



SafeNet Authentication Manager

INTEGRATION GUIDE

Using SAM as an Identity Provider for Remedyforce

Contents

Support Contacts	2
Description	3
Single Sign-On Dataflow	3
Configuring SAM as an Identity Provider	4
Configuring Remedyforce to Use SAM as an Identity Provider	5
Configuring SAM to use SAML-Based User Federation	10
Running the Solution	12

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.

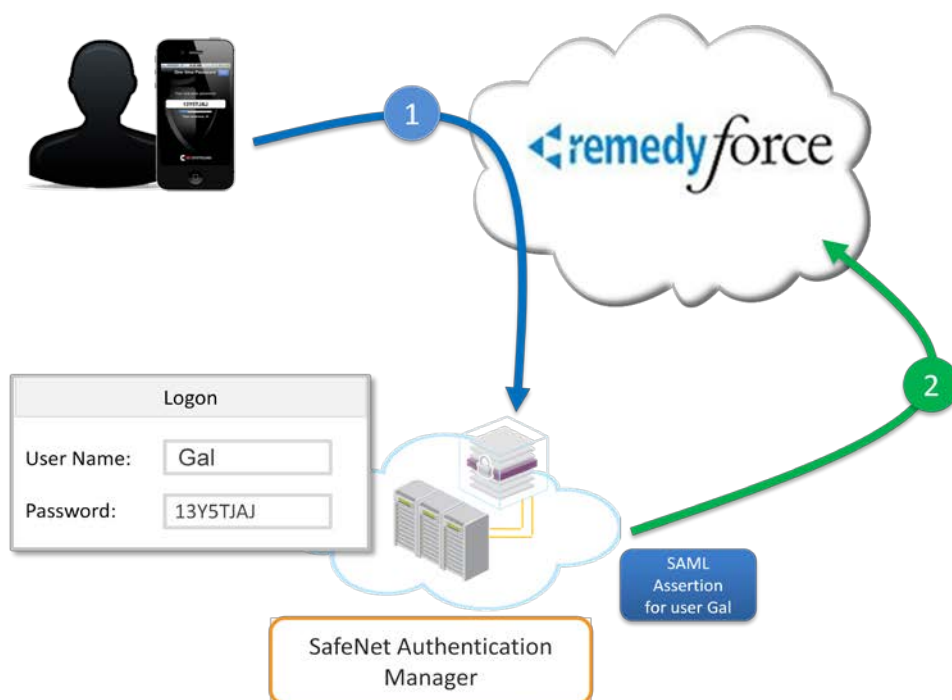
Some instructions in this document are common to many applications that use SAML protocol for user federation.

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

SafeNet Authentication Manager Single Sign-On with Remedyforce



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

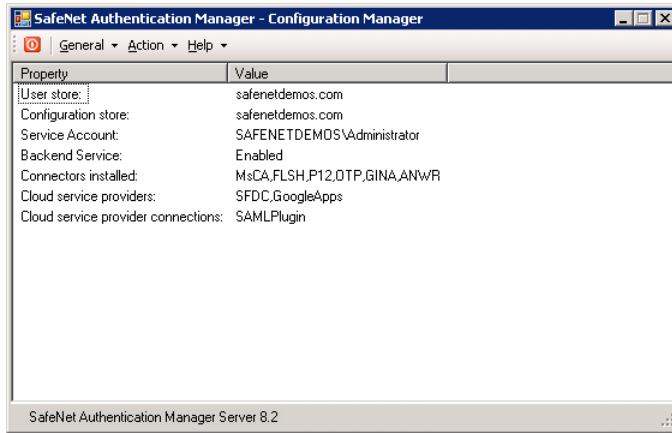
Configuring SAM as an Identity Provider

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**.

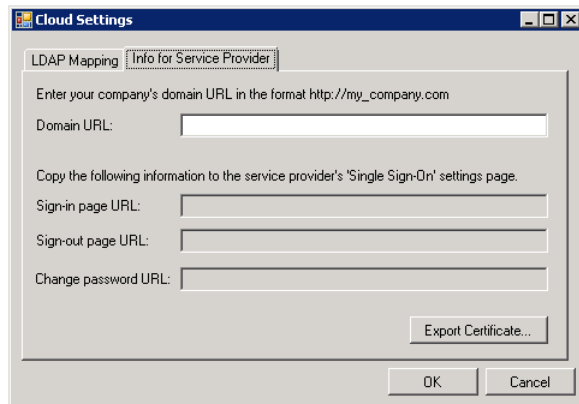
The *Configuration Manager* window opens.



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

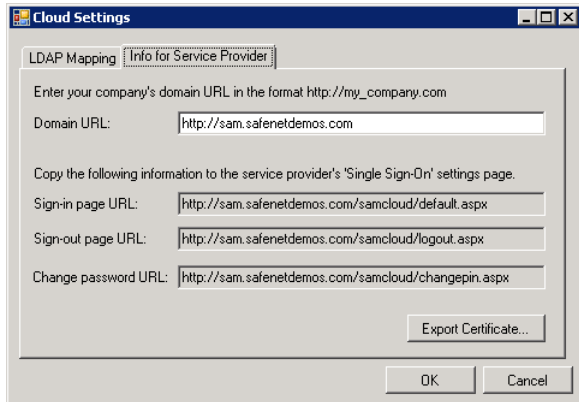
The *Cloud Settings* window opens.

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.

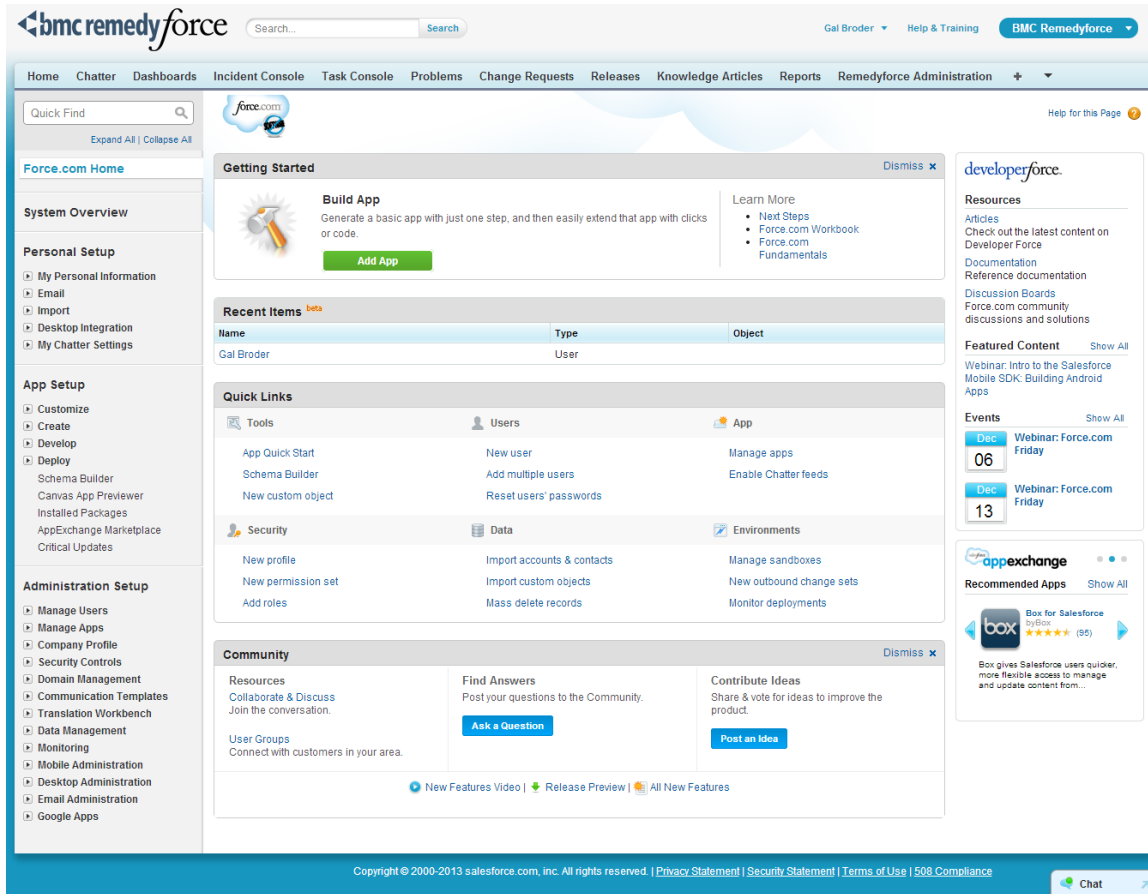
This file will be needed in step 7c *Configuring Remedyforce to Use SAM as an Identity Provider*, on page 7.

Configuring Remedyforce to Use SAM as an Identity Provider

To configure Remedyforce to use SAM as an identity provider:

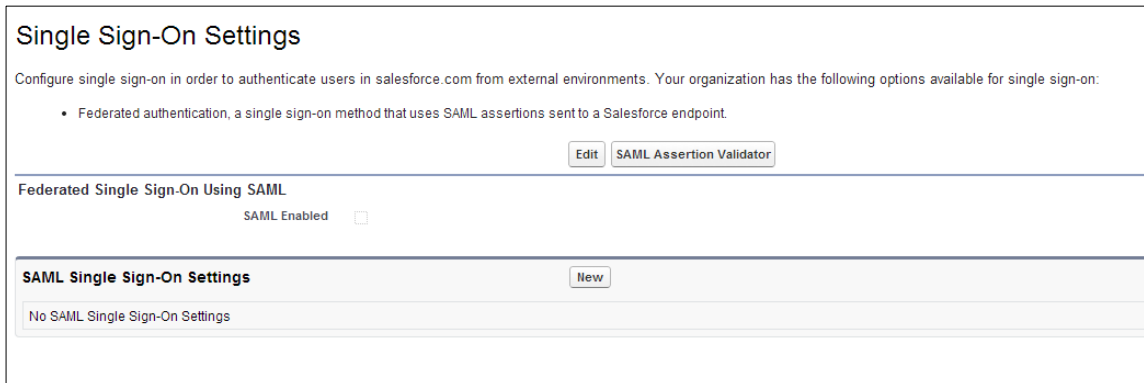
1. Log on to Remedyforce.
2. At the top right of the window, open the **<your user name>** dropdown menu, and select **Setup**.

The *Settings* window opens.

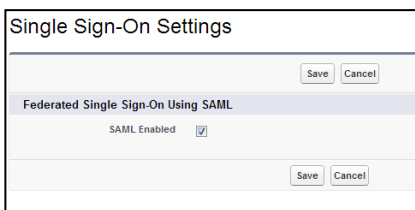


- In the left pane, select **Administration Setup > Security Controls > Single Sign-On Settings**.

The *Single Sign-On Settings* window opens.



- 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 Remydforce.
 - 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 Remydforce 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.

SAML Single Sign-On Setting Help for this Page

SAML Single Sign-On Setting Edit Save Save & New Cancel

Name	SAM	API Name	SAM
SAML Version	2.0	User Provisioning Enabled	<input type="checkbox"/>
Issuer	http://sam.safenetdemos.com	Entity Id	https://RemedyForce
Identity Provider Certificate	Choose File No file chosen	Current Certificate	CN=safenetdemos.com_6D5D601A-1ABF-4e39-B0EA-2BF3198E4DD0 Expiration: 19 Feb 2033 08:48:22 GMT
Signing Certificate	Default Certificate		
SAML Identity Type	<input checked="" type="radio"/> Assertion contains User's salesforce.com username <input type="radio"/> Assertion contains the Federation ID from the User object <input type="radio"/> Assertion contains the User ID from the User object		
SAML Identity Location	<input checked="" type="radio"/> Identity is in the NameIdentifier element of the Subject statement <input type="radio"/> Identity is in an Attribute element		
Identity Provider Login URL	http://sam.safenetdemos.com/samcloud/default.aspx		
Identity Provider Logout URL	http://sam.safenetdemos.com/samcloud/logout.aspx		
Custom Error URL			
Service Provider Initiated Request Binding	<input type="radio"/> HTTP POST <input checked="" type="radio"/> HTTP Redirect		

Save Save & New Cancel

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.

SAML Single Sign-On Setting

[Back to Single Sign-On Settings](#)

SAML Single Sign-On Setting Detail Edit Delete Clone Download Metadata SAML Assertion Validator

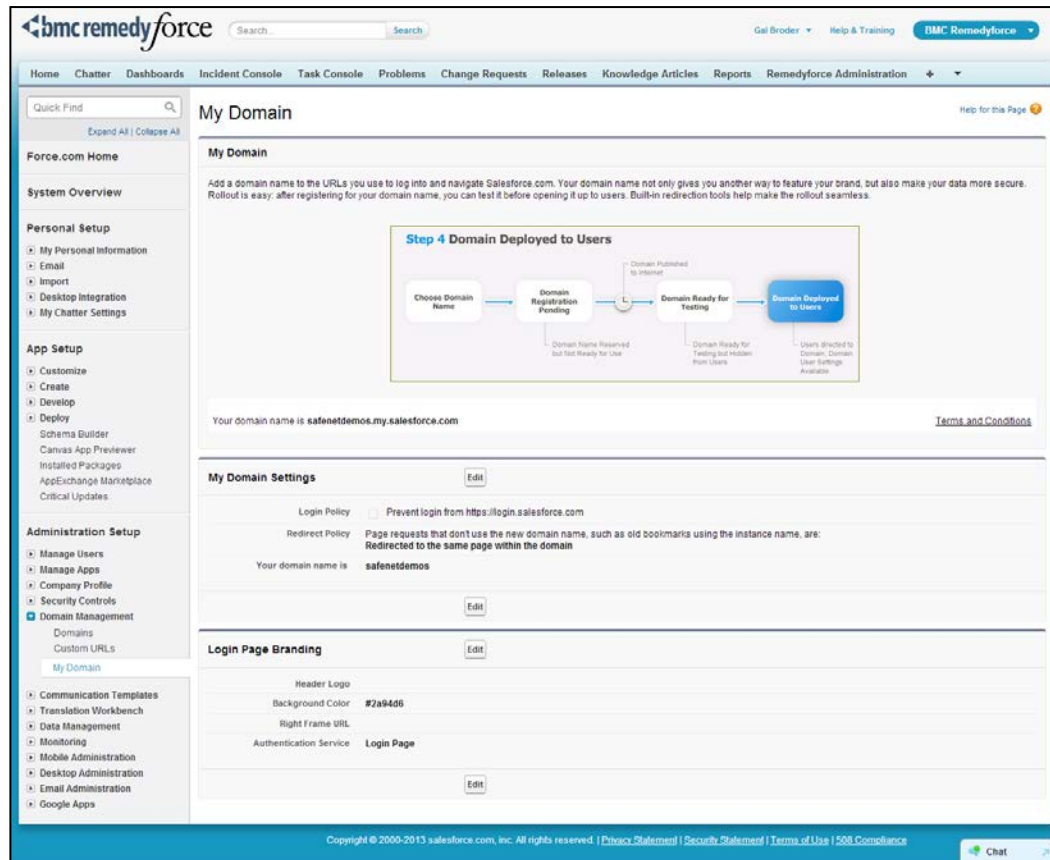
Name	SAM	API Name	SAM
SAML Version	2.0	User Provisioning Enabled	<input type="checkbox"/>
Issuer	http://sam.safenetdemos.com	Entity Id	https://RemedyForce
Identity Provider Certificate	CN=safenetdemos.com_6D5D601A-1ABF-4e39-B0EA-2BF3198E4DD0 Expiration: 19 Feb 2033 08:48:22 GMT		
Signing Certificate	Default Certificate		
SAML Identity Type	Username		
SAML Identity Location	Subject		
Identity Provider Login URL	http://sam.safenetdemos.com/samcloud/default.aspx		
Identity Provider Logout URL	http://sam.safenetdemos.com/samcloud/logout.aspx		
Custom Error URL			
Service Provider Initiated Request Binding	HTTP Redirect		
Salesforce Login URL	https://safenetdemos.my.salesforce.com?so=00D60000000b91R		
OAuth 2.0 Token Endpoint	https://safenetdemos.my.salesforce.com/services/oauth2/token?so=00D60000000b91R		

Edit Delete Clone Download Metadata SAML Assertion Validator

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.

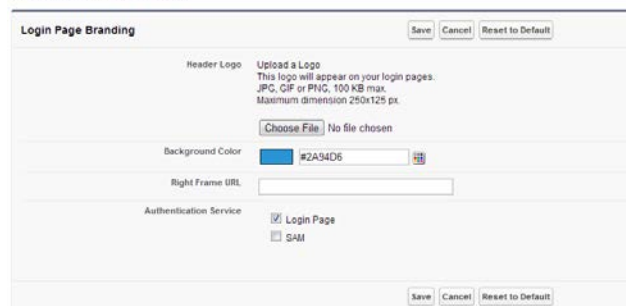


Your own Salesforce domain must have been registered.

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

The *Login Page Branding* window opens.

Login Page Branding



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.

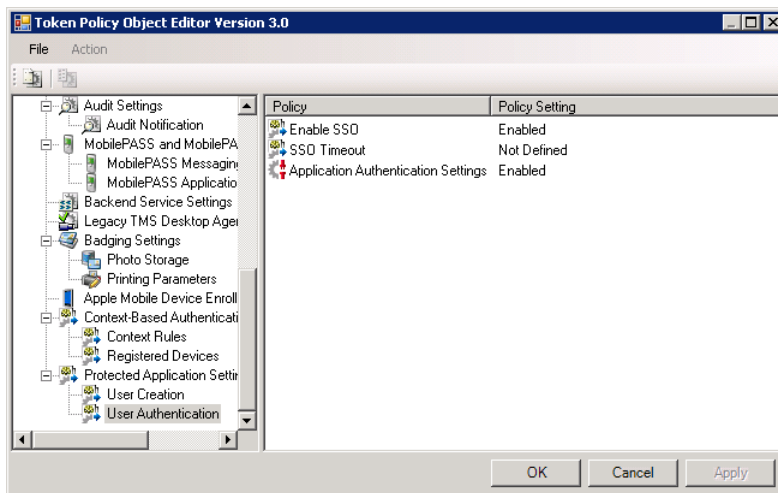


See *SafeNet Authentication Manager Version 8.2 Administrator's Guide* for general portal configuration.

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

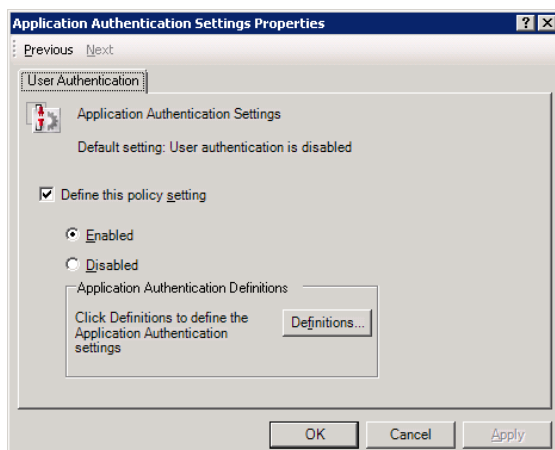
1. Open the *Token Policy Object Editor* for the appropriate group. See the *SafeNet Authentication Manager Version 8.2 Administrator's Guide* for more information.
2. In the left pane, select **Protected Application Settings > User Authentication**.

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



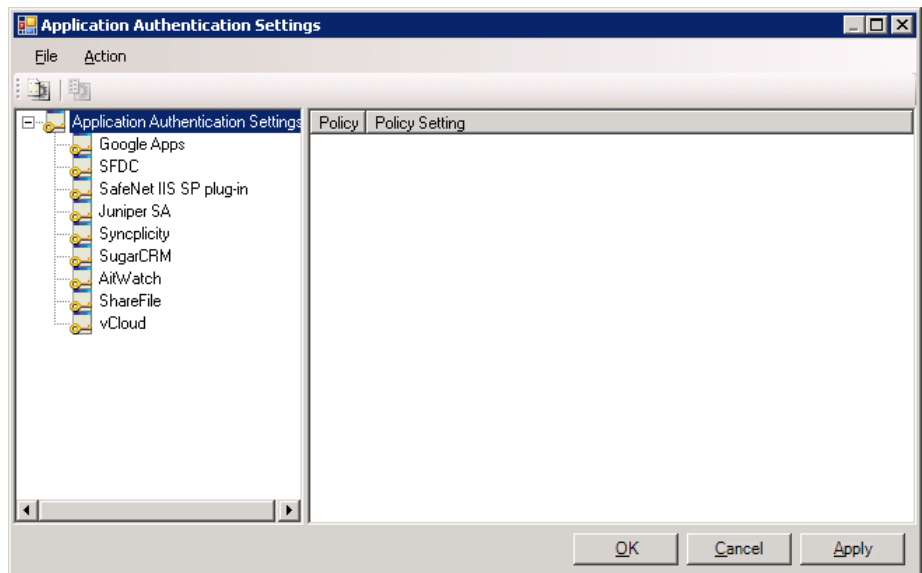
3. In the right pane, double-click **Application Authentication Settings**.

The *Application Authentication Settings Properties* window opens.



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

The *Application Authentication Settings* window opens.

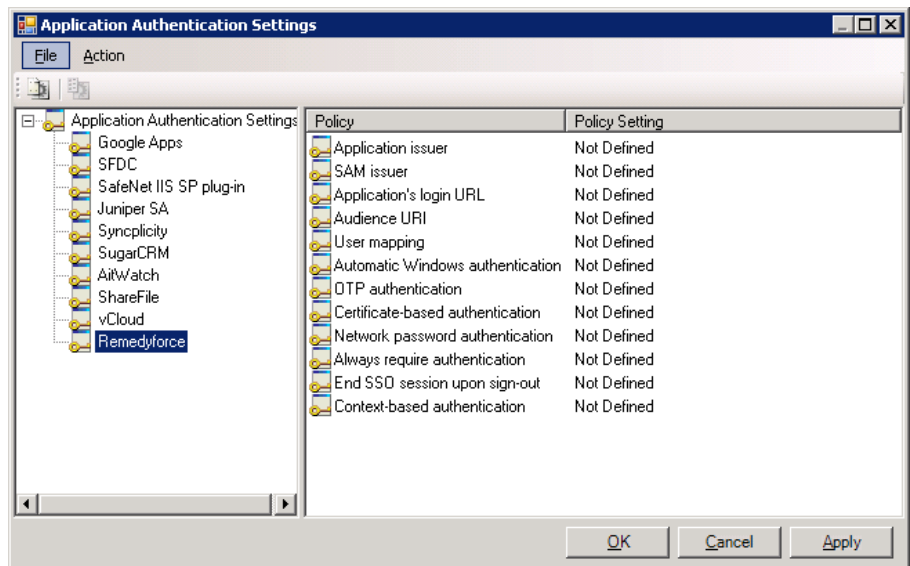


5. In the left pane, right-click **Application Authentication Settings**, and from the dropdown menu, select **Create a new profile**.

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**.

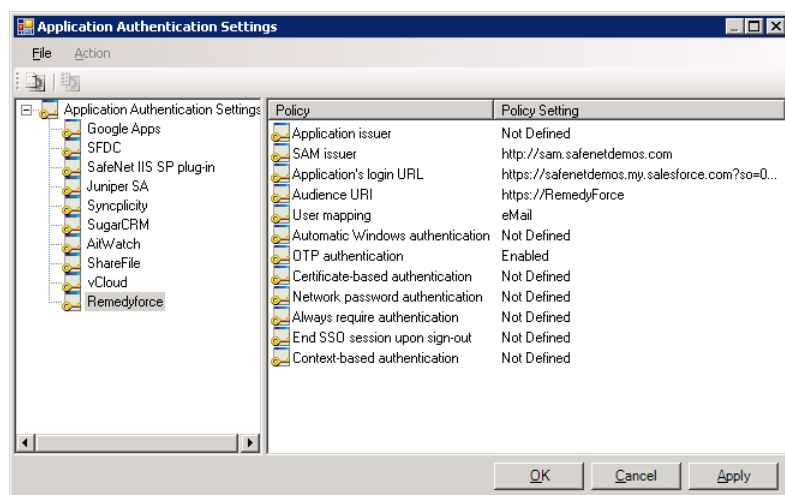
The profile's policies are displayed in the right pane.



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.

User Identification

Enter your username, select the computer's security level, and click 'OK'.

Username:

Remember my username

Security:

- This is a public computer that is used by others
- This is a private computer for authorized users only

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

Gal is logged in to the Remedyforce account.

The screenshot displays the BMC Remedyforce user interface for user Gal Broder. The top navigation bar includes the BMC Remedyforce logo, a search bar, and user information (Gal Broder, Help & Training, BMC Remedyforce). The main navigation menu lists various sections like Home, Chatter, Dashboards, Incident Console, Task Console, Problems, Change Requests, Releases, Knowledge Articles, Reports, and Remedyforce Administration.

The central feed shows a post by Gal Broder from Wednesday 27 November 2013. Below it are three posts from other users: Allen Allbrook, IT Staff, and another IT Staff member, all dated 16 October 2013. The posts discuss incident management and server issues.

Below the feed is the 'Items to Approve' section, which contains a table with the following data:

Action	Related To	Type	Most Recent Approver	Date Submitted
Reassign Approve / Reject	CR00000002	Change Request	Broder_Gal	16/10/2013 14:44
Reassign Approve / Reject	CR00000000	Change Request	Broder_Gal	16/10/2013 14:44

The 'Dashboard' section provides a summary of records assigned to the user and includes two charts:

- Records Assigned to Me:** A list showing 8 Incidents, 5 Tasks, 7 Broadcasts, 1 Change Request, and 2 Problems.
- Priority 1 Incidents:** A gauge chart showing 3 out of 20 records, representing 15%.
- Incidents per client:** A bar chart showing the number of incidents for various clients, with the highest count being 4.

The footer contains copyright information for 2000-2013 Salesforce.com, Inc., and links to Privacy Statement, Security Statement, Terms of Use, and 508 Compliance. A chat icon is also present in the bottom right corner.