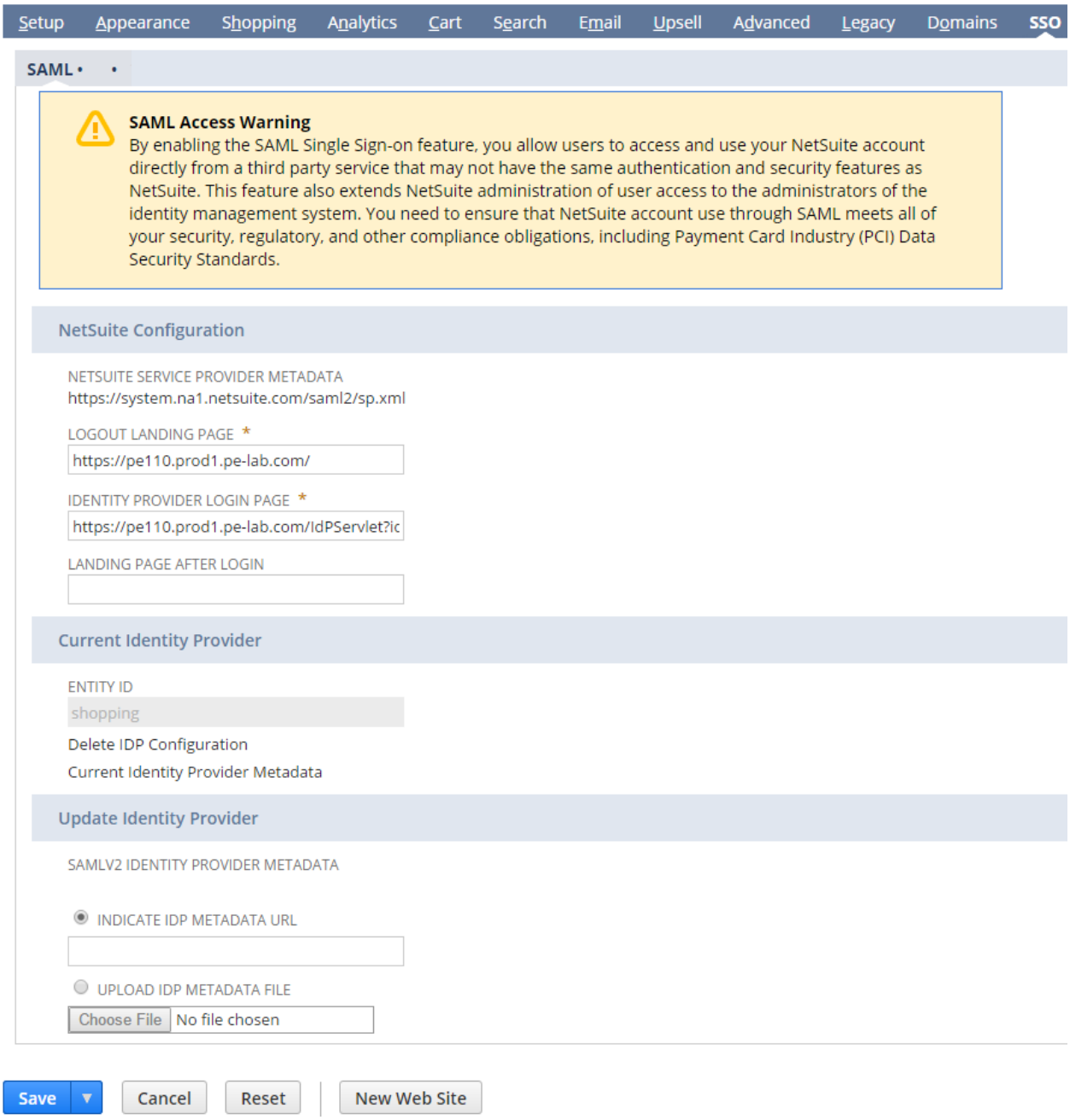
Add SAML on the Shopping Site

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



Copyright © 2016 EMC Corporation. All Rights Reserved.

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.

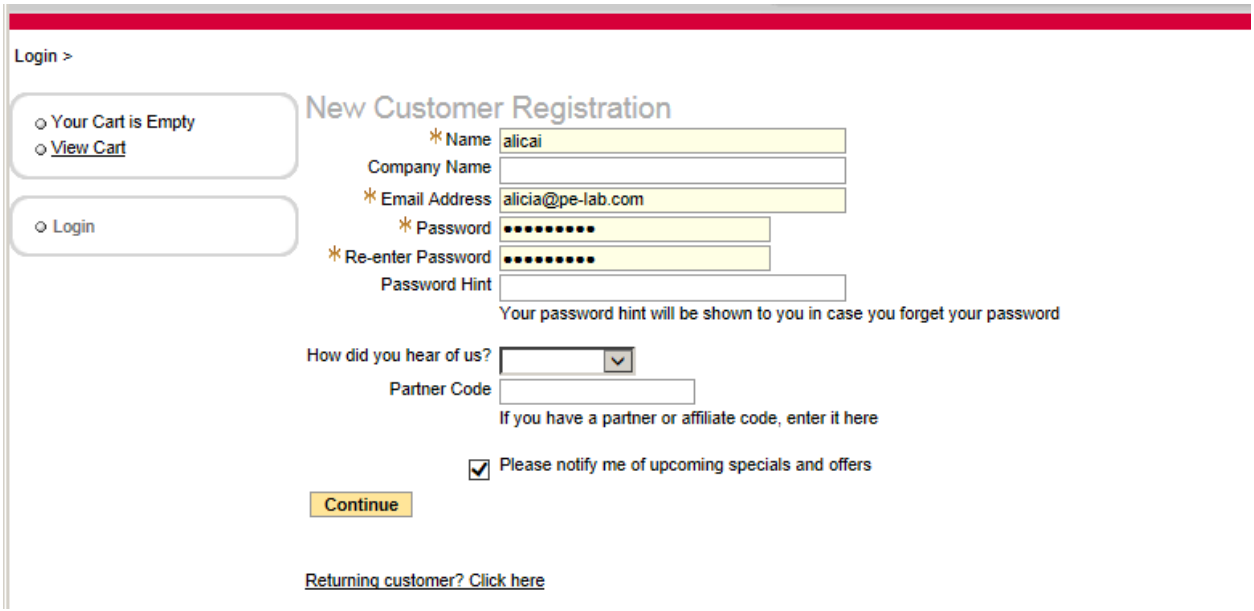


5. Select **Browse**, and upload the RSA SecurID Access metadata file.
6. Click **Save**.

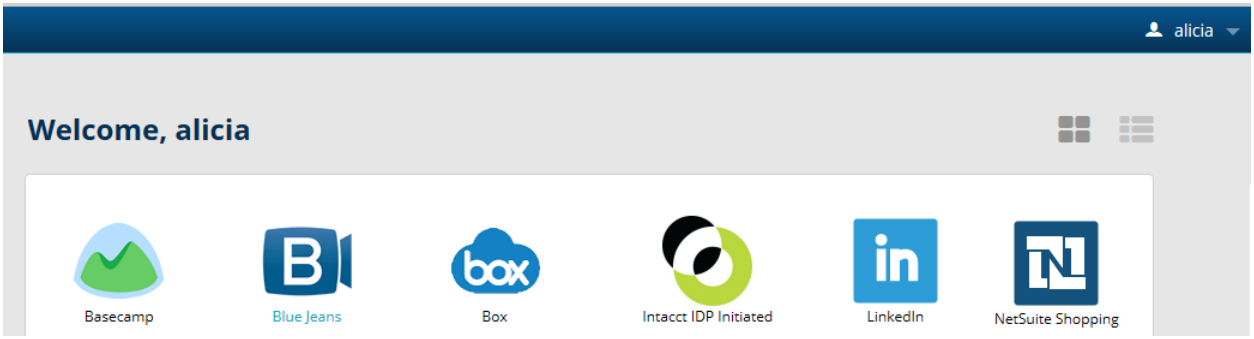
Copyright © 2016 EMC Corporation. All Rights Reserved.

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.



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.



GLS

Copyright © 2016 EMC Corporation. All Rights Reserved.