

SafeNet Authentication Client Integration Guide

Certificate-based Authentication on Microsoft FIM CM
2010 R2



THE
DATA
PROTECTION
COMPANY

Document Information

Product Version	8.3
Document Part Number	007-012589-001, Rev A
Release Date	July 2014

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.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Introduction	4
Third-Party Software Acknowledgement	4
Overview	4
Audience	4
Architecture	5
Applicability	5
Prerequisites	6
AdminKey.exe	6
Configurations	7
Creating a Profile Template for SAC or Minidriver	7
Configuring a Profile Template for SAC	7
Configuring a Profile Template for Minidriver	8
Downloading Minidriver using Microsoft Windows Update	10
Assigning the FIM CM Subscriber Group Permission on the Smart Card Logon Certificate Template	11
Assigning the FIM CM Subscriber Group Permission on the SAC and Minidriver Profile Template	12
Editing the Registry for SAC	13
Editing the Registry for Minidriver	14
Running the Solution	14
Enrolling a Certificate	14
Testing the Solution	16
Support Contacts	17

Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Microsoft® Forefront Identity Manager.

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.

Overview

Microsoft Forefront Identity Manager (FIM) provides identity synchronization, user provisioning, certificate and password management, and policy management in a single solution that works across heterogeneous systems. Forefront Identity Manager Certificate Management (FIM CM) provides functionality to support certificate and smart card management. FIM also provides sophisticated credential management features to both Windows Server and third-party certificate authorities (CAs) by acting as an administrative proxy. Once installed within an organization, all digital certificate and smart card management functions pass through FIM.

FIM Certificate Management (FIM CM) consists of the Certificate Management database, which holds the workflows and certificate information, the Certificate Management Portal, the FIM CM Certification Authority (CA) modules that are installed on the CA servers, and various clients that interact with the Certificate Management Portal's underlying web service.

FIM CM extends the functionality of the certificate authority services that exist out of the box with Windows by adding a workflow approach, auditing capabilities, and notifications, and by introducing many management roles such as Request Renew, Request Offline Unblock, and more. All of this can be defined inside a management policy approach by utilizing Profile Templates inside FIM CM.

Besides extending the functionality, FIM CM acts as a security context proxy by using the concept of FIM CM Agents. Every action that FIM CM performs is done in the context of one of FIM CM Agents. Those agents are also used to sign and encrypt traffic between the FIM server and the database server, and between the FIM server and the CA server, besides encrypting some data inside the FIM SQL database itself.

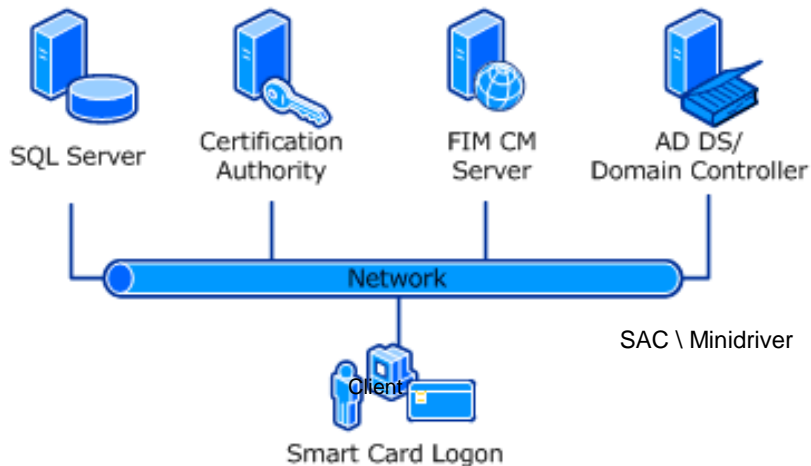
As FIM CM is using those agents for almost all operations, FIM agents need to be enrolled for Encryption and Signing certificates, Enrollment Agent certificates, and Key Recovery Agent certificates. Those certificates can be protected by an HSM, as gaining access to the Enrollment Agent certificate is very dangerous. The system administrators only need to have a management role for the FIM CM management policies, and they don't need to have Enrollment Agent certificates any longer because the Enrollment Agent certificate is now owned and managed by FIM CM agents (via HSM, if needed).

Audience

This document is targeted to system administrators familiar with Microsoft FIM CM 2010 R2, and who are interested in adding certificate-based authentication capabilities using SafeNet Authentication Client (SAC).

Architecture

FIM CM can be used to enroll certificates to a smart card. The user can request a certificate using the FIM CM portal, which needs to be accessed from the client machine where the SafeNet Authentication Client (SAC) is installed. Then, the FIM CM server interacts with the certificate authority to issue a certificate, and the database (in SQL Server) is updated for that user. The certificate gets written to the SafeNet smart card, and the user can now use the card for certificate-based authentication (CBA).



You can use SafeNet Authentication Client (SAC) to:

- Initialize a SafeNet smart card or change its PIN
- View SafeNet smart card information and its certificate

Minidriver does not provide the above functions. It only provides the required library files, which are used by FIM CM to interact with SafeNet smart cards.

Applicability

Operating System	
FIM CM Server	Windows Server 2008
FIM CM Client	Windows Server 2008
Middleware	
SafeNet Authentication Client	Version 8.3
Software	
Forefront Identity Manager Certificate Management	2010 R2
Forefront Identity Manager Certificate Management Client	2010 R2
Tokens	

SafeNet Authentication Client	<ul style="list-style-type: none"> • SafeNet eToken 5100/5105, 5200/5205, 5200/5205 HID, 4100 • SafeNet eToken Virtual Family • SafeNet iKey 2032, 2032u, 2032i, 4000 • SafeNet Smart Cards: SC330, SC330u, SC330i, SC400
SafeNet eToken Minidriver (Mask 9)	SafeNet eToken 5100/5105, 5200/5205, 4100, NG-OTP, 3410



NOTE: Using Windows Server 2008 R2 for FIM CM server or for FIM CM client may produce the following error during enrollment:

*The version of OLE on the client and server machines does not match.
(Exception from HRESULT: 0x80010110)*

This issue is reported online by many users. This integration is tested on Windows Server 2008.

Prerequisites

- Forefront Identity Manager Certificate Management 2010 R2 should be installed and configured on the Windows server. Refer to [http://technet.microsoft.com/en-us/library/ee534914\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/ee534914(v=ws.10).aspx).
- Forefront Identity Manager Certificate Management Client should be installed on all the client machines. Refer to [http://technet.microsoft.com/en-us/library/ee534899\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/ee534899(v=ws.10).aspx).
- For using SafeNet smart cards with FIM CM through SAC, SAC should be installed on the client machine.
- For using SafeNet smart cards with FIM CM through Minidriver, Microsoft Windows Update should be allowed on the client machine, along with access to Internet.

AdminKey.exe

The **AdminKey.exe** application is used to retrieve the hexadecimal-encoded value for the Admin PIN in FIM CM 2010. It generates the hexadecimal value corresponding to the value given to it. For example, if the Admin PIN of the smart card or token is 1234567890, its corresponding hexadecimal code can be obtained by running the following command:

C:\>AdminKey.exe 1234567890

Key: 1d6a4f7a652e18203e3d3b0c70451022107f7420216e611b

where **C:** indicates the location of the **AdminKey.exe** application.



NOTE: The **AdminKey.exe** application is required only when you are using the FIM CM with eToken Minidriver. It is not required with SAC.

The **AdminKey.exe** application can be downloaded from the following link:

<http://bel1web002:9876/Files/5207fcb449c14d078a0d66830e106a34>

Configurations

Creating a Profile Template for SAC or Minidriver

To create a new Profile Template, copy an existing template and modify as required. Two sample templates are provided with FIM CM for this purpose.

1. Open **FIM CM Portal** and log in as a user who has the permission to create a Profile Template.
2. Under **Administration**, click **Manage profile templates**.
3. Select **FIM CM Sample Smart Card Logon Profile Template**, and then click **Copy a selected profile template**.
4. In the **New profile template name** field, enter the name of the template and then click **OK**.

Configuring a Profile Template for SAC

For each profile template, configure the general settings and the certificate template settings that will be used by the profile template.

1. Open **FIM CM Portal** and log in as a user who has administrative privileges.
2. Under **Administration**, click **Manage profile templates**.
3. In the **Profile Template List**, click on the Profile Template name to edit it.
4. Under **General Settings**, click **Change General Settings**.
5. Ensure that **Supports smart cards** is selected, and then click **OK**.
6. Under **Smart Card Configuration**, click **Change Settings**.
7. Complete the details as specified in the table below and then click **OK**.

Provider name	Select Aladdin eToken .
Initialize new card prior to use	Select this option.
Reuse retired card	Select this option.
Install certificate authority certificates	Select this option.
Administrative PIN length	Enter the Smart Card Admin PIN length.
Administrative PIN initial value	Enter the Smart Card Admin PIN initial value.
User PIN policy	Select User Provided .

8. Under **Select a view** on the left side of the **Edit Profile Template** window, click **Enroll Policy**.
9. Under **Workflow: Initiate Enroll Requests**, click **Add new principal for enroll request initiation**.
10. To set permissions for the principal user or group, click **Lookup**.

11. Complete the details as specified in the table below.

Location	Select your domain name.
Name	Enter the name of the user or group to whom you want to give permission to use the Profile Template.

12. Click **Search**.

13. In the search result, click the user or group you want to allow.

14. In the **Enroll Initiate permission** field, select **Grant** and then click **OK**.

15. Under **Data Collection**, perform the following:

- a. Select the **Sample Data Item** option.
- b. Click **Delete data collection items**.
- c. Click **OK** to delete the selected items.

16. Under **Select a view** on the left side of the **Edit Profile Template** window, click **Retire Policy**.

17. Under **Data Collection**, perform the following:

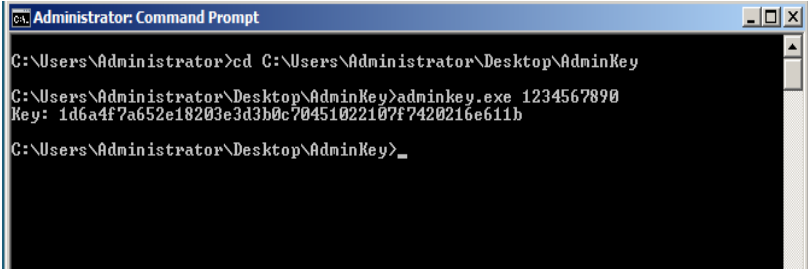
- a. Select the **Sample Data Item** option.
- b. Click **Delete data collection items**.
- c. Click **OK** to delete the selected items.

Configuring a Profile Template for Minidriver

For each profile template, configure the general settings and the certificate template settings that will be used by the profile template.

1. Open **FIM CM Portal** and log in as a user who has administrative privileges.
2. Under **Administration**, click **Manage profile templates**.
3. Click on the Profile Template name to edit it.
4. Under **General Settings**, click **Change General Settings**.
5. Ensure that **Supports smart cards** is selected, and then click **OK**.
6. Under **Smart Card Configuration**, click **Change Settings**.
7. Complete the details as specified in the table below and then click **OK**.

Provider name	Select Microsoft Smart Card Base CSP .
Initialize new card prior to use	Select this option.
Reuse retired card	Select this option.

Admin key initial value (hex)	<p>Enter the hex value of Admin PIN. Follow these steps to create the Hex value:</p> <ol style="list-style-type: none"> 1. Open the Command Prompt and browse to the location of Adminkey.exe application. 2. Run the Adminkey.exe command as below: <pre>Adminkey.exe 1234567890</pre> where, 1234567890 is the Admin PIN. The Hex value is generated and displayed on the screen.  <p><i>(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)</i></p>
User PIN policy	Select User Provided.

8. Under **Select a view** on the left side of the **Edit Profile Template** window, click **Enroll Policy**.
9. Under **Workflow: Initiate Enroll Requests**, click **Add new principal for enroll request initiation**.
10. To set permissions for the principal user or group, click **Lookup**.
11. Complete the details as specified in the table below.

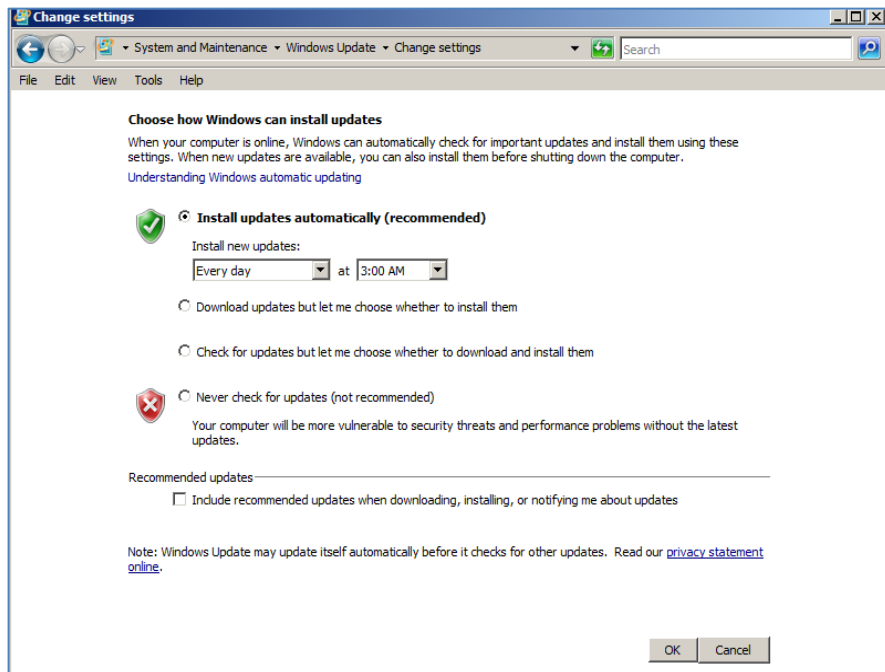
Location	Select your domain name.
Name	Enter the name of the user or group to whom you want to give permission to use the Profile Template.

12. Click **Search**.
13. In the search result, click the user or group you want to allow.
14. In the **Enroll Initiate permission** field, select **Grant** and then click **OK**.
15. Under **Data Collection**, perform the following:
 - a. Select the **Sample Data Item** option.
 - b. Click **Delete data collection items**.
 - c. Click **OK** to delete the selected items.
16. Under **Select a view** on the left side of the **Edit Profile Template** window, click **Retire Policy**.
17. Under **Data Collection**, perform the following:
 - a. Select the **Sample Data Item** option.
 - b. Click **Delete data collection items**.
 - c. Click **OK** to delete the selected items.

Downloading Minidriver using Microsoft Windows Update

Minidriver is the set of drivers that are required to communicate with the SafeNet eTokens. Minidriver can be downloaded using Microsoft Windows Update. Windows Update should be turned on for this purpose. Whenever the user inserts a token, Windows searches for its driver on the Internet and downloads it automatically.

1. On the client machine, click **Start > Windows Update**.
2. Click **Change settings**.
3. Select **Install updates automatically** and then click **OK**.



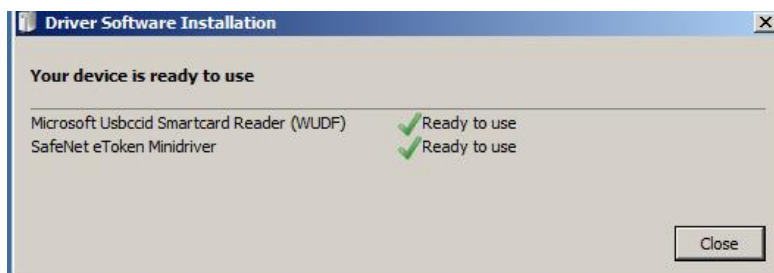
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

4. Insert the eToken into the client machine. Windows starts searching for the driver automatically. To view the search progress, click **Notification** in the bottom right corner of the task bar.



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

- Once the driver search is located, it is automatically installed and eToken is ready to use.

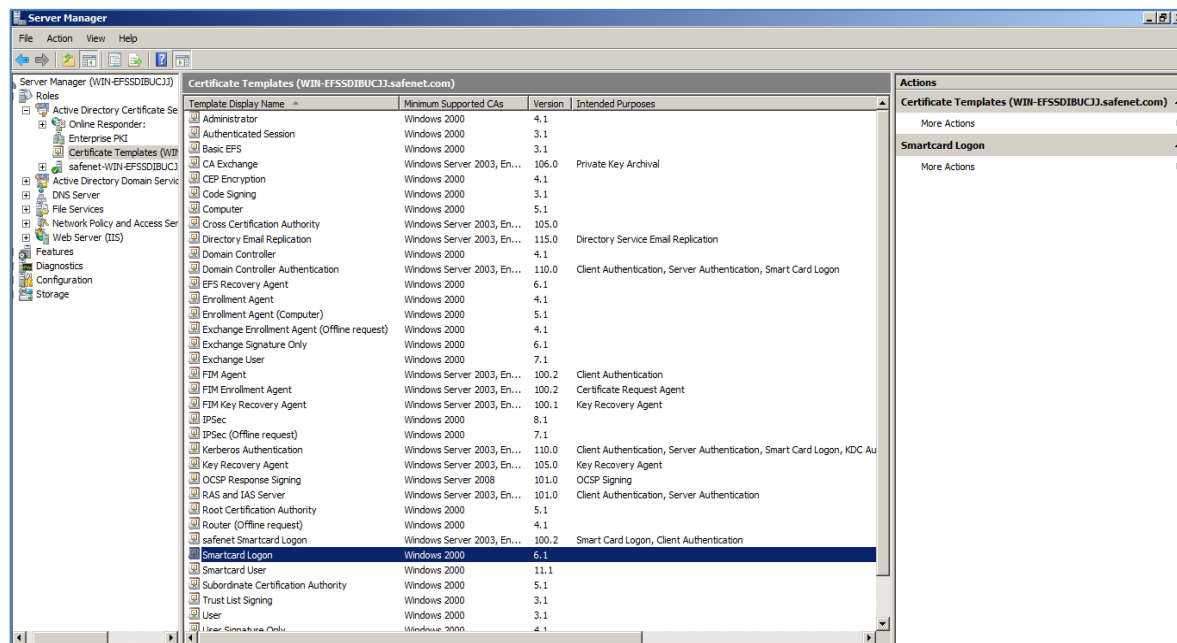


(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

Assigning the FIM CM Subscriber Group Permission on the Smart Card Logon Certificate Template

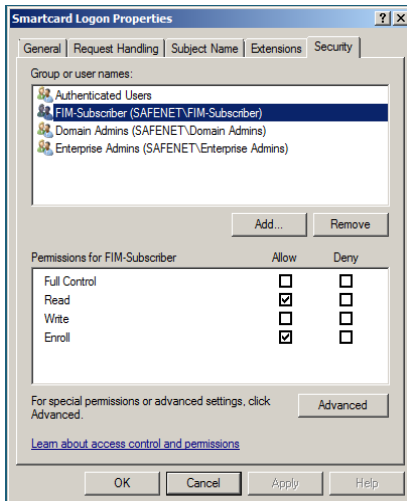
To assign the FIM CM Subscriber group permission on the Smart Card Logon Certificate Template:

- Click **Start > Administrative Tools > Server Manager**.
- In the left pane, click **Roles > Active Directory Certificate Services > Certificate Templates**.



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

- In the right pane, right-click **Smartcard Logon** and select **Properties**.
- On the **Security** tab, click **Add**.
- In the text box below **Enter the object names to select (examples)**, enter **FIM-Subscribers** and then click **Check Names**. This should resolve with underlined text. Click **OK**.
- In the **Group or user names** list, select **FIM CM Subscribers**.
- In the **Permissions for FIM CM Subscribers** list, in the **Allow** column, select **Read** and **Enroll**. Click **OK**.

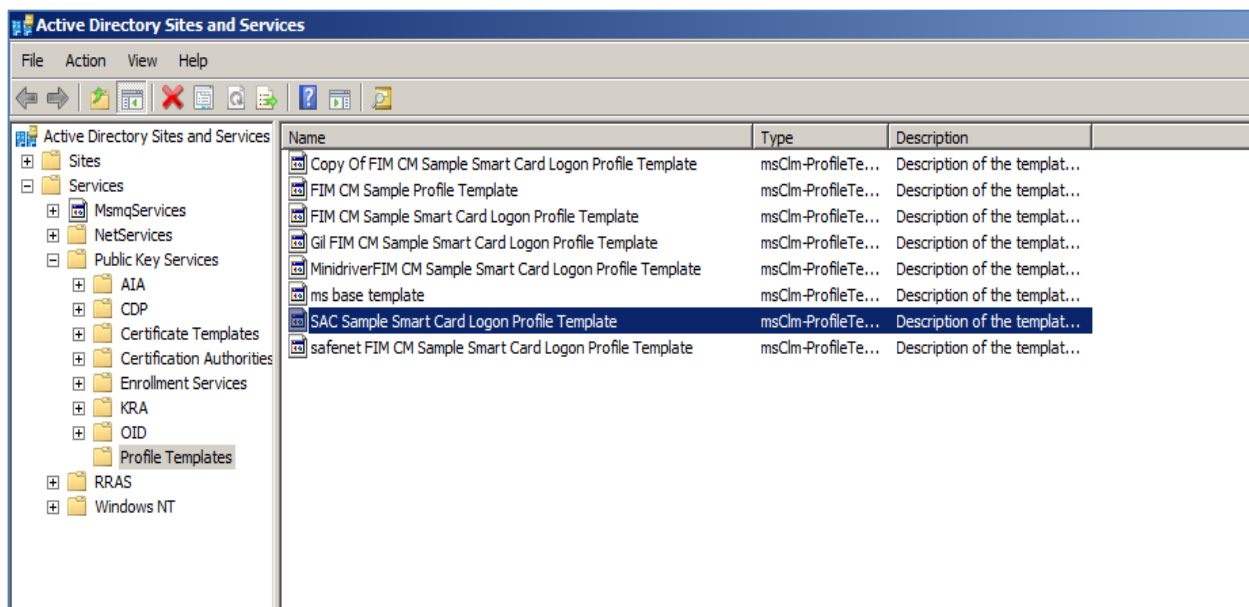


(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

Assigning the FIM CM Subscriber Group Permission on the SAC and Minidriver Profile Template

To assign the FIM CM Subscriber group permission on the Smart Card Profile Template:

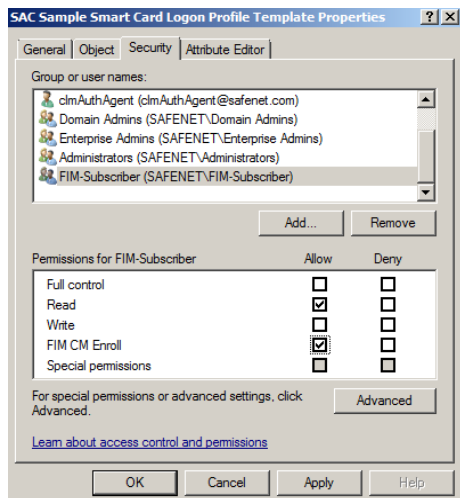
1. Click **Start > Administrative Tools > Active Directory Sites and Services**.
2. On the **View** menu, select **Show Services Node**.
3. In the left pane, click **Services > Public Key Services > Profile Templates**.



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

4. In the right pane, right-click the Profile Template you have created (for example, SAC Sample Smart Card Logon Profile Template) and select **Properties**.

5. On the **Security** tab, click **Add**.
6. In the text box below **Enter the object names to select (examples)**, enter **FIM-Subscribers** and then click **Check Names**. This should resolve with an underlined text. Click **OK**.
7. Under **Group or user names**, select **FIM CM Subscribers**.
8. Under **Permissions for FIM CM Subscribers**, in the **Allow** column, select **Read** and **FIM CM Enroll**. Click **OK**.



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



NOTE: Repeat these steps for the Minidriver Profile Template.

Editing the Registry for SAC

When using SAC as a middleware application, some changes are required in the Windows Registry on the client side.

1. Run **regedit.exe**.
2. Click **Computer > HKEY_LOCAL_MACHINE > SOFTWARE > SafeNet > SAC**.
3. Right-click **SAC** and then click **New > Key**.
4. In the **Name** field, enter **init**.
5. Right-click **init** and then click **New > DWORD (32-bit) Value**.
6. Specify **ignoreopensessions** as a name and **1** as its value.
7. Close the Registry editor.



NOTE: Without this Registry entry, most client operations will fail.

Editing the Registry for Minidriver

When using Minidriver, some changes are required in the Windows Registry on the client side.

1. Run **regedit.exe**.
2. Browse to the following location as appropriate for your machine:
 - For 32-bit clients on a 32-bit operating system or 64-bit clients on a 64-bit operating system:
Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > Defaults > Provider > Microsoft Base Smart Card Crypto Provider
 - For 32-bit clients on a 64-bit operating system:
Computer > HKLM > SOFTWARE > Wow6432Node > Microsoft > Cryptography > Defaults > Provider > Microsoft Base Smart Card Crypto Provider
3. Create the following new **DWORD (32-bit) Value**:
 - Name – **AllowPrivateExchangeKeyImport**
Value – 1
 - Name – **AllowPrivateSignatureKeyImport**
Value – 1
4. Close the Registry editor.

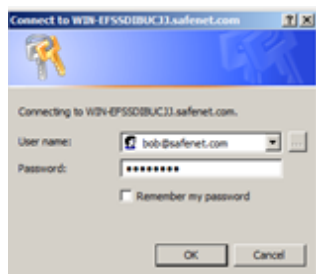
Running the Solution

When configuration is complete, and the necessary permissions are assigned to the users, the user can enroll a certificate using the FIM CM portal.

Enrolling a Certificate

1. Open **FIM CM Portal**.
2. Enter the user name and domain password, and then click **OK**.

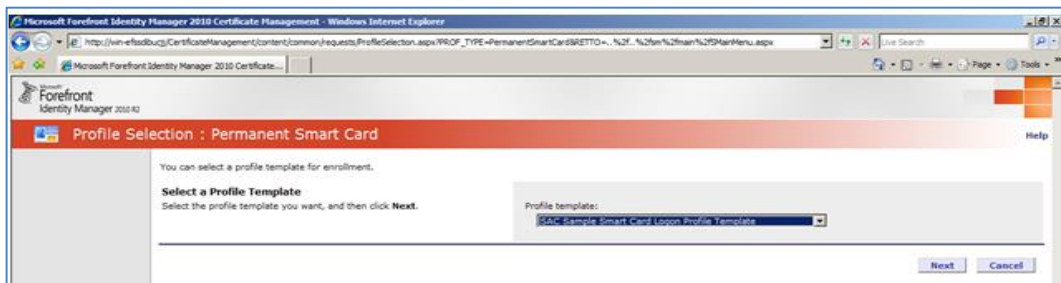
The user should have the permissions required to enroll a certificate.



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

3. Click **Click to enter**.
4. In the left pane, under **Select a View**, select **Manage my info**.
5. Select **Request a permanent smart card**.

- In the **Profile template** field, select your profile template and then click **Next**.



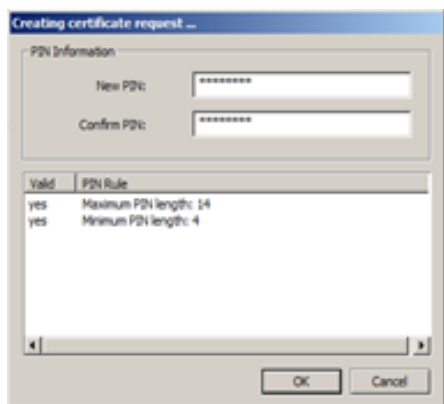
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

- On the **Enrollment Request Initiation** page, click **Next**.
- Insert the smart card on which you want to enroll the certificate.
- Select an appropriate smart card from the list and then click **OK**.



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

- On the **Creating certificate request** window, enter a new user PIN in the **New PIN** and **Confirm PIN** fields. Click **OK** to continue.



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

- On successful completion of the certificate request, the **Request Complete** window is displayed.

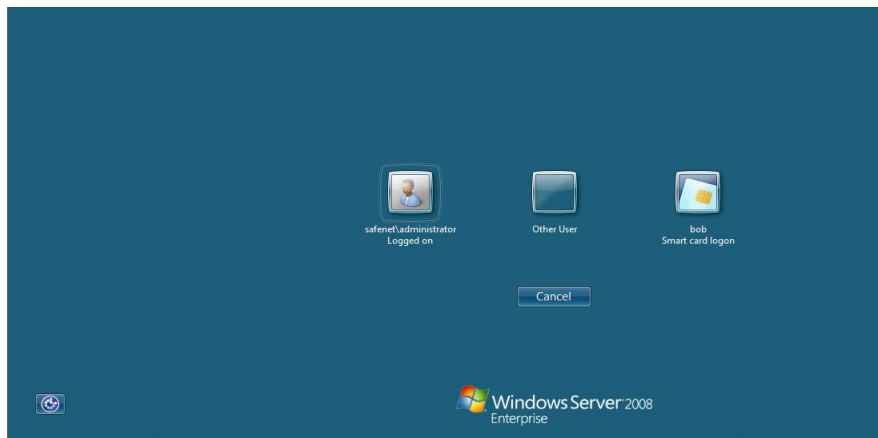


(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

Testing the Solution

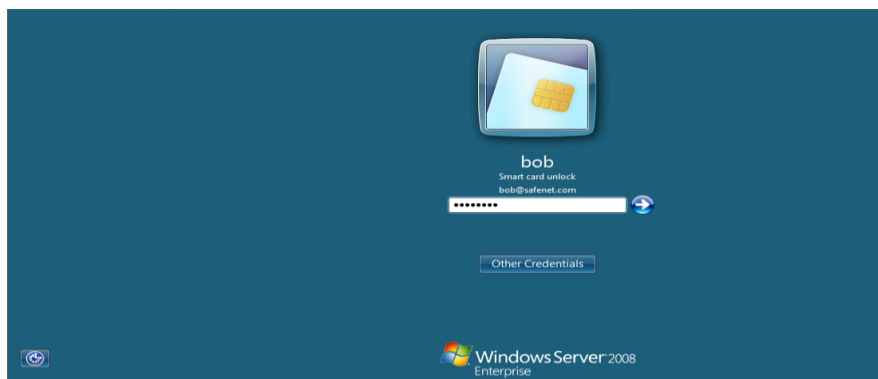
To test smart card logon, perform the following steps:

1. Insert the smart card into the client machine and start the machine. The smart card will be shown on the GINA.



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

2. Click **Smart Card Logon**.



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

3. Enter the **User PIN** and press **Enter**.

The user has logged on successfully.

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 1: Support Contacts

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
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.	