THE DATA PROTECTION COMPANY

SafeNet Authentication Manager

INTEGRATION GUIDE

Using SAM as an Identity Provider for Remedyforce

Contents

Support Contacts

If you have questions or need additional assistance, contact SafeNet Customer Support through the listings below:

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Email	support@safenet-inc.com	
Support and Downloads	www.safenet-inc.com/Support Provides access to the SafeNet Knowledge Base and quick downloads for various products.	
Technical Support Customer Portal	https://serviceportal.safenet-inc.com 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.	

Description

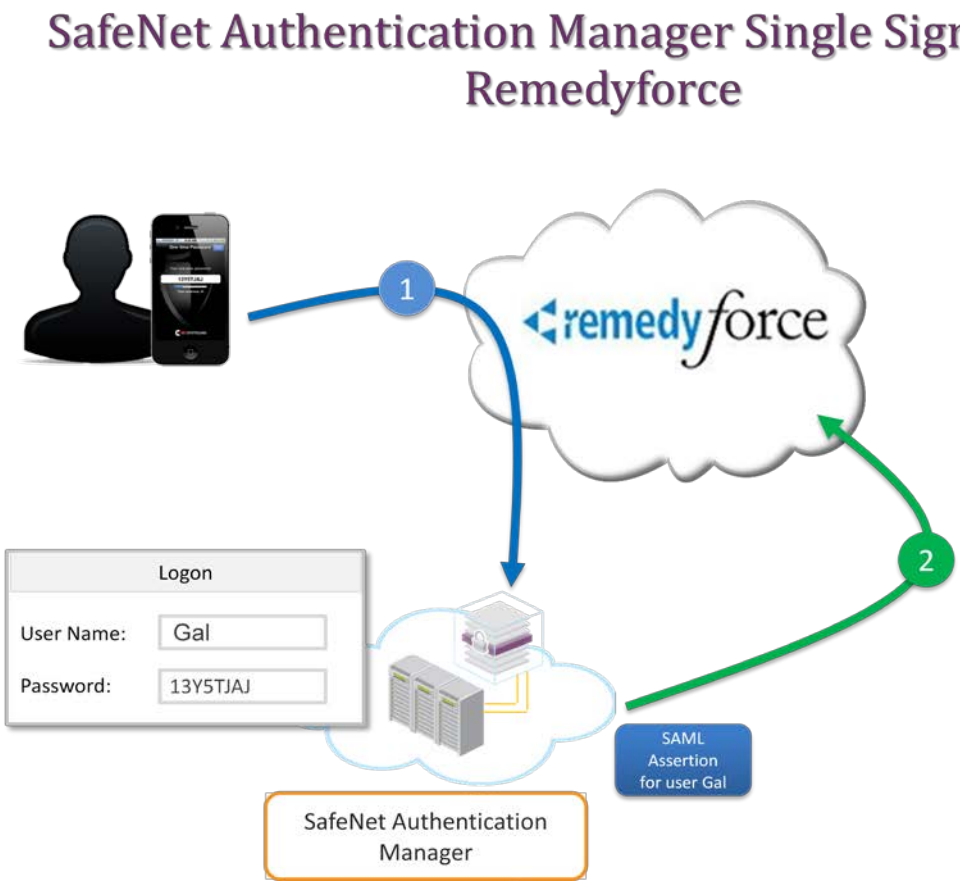
This document describes how to set up and manage SafeNet Authentication Manager (SAM) 8.2 as an Identity Provider for Remedyforce.

Some instructions in this document are common to many applications that use SAML protocol for user federation.

NOTE

The document assumes that Remedyforce is already configured and working with static passwords prior to implementing SafeNet Authentication Manager strong authentication.

Single Sign-On Dataflow



A. Gal, a user, wants to log in to Remedyforce. Gal leverages the single sign-on capabilities embedded in the organization's SafeNet Authentication Manager (SAM) solution.

B. SafeNet Authentication Manager's external portal collects Gal's credentials and passes them to SafeNet Authentication Manager for authentication.
SAM evaluates Gal's credentials, and returns an *accept* or *reject* response to the external portal.

C. The portal uses SAM's response to return an *accept* or *error assertion* to Remedyforce.

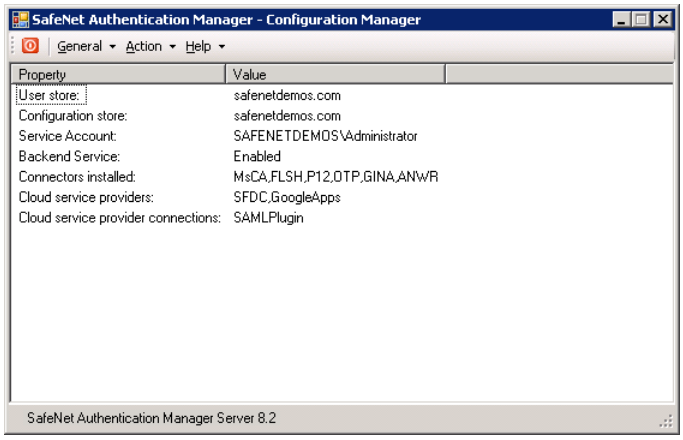
Configuring SAM as an Identity Provider

The SAM Configuration Manager and TPO settings are used for setting SafeNet Authentication Manager (SAM) as the Remedyforce application's identity provider.

To configure SAM as an identity provider:

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

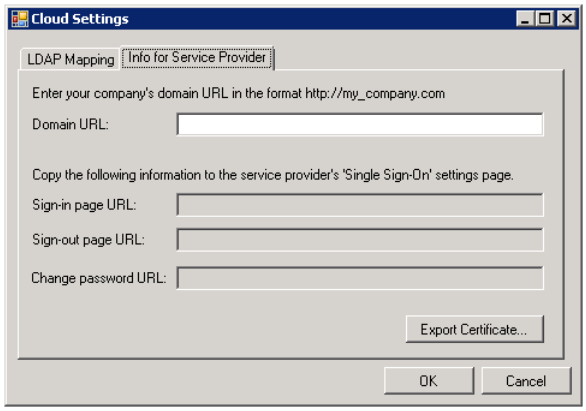
   The *Configuration Manager* window opens.



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

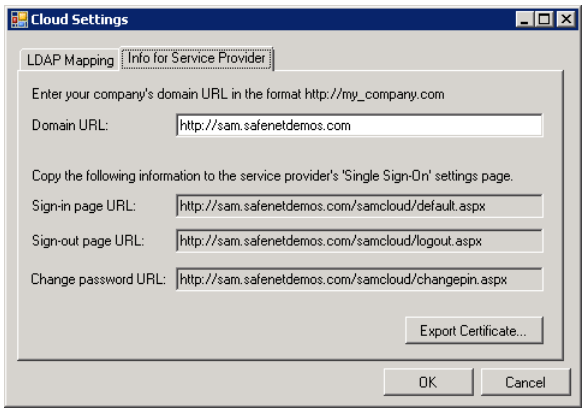
   The *Cloud Settings* window opens.

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



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

The **Single Sign-On** fields are automatically filled.



5. Do not close the *Cloud Settings* window.

   The displayed values will be needed in steps 7d and 7e of *Configuring Remedyforce to Use SAM as an Identity Provider*, on page 7.

6. Click **Export Certificate**, and save the certificate file.

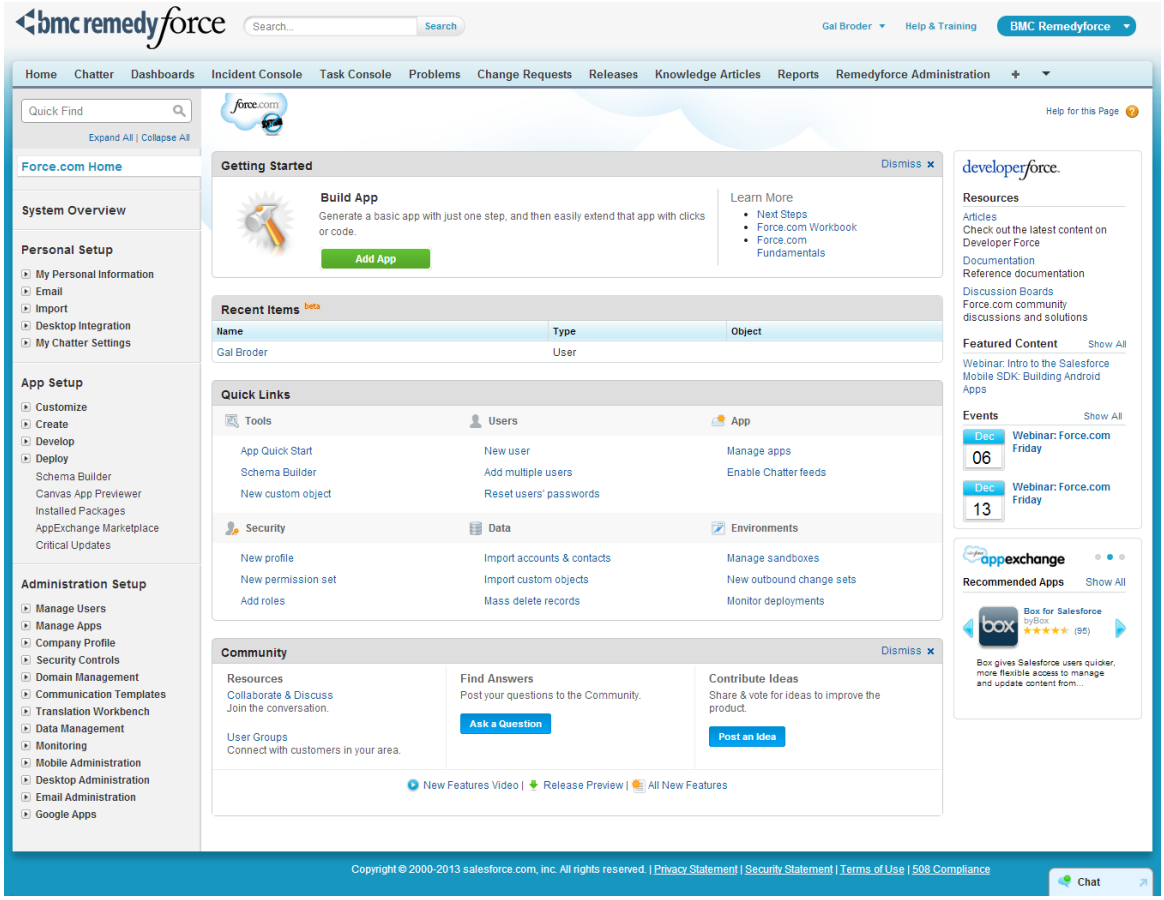
   This file will be needed in step 7c *Configuring Remedyforce to Use SAM as an Identity Provider*, on page 7.

Configuring Remedyforce to Use SAM as an Identity Provider

To configure Remedyforce to use SAM as an identity provider:

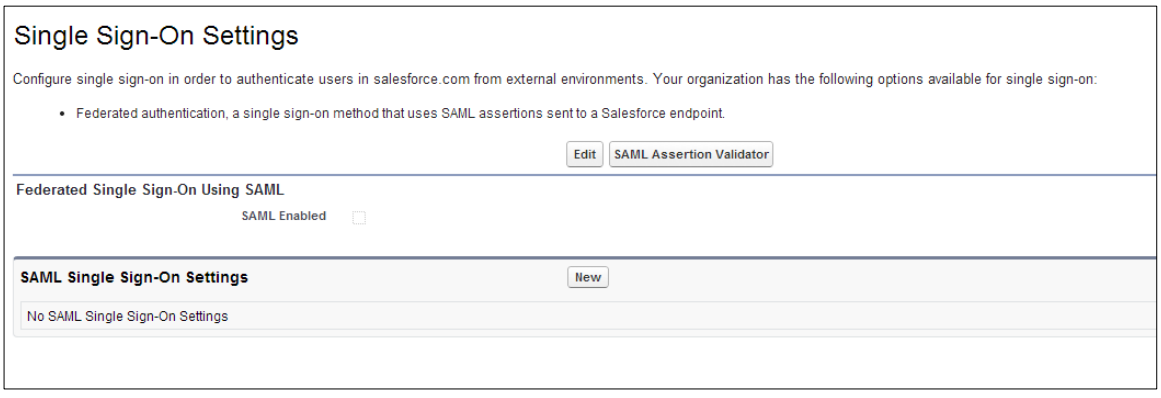
1. Log on to Remedyforce.
2. At the top right of the window, open the **<your user name>** dropdown menu, and select **Setup**.

The *Settings* window opens.

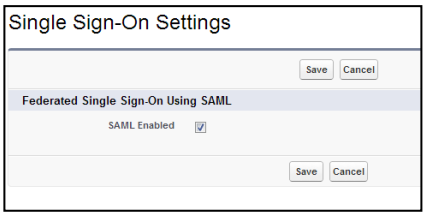


3. In the left pane, select **Administration Setup > Security Controls > Single Sign-On Settings**.

The *Single Sign-On Settings* window opens.

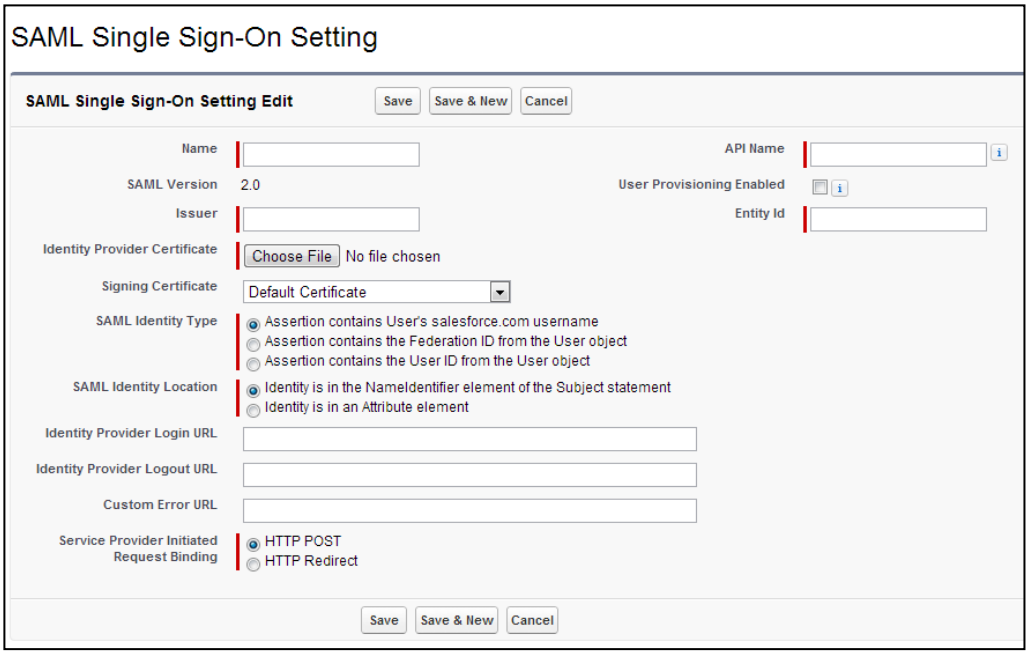


4. Click **Edit**, and then select **SAML Enabled**.



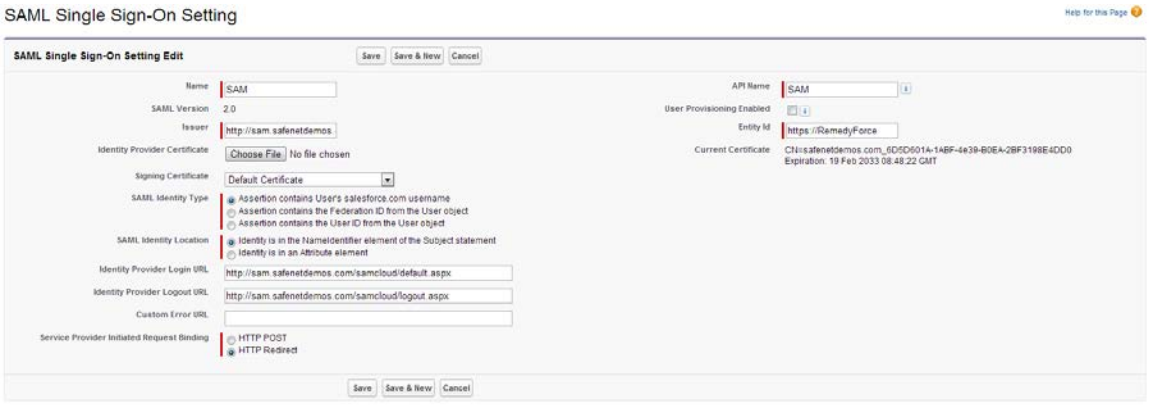
5. Click **Save**.
6. Click **New**.

   The *SAML Single Sign-On* window opens.



7. Do the following:
   a. In the **Name** field, enter a name by which to identify the new Identity Provider, for example, "*SAM*".
   b. In the **Issuer** field, enter a unique SAM ID. This will be SafeNet Authentication Manager's identifier in Remedyforce.
   c. In **Identity Provider Certificate**, click **Choose File** and select the certificate that was exported from the SAM`s *Cloud Settings* window. (See step 6 of *Configuring SAM as an Identity Provider*, on page 5.)
   d. In the **Identity Provider Login URL** field, copy the **Sign-in page URL** value displayed in SAM`s *Cloud Settings* window. (See step 5 of *Configuring SAM as an Identity Provider*, on page 5.)
   e. In the **Identity Provider Logout URL** field, copy the **Sign-out page URL** value displayed in SAM`s *Cloud Settings* window. (See step 5 of *Configuring SAM as an Identity Provider*, on page 5.)
   f. In **Service Provider Initiated Request Binding**, select **HTTP Redirect**.
   g. In the **API Name** field, enter any string.
   h. In the **Entity ID** field, enter a unique string that start with https. This will identify Remedyforce in the connection with SAM.

The following shows an example of the entry fields in a completed setup in the Remedyforce`s *SAML Single Sign-On Setting* configuration window.

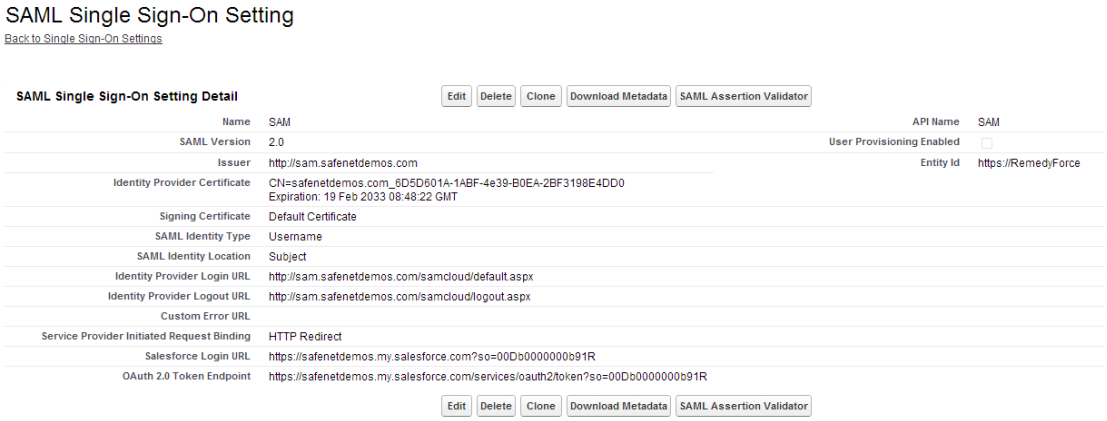


8. Click **Save**.

   The *Single Sign-On Settings* window now contains the IdP name that was just created for SAM.

9. Click the IdP name that was just created.

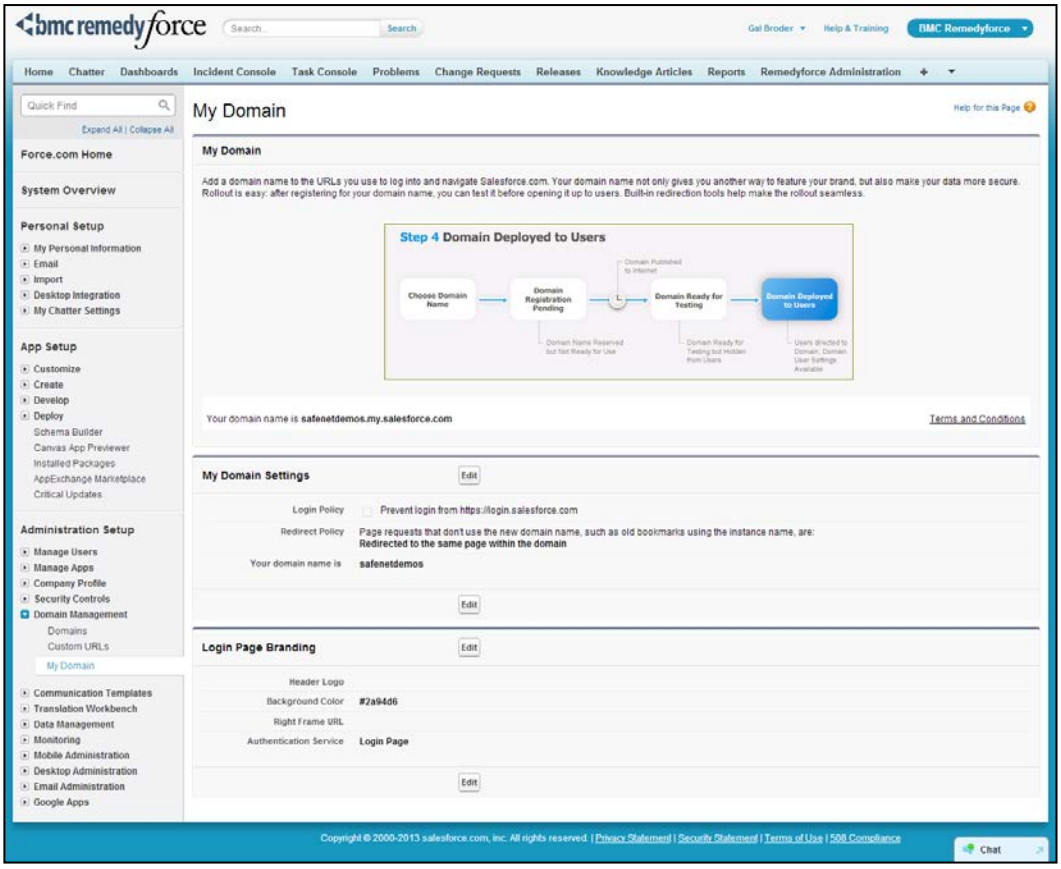
   The *SAML Single Sign-On Setting* window opens, summarizing the configuration.



   The displayed values will be needed in step 9 of *Configuring SAM to use SAML-Based User Federation*, on page 11.

10. In the left pane, select **Administration Setup > Domain Management > My Domain**.

The *My Domain* window opens.

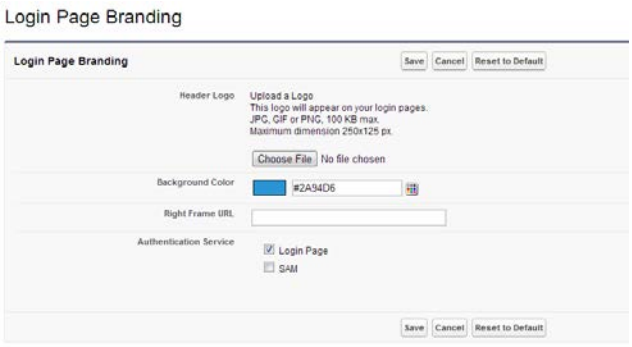


NOTE

Your own Salesforce domain must have been registered.

11. Under **Login Page Branding**, click **Edit**.

    The *Login Page Branding* window opens.



12. Under **Authentication Service**, uncheck **Login Page**, and select the IdP representing SAM.
13. Click **Save**.

Configuring SAM to use 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.

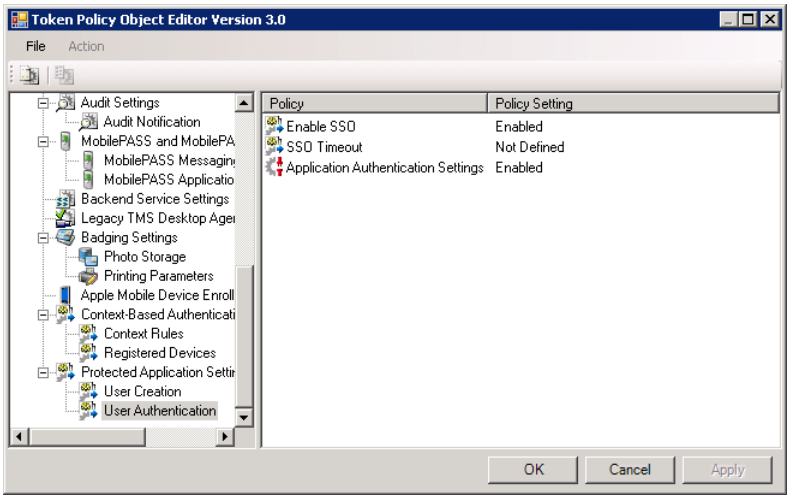
NOTE

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

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

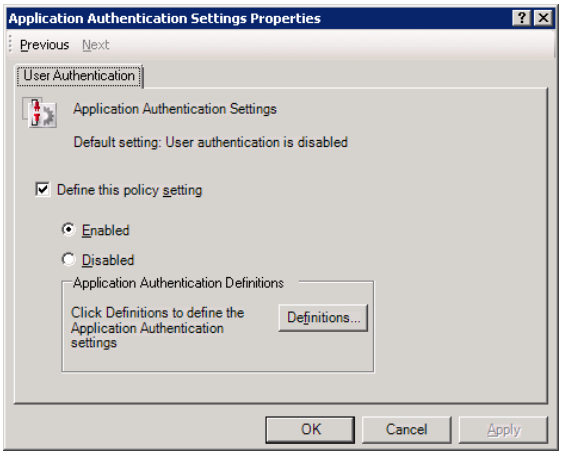
1. Open the *Token Policy Object Editor* for the appropriate group. See the *SafeNet Authentication Manager Version 8.2 Administrator's Guide* for more information.
2. In the left pane, select **Protected Application Settings > User Authentication**.

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



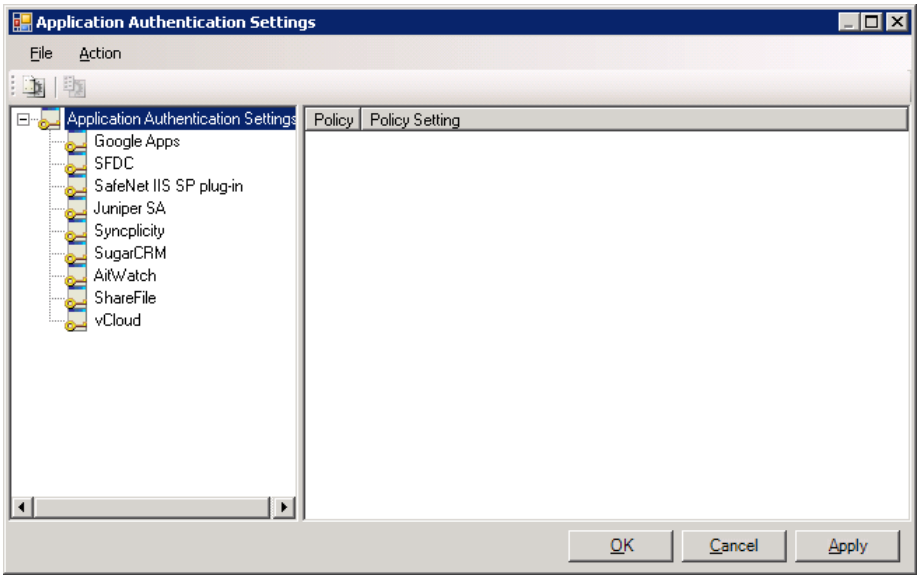
3. In the right pane, double-click **Application Authentication Settings**.

   The *Application Authentication Settings Properties* window opens.



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

The *Application Authentication Settings* window opens.

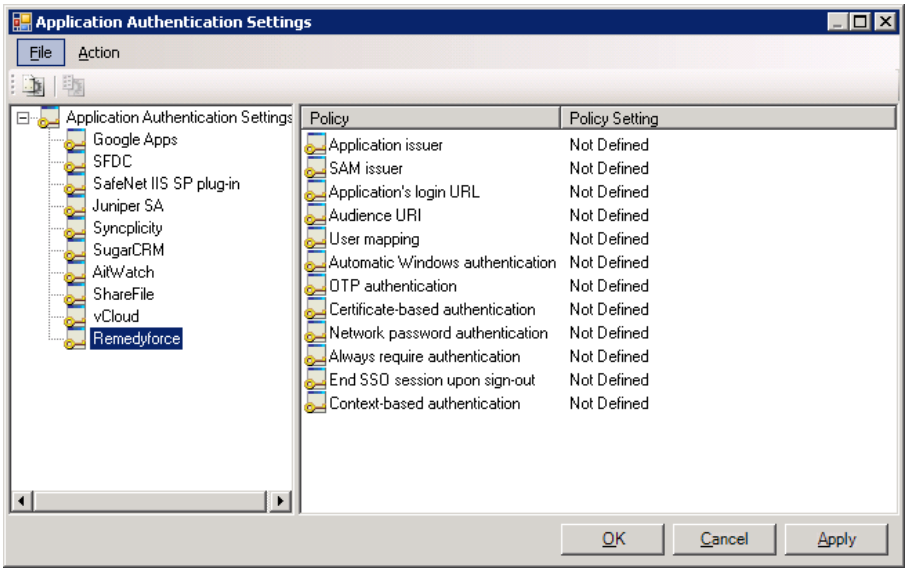


5. In the left pane, right-click **Application Authentication Settings**, and from the dropdown menu, select **Create a new profile**.

   A new profile is created.

6. In the left pane, right-click the new profile, and from the dropdown menu, select **Rename**.
7. Rename the profile to **Remedyforce**.
8. In the left pane, select the new profile, **Remedyforce**.

   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. **SAM issuer**: Enter the unique **SAM ID** that was entered in step 7b of *Configuring Remedyforce to Use SAM as an Identity Provider*, on page 7.

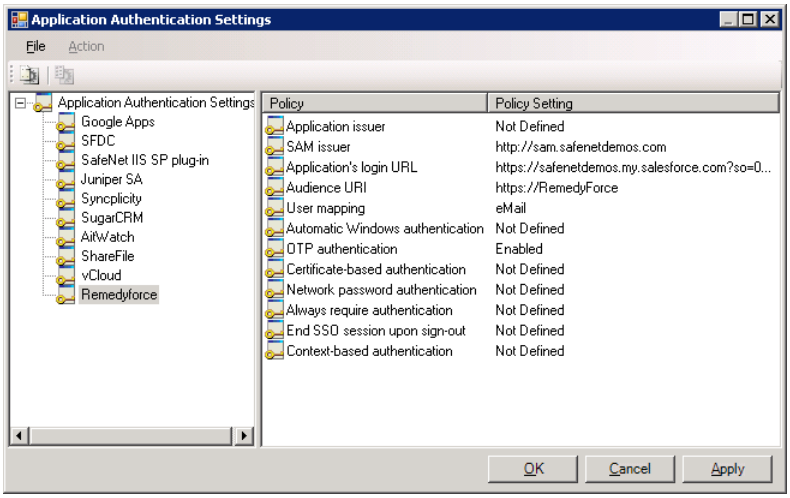
b. **Application's login URL**: Enter the **Salesforce Login URL** value shown in the Remedyforce *SAML Single Sign-On Setting* window. (See step 9 of *Configuring Remedyforce to Use SAM as an Identity Provider*, on page 8.)

c. **Audience URI**: Enter the **Entity Id** value that was entered in step 7h of *Configuring Remedyforce to Use SAM as an Identity Provider*, on page 7.

d. **User mapping**: Enter the field name from your user repository by which users will be identified to Remedyforce. This field will be used as the user's login name to Remedyforce.

e. Enable the appropriate authentication methods 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 completed fields in the *Application Authentication Settings* window:



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

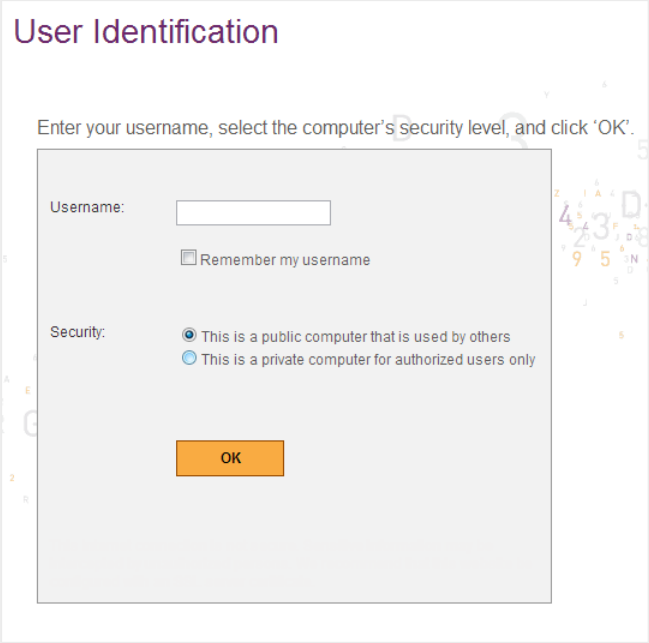
Running the Solution

After Remedyforce is configured to use SafeNet Authentication Manager as its Identity Provider, and SafeNet Authentication Manager is configured to use Remedyforce as a SAML Service Provider, users can securely log in to Remedyforce.

To log in:

1. A user, Gal, browses to **https://<subdomain>.my.salesforce.com/**, where <subdomain> is the name of the domain that was set in the Salesforce configuration.

Gal is redirected to SafeNet Authentication Manager's external portal's authentication page.



2. Gal enters the SafeNet Authentication Manager credentials, and clicks **OK.**

Gal is logged in to the Remedyforce account.