Preface

© 2013 SafeNet, Inc. All rights reserved.

Part Number: 007-011483-001 (Rev F, 07/2013)

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.

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.

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 below.

SafeNet, Inc.
4690 Millennium Drive
Belcamp, Maryland 21017
USA

Limitations

This document does not include the detailed steps to set up the third-party software. The steps given in this document must be modified accordingly. Refer to Luna SA documentation for general Luna setup procedures.

Disclaimers

The foregoing integration was performed and tested only with the specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

Technical Support

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, please contact your supplier or SafeNet support.

SafeNet 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.

Technical Support Contact Information:
Phone: 800-545-6608, 410-931-7520
Email: support@safenet-inc.com
# Table of Contents

**Preface** ........................................................................................................................................................................... i

**Chapter 1 Introduction** .................................................................................................................................................. 5
  - Scope ........................................................................................................................................................................... 5
  - Common Terms and Phraseology .......................................................................................................................... 5
  - 3rd Party Application Details ................................................................................................................................. 5
  - Supported Platforms ................................................................................................................................................. 5
  - HSMs and Firmware Version ................................................................................................................................. 6
  - Distributions ............................................................................................................................................................ 6
  - Prerequisites ........................................................................................................................................................... 6
  - Prerequisites for HSM ............................................................................................................................................. 6

**Chapter 2 Installing and Configuring FIM CM** ............................................................................................................. 7
  - Prerequisites for FIM ................................................................................................................................................. 7
  - Software requirements .............................................................................................................................................. 7
  - Modify the Active Directory Schema ..................................................................................................................... 8
  - Creating the Active Directory user accounts ....................................................................................................... 8
  - Installing the FIM CM .............................................................................................................................................. 8
  - Prepare and Publish the certificate templates used within the FIM CM .............................................................. 9
  - Deploying the three agent account certificates .................................................................................................. 16
  - Configure the FIM CM server ................................................................................................................................ 17
  - Designating the pre-enrolled FIM CM agent certificates ......................................................................................... 23
  - Enabling SSL on the FIM CM website ..................................................................................................................... 24
  - Configuring SSL ...................................................................................................................................................... 25
  - Disabling kernel-mode authentication ................................................................................................................... 25
  - Connecting to the FIM CM web portal ................................................................................................................... 26
Chapter 1
Introduction

Microsoft® Forefront Identity Manager (FIM) 2010 enables IT organizations to reduce the cost of managing the identity and access lifecycle by providing a single view of a user's identity across the heterogeneous enterprise and through the automation of common tasks. Part of the Microsoft Identity and Access Management platform product line, Forefront Identity Manager (FIM) 2010 superseded Microsoft Identity Lifecycle Manager (ILM) 2007, and was known as ILM 2 during development. ILM 2007 was created by merging Microsoft Identity Integration Server 2003 (MIIS) and Certificate Lifecycle Manager (CLM) 2007.

Microsoft® Forefront Identity Manager (FIM) 2010 - Certificate management is an identity-assurance management system that maximizes the trust and flexibility associated with digital certificates and smart cards by providing enhanced management facilities for Windows Server 2008 R2 and Windows 2012 Active Directory, and smart cards.

Microsoft® Forefront Identity Manager (FIM) 2010 - Certificate management uses HSM for the following purposes:

- Protect the agent private keys that are used by FIM Certificate Management.
- Use as a Random Number Generator for server key generation.
- To store the Global Platform Master Keys for Applet Management operations (This integration is outside of the scope of this document).

Note – Currently HSM can not be used for Hardware based Random Number Generation due to a known bug with Forefront Identity Manager 2010.

Scope

This document outlines the steps to install, configure and integrate Microsoft® Forefront Identity Manager (FIM) 2010 - Certificate management with Luna SA 5.0/5.1 and Luna 5.2.

Common Terms and Phraseology

This or other documentation may refer to Forefront Identity Manager 2010 – Certificate Management as FIM CM.

3rd Party Application Details

- Microsoft® Forefront Identity Manager 2010
- Microsoft® Forefront Identity Manager 2010 R2 SP1

Supported Platforms

- Windows Server 2008 R2 (running on Hyper-V/ESXi v 4.1.0)
- Windows Server 2012 (running on Hyper-V/ESXi v 4.1.0)
HSMs and Firmware Version

- K5 HSM f/w 4.6.8
- K6 HSM f/w 6.0.8
- K6 HSM f/w 6.2.1
- K6 HSM f/w 6.10.1

Distributions

- Luna SA 1U Appliance s/w 4.4.1
- Luna SA Client s/w v4.4.1 (64-bit)
- Luna SA 1U Appliance s/w 5.0
- Luna SA Client s/w v5.0 (64-bit)
- Luna SA 1U Appliance s/w 5.1
- Luna SA Client s/w v5.1 (64-bit)
- Luna SA 1U Appliance s/w 5.2
- Luna Client s/w v5.2.1 (64-bit)

Prerequisites

Refer to either Luna SA or FIM Certificate Management documentation for more details as to how to configure and setup the Luna SA to be used by the ILM for above-mentioned purposes.

Prerequisites for HSM

Before you get started ensure the following:

- Luna SA appliance has a secure admin password
- Luna SA has a hostname suitable for your network
- Luna SA network parameters are set to work with your network
- Initialized the HSM on the Luna SA appliance
- Created and exchanged certificates between the Luna SA and the “Client” system (registered the Client with the Partition).
- Created a partition on the HSM and allocated a partition password to be used later. Run the command, vtl verify to display a partition from Luna SA. The general form of command is C:\Program Files\Luna SA > vtl verify.
- Run the command, registerCSP64.exe to register Luna CSP. The general form of command is C:\Program Files\Luna SA\CSP > register.exe.

For SA v5.0, run the command, registerCSP64.exe to register Luna CSP. The general form of command is C:\Program Files\Luna SA\CSP > registerCSP64.exe. Also, run this command with parameter ‘l’. The general form of command is C:\Program Files\Luna SA\CSP > registerCSP64.exe /l.

- Enabled Partition “Activation” and “Auto Activation” (Partition policy settings 22 and 23 (applies to Luna SA with Trusted Path Authentication [which is FIPS 140-2 level 3] only).
- The hardware and software requirements are met for FIM. Refer to the FIM Certificate Management Installation and Configuration details in FIM Documentation for more details.
Chapter 2
Installing and Configuring FIM CM

Prerequisites for FIM

Table 1: Computers

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2008 R2 / Windows 2012</td>
<td>Domain Controller</td>
</tr>
</tbody>
</table>

Software requirements

The following table summarizes the software that is required to implement the procedures in this document.

Table 2: Software Requirements for FIM CM

<table>
<thead>
<tr>
<th>Software</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification authority (CA)</td>
<td>FIM CM requires at least one or more of the following: 32-bit Windows Server 2003 CA, 32-bit Windows Server 2008 CA, 64-bit Windows Server 2008 CA or 64-bit Windows 2012 CA. The certification authority must be an Enterprise CA.</td>
</tr>
<tr>
<td>IIS 7.x / 8.x</td>
<td>FIM CM uses IIS as its Web server to run the FIM CM Portal.</td>
</tr>
<tr>
<td>Microsoft .NET Framework 3.5</td>
<td>FIM CM is a Microsoft .NET–connected application. You must install .NET Framework 3.5 on the server. If FIM CM is installed on the same server as SQL Server 2008, then .NET Framework 3.5 Service Pack 1 (SP1) is required.</td>
</tr>
</tbody>
</table>

Install IIS 7.x / 78.x, Microsoft Framework 3.5, SQL Server 2008 & CA on machine where FIM CM will be installed.
Modify the Active Directory Schema

FIM CM requires that the schema be extended. The schema extension includes the following objects:

- Profile Template object
- Profile Template string attribute
- Custom CLM permissions

To install the schema updates, you should log on to the domain controller as Administrator or must be a member of the Active Directory forest's Schema Admins group.

- Open the `<FIM Source>\Certificate Management\X64\Schema` folder.
- Double click the `ModifySchema.vbs` file to update the schema.
- When the schema update is complete, in the Success message box, click OK.

Creating the Active Directory user accounts

FIM CM uses six accounts to perform its various operations. To create the Active Directory user accounts log on to the Domain Controller as the administrator and create the six default agent accounts used by FIM Certificate Management.

The six agent accounts that must be created are:

- clmAgent
- clmEnrollAgent
- clmAuthAgent
- clmKRAgent
- clmCAMngr
- clmWebPool

Installing the FIM CM

- On FIM CM server insert the FIM 2010/ FIM 2010 R2 SP1 CD in the CD/DVD drive.
- Open an Administrative command prompt.
- Open the `<FIM Source>: \Certificate Management\X64` folder.
- Right-click Setup.exe, and then click Run as administrator.
- On the Welcome to the Forefront Identity Manager Certificate Management Setup Wizard page, click Next.
- On the End-User License Agreement page, read the agreement, enable the I accept the terms in the license agreement check box, and then click Next.
- On the Custom Setup page, select the FIM CM Portal and FIM CM Update Service components (only select FIM CM CA Files if the CA is also installed on the same server), verify that the install location is: `C:\Program Files\Microsoft Forefront Identity Manager\2010`, and then click Next.
• On the Virtual Web Folder page, ensure that the Virtual folder name is CertificateManagement, and then click Next.

• On the Install Forefront Identity Manager Certificate Management page, click Install.

• On the Completed the Forefront Identity Manager Certificate Management Setup Wizard page, click Finish.

**Prepare and Publish the certificate templates used within the FIM CM**

Before enrolling the agent certificates, you must create custom V2 certificate templates for each certificate.

Make a duplicate copy of following Certificate Templates:

- User
- Key Recovery Agent
- Enrollment Agent

**Preparing the certificate template**

Perform the following steps to prepare the certificate template:

**User Template**

- Click **Start**, point to Administrative tools, and then click **Certificate Authority**.

- In **Certification Authority**, expand your CA set of folders and select **Certificate Templates** in the console tree.

- Right-click **Certificate Templates**, and click **Manage**.
• In Certificate Templates, select User.

• Right-click User, and click Duplicate Template.
In the **Duplicate Template** dialog box, click **Windows Server 2003, Enterprise Edition**, and then click **OK**.

On Windows 2012 select **Windows 2003** for **“Compatibility Settings”**

*Do not select Windows Server 2008, Enterprise Edition as the certificate template version. FIM CM does not support the use of CNG with its agent certificates*

The **Properties of New Template** window appears:
### Installing and Configuring FIM CM

1. Click the **General** tab on the **Properties of New Template** window and enter the **Template display name** for your newly created certificate template.

2. Click the **Request Handling** tab on the **Properties of New Template** window, unmark option **Allow private Keys to be exported**

3. Click CSPs on Windows 2008 R2 and select **Cryptography** tab on Windows 2012.

4. From the list of CSPs provided, select only **Luna Cryptographic Services for Microsoft Windows** checkbox.
On the Subject Name tab, clear the Include e-mail name in subject name and E-mail name check boxes.

On the Extensions tab, in the Extensions included in this template list, ensure that Application Policies is selected, and then click Edit.

In the Edit Application Policies Extension dialog box, select both the Encrypting File System and the Secure Email application policies, click Remove, and then click OK.

On the Security tab perform the following:
  - Add clmAgent.
  - Assign Read and Enroll permissions to clmAgent.

In the Properties of New Template dialog box, click OK.

Close the Certificate Templates console.

Key Recovery Agent

Ensure that the Certificate Templates console is still open.

In the Certificate Templates console, in the details pane, right click Key Recovery Agent, and then click Duplicate Template.

In the Duplicate Template dialog box, click Windows Server 2003, Enterprise Edition, and then click OK.

In the Properties of New Template dialog box, on the General tab, in the Template display name box, type FIM Key Recovery Agent, verify that the Validity Period is set to 2 years.

On the Request Handling tab, click CSPs.

In the CSP Selection dialog box, click Requests must use one of the following CSPs, enable only Luna Cryptographic Services for Microsoft Windows Provider, and then click OK.
• On the Issuance requirements tab, clear the CA certificate manager approval check box.

• On the Security tab perform the following:
  o Add clmKRAgent.
  o Assign Read and Enroll permissions to clmKRAgent.

• In the Properties of New Template dialog box, click OK.

Enrollment Agent

• Ensure that you are still in the Certificate Templates console.

• In the Certificate Templates console, in the details pane, right-click Enrollment Agent, and then click Duplicate Template.

• In the Duplicate Template dialog box, click Windows Server 2003, Enterprise Edition, and then click OK.

• In the Properties of New Template dialog box, on the General tab, in the Template display name box, type FIM Enrollment Agent, verify that the Validity Period is set to 2 years.

• On the Request Handling tab, click CSPs.

• In the CSP Selection dialog box, click Requests must use one of the following CSPs, enable only Luna Cryptographic Services for Microsoft Windows Provider, and then click OK.

• On the Security tab, perform the following:
  o Add clmEnrollAgent.
  o Assign Read and Enroll permissions to the clmEnrollAgent account.

• In the Properties of New Template dialog box, click OK.

The Luna Cryptographic Services generates private key of the user’s certificate inside the HSM confine, and stores it securely inside its hardware. Any subsequent usage of this certificate would require the private key; hence the HSM’s availability and access rights are must.

Once the certificate template is ready, proceed to publish the same.

Publishing the certificate template

• Perform the following steps to publish the certificate template:

• Click Start, point to Administrative Tools, and then click Certificate Authority.

• In Certification Authority, expand your CA set of folders and select Certificate Templates in the console tree.

• Right-click Certificate Templates, point to New and click Certificate Template to Issue.
In the **Enable Certificate Templates** dialog box, select FIM Signing, FIM Enrollment Agent, and FIM Key Recovery Agent, and then click OK.

The newly created certificate templates are listed in the Certificate Authority window (Select **Certificate Templates** in the console tree). These certificate templates are now ready to be used at the time of request and issuance.
Deploying the three agent account certificates

When using an HSM, you cannot use the FIM CM Configuration Wizard to deploy the agent certificates. The certificates must be manually enrolled by each agent account, and the thumbprints of the certificates recorded in the Web.Config file.

To manually enroll each certificate, you must allow the agent accounts the ability to log on locally to the FIM CM server to allow them to request certificates and store the certificates in the agent account’s profile on the FIM CM server.

Once you have enabled logon, you can now log on as each account and request the assigned agent certificate.

Log on with the following credentials:

- **Username:** `clmAgent|clmEnrollAgent|clmKRAgent`
- **Password:** *Assigned Password*
- **Domain:** `Domain`

- Run `certmgr.msc`.
- If prompted to provide your credentials, provide the credentials listed in first step.
- In the console tree, right-click **Personal**, point to **All Tasks**, and then click **Request New Certificate**.
- On the **Before You Begin** page, click **Next**.
- On the **Request Certificates** page, select the certificate listed in the table below, and then click **Enroll**.
## FIM CM Agent Accounts

<table>
<thead>
<tr>
<th>Agent account</th>
<th>Certificate to request</th>
</tr>
</thead>
<tbody>
<tr>
<td>clmAgent</td>
<td>FIM Signing</td>
</tr>
<tr>
<td>clmEnrollAgent</td>
<td>FIM Enrollment Agent</td>
</tr>
<tr>
<td>clmKRAgent</td>
<td>FIM Key Recovery Agent</td>
</tr>
</tbody>
</table>

- On the **Certificate Installation Results** page, ensure that the status is reported as **Succeeded**, and then click **Finish**.

- In the console tree, expand **Personal**, and then click **Certificates**.
- On the **Details** tab, in the **Field** listing, select **Thumbprint**. Record the **thumbprint** below:
  - clmAgent: ______________________________________________
  - clmEnrollAgent: _________________________________________
  - clmKRAgent: ____________________________________________

- Click **OK**.

- Close the **CertMgr** console.

- Open a command prompt.

- At the command prompt, type `certutil –user –verifystore my` and then press ENTER.

- Ensure in the output that the **Provider** is **Luna Cryptographic Services for Microsoft Windows** and that the **Certificate is valid**.

- Close the command prompt.

- Close all open windows and log off.

Repeat this process for all three agent accounts.

## Configure the FIM CM server

Once the CLM server is installed, you now need to configure the same along with its components.

Microsoft recommends that you run the **Certificate Management Configuration Wizard** with a user account that is a member of the Enterprise Administrators group.

The Enterprise Administrator’s group already has the necessary permissions to the relevant profile templates and certificate templates.

To run the **Certificate Management Configuration Wizard**, perform the following:

- Click **Start**, point to **Microsoft Forefront Identity Manager**, and then click **Certificate Management Configuration Wizard**.
• Click Next to continue.

• Provide the CA information and click Next to continue.
• Provide the SQL server information and click **Next** to continue.

• Provide the database settings details and click **Next** to continue.
• Specify the Active Directory settings and click **Next** to continue. It is recommended to use the default settings.
On the Agents – FIM CM page, clear the Use the FIM CM default settings check box, and then click Custom Accounts.

In the Agents – FIM CM multi-tabbed dialog box, on each tab, enter the following information:

- User name: Name of the specific FIM CM agent account
- Password: Password assigned to the FIM CM agent account
- Confirm Password: Same password
- Use an existing user: Enabled

When all account information is inputted, click OK.

On the Agents – FIM CM page, click Next.

Select the Create and configure certificates manually checkbox. This illustrates the way you can create these certificates inside the Luna HSM later on.

Click Next to continue.

On the Setup E-mail Server, Document Printing page, accept the default settings, and then click Next.

On the Ready to Configure page, click Configure.
In the Warning dialog box, click OK to acknowledge that SSL is not enabled on the IIS virtual directory.

Do not click the Finish button until the wizard is completed. Clicking Finish before execution is complete will prevent FIM CM from operating correctly.
Designating the pre-enrolled FIM CM agent certificates

You must now modify the web.config file to record the thumbprints of each agent certificate.

The certificate thumbprints are referenced in four different lines in the Web.Config file: one for the clmEnrollmentAgent and three for the clmAgent. You must now manually modify the web.config file to register these thumbprints.

- Open C:\Program Files\Microsoft Forefront Identity Manager\2010\Certificate Management\Web in Windows Explorer.
- Open the Web.Config file in Notepad.
- In Notepad, from the Edit menu, click Find.
- In the Find dialog box, in the Find what box, type Clm.EnrollAgent.Certificate, and then click Find Next.
- Modify the line so that the thumbprint from the clmEnrollmentAgent certificate is referenced in the following line (removing the spaces from the thumbprint value):

  ```xml
  <add key="Clm.EnrollAgent.Certificate.Hash" value="4778eb98ff0e9fe036ab9e85076c7f7eb9e1086" />
  *Value will be thumbprint of your clmEnrollmentAgent certificate*
  ```
- Press Control-Home to return to the beginning of the file.
- In Notepad, from the Edit menu, click Find.
- In the Find dialog box, in the Find what box, type Clm.SigningCertificate.Hash, and then click Find Next.
- Modify the line so that the thumbprint from the clmAgent certificate is referenced in the following line (removing the spaces from the thumbprint value):

  ```xml
  <add key="Clm.SigningCertificate.Hash" value="66209461b668c99c2da361ce393a24f011f5732b" />
  *Value will be thumbprint of your clmAgent certificate*
  ```
- Press Control-Home to return to the beginning of the file.
- In Notepad, from the Edit menu, click Find.
- In the Find dialog box, in the Find what box, type Clm.ValidSigningCertificates.Hashes, and then click Find Next.
- Modify the line so that the thumbprint from the clmAgent certificate is referenced in the following line (removing the spaces from the thumbprint value):

  ```xml
  <add key="Clm.ValidSigningCertificates.Hashes" value="66209461b668c99c2da361ce393a24f011f5732b" />
  ```
Value will be thumbprint of your clmAgnent certificate

• Press Control-Home to return to the beginning of the file.

• In Notepad, from the Edit menu, click Find.

• In the Find dialog box, in the Find what box, type Clm.SmartCard.ExchangeCertificate.Hash, and then click Find Next.

• In the Find dialog box, click Cancel.

• Modify the line so that the thumbprint from the clmAgnent certificate is referenced in the following line (removing the spaces from the thumbprint value):

<add key="Clm.SmartCard.ExchangeCertificate.Hash" value="66209461b668c99c2da361ce393a24f011f5732b" />

• Press Control-Home to return to the beginning of the file.

• In Notepad, from the Edit menu, click Find.

• In the Find dialog box, in the Find what box, type Clm.Encryption.Algorithm and set encryption algorithm to TripelDes (By default AES would be provided as value)

<add key="Clm.Encryption.Algorithm" value="TripelDes" />

• Close the web.config file, saving all changes.

• Close all open windows.

Enabling SSL on the FIM CM website

When you enable SSL on the FIM CM web portal, you must ensure that the DNS name used to access the FIM CM web portal is registered as a service principal name (SPN) for the clmWebPool account. For integrated authentication to work, the clmWebPool account must have the same SPN registered to allow the account to impersonate the user when requesting certificates. If the SPN does not match the DNS name used by the user to connect to the FIM CM web portal, the connection attempt will fail.

Verifying and changing the SPN When users connect to a website, they typically use a CNAME record in DNS, rather than the actual machine name. For example, if the machine name is GMBFIM01.accounts.example.com, you may prefer that the users connect to fimcm.example.com.

To set up FIM CM to allow connections to fimcm.example.com, you must:

• Set up any DNS CNAME records.

• Register the fimcm.example.com SPN with the clmWebPool account.

To set up the CNAME record, use the following procedure:

• Log on to a domain controller as a user who can modify DNS entries.

• In the console tree, expand DCName, expand Forward Lookup Zones, and then click example.com.
• Right click example.com, and then click New Alias (CNAME).
• In the Alias name box, type fimcm, and then click Browse.
• In the Browse dialog box, navigate to the A record for the FIM CM server, and then click OK.
• Ensure that the new CNAME record exists in the details pane.
• Close the DNS Manager console.

Once the CNAME is registered, you must add the CNAME to the clmWebPool’s SPN listing.

• Open an Administrative command prompt.
• At the command prompt,
  o For Windows 2008 R2 type setspn –a HTTP/fimcm.example.com example\clmWebPool and then press ENTER.
  o For Windows 2012 type setspn –S HTTP/fimcm.example.com example\clmWebPool and then press ENTER.
• At the command prompt, type setspn –l example\clmWebPool and then press ENTER.
• Ensure that the new SPN is included in the list of SPNs and that there are no typographical errors.
• Close the command prompt.

Configuring SSL

After SPN is registered with the clmWebPool account, you can request an SSL certificate for the FIM CM web portal. Once you have requested the web server certificate, you must bind the certificate to a website.

Once this is done the final step is to enable SSL for the CertificateManagement application. Use the following procedure:

• Ensure you are in the Internet Information Services (IIS) Manager console.
• In the console tree, expand ServerName, expand Sites, expand Default Web Site, and then click CertificateManagement.
• On the /CertificateManagement Home page, in the IIS section, double click SSL Settings.
• On the SSL Settings page, enable the Require SSL check box, enable the Require 128-bit SSL check box, and then in the Actions list, click Apply.
• SSL is now enabled for the CertificateManagement website.

Disabling kernel-mode authentication

To use FIM CM with IIS 7.x/8.x, you must disable kernel-mode authentication.

To disable kernel-mode authentication
Log on to the FIMCM server as the administrator.
On the QS-FIMCM server, click Start, click Administrative Tools, and open the Internet Information Services Manager.

In the console tree, expand Sites, expand Default Web Site, and then click CertificateManagement.

1. In the center pane, scroll down and double-click Authentication.
2. Right-click Windows Authentication, and then click Advanced Settings.
3. Clear the Enable kernel-mode authentication check box.
4. Click OK.
5. Close Internet Information Services Manager.

Connecting to the FIM CM web portal

Once you have completed configuring the FIM CM web portal, you should use Internet Explorer to connect to the website. Before you connect, the following items must be configured in Internet Explorer:

- The website must be added to the Trusted Sites security zone.
- The Trusted Sites security zone must enable automatic logon with current user name and password.
- The Trusted Sites security zone must enable the option to initialize and script ActiveX controls not marked as safe for scripting.

Once connected, you can then connect to the website using the URL

`https://fimcm.example.com/certificatemanagement`