Protecting Syncplicity with SafeNet Authentication Manager

Version 8.2

Integration Guide

All attempts have been made to make the information in this document complete and accurate.

SafeNet, Inc. is not responsible for any direct or indirect damages or loss of business resulting from inaccuracies or omissions. The specifications contained in this document are subject to change without notice.

SafeNet Hardware and/or Software products described in this document may be protected by one or more U.S. Patents, foreign patents, or pending patent applications.

Please contact SafeNet Support for details of FCC Compliance, CE Compliance, and UL Notification.

Date of Publication: April 2013

Last update: April 29, 2013

Contacting SafeNet

We work closely with our reseller partners to offer the best worldwide technical support services. Your reseller is the first line of support when you have questions about products and services. However, if you require additional assistance you can contact the SafeNet technical support team help-desk which is available 24 hours a day, seven days a week:

Country/Region	Telephone
USA	+1-800-545-6608
International	+1-410-931-7520

For further assistance submit additional questions to the SafeNet technical support team at the following web page:

http://c3.safenet-inc.com/secure.asp

For assistance via email to SafeNet technical support send the request to the following address:

support@safenet-inc.com

Publication History

Date	Description	Revision
2013.04.08	Initial release	1.0
2013.04.29	Minor text change	1.1

Table of Contents

About This Guide

The goal of this document is to provide guidance for enabling SafeNet Authentication Manager (SAM) strong authentication with Syncplicity.

Applicability

The information in this document applies to:

- SafeNet Authentication Manager version 8.2

Resources

This document may refer to additional resources. Please see the *SafeNet Authentication Manager 8.2 User's Guide* and *SafeNet Authentication Manager 8.2 Administrator's Guide*.

Environment

Environment	Configuration
Syncplicity	Syncplicity Business Edition account, or higher
SafeNet Authentication Manager version 8.2	SafeNet external portal installed and configured

Overview

This guide describes the process for enabling SafeNet Authentication Manager (SAM) strong authentication with Syncplicity's cloud-based solution for file backup, sharing, and synchronization. This document assumes that the Syncplicity environment is already configured and working with 'static' passwords prior to implementing SAM strong authentication. In this document, we configure Syncplicity for Single Sign-On (SSO) using SafeNet Authentication Manager for strong authentication.

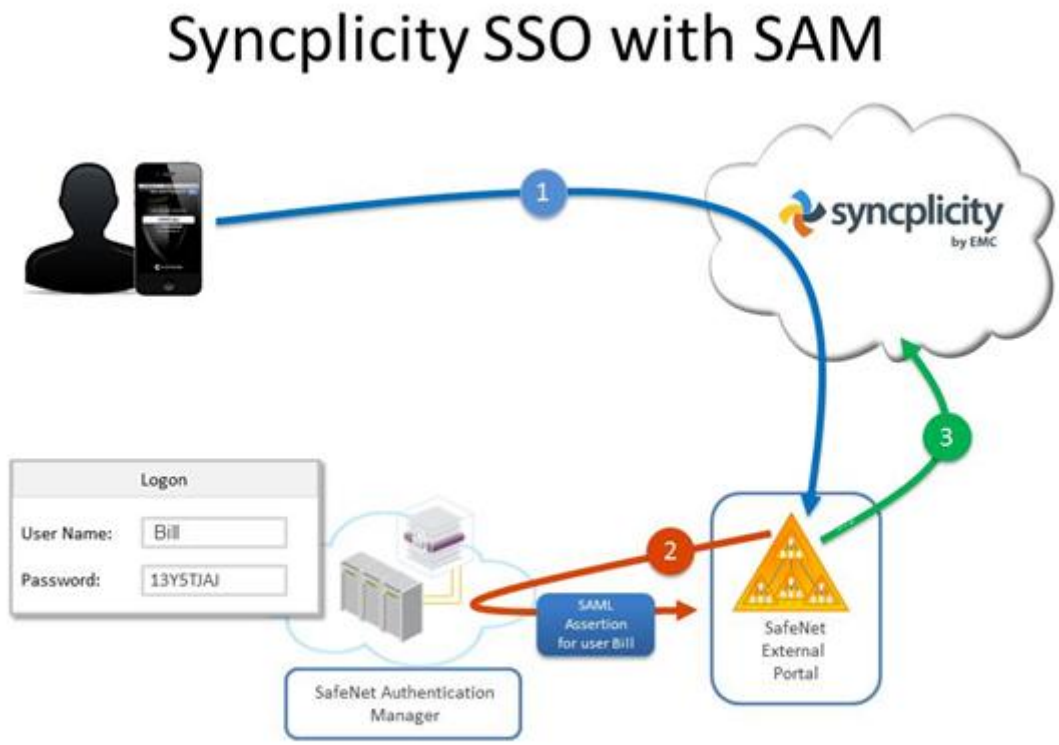


Figure 1: SafeNet Authentication Manager with Syncplicity

1. Bill, a user, wants to connect to Syncplicity using an external portal provided by SafeNet Authentication Manager (SAM).
2. The external portal collects Bill's credentials and passes them to SafeNet Authentication Manager for authentication.
   SAM evaluates Bill'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 *error assertion* to Syncplicity.

Syncplicity Configuration

Set SafeNet Authentication Manager as an Identity Provider in Syncplicity.

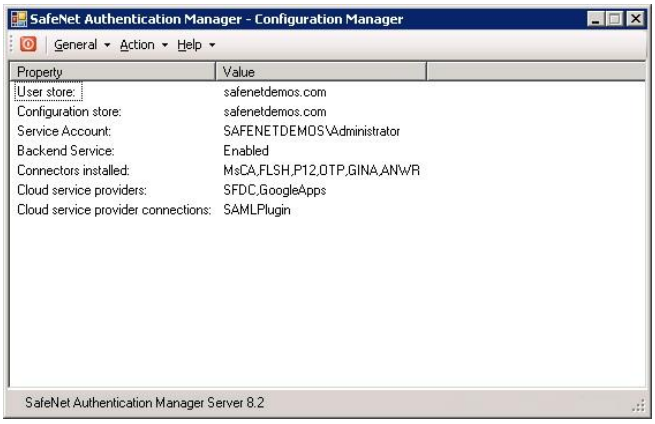
Viewing SAM's Cloud Settings

Display the SAM data that will be needed for Syncplicity configuration in *Adding SAM as an Identity Provider in Syncplicity* on page 9.

To access the SAM Cloud Settings required for Syncplicity configuration:

1. From the Windows *Start* menu, go to *SafeNet Authentication Manager* > *Configuration Manager*.

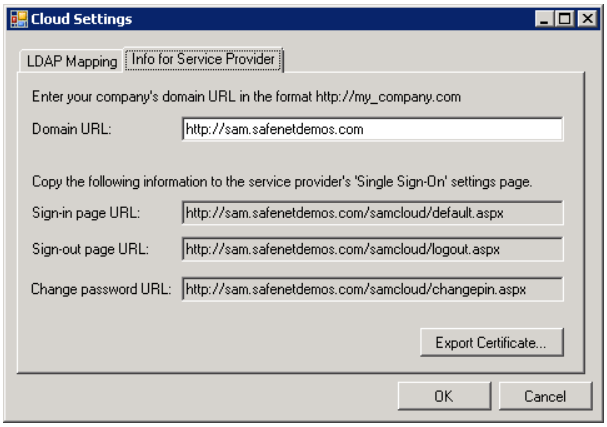
   The *Configuration Manager* window opens.



2. From the menu bar, go to *Action* > *Cloud Configuration*.

   The *Cloud Settings* window opens.

3. Select the *Info for Service Provider* tab.



4. In the **Domain URL** field, enter the domain URL of your company's SAM external portal.

The *Single Sign-On* fields are displayed.
Do not close the *Cloud Settings* window. The displayed values will be needed in step 4 of *Adding SAM as an Identity Provider in Syncplicity*.

5. Click **Export Certificate**, save the signing certificate to a known location, and change the certificate filename's extension to `.pem`.
The filename will be needed in step 4e of *Adding SAM as an Identity Provider in Syncplicity*.

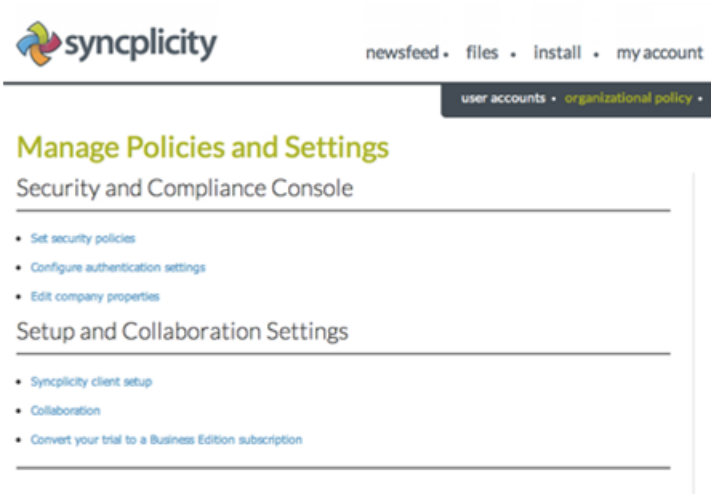
Adding SAM as an Identity Provider in Syncplicity

Use SAM's Cloud Settings to configure Syncplicity.
See *Viewing SAM's Cloud Settings* on page 8 to view the Cloud Settings.

To add SAM as an Identity Provider in Syncplicity:

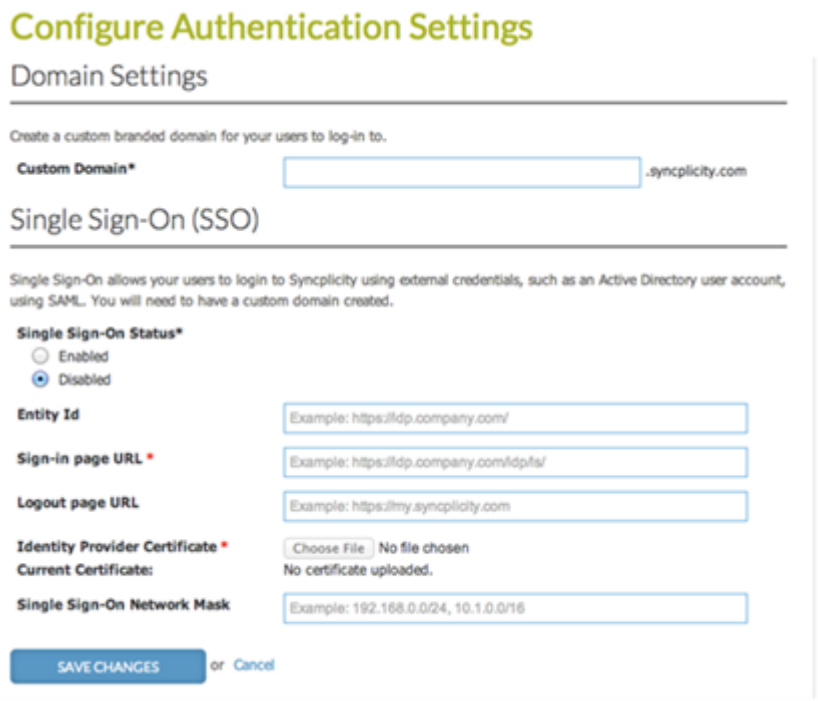
1. Log in as an administrator to Syncplicity.

   Syncplicity's *Manage Policies and Settings* window opens.



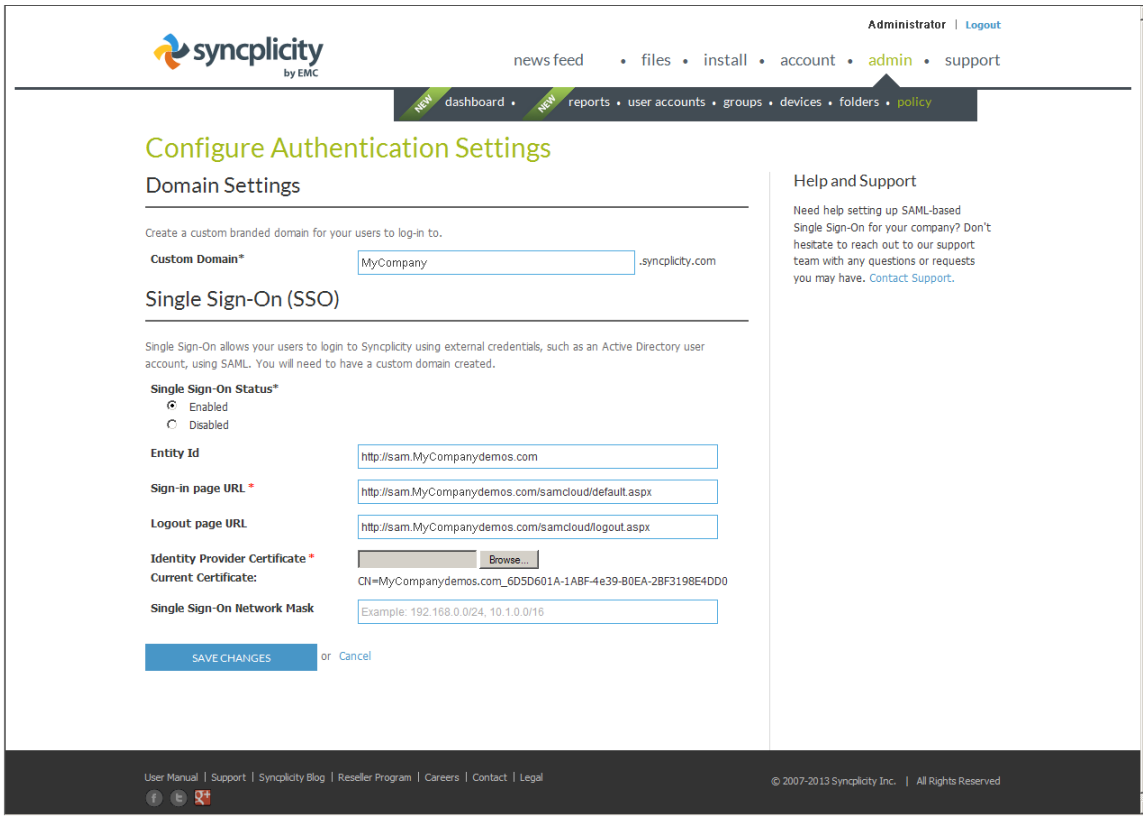
2. In the left panel, select **Configure authentication settings**.

   The *Configure Authentication Settings* window opens.



3. In the *Custom Domain* field, enter a value to create a custom domain for your users to log in to.
4. In the *Single Sign-On (SSO)* area, do the following:
   a. Enable **Single Sign-On Status**.
   b. In the **Entity Id** field, enter a unique string in URL format.
      This will be used for communication between Syncplicity and your company's SAM server.
      This value will be needed for *SAML Authentication Configuration*, step 9b, on page 14.
   c. In the **Sign-in page URL** field, copy the *Sign-in page URL* field from SAM's *Cloud Settings* window displayed in step 4 of *Viewing SAM's Cloud Settings*.
   d. In the **Logout page URL** field, copy the *Sign-out page URL* field from SAM's *Cloud Settings* window displayed in step 4 of *Viewing SAM's Cloud Settings*.
   e. In the **Identity Provider Certificate** field, browse to the signing certificate saved in step 5 of *Viewing SAM's Cloud Settings*, and open it.

   The following is an example of the completed fields in the *Syncplicity* console.



5. In the *Syncplicity* console, click **Save Changes**.
6. In SAM's *Cloud Settings* window, click **OK**, and close the *SAM Configuration Manager*.

SAM is now configured as an Identity Provider in Syncplicity.

SAML Authentication Configuration in SAM

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

Note

See the *SafeNet Authentication Manager 8.2 Administrator's Guide* for general portal configuration.

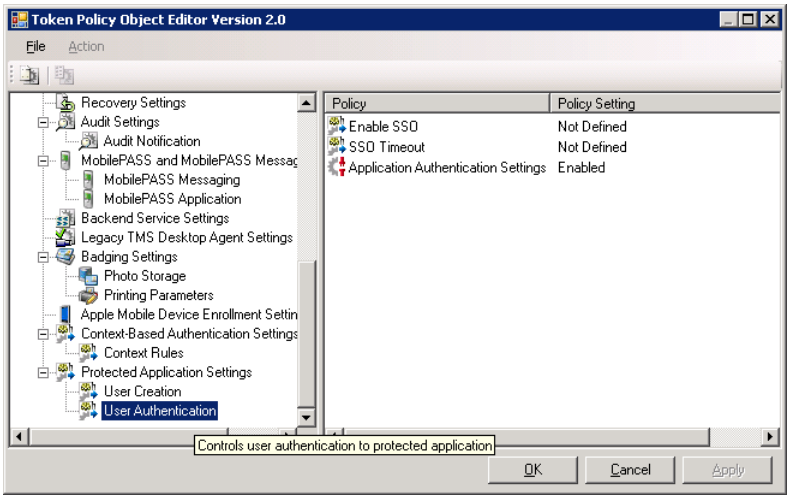
To edit the TPO policies for SAM portal configuration:

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

   The *Token Policy Object Editor* window opens.

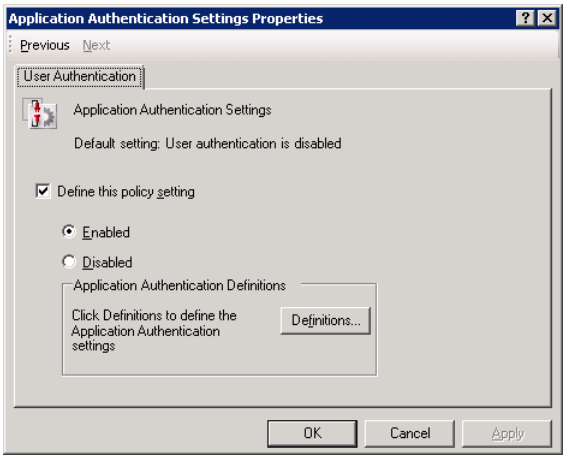
2. In the left pane, go to **Protected Application Settings > User Authentication**.

   Policies are displayed in the right pane.



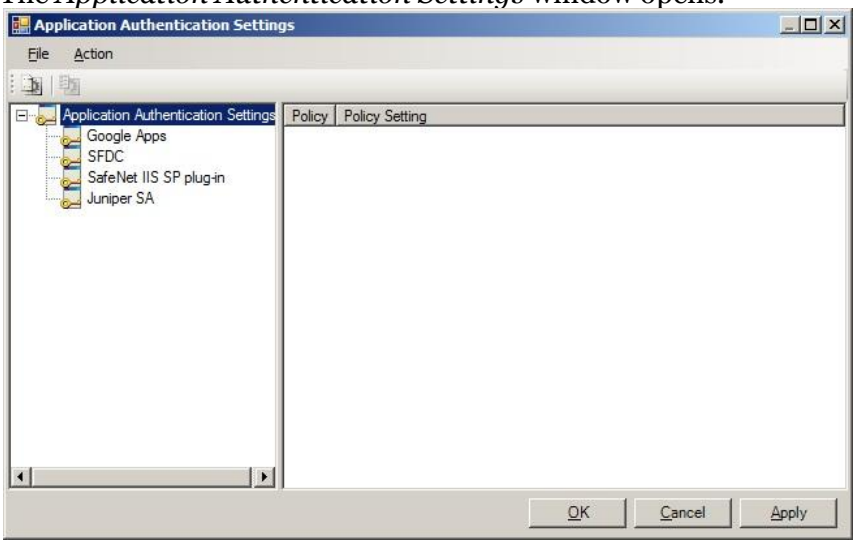
3. In the right pane, double-click **Application Authentication Settings**.

   The *Application Authentication Settings Properties* window opens.



4. Select **Define this policy setting**, and select **Enabled**.
5. Click **Definitions**.

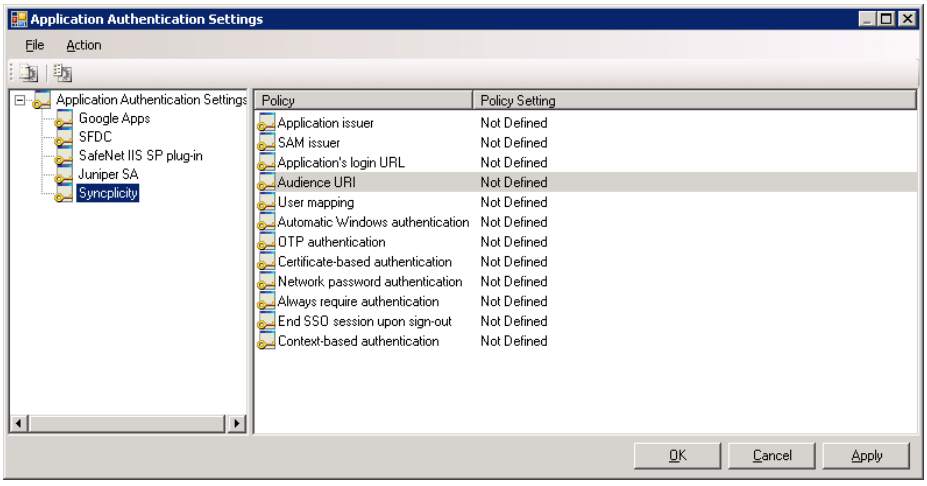
   The *Application Authentication Settings* window opens.



6. In the left pane, right click **Application Authentication Settings**, and from the dropdown menu, select **Create a new profile**.

   A new profile is created.
7. In the left pane, right click the new profile, and from the dropdown menu, select **Rename**.
8. Rename the profile **Syncplicity**, and select it.

   The profile's policies are displayed in the right pane.



9. In the right pane, double-click the following policies, and enter the appropriate information:

   a. **Application Issuer**: Enter

   `https://<your-subdomain>.syncplicity.com/sp`

   where

   `<your-subdomain>.syncplicity.com` is your users' logon domain defined in *Adding SAM as an Identity Provider in Syncplicity*, step 3, on page 10.

b. **SAM Issuer**: Enter the unique string that was entered into the Syncplicity console's **Entity Id** field during *Adding SAM as an Identity Provider in Syncplicity*, step 4b, on page 10.

c. **Application's login URL**: Enter

`https://<your-subdomain>.syncplicity.com/Auth/AssertionConsumerService.aspx`

where

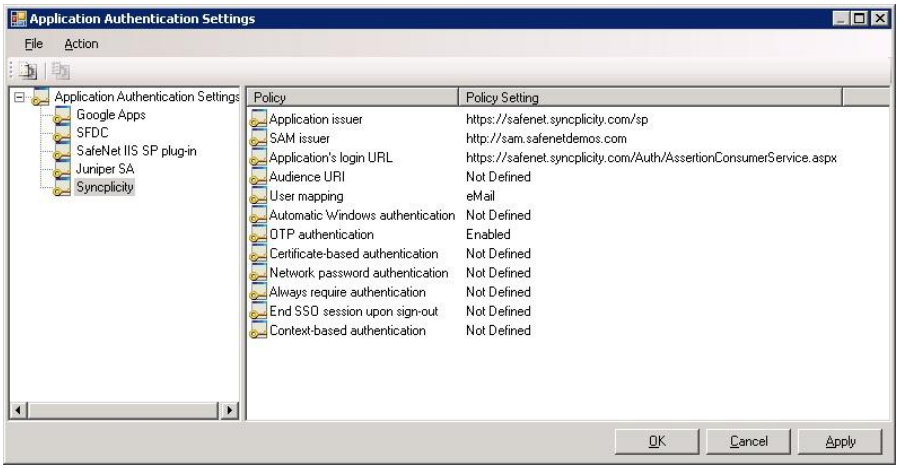
`<your-subdomain>.syncplicity.com` is your users' logon domain defined in *Adding SAM as an Identity Provider in Syncplicity*, step 3, on page 10.

d. **User mapping**: Set to **eMail**.

e. Enable the appropriate authentication methods for your organization.

See the *SafeNet Authentication Manager 8.2 Administrator's Guide* for information about authentication methods.

The following is an example of completed fields in the *Application Authentication Settings* window:



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

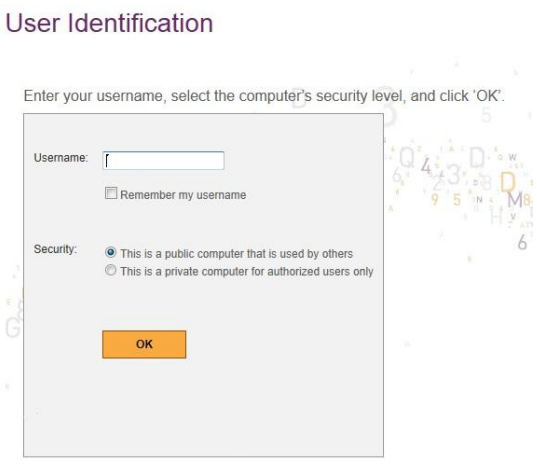
Running the Solution

User logon to Syncplicity uses SAML authentication through SafeNet Authentication Manager.

To log on to your Syncplicity environment:

1. Browse to
   `https://<your-subdomain>.syncplicity.com`
   where
   `<your-subdomain>.syncplicity.com` is the logon domain defined in *Adding SAM as an Identity Provider in Syncplicity*, step 3, on page 10.

   You are redirected to the SAM external portal's authentication page.

2. Enter your SAM credentials, and click **OK**.

You are logged on to your Syncplicity portal.