Microsoft Identity Manager 2016

Integration Guide

gemalto
security to be free

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Document Part Number: 007-013502-001, Rev. A

Release Date: April 2016

Contents

Preface

This document is intended to guide administrators through the steps for Microsoft Identity Manager 2016 and SafeNet Luna HSM integration. This guide provides the necessary information to install, configure, and integrate Microsoft Identity Manager 2016 with SafeNet Luna Hardware Security Modules (HSM).

Scope

This guide provides instructions for setting up a small test lab with Microsoft Identity Manager 2016 running with SafeNet Luna HSM for securing the private keys. It explains how to install and configure the software that is required for setting up Microsoft Identity Manager 2016 while storing private keys on SafeNet Luna HSM.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

NOTE: Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

CAUTION: Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

WARNING: Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Command Syntax and Typeface Conventions

Convention	Description
bold	The bold attribute is used to indicate the following: Command-line commands and options (Type **dir /p**.) Button names (Click **Save As**.) Check box and radio button names (Select the **Print Duplex** check box.) Window titles (On the **Protect Document** window, click **Yes**.) Field names (**User Name:** Enter the name of the user.) Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) User input (In the **Date** box, type **April 1**.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
`Consolas`	Denotes syntax, prompts, and code examples.

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 Gemalto Customer Support. Gemalto 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 Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	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 Gemalto Knowledge Base.	

1
Introduction

Overview

SafeNet Luna HSM integrates with Microsoft Identity Manager (MIM) 2016 to provide significant performance improvements by off-loading cryptographic operations from the server to HSM. In addition, SafeNet Luna HSM provides extra security by protecting the keys within a FIPS 140-2 certified hardware security module.

This integration between SafeNet Luna HSM and Microsoft Identity Manager (MIM) 2016 uses the MSCAPI interface. Microsoft Identity Manager (MIM) 2016 generates the 2048 bit RSA keys on SafeNet Luna HSM and it is used by the MIM for various functions like Certificate Enrollment for Smart Card and Key Recovery.

The installation is performed in several steps:

- Install and configure SafeNet Luna HSM.
- Install and configure Microsoft Identity Manager 2016 using SafeNet Luna HSM.

Understanding the Microsoft Identity Manager 2016

Microsoft Identity Manager (MIM) 2016 is the latest version of Microsoft's Identity and Access management (IAM) product suite, and replaces Forefront Identity Manager (MIM) 2010 R2. MIM provides identity data management and synchronization, authentication and authorization workflows, and self-service identity management capabilities for end-users – group management, credentials management, certificate management, etc.

For more information about Microsoft Identity Manager (MIM) 2016, refer Microsoft online documentation.

3rd Party Application Details

- Microsoft Identity Manager 2016

Supported Platforms

The following platforms are tested with SafeNet Luna HSM:

Operating Systems	SafeNet HSM	SafeNet HSM Client	MICROSOFT IDENTITY MANAGER
Windows Server 2012 R2	Luna SA Appliance Software v6.2.0 Firmware 6.24.0	Luna Client 6.2.0	2016

Prerequisites

SafeNet Network HSM Setup

Refer to the SafeNet Network HSM documentation for installation steps and details regarding the configuration and setup of the box on Windows systems. Before you get started, ensure the following:

- SafeNet Network HSM appliance and a secure admin password.
- SafeNet Network HSM, and a hostname, suitable for your network.
- SafeNet Network HSM network parameters are set to work with your network.
- Initialize the HSM on the SafeNet Network HSM appliance.
- Create and exchange certificates between the SafeNet Network HSM and your Client system.
- Create a partition on the HSM, remember the partition password that will be later used by Microsoft Identity Manager.
- Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from SafeNet Network HSM. The general form of command is “C:\Program Files\SafeNet\LunaClient> vtl verify”.
- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to SafeNet Network HSM with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

SafeNet Luna HSM Configuration Settings

The Luna Client configuration file located at the following path needs to be changed for Luna v6.x:

C:\Program Files\SafeNet\LunaClient\crystoki.ini

This configuration file needs to be edited for slot id because by default it is set to 0. Set the slot id to 1 by making the following changes in the configuration file:

```
[Presentation]
OneBaseSlotId=1
```

If using Luna 6.x is in FIPS mode:

Under FIPS 186-3/4, the RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. This means that RSA PKCS and X9.31 key generation is no longer approved for operation in a FIPS-compliant HSM. If you are using the SafeNet Luna HSM in FIPS mode, you have to make the following change in configuration file:

```
[Misc]
RSAKeyGenMechRemap = 1
```

The above setting will redirect the older calling mechanism to a new approved mechanism when SafeNet Luna HSM is in FIPS mode.

NOTE: SafeNet Luna HSM Configuration Settings are required only for Luna HSM f/w 6.22.0 or above. All other SafeNet Luna HSM f/w does not require this setting for FIPS mode.

Microsoft Identity Manager 2016 Setup

Before proceeding, it is recommended to familiarize yourself with Microsoft Identity Manager. Refer to the Microsoft Identity Manager documentation for more information on installation instructions.

2

Integrating SafeNet Luna HSM with Microsoft Identity Manager 2016

SafeNet Luna HSM with Microsoft Identity Manager 2016

Perform the following steps to set up Microsoft Identity Manager 2016 with SafeNet Luna HSM:

Prerequisites for MIM

Table 1: Computers

Operating System	Machine Name	Description
Windows Server 2012 R2	CORPDC	Domain Controller
Windows Server 2012 R2	CORPMIM	MIM CM, AD CS, Microsoft SQL Server® 2014, Internet Information Services (IIS)

Ensure that domain controller is installed on CORPDC and CORPMIM is joined in the domain. For demonstration purpose, we have used the CONTOSO.com as domain.

Software requirements

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

Table 2: Software Requirements for MIM CM

Software	Description
AD DS	An Active Directory infrastructure with a domain controller running Windows Server 2012 R2
Certification Authority (CA)	MIM CM requires at least one or more of the following: Windows Server 2012 R2 CA. The certification authority must be an Enterprise CA.
MIM CM	MIM CM software installed on Windows Server 2012 R2
SQL Server 2014	MIM CM supports the 64-bit edition of SQL Server 2014 Enterprise or SQL Server 2014 Standard.

Software	Description
IIS	MIM CM uses IIS as its Web server to run the MIM CM Portal.
Microsoft .NET Framework	MIM CM is a Microsoft .NET–connected application. You must install .NET Framework 3.5 and 4.5 on the server. If MIM CM is installed on the same server as SQL Server 2014, then .NET Framework 3.5 Service Pack 1 (SP1) is required.

IIS, Microsoft .NET Framework, SQL Server 2014 & CA are installed on the same machine where MIM CM will be installed for the demonstration purpose in this guide.

Ensure that above listed software are installed on the MIM Server machine.

CA Installation:

Refer the SafeNet Integration guide for Microsoft Active Directory Certificate Services for installing the CA on MIM CM Server.

Database Installation:

Refer the Microsoft SQL Server 2014 online installation documentation to install the SQL Server.

IIS Installation:

IIS installation require the following IIS Role Services are either already installed or select them for installation.

1. Common HTTP Features
   - Static Content
   - Default Document
   - Directory Browsing
   - HTTP Errors
   - HTTP Redirection
2. Application Development
   - ASP.NET
   - .NET Extensibility
   - ISAPI Extensions
   - ISAPI Filters
3. Health and Diagnostics
   - HTTP Logging
   - Request Monitor
4. Security

- Windows Authentication
- Request Filtering

5. Performance
   - Static Content Compression
   - Dynamic Content Compression
6. Management Tools
   - IIS Management Console
   - IIS 6 Management Compatibility

Microsoft .NET Framework Installation:

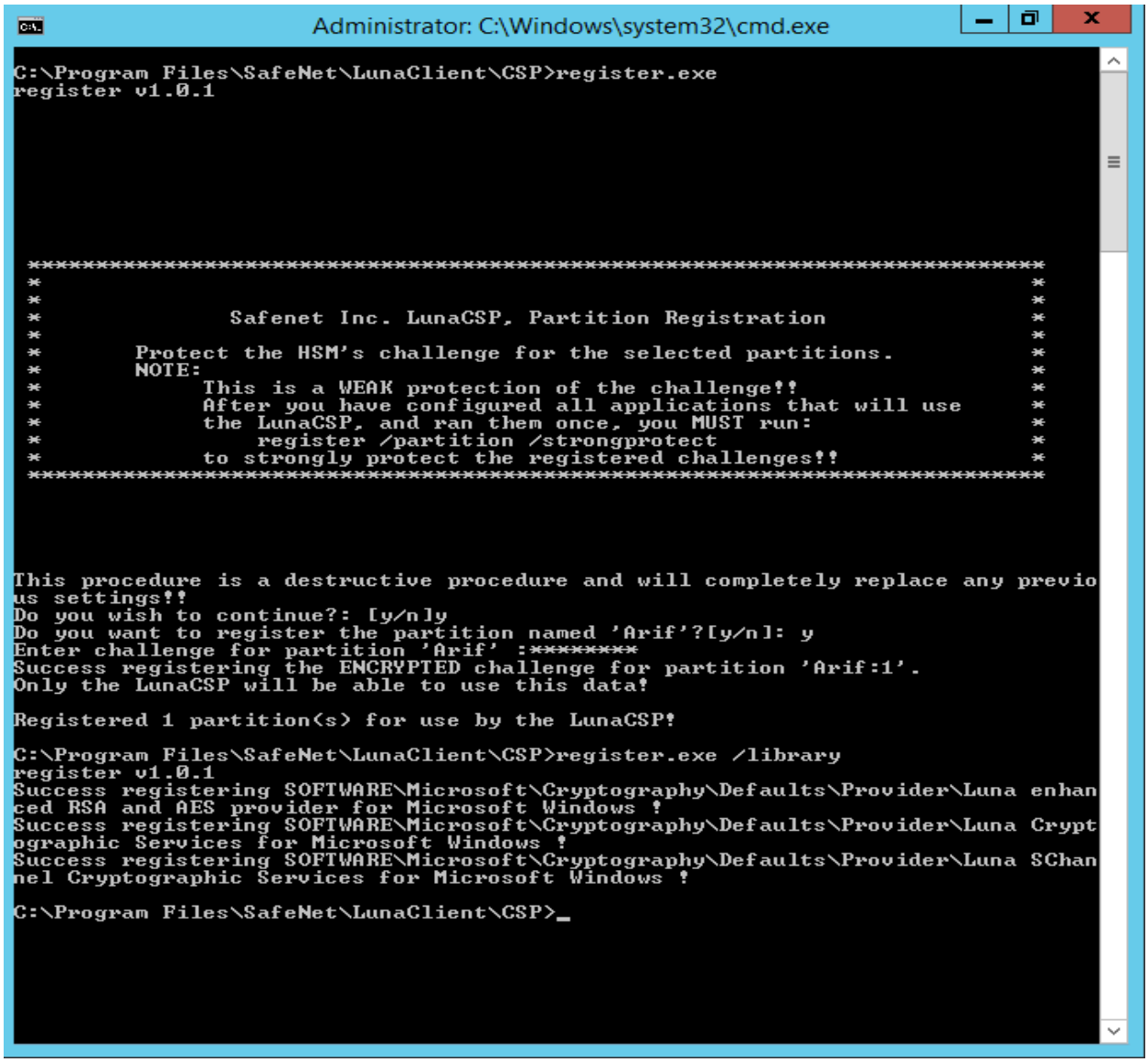
Use Server Manager to install the .Net Framework 3.5 & 4.5

Before you Begin

Luna CSP must be registered on the MIM CM server before proceeding further. To install the Luna CSP perform the following steps:

1. Log on to CORPMIM as CONTOSO\Administrator.
2. Browse the SafeNet Luna Client installation directory and open the CSP folder.
3. Click **File** and select **Open command prompt**.
4. In command prompt, type register.exe and press **Enter**. The general form of command is `C:\Program Files\SafeNet\LunaClient\CSP>register.exe`
5. Follow the instructions and provide the partition password when prompt. It register the Luna CSP on the system.

6. After registering the CSP, run the “register.exe /library” command to list available CSP. The general form of command is `C:\Program Files\SafeNet\LunaClient\CSP>register.exe /library`



Active Directory Schema Extension

MIM CM requires some additional attributes and extended rights to be added to the Schema. The schema extension includes the following objects:

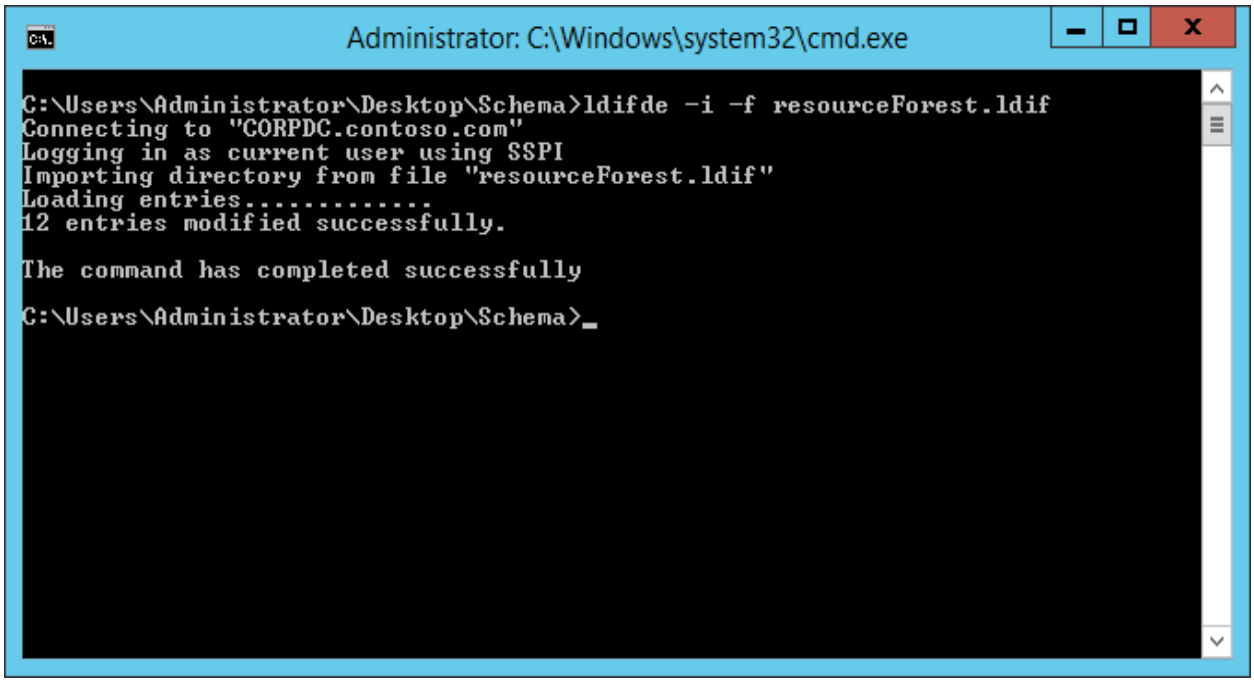
- Profile Template object
- Profile Template string attribute
- Custom CLM permissions

To install the schema updates, log on to the domain controller as Domain Administrator or an account that must be a member of the Active Directory forest's Schema Admins group

1. Log on to **CORPDC** as **CONTOSO\Administrator**.

2. Open the <MIM Source>\Certificate Management\X64\Schema folder.
3. Edit the **resourceForest.ldif** file and replace the "**DC=company,DC=com**" with your domain. For example "**DC=contoso,DC=com**"
4. Click **File** and select **Open command prompt**.
5. Run the following command to extend the schema.

   ```
   ldifde -i -f resourceForest.ldif
   ```



6. When the schema update is complete, a Success message displays. Close the command prompt.

> **NOTE:** It's a one way process and you cannot modify it, once it is changed. So execute the above steps carefully. We executed the above steps on single forest, single domain installation.

Creating the Active Directory User Accounts

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

The six agent accounts that need to be created are:

Full Name	User logon name
MIM CM Agent	MIMCMAgent

Full Name	User logon name
MIM CM Key Recovery Agent	MIMCMKRAgent
MIM CM Authorization Agent	MIMCMAuthAgent
MIM CM CA Manager Agent	MIMCMManagerAgent
MIM CM Web Pool Agent	MIMCMWebAgent
MIM CM Enrollment Agent	MIMCMEnrollAgent

To create an Accounts for MIM CM perform the following steps:

1. Log on to **CORPDC** as **CONTOSO\Administrator**, open **Active Directory Users and Computers**.
2. In the console tree, right-click the **contoso.com** domain, click **New** and then click **User**.
3. In the **New Object – User** dialog box, in **Full Name** type **MIM CM Agent**.
4. In **User logon name**, type **MIMCMAgent** and then click **Next**.

NOTE: The actual account name that you use is up to your organizational naming scheme or your discretion. You can name the MIM CM whatever you would like, the important part is that you assign them the appropriate permissions. This can be done automatically by using the CM installation wizard or you may choose to do this manually.

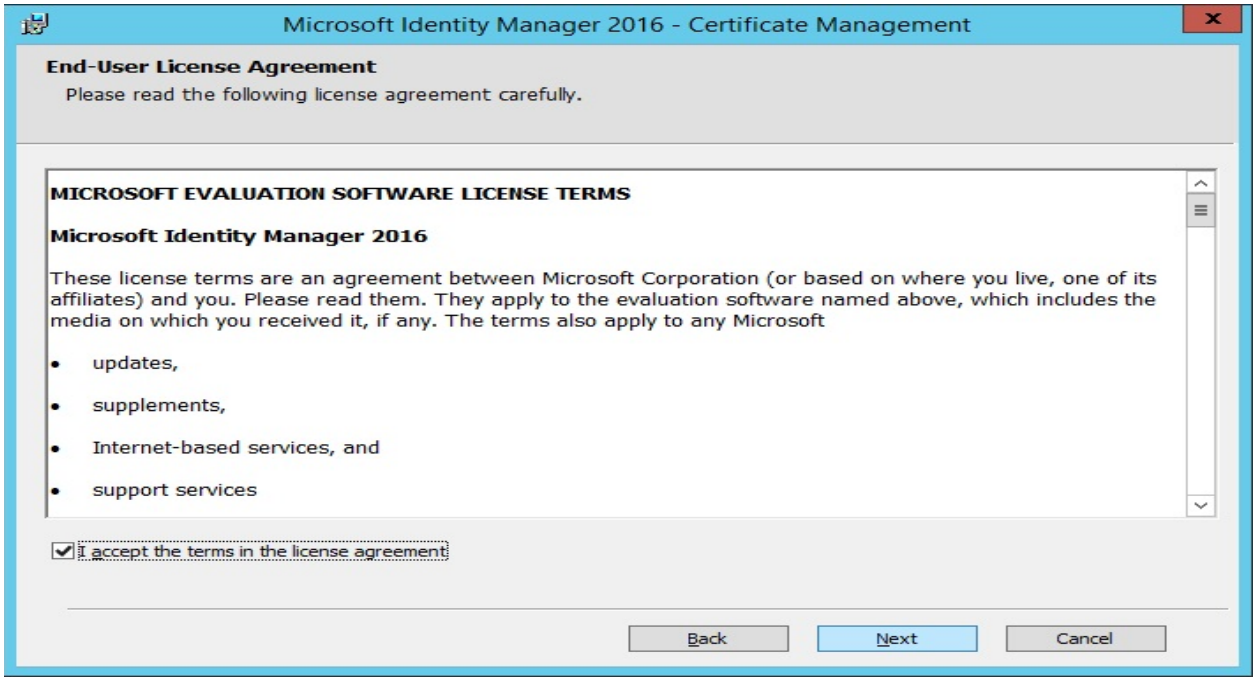
5. Type a password for both **Password** and **Confirm password** and remember it.
6. Clear **User must change password at next logon**.
7. Select the **Password never expires**.
8. Click **Next** and then click **Finish**.
9. Create the additional five accounts that are required by MIM CM using the same settings as described in this procedure, but with the names described in the above table.

Installing the MIM CM

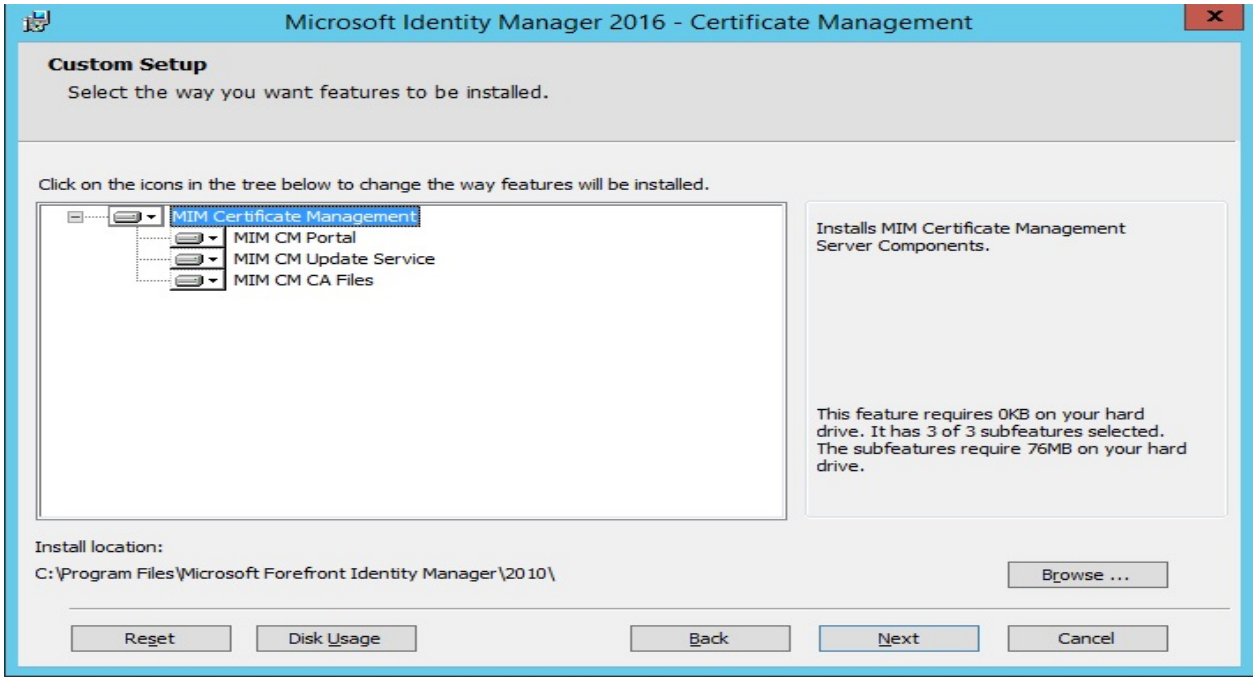
1. Log on to **CORPMIM** as **Contoso\Administrator**.
2. On MIM CM server insert the MIM 2016 CD in the CD/DVD drive.
3. Open the <MIM Source>:\Certificate Management\x64 folder.
4. Right-click **Setup.exe**, and then click **Run as administrator**.

5. On the Welcome to the Microsoft Identity Manager Certificate Management Setup Wizard page, click **Next**.

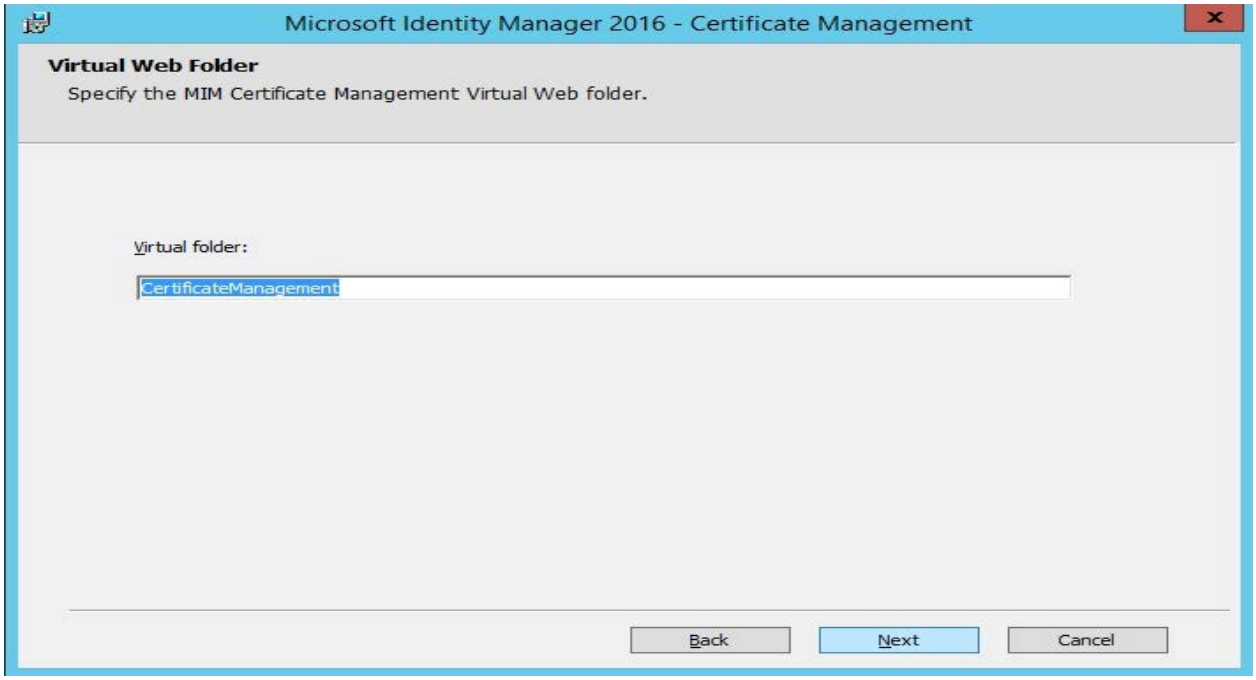
6. On the End-User License Agreement page, read the agreement, select the **I accept the terms in the license agreement** check box, and then click **Next**.



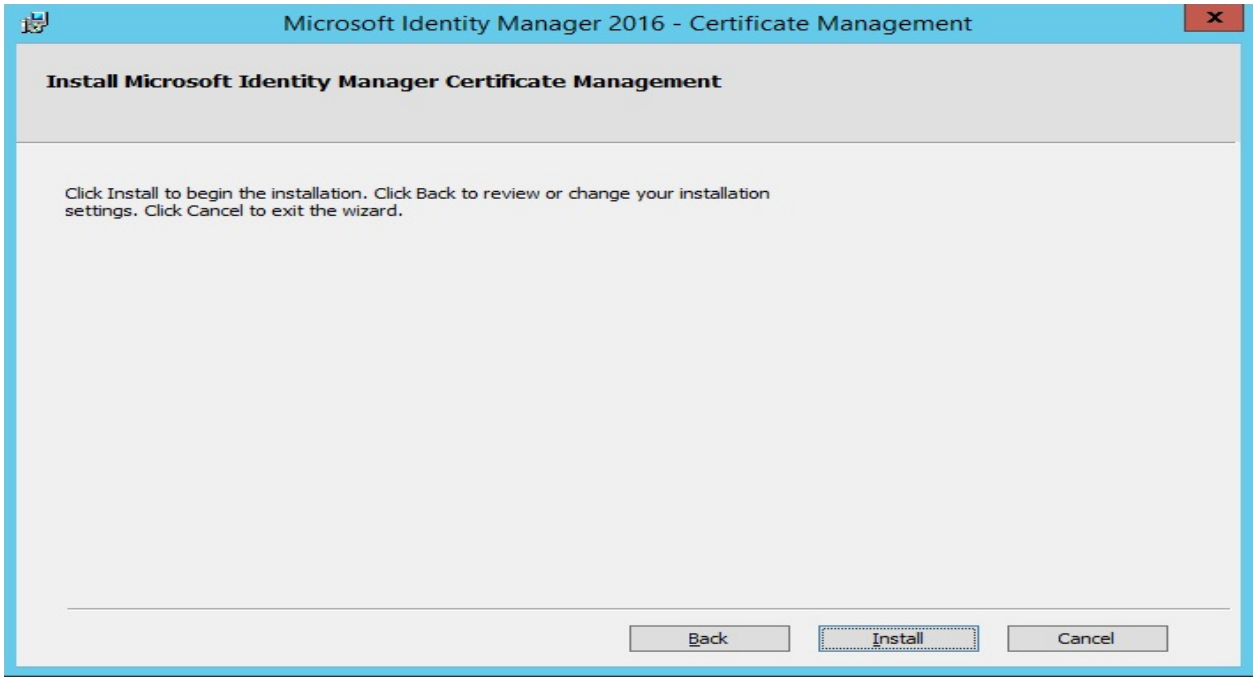
7. On the Custom Setup page, select the MIM CM Portal and MIM CM Update Service components (select MIM CM CA Files only if the CA is also installed on the same server), verify that the install location is: C:\Program Files\Microsoft Forefront Identity Manager\2010\, and then click **Next**.



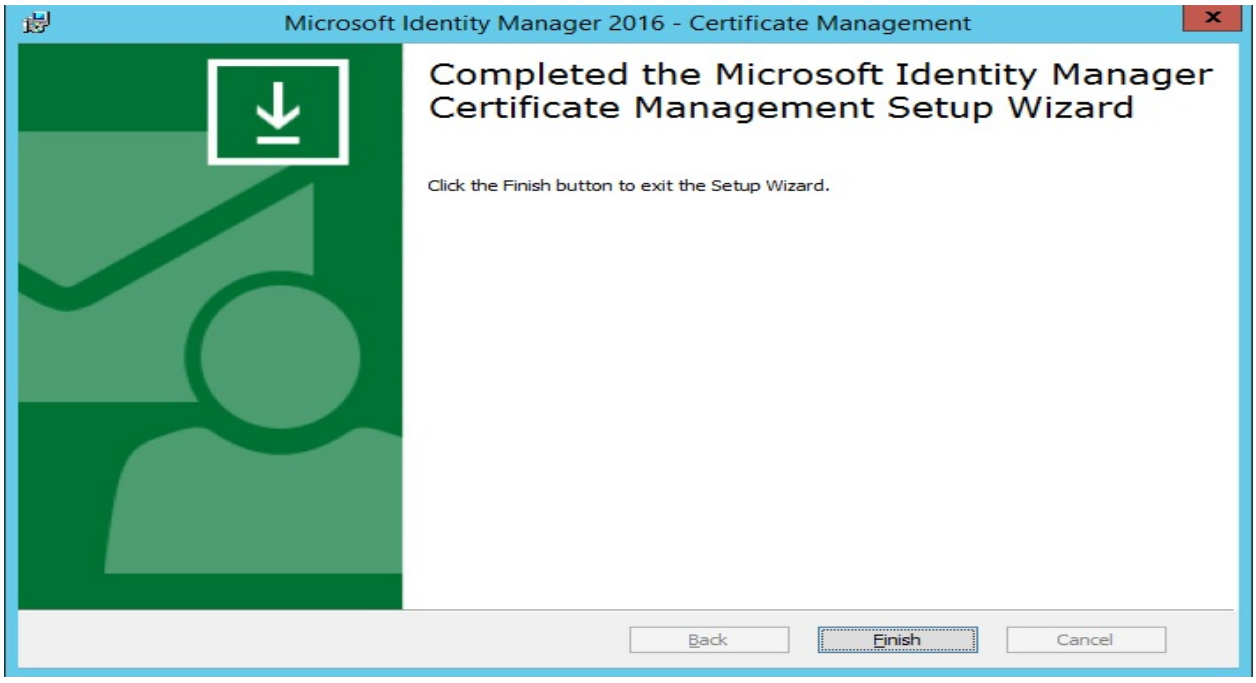
8. On the Virtual Web Folder page, ensure that the Virtual folder name is CertificateManagement, and then click **Next**.



9. On the Install Microsoft Identity Manager Certificate Management page, click **Install**.



10. On the Completed the Microsoft Identity Manager Certificate Management Setup Wizard page, click **Finish**.



Prepare and Publish the Certificate Templates used within the MIM CM

Before enrolling the agent certificates, custom certificate template for each certificate needs to be created. 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

1. Log on to **CORPMIM** as **Contoso\Administrator**.
2. Click **Start**, point to **Administrative tools**, and then click **Certificate Authority**.
3. In **Certification Authority**, expand your CA set of folders and select **Certificate Templates** in the console tree.
4. Right-click **Certificate Templates**, and click **Manage**.
5. In **Certificate Templates**, select **User**.
6. Right-click **User**, and click **Duplicate Template**.
7. On **Compatibility** tab, in **Compatibility Settings**, select **Certificate Authority** as **Windows Server 2003** and **Certificate recipient** as **Windows XP / Server 2003**.
8. Click the **General** tab and type **MIM Signing** in the **Template display name**. Select **Publish certificate in Active Directory** check box.
9. Click the **Request Handling** tab, uncheck the **Allow private key to be exported** option.
10. Click the **Cryptography** tab, select **Requests can use any provider available on subject's computer**.
11. Click the **Subject Name** tab, uncheck the **Include e-mail name in subject name** and **E-mail name** check box.
12. On the **Extensions** tab, in the **Extensions included in this template** list, select **Application Policies** and then click **Edit**.
13. 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**.
14. On the **Security** tab perform the following:
    - Add MIMCMAgent.
    - Assign Read and Enroll permissions to MIMCMAgent.
15. In the Properties of New Template dialog box, click **OK**.

Key Recovery Agent

1. Ensure that the Certificate Templates console is still open.
2. In the Certificate Templates console, in the details pane, right-click **Key Recovery Agent**, and then click **Duplicate Template**.
3. On the **Compatibility** tab, in **Compatibility Settings**, select **Certificate Authority** as **Windows Server 2003** and **Certificate recipient** as **Windows XP / Server 2003**.
4. Click the **General** tab, in the **Template display name** box, type **MIM Key Recovery Agent**, verify that the **Validity Period** is set to 2 years.
5. Select the **Publish certificate in Active Directory** check box.
6. Click the **Cryptography** tab, select **Requests can use any provider available on subject's computer**.

7. On the **Issuance Requirements** tab, uncheck the **CA certificate manager approval** check box.
8. On the **Security** tab perform the following:
   - Add MIMCMKRAgent.
   - Assign Read and Enroll permissions to MIMCMKRAgent.
9. In the Properties of New Template dialog box, click **OK**.

Enrollment Agent

1. Ensure that you are still in the Certificate Templates console.
2. In the Certificate Templates console, in the details pane, right-click **Enrollment Agent**, and then click **Duplicate Template**.
3. On the **Compatibility** tab, in **Compatibility Settings**, select **Certificate Authority** as **Windows Server 2003** and **Certificate recipient** as **Windows XP / Server 2003**.
4. Click the **General** tab, in the **Template display name** box, type **MIM Enrollment Agent**, verify that the **Validity Period** is set to 2 years.
5. Select the **Publish certificate in Active Directory** check box.
6. Click the **Cryptography** tab, select **Requests can use any provider available on subject's computer**.
7. On the **Security** tab, perform the following:
   - Add MIMCMEnrollAgent.
   - Assign Read and Enroll permissions to the MIMCMEnrollAgent account.
8. In the Properties of New Template dialog box, click **OK**.
9. Close the Certificate Template Console.

The Luna CSP is used to generate certificates for these accounts that generates private key of the user's certificate inside the HSM box, and stores it securely inside its hardware. Any subsequent usage of this certificate would require the private key, hence the HSM 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:

1. Click **Start**, point to **Administrative Tools**, and then click **Certificate Authority**.
2. In **Certification Authority**, expand your CA set of folders and select **Certificate Templates** in the console tree.
3. Right-click **Certificate Templates**, point to **New** and click **Certificate Template to Issue**.
4. In the **Enable Certificate Templates** dialog box, select **MIM Signing**, **MIM Enrollment Agent**, and **MIM 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 Agents Account Certificates

When using an HSM, MIM CM Configuration Wizard do not deploy the agent certificates. The certificates must be manually enrolled by each agent account, and the thumbprints of the certificates needs to be recorded in the Web.Config file.

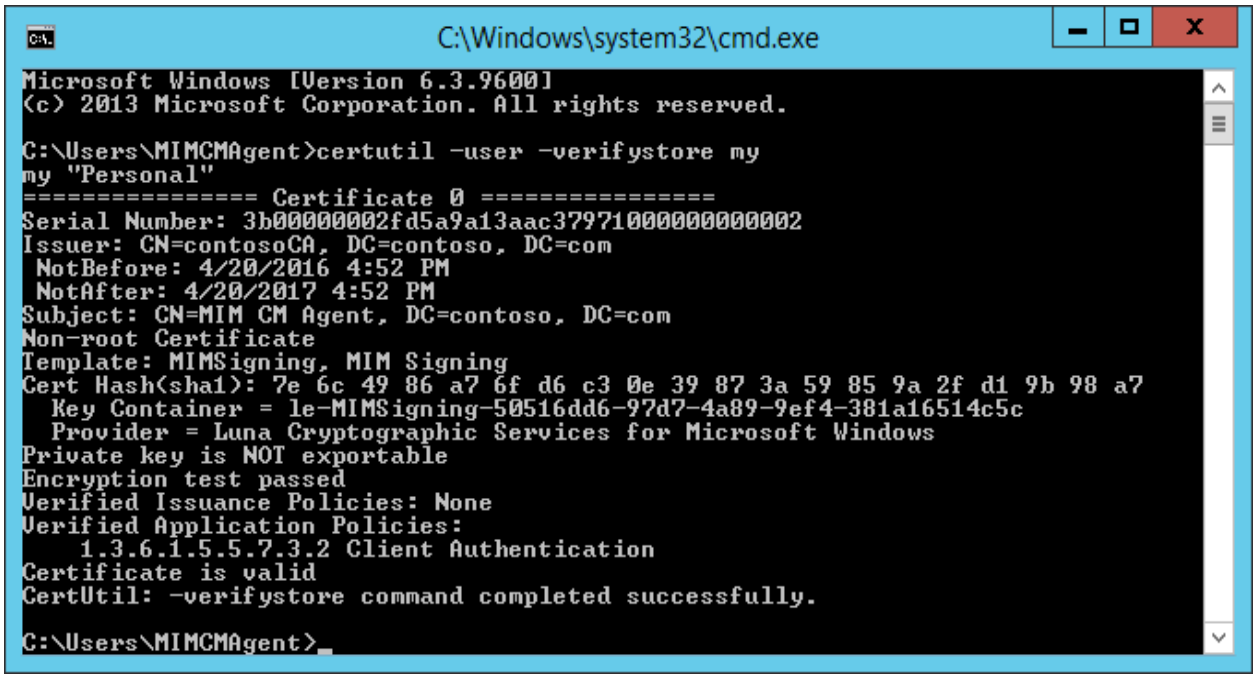
To manually enroll each agent's certificate, provide permission to the agent account to log on locally on the MIM CM server and allow them to request certificates and store the certificates in the agent account's profile on the MIM CM server.

Once the logon is enabled, now log on as each account and enroll the assigned agent certificate.

MIM CM Agent

1. Log on to **CORPMIM** as **CONTOSO\MIMCMAgent**.
2. Right-click on **Start**, select **Run** and type **certmgr.msc**. Press **Enter**.
3. If prompted to provide credentials, provide the credentials of MIM CM Agent.
4. In the console tree, right-click **Personal**, point to **All Tasks**, and then click **Request New Certificate**.
5. On the Before You Begin page, click **Next**.
6. On the Request Certificates page, select the certificate **MIM Signing**, and then click **Details** and then **Properties**.
7. In the Certificate Properties window, click on **Private Key** tab and ensure that only **Luna Cryptographic Services for Microsoft Windows** is selected under **Cryptographic Service Provider**.
8. Click **OK** and then click **Enroll**.
9. On the Certificate Installation Results page, ensure that the status is reported as Succeeded, and then click **Finish**.
10. In the console tree, expand **Personal**, and then click **Certificates**. Double-click the enrolled certificate.
11. On the **Details** tab, in the Field listing, select Thumbprint. Record the thumbprint of the Certificate and remove the spaces.
    - MIMCMAgent: `7e6c4986a76fd6c30e39873a59859a2fd19b98a7`
12. Click **OK**.
13. Close the Certificate Manager console.
14. Open command prompt.
15. At the command prompt, type `certutil -user -verifystore my` and then press **Enter**.

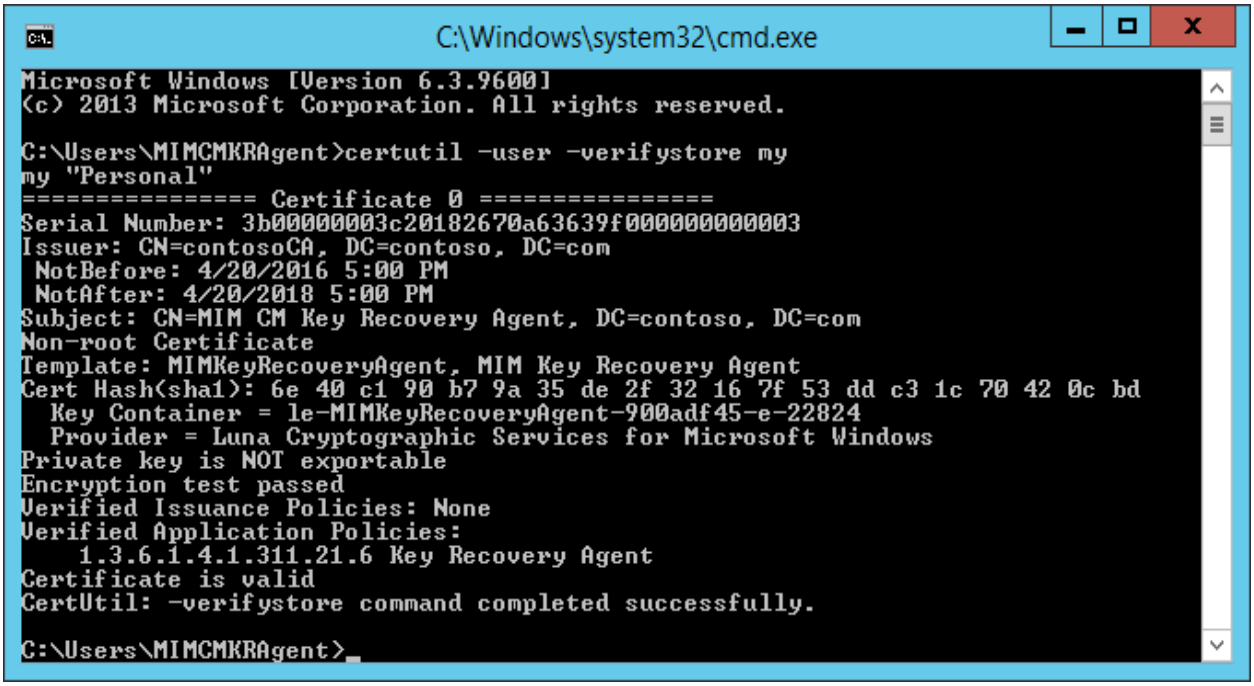
16. Ensure in the output that the Provider is Luna Cryptographic Services for Microsoft Windows and that the Certificate is valid.



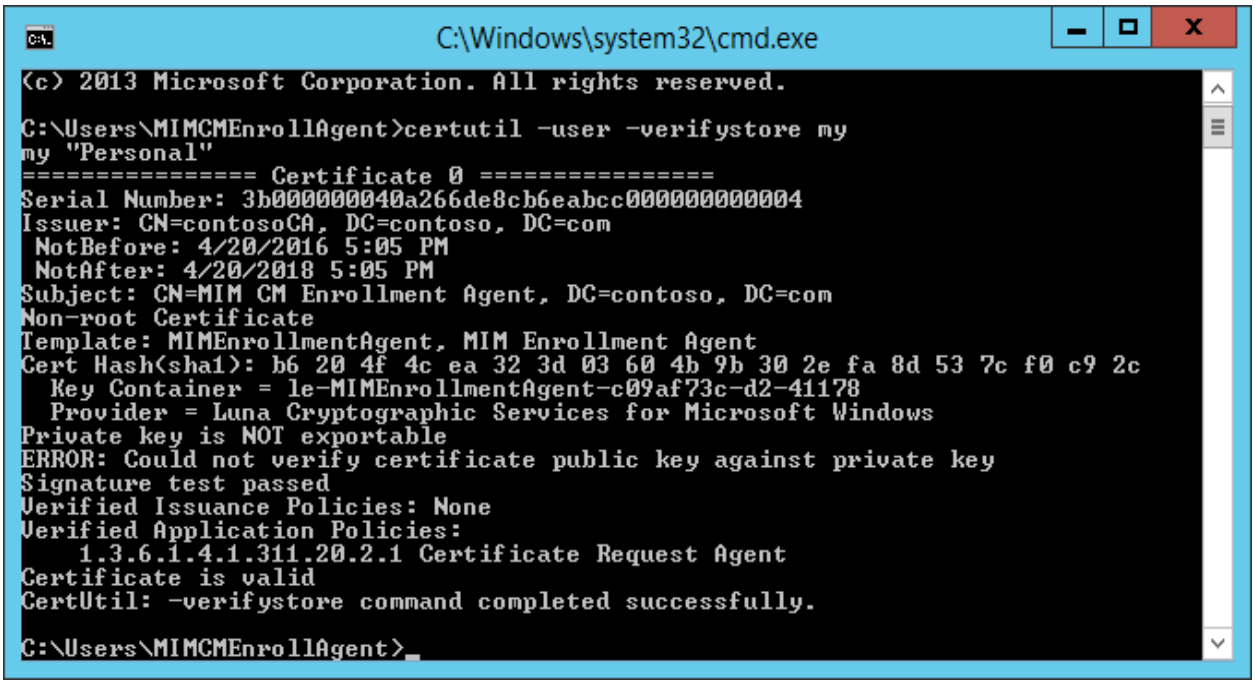
17. Close the command prompt.
18. Close all open windows and log off.

Repeat the above process for other two agent accounts **MIMCMKRAgent** and **MIMCMEnrollAgent** and record the Thumbprint for both Agents certificate.

- MIMCMKRAgent: `6e40c190b79a35de2f32167f53ddc31c70420cbd`



- MIMCMEnrollAgent: `b6204f4cea323d03604b9b302efa8d537cf0c92c`



Ensure that the both certificates are generated using Luna Cryptographic Services for Microsoft Windows and that the Certificate is valid using the certutil command.

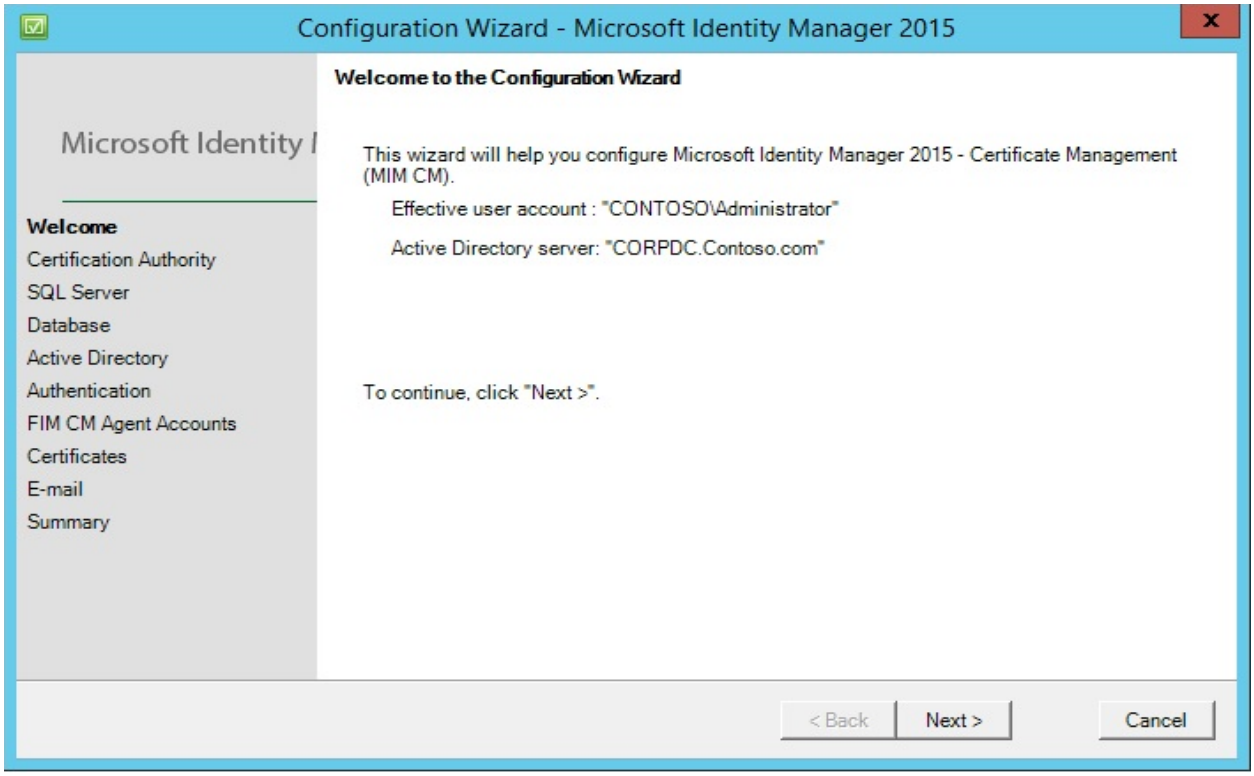
Configure the MIM CM server

Once the CM server is installed and agent certificate enrolled, it's time to configure the CM server with its components. Microsoft recommends running 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.

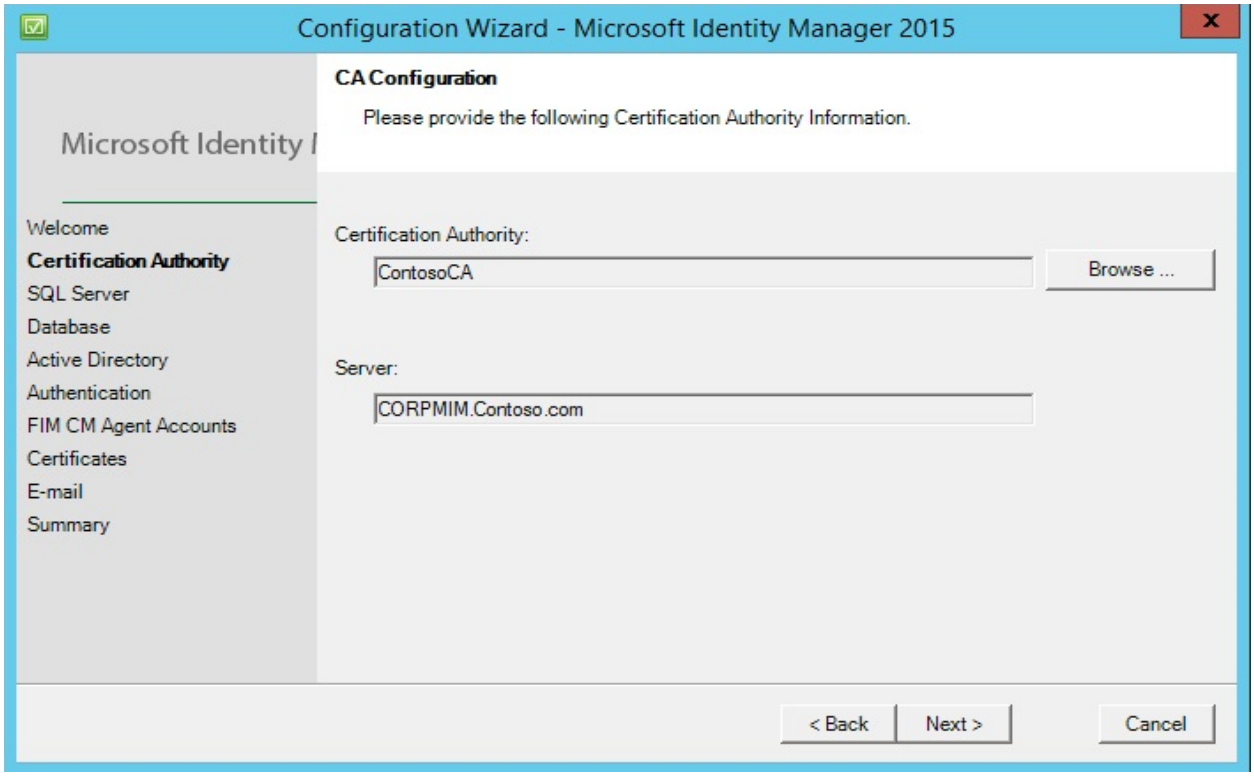
To run the Certificate Management Configuration Wizard, perform the following:

1. Log on to **CORPMIM** as **CONTOSO\Administrator**.
2. Click **Start**, point to Microsoft Identity Manager, and then click Certificate Management Configuration Wizard.

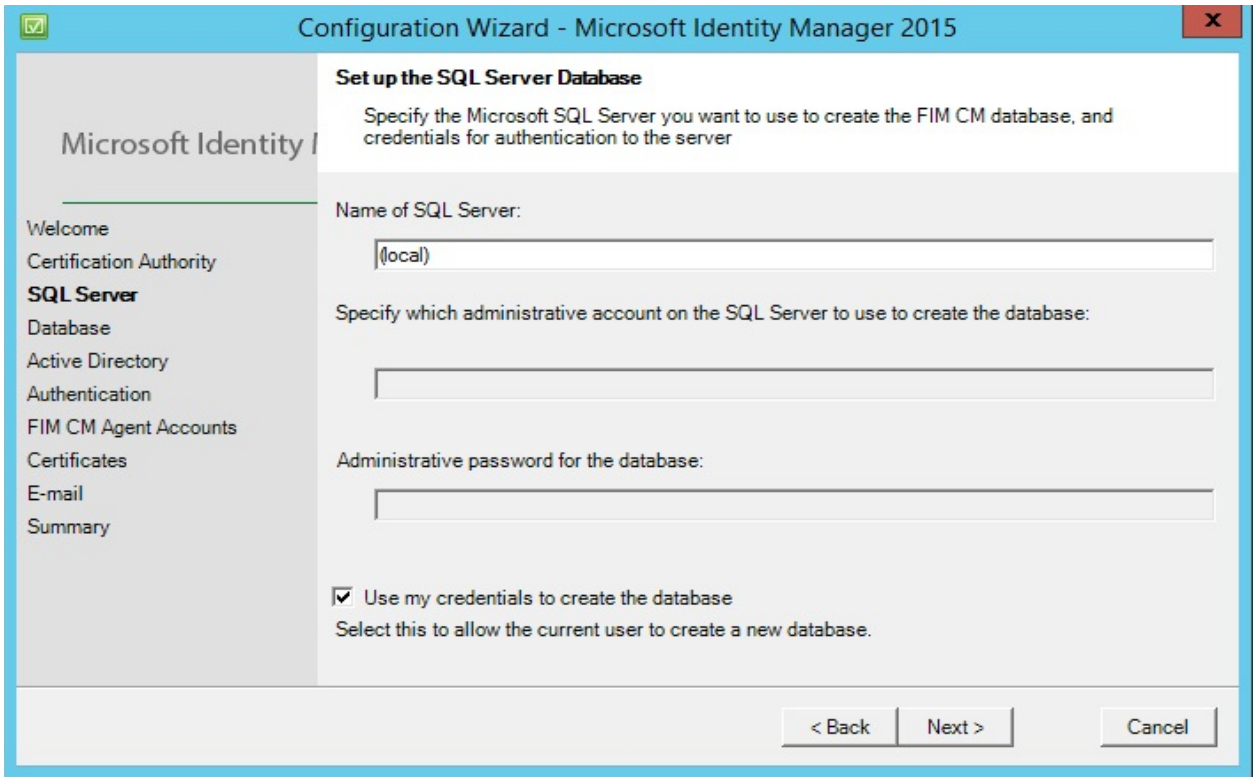
3. On the Welcome to the Configuration Wizard page, click **Next**.



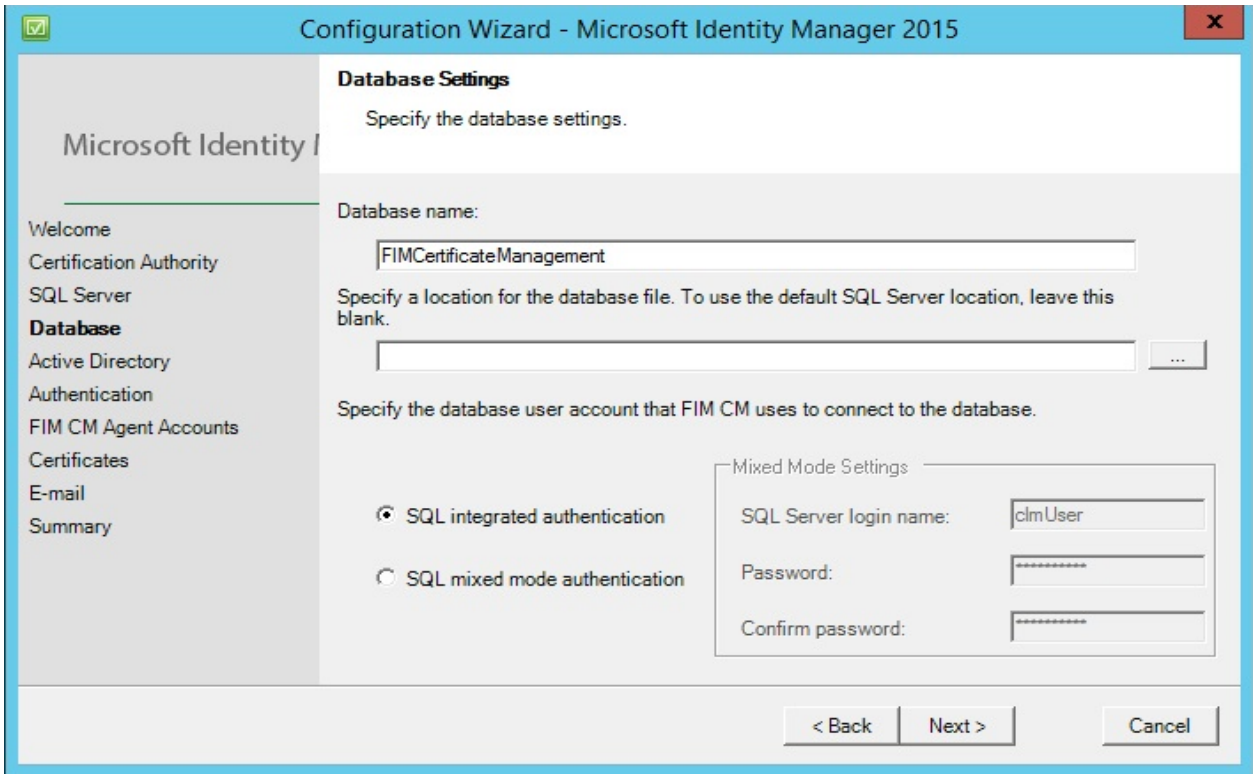
4. On the CA Configuration page, ensure that **Certificate Authority** and **Server** are listed. Click **Next**.



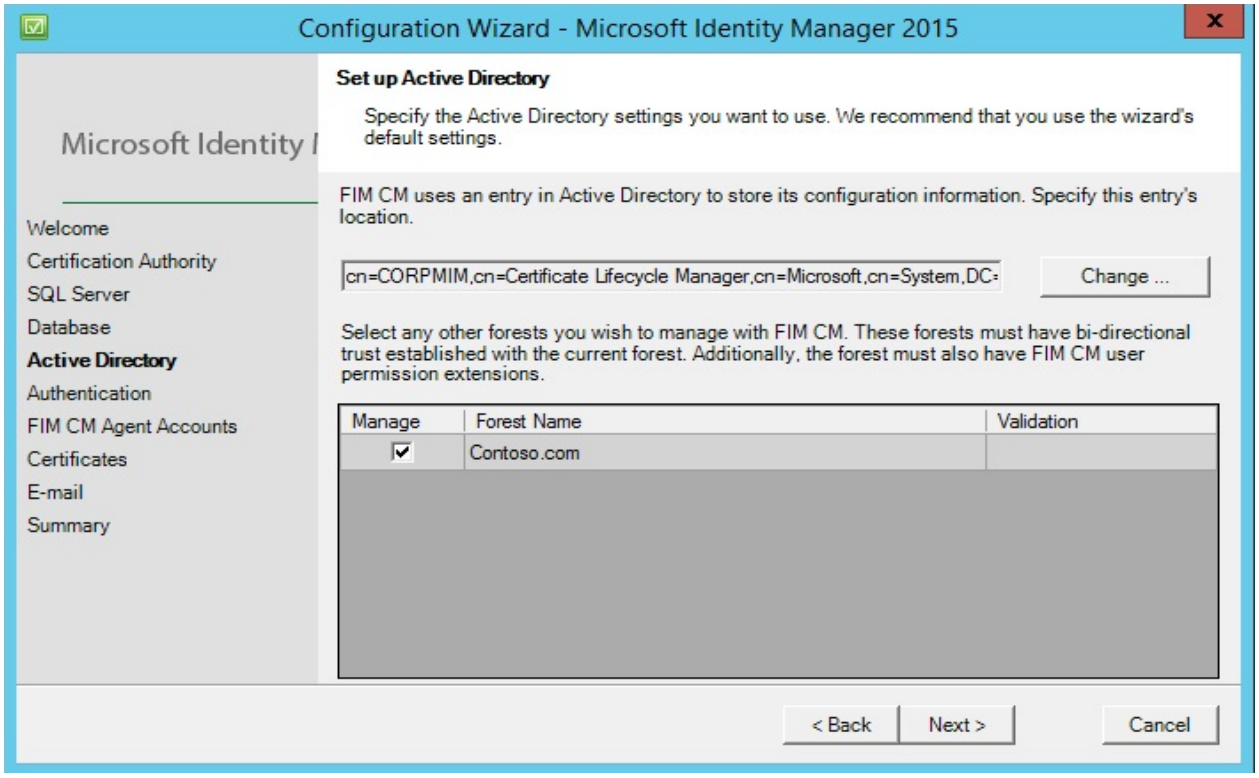
5. On the Set up the SQL Server Database page, **Name of SQL Server** is listed and select the **Use my credentials to create the database** check box. Click **Next**.



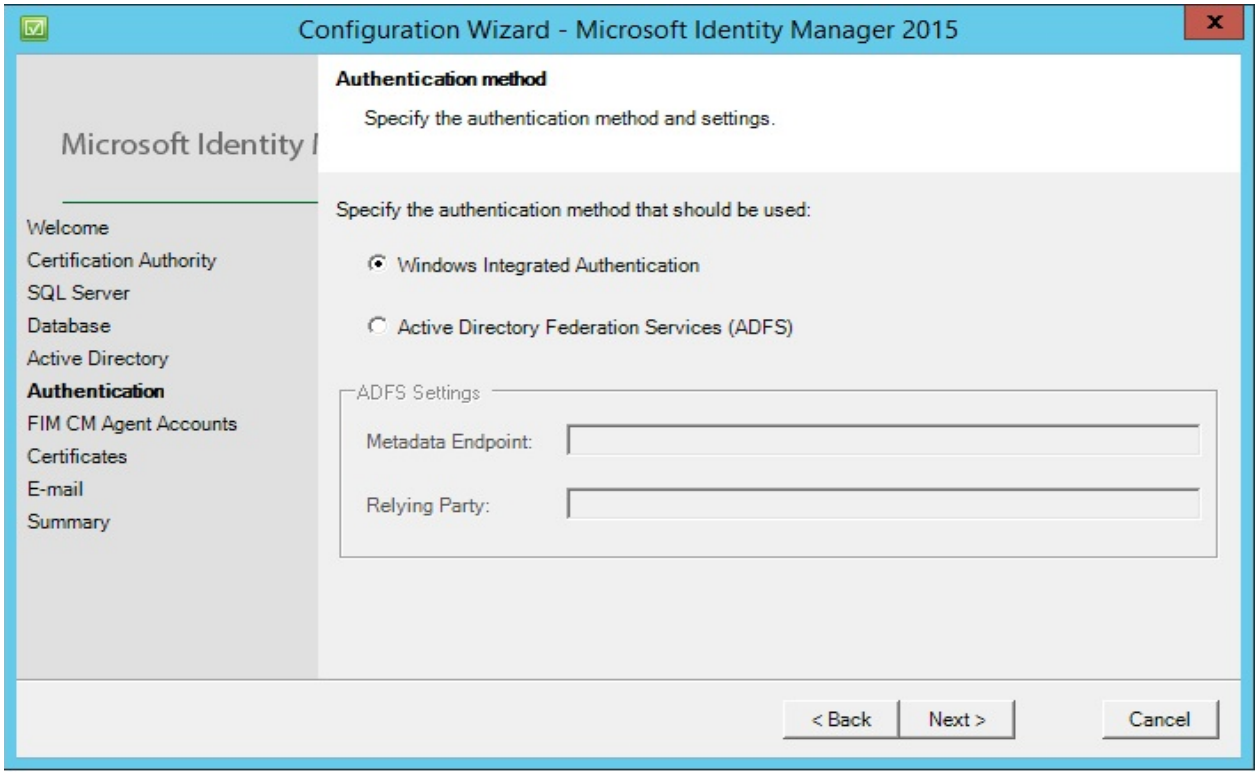
6. On the Database Settings page, ensure **Database name** is listed and select **SQL integrated authentication**.



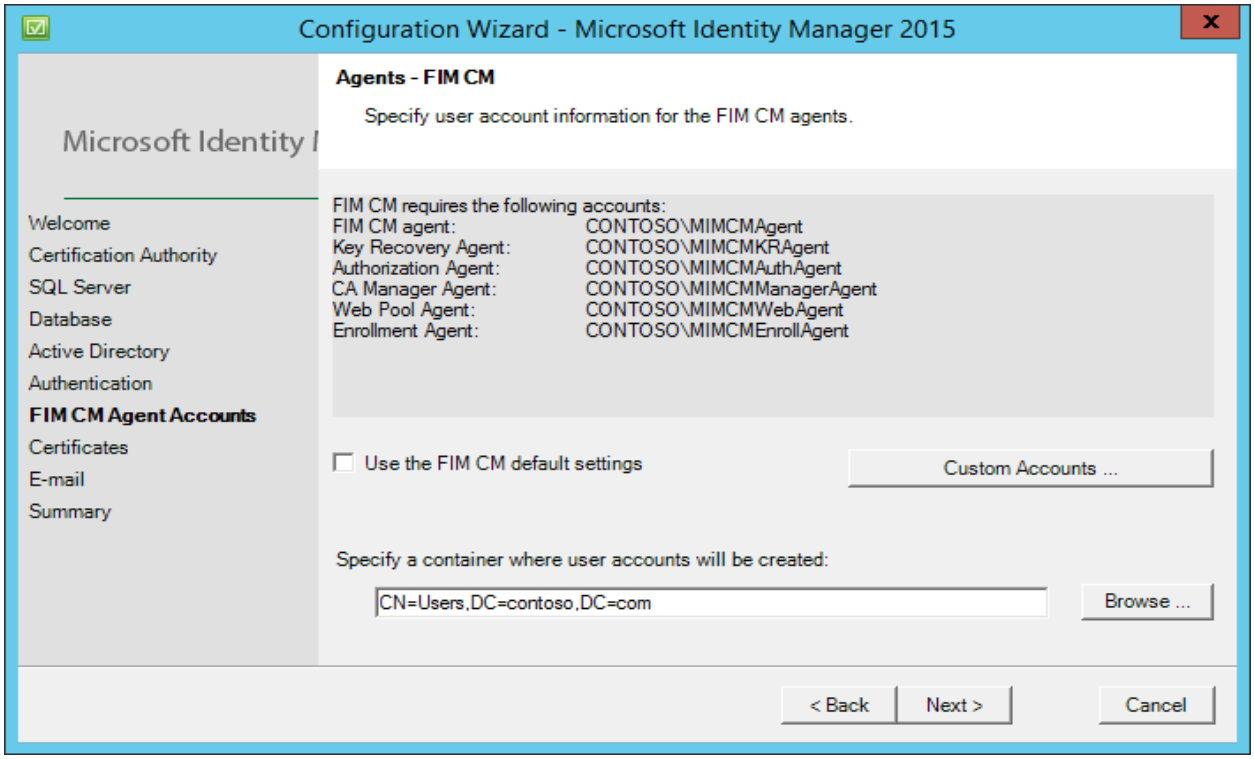
7. On the Set up Active Directory page, use default settings and click **Next**.



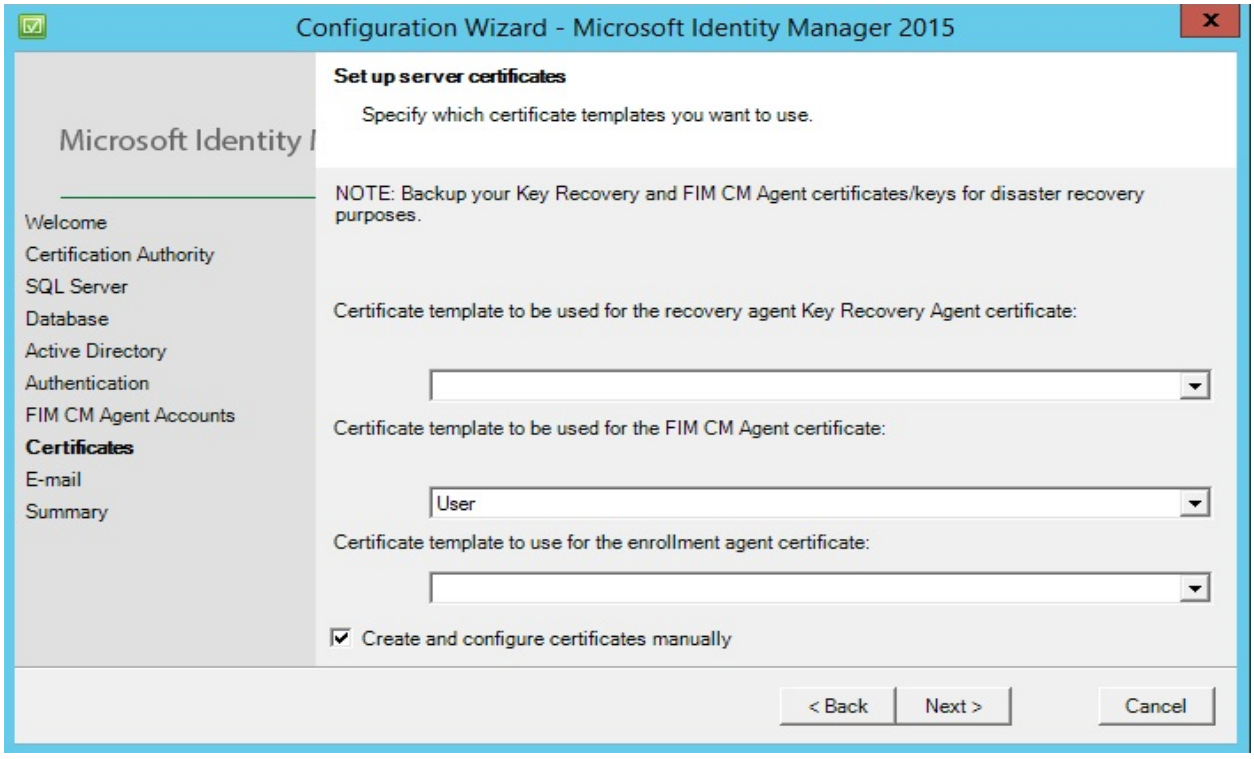
8. On the Authentication method page, select **Windows Integrated Authentication** and click Next.



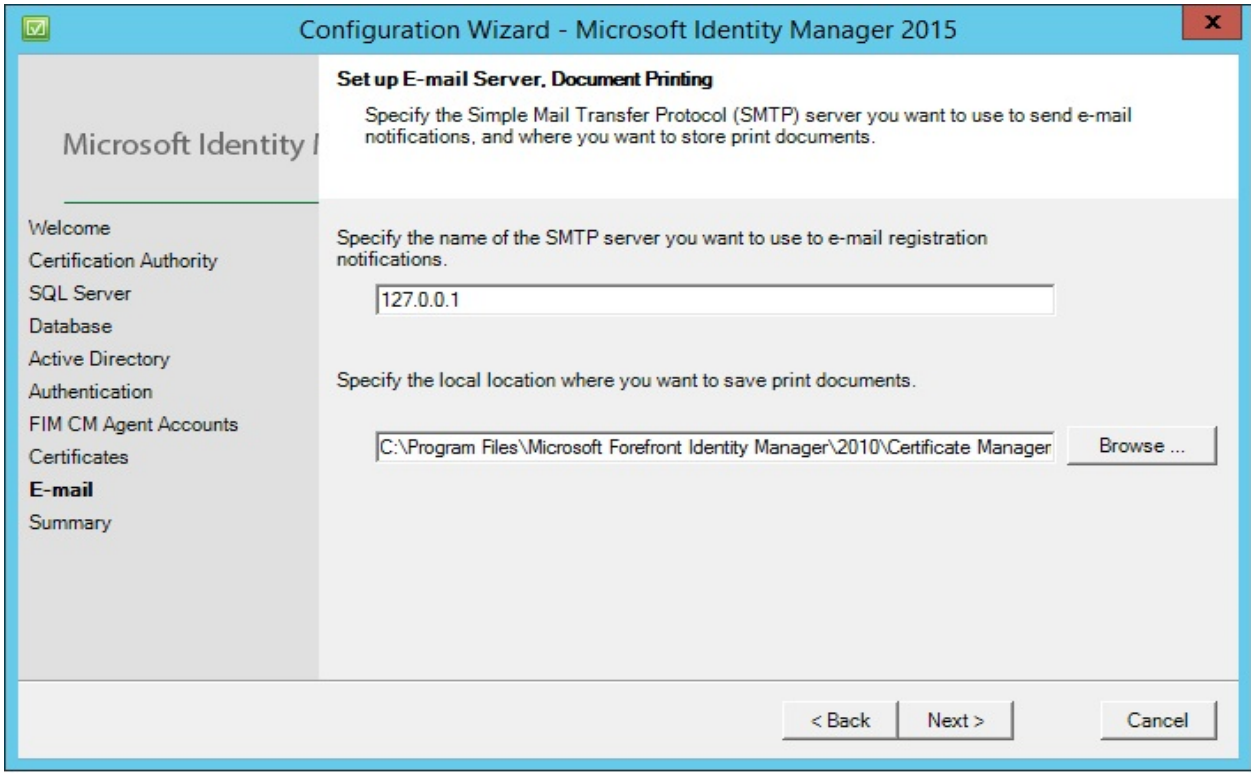
9. On the Agents-FIM CM page, uncheck **Use the FIM CM default settings** check box. Click **Custom Accounts …** a window displays, provide the User name and Password for all six agents that you have created in the beginning. Click **Next**.



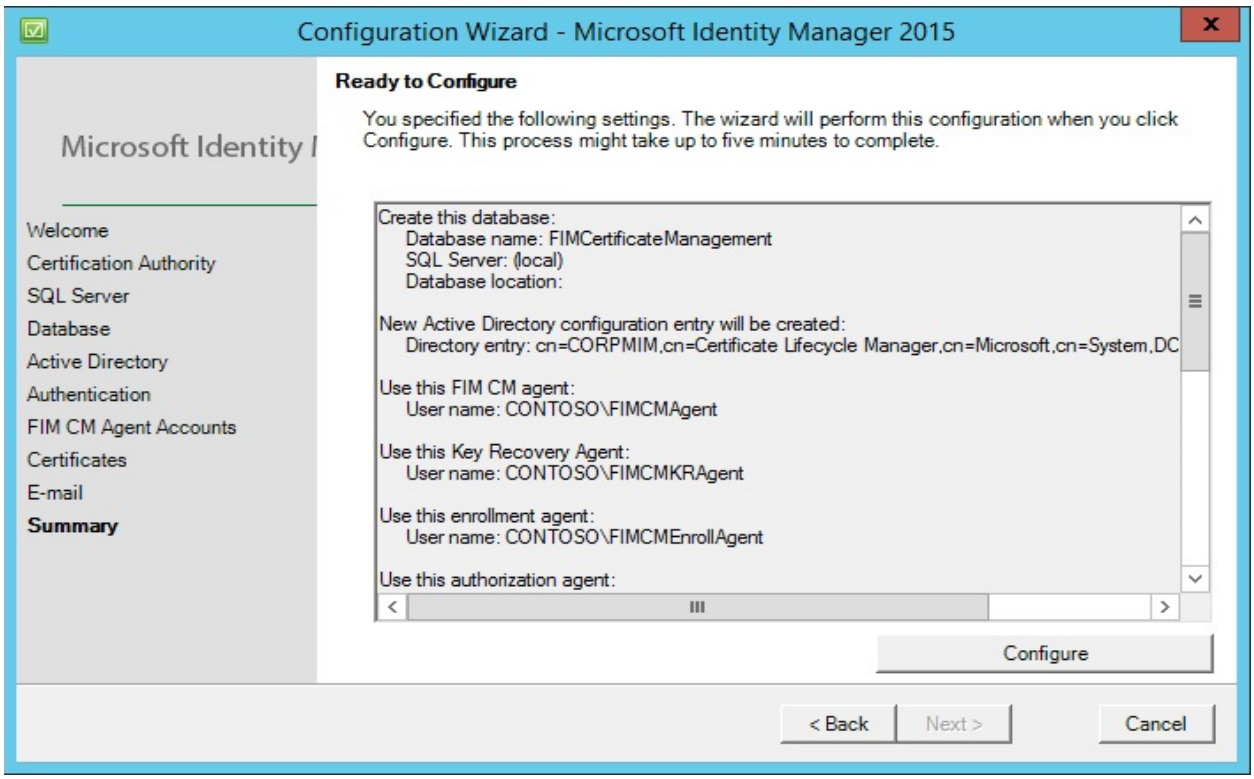
10. On the Setup server certificate page, select the **Create and configure certificate manually** check box. Click **Next**.



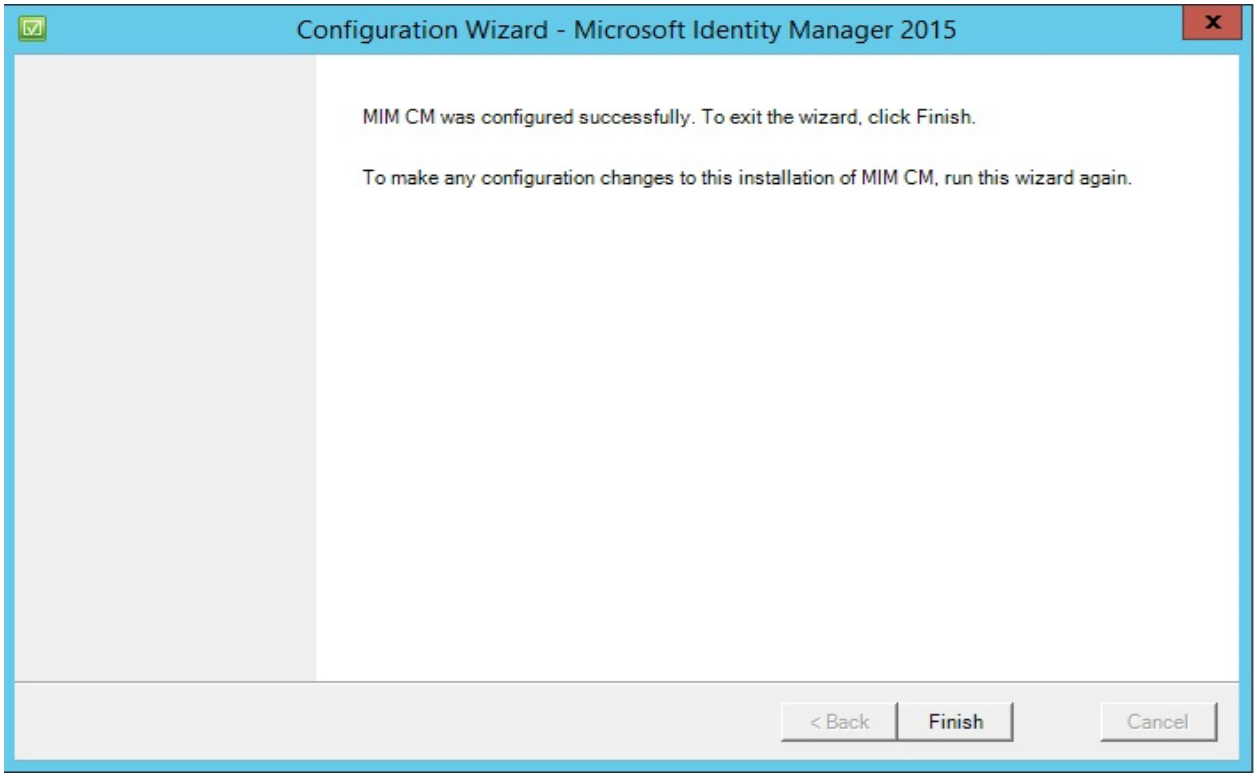
11. On the Set up E-mail Server, Document Printing page, use default settings and click **Next**.



12. On the Ready to Configure page, review the settings and click **Configure**. A warning message to configure the SSL on IIS directory displays. Click **OK** to acknowledge that SSL is not enabled on the IIS virtual directory.



13. Click **Finish** when configuration completes successfully.



Designating the pre-enrolled MIM CM agent certificates

Now Web.config file needs to modify to record the thumbprints of MIM CM Agent and MIM CM Enrollment Agent certificate and MIM CM Key Recovery Agent certificate needs to be configured in the certificate authority.

The certificate thumbprints are referenced in four different lines in the Web.config file: one for the CM Enrollment Agent and three for the CM Agent. Web.config file must be modified to register these thumbprints.

1. Open C:\Program Files\Microsoft Forefront Identity Manager\2010\Certificate Management\Web in Windows Explorer.
2. Open the Web.config file in Notepad.
3. In Notepad, from the **Edit** menu, click **Find**.
4. In the **Find** dialog box, in the **Find what** box, type **Clm.EnrollAgent.Certificate**, and then click **Find Next**.
5. Modify the line so that the thumbprint from the MIM CM Enrollment Agent certificate is referenced in the following line (removing the spaces from the thumbprint value):

   <add key="Clm.EnrollAgent.Certificate.Hash" value=“ b6204f4cea323d03604b9b302efa8d537cf0c92c" />

   NOTE: Value will be thumbprint of your MIMCMEnrollAgent certificate.

6. Press **Control-Home** to return to the beginning of the file.
7. In Notepad, from the **Edit** menu, click **Find**.
8. In the **Find** dialog box, in the **Find what** box, type **Clm.SigningCertificate.Hash**, and then click **Find Next**.

9. Modify the line so that the thumbprint from the MIM CM Agent certificate is referenced in the following line (removing the spaces from the thumbprint value):

   <add key="Clm.SigningCertificate.Hash" value="7e6c4986a76fd6c30e39873a59859a2fd19b98a7" />

   NOTE: Value will be thumbprint of your MIMCMAgent certificate.

10. Press **Control-Home** to return to the beginning of the file.
11. In Notepad, from the **Edit** menu, click **Find**.
12. In the **Find** dialog box, in the **Find what** box, type **Clm.ValidSigningCertificates.Hashes**, and then click **Find Next**.
13. Modify the line so that the thumbprint from the MIM CM Agent certificate is referenced in the following line (removing the spaces from the thumbprint value):

    <add key="Clm.ValidSigningCertificates.Hashes" value="7e6c4986a76fd6c30e39873a59859a2fd19b98a7" />

    NOTE: Value will be thumbprint of your MIMCMAgent certificate.

14. Press **Control-Home** to return to the beginning of the file.
15. In Notepad, from the **Edit** menu, click **Find**.
16. In the **Find** dialog box, in the **Find what** box, type **Clm.SmartCard.ExchangeCertificate.Hash**, and then click **Find Next**.
17. Modify the line so that the thumbprint from the clmAgent certificate is referenced in the following line (removing the spaces from the thumbprint value):

<add key="Clm.SmartCard.ExchangeCertificate.Hash" value="7e6c4986a76fd6c30e39873a59859a2fd19b98a7" />

   NOTE: Value will be thumbprint of your MIMCMAgent certificate.

18. Press **Control-Home** to return to the beginning of the file.
19. In Notepad, from the **Edit** menu, click **Find**.
20. 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="TripleDes" />

21. Close the Web.config file, saving all changes.
22. Click **Start**, point to **Administrative Tools**, and then click **Certificate Authority**.
23. Right-click on the CA name and click **Properties**.
24. On the **Recovery Agents** tab, select **Archive the key**.
25. Click **Add**… and select MIM CM Key Recovery Agent certificate that you enrolled. Click **OK**.
26. Click **Apply**, and then click **Yes** when prompt for Certificate Services Restart.
27. When Certificate Services restarts, click **OK** to close the properties window.

28. Close the Certificate Authority console.

Enabling SSL on the MIM CM Website

When enabling SSL on the MIM CM web portal, ensure that the DNS name used to access the MIM CM web portal is registered as a service principal name (SPN) for the MIM CM Web Pool Agent account. For integrated authentication to work, the MIM CM Web Pool Agent 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 MIM CM web portal, the connection attempt will fail.

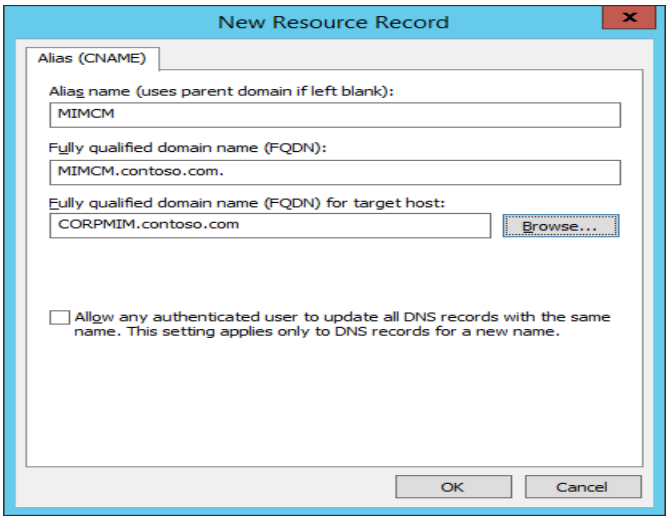
Verifying and changing the SPN when users connect to a website, they typically use a CNAME record in DNS, rather than the actual machine name. For example, if the machine name is CORPMIM.contoso.com, it may prefer that the users connect to MIMCM.contoso.com.

To set up MIM CM to allow connections to MIMCM.contoso.com requires:

- Set up any DNS CNAME records.
- Register the MIMCM.contoso.com SPN with the MIMCMWebAgent account.

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

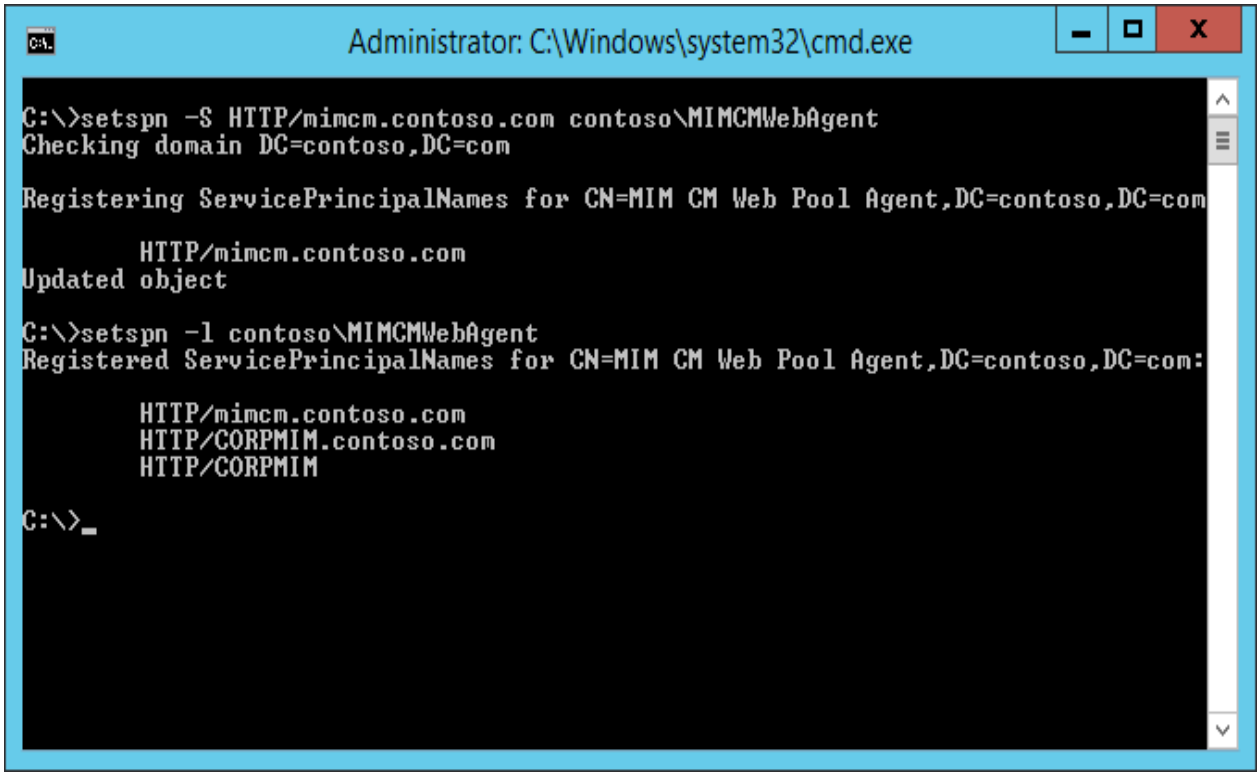
1. Log on to a domain controller (CORPDC) as a user (CONTOSO\Administrator) who can modify DNS entries.
2. Click **Start**, point to **Administrative Tools**, and then click **DNS.**
3. In the console tree, expand **CORPDC.contoso.com**, expand **Forward Lookup Zones**, and then click **contoso.com**.
4. Right-click **contoso.com**, and then click **New Alias (CNAME)…**.
5. In the **Alias name** box, type **MIMCM**, and then click **Browse**.
6. In the **Browse** dialog box, navigate to the A record for the MIM CM server, and then click **OK**.



7. Ensure that the new CNAME record exists in the details pane.
8. Close the DNS Manager console.

   Once the CNAME is registered, CNAME must be added to the MIM CM WebPool's SPN listing.
9. Open an Administrative command prompt.

10. At the command prompt, type "`setspn -S HTTP/mimcm.contoso.com contoso\MIMCMWebAgent`" and then press **Enter**.
11. At the command prompt, type "`setspn -l contoso\MIMCMWebAgent`" and then press **Enter**.
12. Ensure that the new SPN is included in the list of SPNs and there is no typographical error.



13. Close the command prompt.

Configuring SSL

After SPN is registered with the MIMCMWebAgent account, log on to the MIM CM server to request an SSL certificate for the MIM CM web portal. Once you have requested the web server certificate, you must bind the certificate to a website.

> **NOTE:** Refer the SafeNet Microsoft IIS Integration Guide for requesting the certificate and binding it to the Default website.

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

1. Open the Internet Information Services (IIS) Manager console.
2. In the console tree, expand Server Name, expand **Sites**, expand **Default Web Site**, and then click **CertificateManagement**.
3. On the /CertificateManagment Home page, in the IIS section, double-click **SSL Settings**.
4. On the SSL Settings page, enable the **Require 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 MIM CM with IIS, kernel-mode authentication should be disabled. To disable kernel-mode authentication, perform the following steps:

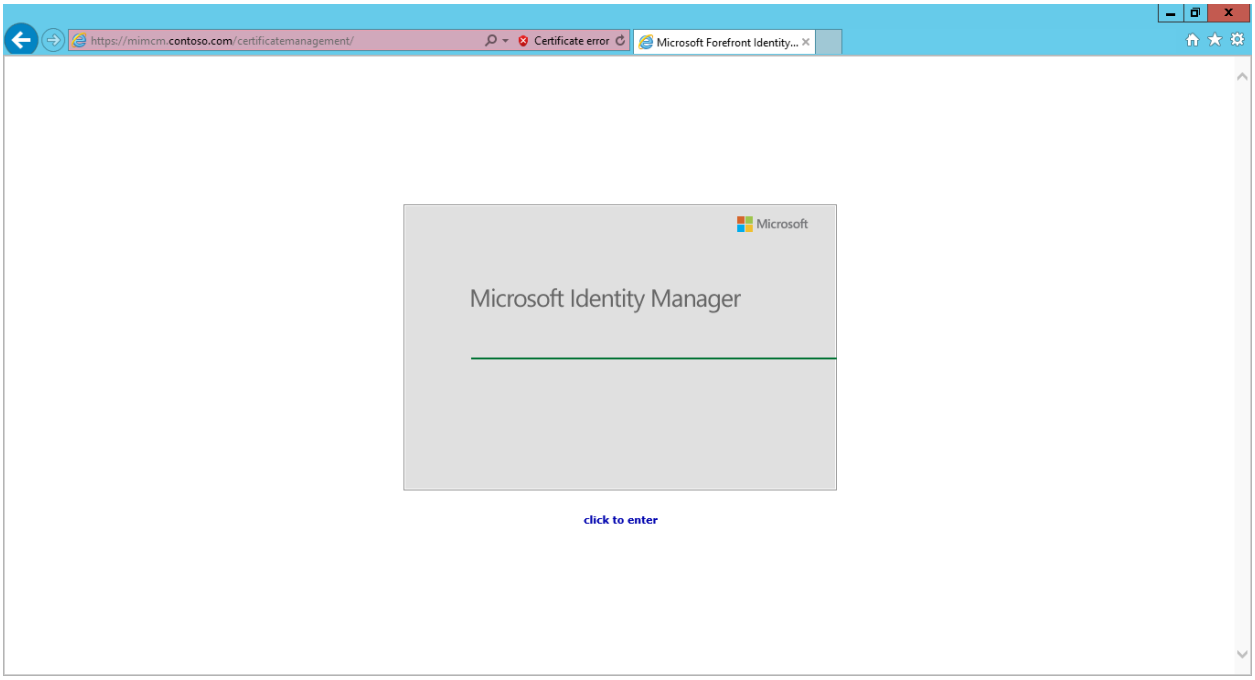
1. Log on to the **CORPMIM** as the **CONTOSO\Administrator**.
2. Click **Start**, point to **Administrative Tools**, and open the **Internet Information Services Manager**.
3. In the console tree, expand **Sites**, expand **Default Web Site**, and then click **CertificateManagement**.
4. In the center pane, scroll down and double-click **Authentication**.
5. Right-click **Windows Authentication**, and then click **Advanced Settings**.
6. Clear the **Enable Kernel-mode authentication** check box.
7. Click **OK**.
8. Close Internet Information Services Manager.

Connecting to the MIM CM web portal

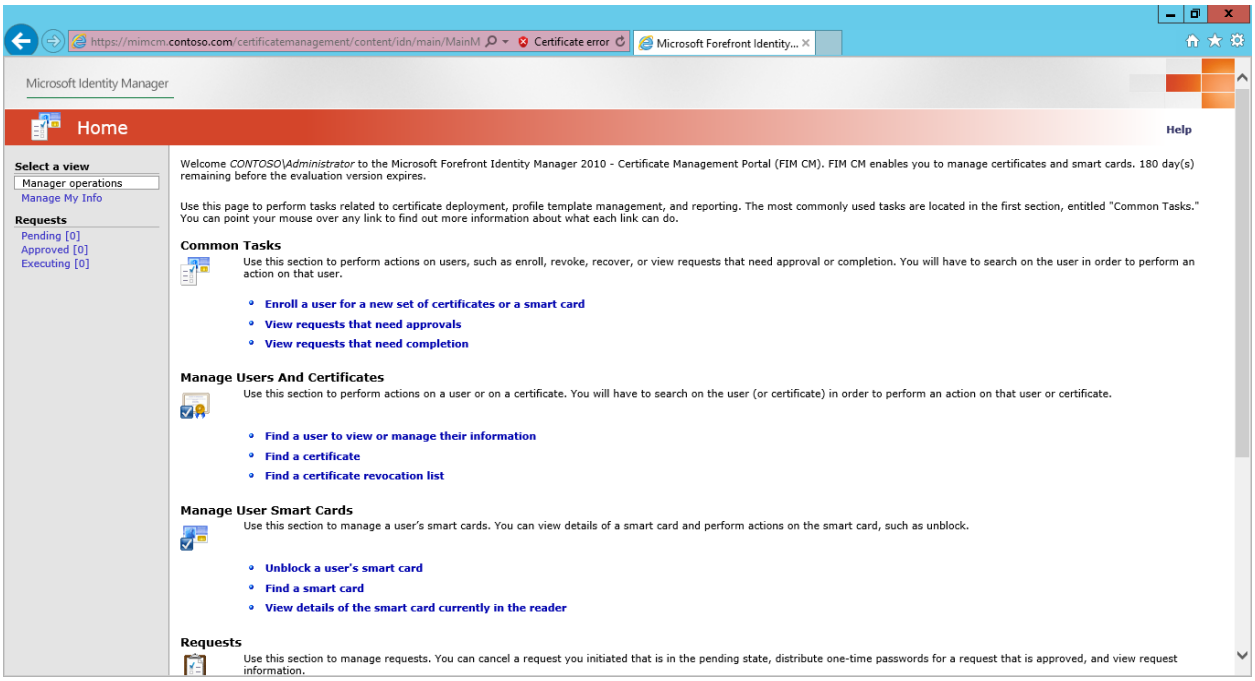
Once the MIM CM web portal configuration is completed, use Internet Explorer to connect to the website. Before connecting, ensure the following:

- The website must be added to the Trusted Sites security zone in Internet Explorer.
- 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 done, connect to the website using the URL https://mimcm.contoso.com/certificatemanagement.



Click on the link to enter the website.



The integration of Microsoft Identity Manager 2016 is completed successfully. Now MIM CM only issues certificates to the users as long as the private keys of MIMCMAgent, MIMCMEnrollAgent, and MIMCMKRAgent certificates are available from within the HSM. In another words, the protection and security of the private keys of these Agents used for certificate issuance, enrolment and key recovery purposes is ensured.