SafeNet. THE DATA PROTECTION COMPANY

SafeNet Authentication Manager

TECHNICAL BRIEF

Using SafeNet Authentication Manager as Identity Provider for AirWatch

Contents

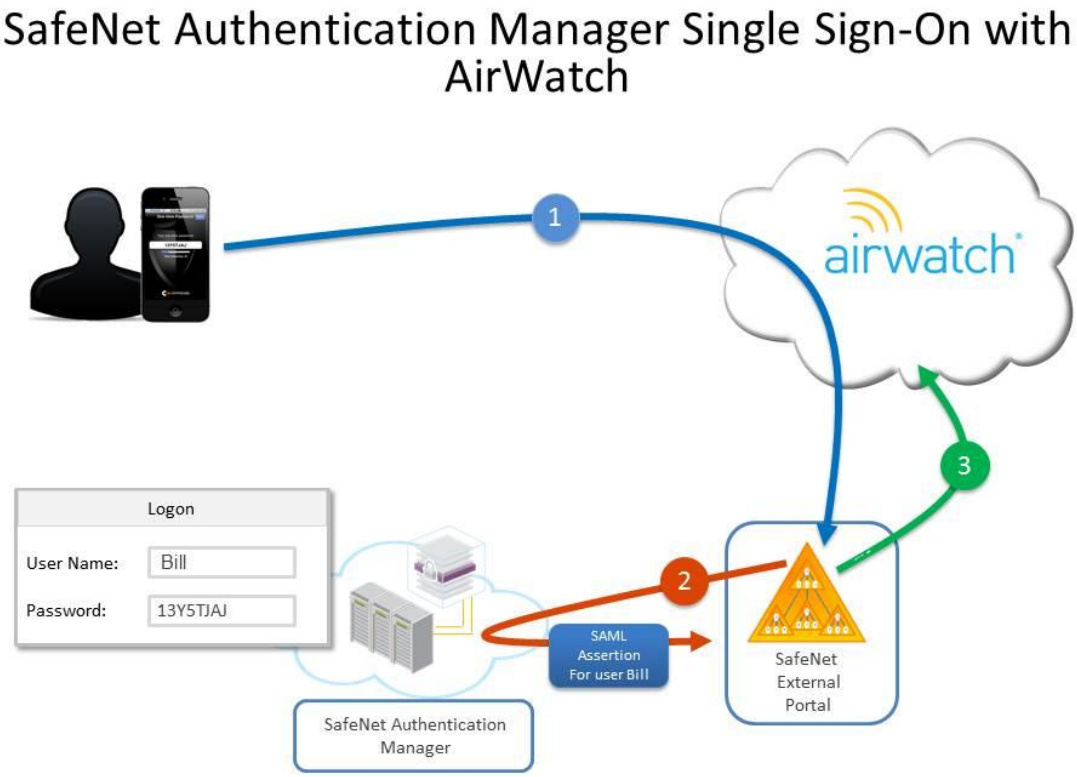
Description

This document provides guidelines for enabling strong-authentication for AirWatch's administrators account using SafeNet Authentication Manager (SAM).

NOTE

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

Single Sign-On Dataflow

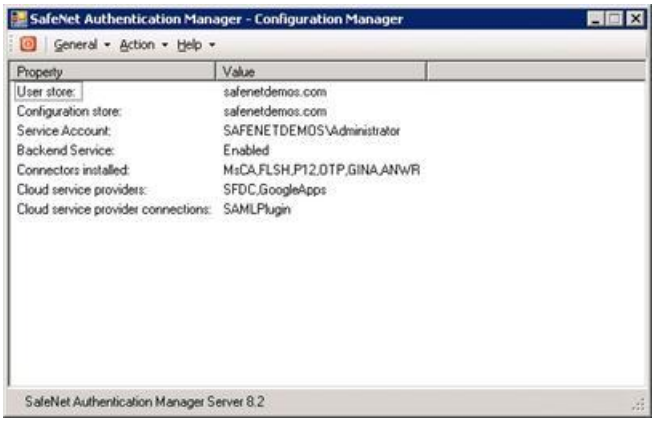


1. Bill, an administrator, wants to login to AirWatch's Administrators Portal. Bill wants to leverage the single sign-on capabilities embedded in the organization's SafeNet Authentication Manager solution.
2. SafeNet Authentication Manager's portal collects Bill's credentials and passes them to SafeNet Authentication Manager (SAM) 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 AirWatch.

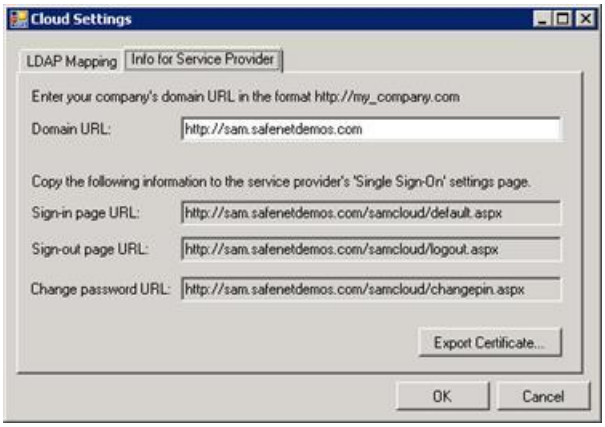
Identity Provider Configuration

The following section is common in many applications that use SAML protocol for user-federation. We will provide the information that the application (in this case AirWatch) needs for setting up SafeNet Authentication Manager as its identity provider from the SAS`s console SAML 2.0 settings.

1. Choose ***SafeNet Authentication Manager > Configuration Manager*** from Windows Start Menu. The *Configuration Manager* window opens.



2. Chose ***Action > Cloud Configuration*** on the Menu bar. The *Cloud Settings* window opens.
3. Select the **Info for Service Provider** tab.



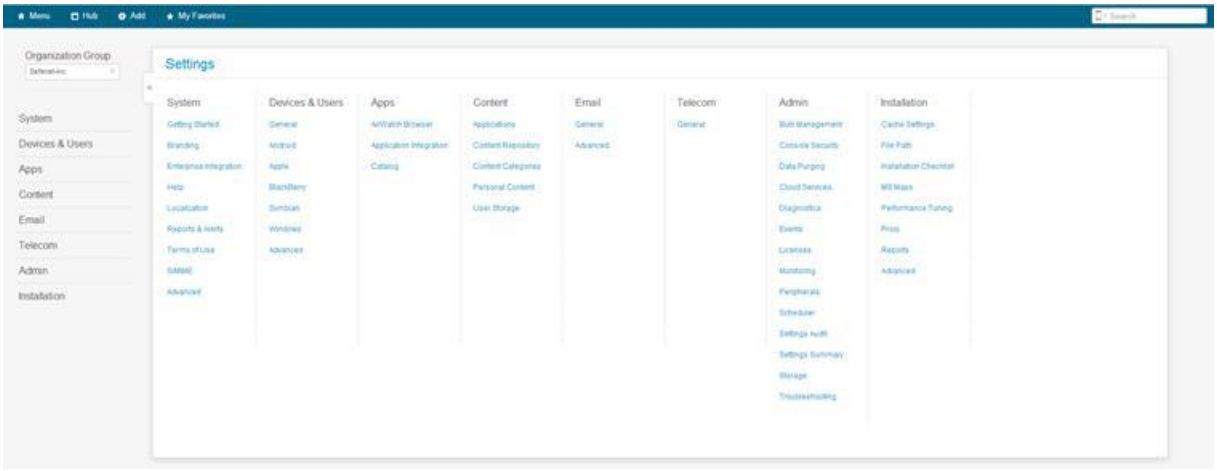
In the ***Domain URL*** field, enter the domain URL of your organization's SAM external portal.
The ***Single Sign-On*** fields are displayed. Do not close the *Cloud Settings* window.
The displayed values will be needed in step 8a of ***Configuring AirWatch to use SafeNet Authentication Manager as Identity Provider*** on page 5.

4. Click **Export Certificate**, and save the file. This file will be needed in step 8i of ***Configuring AirWatch to use SafeNet Authentication Manager as Identity Provider*** on page 6.

Configuring AirWatch to use SafeNet Authentication Manager as Identity Provider

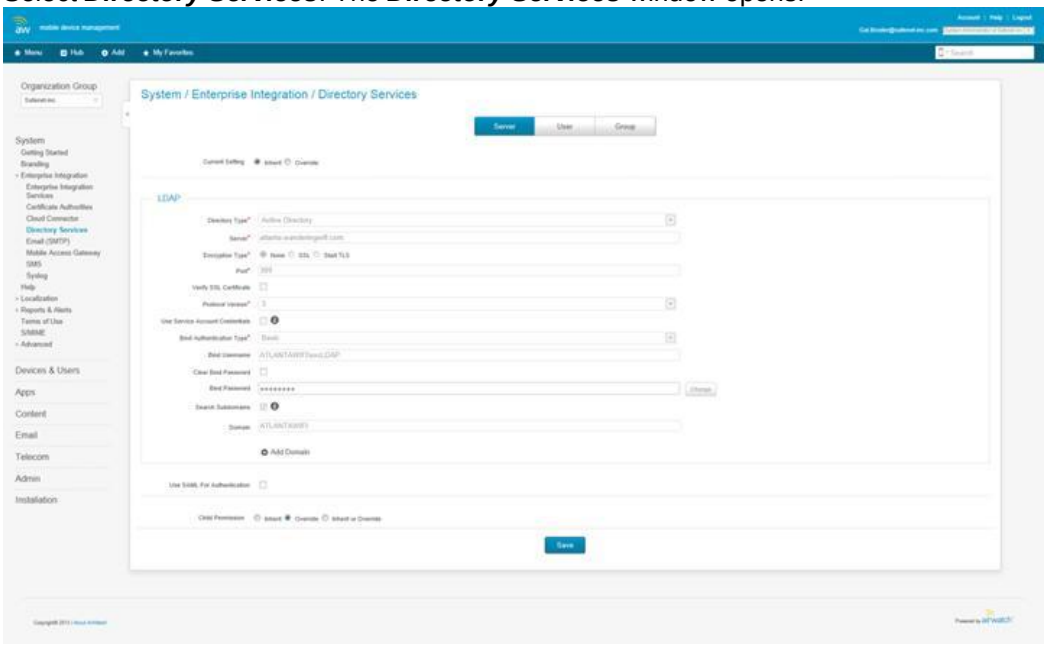
To add SAM as an Identity Provider to AirWatch, we would need to use SafeNet Authentication Manager's Single Sign On configuration that was retrieved in the previous section. Using this information follow these steps:

1. Log in to AirWatch, and in the upper left corner, click ***Menu> Configuration> System Configuration***.The ***System Configuration*** window opens.



2. Select ***System > Enterprise Integration***. The ***Enterprise Integration option*** window opens.

3. Select ***Directory Services***. The ***Directory Services*** window opens.



4. In the ***Server*** tab, on the ***Current Setting*** choose **Override**.

5. The *LDAP* options have been enabled.

6. In ***Directory Type*** choose **None**.
7. Enable the ***Use SAML For Authentication***.

The SAML settings opens.

8. Use the following settings:
   a. In the ***Service Provider (AirWatch) ID*** field, enter a unique AirWatch ID to be identified to SafeNet Authentication Manager.
   b. In the ***Identity Provider ID*** field, enter a unique ***SAM ID*** as SafeNet Authentication Manage identifier in AirWatch.
   c. In the ***Request*** section, choose the option of ***Redirect***.
   d. In the ***Identity Provider Single Sign On URL*** field, copy the **Sign-in Page URL** value from SAM's ***Cloud Configuration*** window retrieved in step 0 of the ***Identity Provider Configuration*** section***.***
   e. In the ***NameID Format*** choose ***Unspecified***.

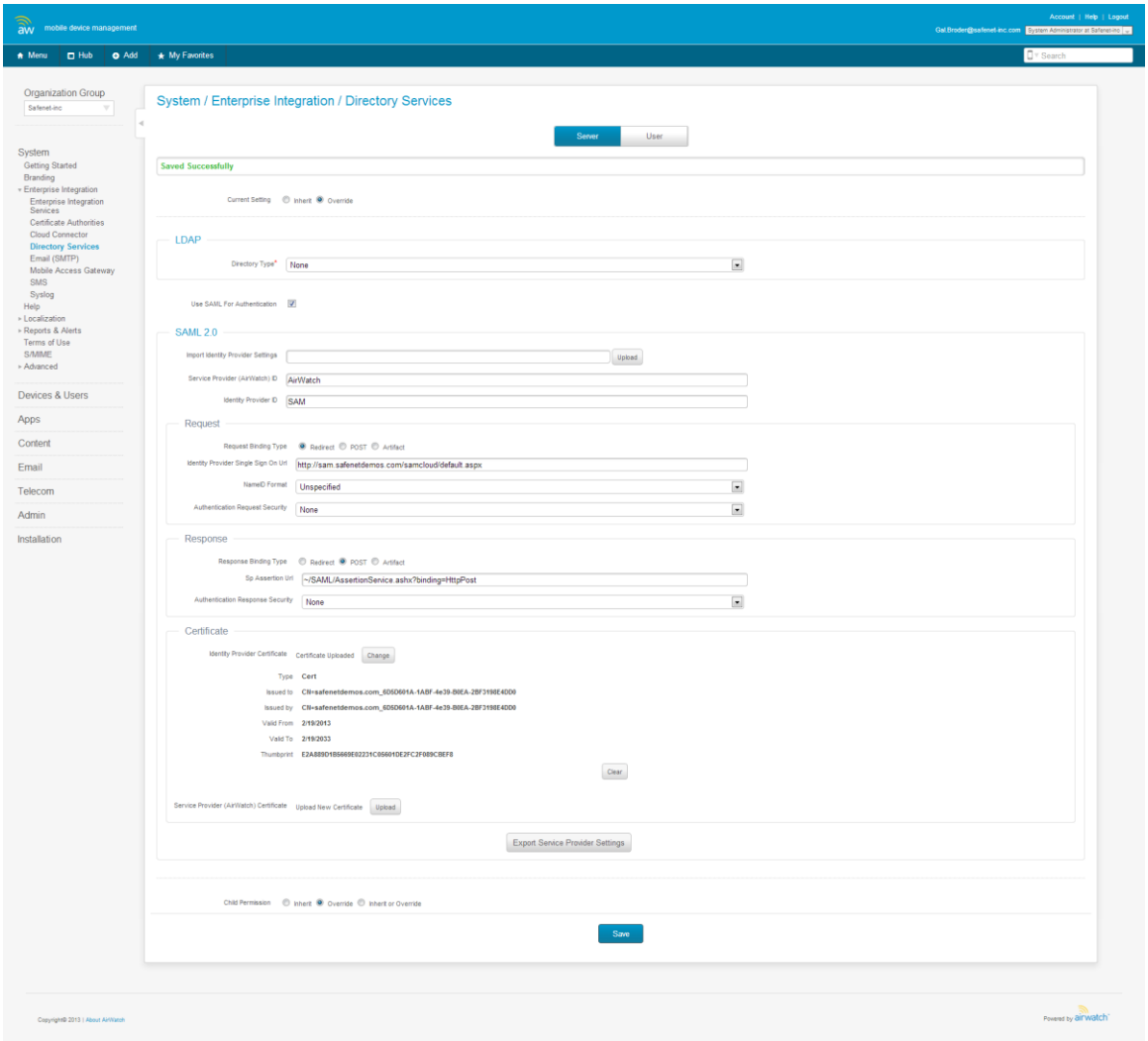
f. In the ***Authentication Request Security*** choose ***None***.

g. In the ***Response*** section, choose ***Post***.

h. In the **Authentication Response Security** choose ***None***.

i. In the ***Certificates*** section, choose to upload the ***Identity Provider Certificate***. Choose the certificate that has been exported from SafeNet Authentication Manage configuration manager in step 5 of the ***Identity Provider Configuration*** section. Click Save.

Next diagram is an example of the completed fields in the *AirWatch* console.



9. Click **Save**.
10. Select the ***User*** tab from the top bar. The ***User Options*** window appears.
11. In the ***Username*** field, change the value to "***uid***".
12. Click ***Save***.

SafeNet Authentication Manager is now set as an Identity Provider in AirWatch.

Configuring SafeNet Authentication Manager to use SAML based User Federation

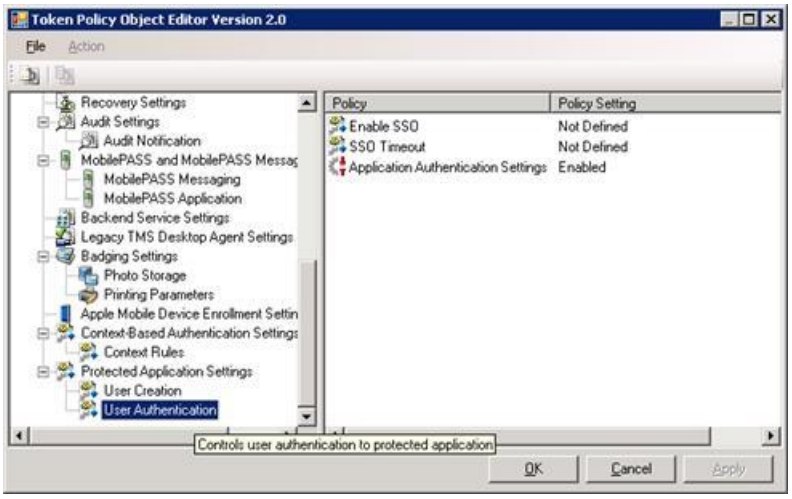
SafeNet Authentication Manager\s Token Policy Object (TPO) policies include ***Application Authentication Settings*** for SAML service providers. These settings are used by SafeNet Authentication Manager's external portal to communicate with service providers.

NOTE

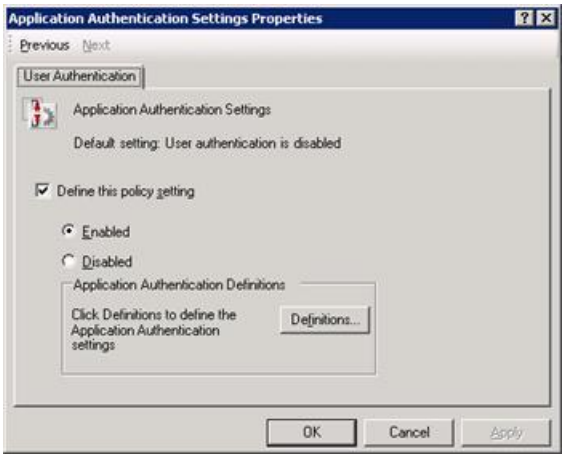
See SafeNet Authentication Manager (version 8.2) Administrator's Guide for general portal configuration.

Edit the TPO policies for SafeNet Authentication Manager's portal configuration by following these steps:

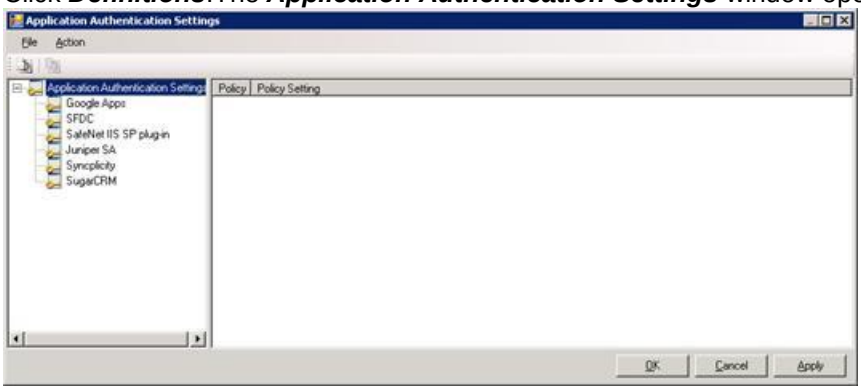
1. Open the Token Policy Object Editor for the appropriate group. See the SafeNet Authentication Manager (version 8.2) Administrator's Guide for more information. The ***Token Policy Object Editor*** window opens.
2. In the left pane, go to ***Protected Application Settings > User Authentication***.
   Policies are displayed in the right pane.



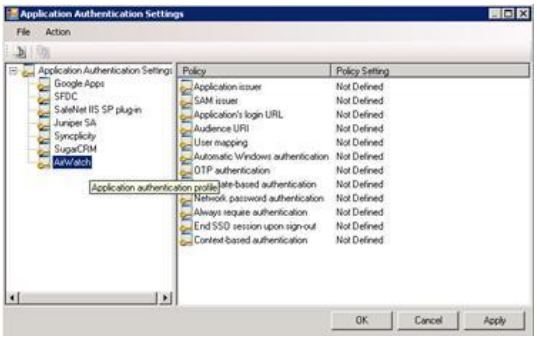
3. In the right pane, double-click ***Application Authentication Settings***. The ***Application Authentication Settings Properties*** window opens.



4. Select ***Define this policy setting***, and select ***Enabled***.
5. Click ***Definitions***.The ***Application Authentication Settings*** window opens.



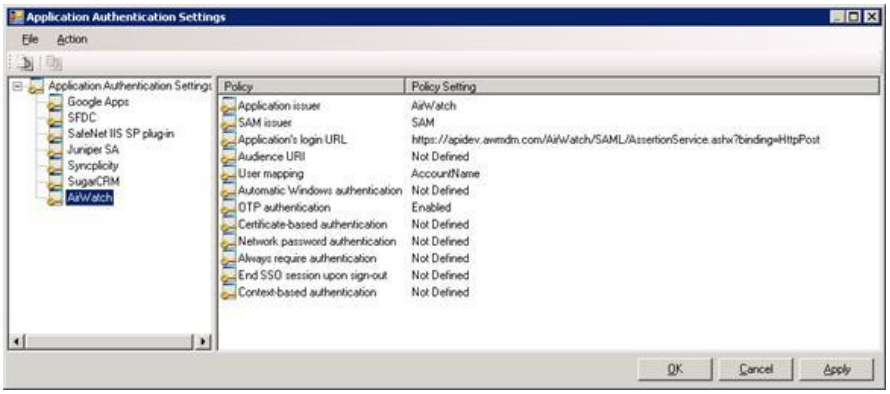
6. In the left pane, right click ***Application Authentication Settings***, and from the dropdown menu, select ***Create a new profile***. A new profile is created.
7. In the left pane, right click the new profile, and from the dropdown menu, select ***Rename***.
8. Rename the profile **AirWatch**, and 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 the AirWatch's **Service Provider ID** value that was entered in step 8a on page 5.
   b. **Application's login URL**: Enter https://<AirWatch_service_url>/AirWatch/SAML/AssertionService.ashx?binding=HttpPost replacing <AirWatch_service_url> with the URL of your AirWatch service.
   c. **User mapping**: Set to the field in your user repository that identify your AirWatch login name.

d. Enable the appropriate authentication methods for your organization.
See the *SafeNet Authentication Manager (Version 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 will be closed.

Running the Solution

The user logs on to AirWatch Administrator's console using SAML authentication and with SafeNet Authentication Manager.

To log on to the organization's AirWatch environment follow these steps:

1. Browse to https:// <AirWatch_service_url>/airwatch/login?GID=<Group_ID> replacing `<AirWatch_instance_name>` with the URL of the organization's AirWatch service and `<Group_ID>` with the group ID of the organization (Can be found using the Admin console: **Menu > Configuration > Organization Group > Group ID** field).
2. User will be redirected to SafeNet Authentication Manager's external portal's authentication page.

3. Enter your SafeNet Authentication Manager authentication credentials, and click **OK**.
4. You are logged on to your AirWatch account.