SafeNet Authentication Manager Integration Guide

Using SAM as an Identity Provider for Tableau Server
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012985-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>April 2015</td>
</tr>
</tbody>
</table>

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

- Third-Party Software Acknowledgement ................................................................. 4
- Description .................................................................................................................. 4
- Applicability ............................................................................................................... 4
- Environment .............................................................................................................. 4
- Audience ................................................................................................................... 5
- SAML Authentication using SAM .............................................................................. 5
- Authentication Dataflow using SAM .......................................................................... 5
- SAML Prerequisites .................................................................................................. 6
- Configuring Tableau Server ...................................................................................... 6
- Configuring SafeNet Authentication Manager ........................................................... 8
  - Synchronizing User Stores to SAM ........................................................................ 8
  - Assigning a Token in SAM ..................................................................................... 9
  - Configuring SAM as an Identity Provider ............................................................. 10
  - Downloading the SAM’s Metadata ....................................................................... 12
  - Configuring SAM for SAML-based User Federation ............................................ 13
- Running the Solution ................................................................................................. 17
- Support Contacts ...................................................................................................... 18
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Tableau Server.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

Tableau Server is an enterprise-class data governance platform that offers powerful mobile and browser-based analytics. Administrators can define data sources, add metadata, and author new calculations and data fields for users to securely access.

This document describes how to:

- Configure SAML authentication in Tableau Server using SafeNet Authentication Manager as an identity provider.

It is assumed that the Tableau Server environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager.

Tableau Server can be configured to support multi-factor authentication in several modes. The SAML authentication will be used for the purpose of working with SafeNet Authentication Manager.

Applicability

The information in this document applies to:

- **SafeNet Authentication Manager**—A server version of SAM that is used to deploy the solution on-premises in the organization.

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Manager**—Version 8.2 (HF 468)
- **Tableau Server**—Version 8.3
Audience

This document is targeted to system administrators who are familiar with Tableau Server, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Manager.

SAML Authentication using SAM

SAM provides a SAML authentication option that is already implemented in the SAM environment, and can be used without any installation.

![Diagram of SAML authentication using SAM](image)

Authentication Dataflow using SAM

SafeNet Authentication Manager communicates with a large number of service providers and cloud-based services solutions using the SAML protocol.

The image below describes the dataflow of a multi-factor authentication transaction for Tableau Server.

![Diagram of authentication dataflow using SAM](image)

1. A user attempts to log on to Tableau Server using a one-time password (OTP) token.
2. The user is redirected to SafeNet Authentication Manager (SAM). SAM collects and evaluates the user's credentials.
3. SAM returns a response to Tableau Server, accepting or rejecting the user's authentication request.
SAML Prerequisites

To enable SafeNet Authentication Manager to receive SAML authentication requests from Tableau Server, ensure the following:

1. The end users can authenticate through the Tableau Server environment with a static password.
2. A PEM-encoded X.509 certificate with a .crt file extension should be available. This file is used by Tableau Server, not the identity provider.
3. An RSA or DSA private key file that is not password-protected, and has a .key file extension should be available. This file is used by Tableau Server, not the identity provider.

NOTE: If you are using a PEM-encoded X.509 certificate file for SSL, you can use the same file for SAML. When it’s used for SSL, the certificate file is used to encrypt traffic. When it’s used for SAML, the certificate is used for authentication. Tableau Server does not support certificate and certificate key files for SAML if the certificate and certificate key require a chain file. If your SSL certificate and certificate key file require a chain file, you need to generate a new certificate and key file to use for SAML.

Configuring Tableau Server

Before you begin, make sure the SAM metadata is downloaded so that it is available for selection in the following procedure. If you have not already downloaded the SAM metadata, please refer to “Download the SAM’s Metadata.”

1. Log in on the machine where Tableau Server is installed.
2. From the Windows Start menu, click All Programs > Tableau Server 8.3 > Stop Tableau Server.
3. Wait until Tableau Server has completely stopped, and then click Start > All Programs > Tableau Server 8.3 > Configure Tableau Server.

(The screen image above is from Tableau Software®. Trademarks are the property of their respective owners.)
4. On the **General** tab, enter the Tableau Server administrator’s password in the **Password** field.

5. Click the **SAML** tab.

6. Click the **Use SAML for single sign-on** check box, and then complete the following fields:

| **Tableau Server return URL** | Enter the Tableau Server URL (for example, `http://<DNS or IP of Tableau Server>`). Do not end the URL with '/'.
| **SAML entity ID** | Enter the entity ID of Tableau Server (for example, **Tableau**).
| **SAML certificate file** | Click **adjacent to the field, and then select the SAML certificate. It should be a PEM-encoded X.509 certificate with a `.crt` file extension.
| **SAML key file** | Click **button adjacent to the field, and then select the SAML certificate key file. It should be an RSA or DSA private key file that is not password-protected, and has a `.key` file extension.
| **SAML IdP metadata file** | Click **adjacent to the field, and then select the SAM metadata file. The SAM metadata must be downloaded in order to select the file here. If you have not already downloaded the SAM metadata, please refer to “Download the SAM’s Metadata.”

7. Click **Export Metadata File**, and save the Tableau Server metadata locally. The metadata will be required to configure SAM (see “Configuring SAM for SAML-based User Federation”).

8. Click **OK**. It will take some time to save the settings.

9. When the settings have been saved, click **OK** again.

(The screen image above is from Tableau Software®. Trademarks are the property of their respective owners.)
10. Open a command prompt window, and then browse to C:\Program Files\Tableau\Tableau Server\8.3\bin.
11. Type the following command, and then press Enter:
   `tabadmin set wgserver.saml.idpattribute.username urn:oid:0.9.2342.19200300.100.1.1`
12. Type the following command, and then press Enter:
   `tabadmin restart`

Configuring SafeNet Authentication Manager

The deployment of multi-factor authentication using SAM as an identity provider for Tableau Server requires the following:

- Synchronizing User Stores to SAM, page 8
Assigning a Token in SAM, page 9
• Configuring SAM as an Identity Provider, page 10
Synchronizing User Stores to SAM

SAM manages and maintains OTP token information in its data store, including the token status, the OTP algorithm used to generate the OTP, and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal (“stand-alone”) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server
Assigning a Token in SAM

SAM supports a number of OTP authentication methods that can be used as a second authentication factor for users authenticating through Tableau Server.

The following tokens are supported:

- eToken PASS
- SafeNet GOLD
- SafeNet eToken 3400
- SafeNet eToken 3500
- eToken NG-OTP
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging
- SafeNet Mobile Authentication (iOS)

Tokens can be assigned to users as follows:

- **SAM Management Center**—Management site used by SAM administrators and help desk personnel for token enrollment and lifecycle management.
- **SAM Self-Service Center**—Self-service site used by end users for managing their tokens.
- **SAM Remote Service**—Self-service site used by employees not on the organization’s premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet's tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.
Configuring SAM as an Identity Provider

To use Tableau Server as a service provider and SAM as an identity provider, SAM must be configured as an identity provider.

1. From the Windows Start menu, click SafeNet > SafeNet Authentication Manager > Configuration Manager.

2. Click the Action tab, and then select Cloud Configuration.
3. Click the **Info for Service Provider** tab.

4. Type the web address of the SAM portal server in the **Domain URL** field.

![Cloud Settings with completed information](image)

The remaining fields are generated according to the Domain URL that was entered.

![Cloud Settings with populated fields](image)

5. Click **OK**.
Downloading the SAM’s Metadata

SAM metadata is required to configure the identity provider in Tableau Server. (Refer to step 6 in “Configuring Tableau Server.”)

1. From the Windows Start menu, click SafeNet > SafeNet Authentication Manager > Configuration Manager.

![Configuration Manager](image1)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

2. Click the Action tab, and then select Cloud Configuration.

![Cloud Configuration](image2)
3. On the **Cloud Settings** window, click the **Info for Service Provider** tab.

   ![Cloud Settings window](image)

4. Click **Download Metadata**, and then save the metadata file that will be imported to Tableau Server.

### 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 the SAM portal to communicate with service providers.

For general portal configuration, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

To edit the TPO for SAM’s portal configuration, complete the following procedure.

1. Open the **Token Policy Object Editor** for the required group. See the *SafeNet Authentication Manager 8.2 Administrator’s Guide* for more information.

2. In the left pane, click **Protected Application Settings > User Authentication**.

   ![Token Policy Object Editor](image)

3. In the right pane, double-click **Application Authentication Settings**.
4. Select **Define this policy setting**, select **Enabled**, and then click **Definitions**.

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

6. Browse to the Tableau Server metadata file that you exported (in step 7 in “Configuring Tableau Server”), and then click **Open**.
7. On the **Import Metadata** window, click **OK**.

8. Rename the Tableau profile to a user-friendly name (for example, **Tableau**).

9. In the left pane, click the new profile.

10. In the right pane, double-click the following policies, and then complete the following fields:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Policy Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAM issuer</td>
<td>Tableau</td>
</tr>
<tr>
<td>Audience URI</td>
<td>Tableau Server entity ID. It should match the entity ID in the <strong>Application issuer</strong> field.</td>
</tr>
<tr>
<td>User mapping</td>
<td>Select the field name in your user repository that identifies your Tableau Server login name.</td>
</tr>
</tbody>
</table>

  **SAM issuer**

  Enter a unique SAM ID to be identified in SAML authentication. This entity ID should match the entity ID of the SAM metadata file.

  **Audience URI**

  Enter the Tableau Server entity ID. It should match the entity ID in the **Application issuer** field.

  **User mapping**

  Select the field name in your user repository that identifies your Tableau Server login name.
11. Enable the appropriate authentication method(s) for your organization. See the SafeNet Authentication Manager Version 8.2 Administrator's Guide for detailed information about authentication methods.

The following is an example of the completed policy settings in the Application Authentication Settings window:

```
12. Click OK until all of the Token Policy Object Editor windows are closed.
```
Running the Solution

Check the configured solution after successfully configuring the Tableau Server for SAML authentication.

In the following solution, the user is enrolled with an NG-OTP Token.

1. Open the web browser and enter the URL of Tableau Server. (For example, http://<IP or DNS of Tableau Server>).

2. The SAM User Identification page is displayed. Enter the username in the Username field, and then click OK.

3. The OTP Authentication page is displayed. Generate a one-time password, and then enter it in the OTP Authentication Code field.
4. Click OK. If the credentials are valid, the user will be redirected to the Tableau Server portal.

(The screen image above is from Tableau Software®. Trademarks are the property of their respective owners.)

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>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
</table>
| Address                        | SafeNet, Inc.  
4690 Millennium Drive  
Belcamp, Maryland 21017 USA |
| Phone                          | United States  
1-800-545-6608  
International  
1-410-931-7520 |
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. |