Zscaler
Integration Guide

Using SAM as an Identity Provider for Zscaler
Document Information

| Release Date | March 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>
Contents

Overview .................................................................................................................................................. 4
Single Sign-On Dataflow .......................................................................................................................... 4
Identity Provider Configuration .............................................................................................................. 5
Configuring Zscaler to Use SAM as an Identity Provider ...................................................................... 7
Configuring SAM for SAML-based User Federation ............................................................................ 10
Running the Zscaler SAML Solution .................................................................................................... 15
  Browser Configuration ......................................................................................................................... 16
  Connecting to Zscaler ......................................................................................................................... 20
Support Contacts ................................................................................................................................... 22
Overview

This document provides guidance for setting up and managing SafeNet Authentication Manager (SAM) 8.2 as an identity provider for Zscaler.

**NOTE:** The document assumes that Zscaler 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 Zscaler. 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. SAM returns a response to Zscaler to accept or reject Bob’s credentials for authentication.
Identity Provider Configuration

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

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.

5. Do not close the **Cloud Settings** dialog box. The displayed values will be needed in step 6 of “Configuring Zscaler to Use SAM as an Identity Provider” on page 9.

6. Click **Export Certificate** and save the certificate file. This file will be needed in step 6 of “Configuring Zscaler to Use SAM as an Identity Provider” on page 9.
Configuring Zscaler to Use SAM as an Identity Provider

1. Log in to Zscaler.
2. In the Zscaler window, click the **Policy & Admin** link.
3. On the **Administration** tab, in the left pane, under **Manage Administrators & Roles**, click **Manage Users & Authentication** to configure single sign-on (SSO) settings.

4. On the **Configure User Authentication** dialog box, click the **Edit** button.
5. Click **Configure SAML Single Sign-On Parameters**.

![Configure SAML Single Sign-On Parameters](image)

6. On the **Configure Single Sign-On using SAML** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL of the SAML Portal to which users are sent for authentication</strong></td>
<td>Copy and paste the <strong>Sign-in page URL</strong> copied from SAM Cloud Settings window.</td>
</tr>
<tr>
<td><strong>Attribute containing Login Name</strong></td>
<td><strong>Type NameID</strong>. This field is case-sensitive.</td>
</tr>
<tr>
<td><strong>Upload SSL Public Certificate</strong></td>
<td>Use the <strong>Choose File</strong> button to locate and upload the certificate downloaded from SAM. In order to upload a certificate, you must convert the downloaded .crt certificate to .der format. You can do so using a tool such as SSL Converter (<a href="https://www.sslshopper.com/ssl-converter.html">https://www.sslshopper.com/ssl-converter.html</a>).</td>
</tr>
<tr>
<td><strong>Sign SAML request</strong></td>
<td><strong>This check box should not be selected.</strong></td>
</tr>
<tr>
<td><strong>Enable SAML Auto-Provisioning</strong></td>
<td><strong>This check box should not be selected.</strong></td>
</tr>
</tbody>
</table>
7. Click **Done**.

SafeNet Authentication Manager is now configured as an identity provider for Zscaler.

### 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.

---

**NOTE:** See *SafeNet Authentication Manager Version 8.2 Administrator’s Guide* for general portal configuration.

---

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

1. Open the Token Policy Object Editor for the appropriate group. See the *SafeNet Authentication Manager Version 8.2 Administrator’s Guide* for more information.
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 **Zscaler**. Click **OK** to save.
7. In the left pane, double-click **Zscaler**. The profile’s policies are displayed in the right pane.

![Application Authentication Settings](image)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Policy Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application issuer</td>
<td>Enter the Zscaler Issuer/Entity ID value, <code>zscaler.net</code></td>
</tr>
<tr>
<td>SAM issuer</td>
<td>Enter the Domain URL copied from SAM’s Cloud Settings window.</td>
</tr>
<tr>
<td>Application’s login URL</td>
<td>Enter <code>https://login.zscaler.net:443/sfc_sso</code></td>
</tr>
<tr>
<td>Audience URI</td>
<td>Enter <code>https://login.zscaler.net:443/sfc_sso</code></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.

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

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

NOTE: The Zscaler 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.

The Zscaler SAML solution works as follows:

1. A user opens a browser and tries to reach a website.
2. The service generates a SAML authentication request, which is encoded and embedded into the URL for the IdP.
3. The service sends a redirect to the user’s browser. It includes the encoded SAML authentication request to be submitted to the IdP.
4. The user’s browser submits the authentication request to the IdP.
5. The IdP does the following:
   - Decodes the SAML request
   - Extracts the URL for the CAS (Customer Assertion Service) of Zscaler
   - Authenticates the user by login credentials or by checking for valid Active Directory session
   - Generates a SAML response with digitally signed public/private DSA/RSA keys, encodes it and sends it to browser
6. The browser forwards the SAML response to the service.
7. The CAS of Zscaler uses the IdP’s public key to verify the response.
8. After the service successfully verifies the response, it logs in the user and redirects the user’s browser to the destination URL.
Browser Configuration

In order to work with the Zscaler proxy, you will need to configure your browser to connect to the Zscaler Security Cloud. This section contains configuration steps for the following browsers:

- Configuring Internet Explorer for Connection to Zscaler Security Cloud – see below
- Configuring Firefox for Connection to Zscaler Security Cloud – see page 18

**Configuring Internet Explorer for Connection to Zscaler Security Cloud**

1. Open Internet Explorer.
2. Click **Tools > Internet Options**.
3. On the **Internet Options** window, click **Connections > LAN settings**.
4. On the **Local Area Network (LAN) Settings** dialog box, perform the appropriate steps for automatic or manual configuration.

**Automatic Configuration**

In the **Automatic configuration** section, do the following:

a. Select **Automatically detect settings**.

b. Select **Use automatic configuration script**. If a custom URL has not been provided in the **Address** field, you can enter the system default URL, **http://pac.zcaler.net/zScaler.net/proxy.pac**.

c. Click **OK**.
Manual Configuration
In the Proxy server section, do the following:

a. Select **Use a proxy server for your LAN**.
b. In the **Address** field, type **gateway.zscaler.net**.
c. In the **Port** field, enter the port number (for example, **80**, which is the most commonly used port).
d. Click **OK**.

---

Configuring Firefox for Connection to Zscaler Security Cloud

1. Open Firefox.
2. Click **Tools > Options**.
3. On the **Options** window, click **Advanced > Network**.
4. On the **Network** tab, click **Settings**.

5. On the **Connection Settings** dialog box, perform the appropriate steps for automatic or manual configuration.

   **Automatic Configuration**

For automatic proxy configuration, do the following:

a. On the **Connection Settings** dialog box, select **Automatic proxy configuration URL**.

b. In the text box, enter the PAC file URL supplied by your sales engineer. If a custom URL has not been provided, use the system default URL, **http://pac.zscaler.net/zscaler.net/proxy.pac**.

c. Click **OK**.
Manual Configuration

For manual proxy configuration, do the following:

a. On the **Connection Settings** dialog box, select **Manual proxy configuration**.

b. In the **HTTP Proxy** field, type `gateway.zscaler.net`.

c. In the **Port** field, enter the port number (for example, **80**, which is the most commonly used port).

d. In the **No Proxy for** text box, type the SAM domain for exclusion, as shown in the example below.

e. Click **OK** to save the configuration.

![Connection Settings Dialog](image)

Connecting to Zcaler

1. Launch a browser and go to any site (for example, google.com).

2. On the **Zcaler** login window, type your user name, then click **Submit**.
3. On the SAM **Login** window, type your username, select the appropriate **Security** option, then click **OK**.

![User Identification](image1)

4. The requested website is opened through the Zscaler proxy.

![Google](image2)
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>Address</td>
<td>SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td>Phone</td>
<td>United States 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 1-410-931-7520</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:support@safenet-inc.com">support@safenet-inc.com</a></td>
</tr>
<tr>
<td>Support and Downloads</td>
<td><a href="http://www.safenet-inc.com/Support">www.safenet-inc.com/Support</a> Provides access to the SafeNet Knowledge Base and quick downloads for various products.</td>
</tr>
<tr>
<td>Technical Support</td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Customer Portal</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>