SafeNet Authentication Manager
Integration Guide

Using SAM as an Identity Provider for NetSuite
Document Information

Release Date | April 2014

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
Overview........................................................................................................................................4
Single Sign-On Dataflow ..................................................................................................................4
Identity Provider Configuration ........................................................................................................5
  Configuring SAM as an Identity Provider ..................................................................................5
Configuring NetSuite to Use SAM as an Identity Provider ...........................................................7
Configuring SAM for SAML-based User Federation ..................................................................11
Running the NetSuite SAML Solution .........................................................................................16
  Connecting to NetSuite .............................................................................................................16
Support Contacts............................................................................................................................18
Overview

This document provides guidance for setting up and managing SafeNet Authentication Manager (SAM) 8.2 (with March 2014 hotfix) as an identity provider for NetSuite.

NOTE: The document assumes that NetSuite is already configured and working with local users and static passwords prior to implementing SafeNet Authentication Manager strong authentication.

Single Sign-On Dataflow

1. Bob, a user, wants to log in to NetSuite. Bob leverages the single sign-on capabilities embedded in the organization’s SafeNet Authentication Manager (SAM) solution. SafeNet Authentication Manager collects and evaluates Bob’s credentials.

2. SafeNet Authentication Manager’s external portal collects Bob’s credentials and passes them to SAM for authentication.

   SAM evaluates Bob’s credentials and returns an “accept” or “reject” response to the external portal.

3. The portal uses SAM’s response to return an “accept” or “reject” assertion to NetSuite.
Identity Provider Configuration

Configuring SAM as an Identity Provider

The SAM Configuration Manager and TPO settings are used to establish SafeNet Authentication Manager (SAM) as the identity provider for the NetSuite.

1. From the Windows Start menu, select SafeNet Authentication Manager > Configuration Manager.
2. On the Configuration Manager window, click Action > Cloud Configuration.
3. On the Cloud Settings dialog box, click the Info for Service Provider tab.
4. In the **Domain URL** field, enter the domain URL of your organization's SAM external portal. The remaining fields contain default entries and cannot be changed.

![Cloud Settings dialog box]

5. Do not close the **Cloud Settings** dialog box. These values will be needed in step 5a “Configuring NetSuite to Use SAM as an Identity Provider” on page 8.

6. Click **Export Certificate** and save the certificate file. This file will be needed in step 5b of “Configuring NetSuite to Use SAM as an Identity Provider” on page 8.

7. Click **Download Metadata** and save the metadata file. This file will be needed in step 5c of “Configuring NetSuite to Use SAM as an Identity Provider” on page 8.
Configuring NetSuite to Use SAM as an Identity Provider

1. Log in to NetSuite.
2. On the NetSuite toolbar, click **Setup > Company > Setup Tasks > Enable Features**.
3. Click the **SuiteCloud** tab. Select the **SAML Single Sign-on** check box.

4. On the NetSuite toolbar, click **Setup > Integration > SAML Single Sign-on**.
5. On the SAML Setup dialog box, do the following:
   a. Under NetSuite Configuration:
      i. Copy and paste the Sign-out page URL from SAM’s Cloud Settings dialog box into the Logout Landing Page box.
      ii. Copy and paste the Sign-in page URL from SAM’s Cloud Settings dialog box into the Identity Provider Login Page box.
   b. Under Update Identity Provider, select Indicate IDP metadata URL or Upload IDP metadata file (the export certificate file from SAM’s Cloud Settings dialog box) as appropriate.
   c. Download the NetSuite metadata .xml file using the NetSuite Service Provider Metadata link under NetSuite Configuration.
   d. Click Submit.
6. Next, you must add a new user rule that includes SAML authentication.
   a. On the NetSuite toolbar, click **Setup > Users/Roles > Manage Roles > New**.

![NetSuite Setup Manager](image)

b. Complete the **Role** dialog box as follows:

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Type a name for this role, such as <strong>SAML Authentication</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Center Type</td>
<td>Select <strong>Classic Center</strong>.</td>
</tr>
</tbody>
</table>

All other fields can be left with the default settings.

c. On the **Permissions** tab, click **Setup**. Add the following permissions:
   - SAML Single Sign-on
   - Set Up SAML Single Sign-on

d. Click **Save**.

![NetSuite Role Permissions](image)
7. Next, you must attach the new profile to a user.
   a. On the NetSuite toolbar, click **Setup > Users/Roles > Manage Users**.
   b. Click on the desired user. On the **Employee** page, click **Edit**.
   c. Click the **Access** tab and choose the **Role Name** that you added in step 6.
   d. Click **Add** to attach the role to the user.

SafeNet Authentication Manager is now configured as an identity provider for NetSuite.
Configuring SAM for SAML-based User Federation

SafeNet Authentication Manager’s Token Policy Object (TPO) policies include Application Authentication Settings for SAML service providers. These settings are used by SAM’s external portal to communicate with service providers.


To edit the TPO policies for SAM’s portal configuration:

1. Open the Token Policy Object Editor for the appropriate group.
2. In the left pane, select Protected Application Settings > User Authentication. The property’s policies are displayed in the right pane.
3. In the right pane, double-click Application Authentication Settings.
4. On the **Application Authentication Settings Properties** dialog box, do the following:
   a. Select the **Define this policy setting** check box, then select **Enabled**.
   b. Click the **Definitions** button.

5. In the left pane, right-click **Application Authentication Settings** and select **Create a new profile**.

6. In the left pane, right-click the new profile and select **Rename**. For the new profile name, type **NetSuite**. Click **OK** to save.
7. In the left pane, double-click **NetSuite**. The profile’s policies are displayed in the right pane.

8. In the right pane, double-click the policies listed below and specify the following settings:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Policy Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application issuer</td>
<td>Enter the NetSuite Issuer/Entity ID value:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.netsuite.com/sp">http://www.netsuite.com/sp</a></td>
</tr>
<tr>
<td>SAM issuer</td>
<td>Enter the <strong>Domain URL</strong> copied from SAM’s <strong>Cloud Settings</strong> dialog box.</td>
</tr>
<tr>
<td>Application’s login URL</td>
<td>Enter <a href="https://system.na1.netsuite.com/saml2/acs">https://system.na1.netsuite.com/saml2/acs</a>.</td>
</tr>
<tr>
<td>Audience URI</td>
<td>Enter the NetSuite Issuer value:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.netsuite.com/sp">http://www.netsuite.com/sp</a></td>
</tr>
</tbody>
</table>
9. On the same window, enable the appropriate authentication method(s) for your organization. (For detailed information on authentication methods, refer to the SafeNet Authentication Manager Version 8.2 Administrator's Guide.)

10. Click OK until all of the TPO Editor windows are closed.

Go to NetSuite's website and locate your Account ID. This can be found at Setup > Integration > Web Services Preferences.

11. On your SAM server, browse to the following location:

   C:\Program Files\SafeNet\Authentication\SAM\x64\Web\samwebapi

12. Edit the web.config file as follows:

   - In the <appSettings> section, add the following:
     
     <add key="SAMLPlugin" value="SAMLPluginSample.dll" /
     
     <add key="SAMLPluginProviderAdditionalField" value="AccountD" />

   - In line 2 above, replace AccountID with the NetSuite Account ID found in step 11.
The following is an example of the web.config file with the added values:

![Web.config Example](image)

13. On the SAM server, browse to the following location:

   `C:\Program Files\SafeNet\Authentication\SAM\x64\Web\samwebapi\bin`

14. Verify that the SAMLPluginSample.dll file resides in that directory.

NetSuite is now added as a SAML service provider.
Running the NetSuite SAML Solution

After NetSuite is configured to use SafeNet Authentication Manager (SAM) as its identity provider, and SafeNet Authentication Manager is configured to use NetSuite as a SAML service provider, users can log in to NetSuite.

NOTE: The NetSuite server and the SAM server time should be NTP synchronized, as a difference in time of more than two (2) seconds will cause a failure.

Connecting to NetSuite

1. Open a browser and go to the following location:
   

   Replace <Application Issuer> with the value indicated in SAM’s Application Authentication Settings (see page 12).

2. On the SAM User Identification window, enter your Username, and then click OK.
3. A message is displayed confirming successful login and you are authenticated to your NetSuite account.
Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Table 1: Support Contacts

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017</td>
</tr>
<tr>
<td></td>
<td>USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>United States</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td><a href="mailto:support@safenet-inc.com">support@safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Support and Downloads</strong></td>
<td><a href="http://www.safenet-inc.com/Support">www.safenet-inc.com/Support</a></td>
</tr>
<tr>
<td></td>
<td>Provides access to the SafeNet Knowledge Base and quick downloads for various products.</td>
</tr>
<tr>
<td></td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>