

CertifyID TrustCentre™ ILM 2007 Edition Integration Guide

*Microsoft Identity Lifecycle Manager 2007 / Certificate Life Cycle Manager (CLM)
WIS@key CertifyID TrustCentre™ (BlackBox™)
WIS@key Smartcards & USB Tokens*

Date: August 2007
Version: 0.1.0
Authors: WIS@key SA

TABLE OF CONTENTS

About this Manual	1
<i>About Microsoft Certificate Lifecycle Manager 2007</i>	<i>1</i>
<i>About WISEKey CertifyID TrustCentre (BlackBox)</i>	<i>2</i>
<i>About WISEKey Smartcards and USB Tokens</i>	<i>3</i>
<i>Copyright.....</i>	<i>6</i>
<i>Target Audience.....</i>	<i>7</i>
<i>Document Conventions.....</i>	<i>7</i>
<i>Terminologies Used in the Document.....</i>	<i>8</i>
<i>Requirements.....</i>	<i>9</i>
Hardware Requirements	9
Software Requirements.....	9
Installation Process	10
<i>Typical Deployment.....</i>	<i>10</i>
<i>Pre-requisite Tasks for Installing CLM.....</i>	<i>10</i>
Installing WISEKey CertifyID BlackBox™ & Certificate Services.....	10
Installing Internet Information Services on CLM Server	11
Installing .NET Framework 2.0.....	11
Installing MS-SQL Server 2005	11
Modifying The Active Directory Schema	11
Enabling The Default KeyRecoveryAgent Certificate Template	11
Enabling The Default EnrollmentAgent Certificate Template	12
<i>Installing CLM on Server.....</i>	<i>12</i>
Installing CLM and CA on same server	12
Installing CLM Website on Server separate from the CA	15
<i>Configuring CLM Using Configuration Wizard</i>	<i>15</i>
Running Configuration Wizard	16
<i>Configuring the CA for CLM.....</i>	<i>22</i>
Configuring Exit Module	22
Configuring Policy Module	23
<i>Creating Users in Active Directory and giving Access Permissions</i>	<i>25</i>
<i>Creating and Configuring CLM Profile Template</i>	<i>25</i>
Creating Profile Template	25
Configuring Profile Templates.....	26
Configuring the Enroll Policy	31
<i>Requesting Web Server Certificates through CLM Website.....</i>	<i>32</i>
<i>Requesting Smart Card Certificates through CLM Website</i>	<i>33</i>
Installing CLM client	33
Enrolling for a Smart Card Certificate	34

Executing the Smart Card Certificate Request 35

Troubleshooting..... 38

CertifyID TrustCentre (CertifyID BlackBox)..... 38

Troubleshooting Microsoft CLM 2007..... 38

Troubleshooting WISEKey Smart Cards, Readers, USB Tokens..... 38

About this Manual

This manual describes the installation and integration of Microsoft Certificate Lifecycle Manager 2007 (CLM) with a WISEKey CertifyID Standard or Advanced CA.

Please see the separate CertifyID TrustCentre (BlackBox) User Guide for guidance on installing that product.

About Microsoft Certificate Lifecycle Manager 2007

Microsoft Certificate Lifecycle Manager 2007 (herein referred in this document as MS-CLM or CLM) is a policy and workflow driven solution that helps organizations manage the lifecycle of digital certificates and smart cards.

MS CLM is part of a Microsoft Identity Lifecycle Manager 2007.

CLM lowers the costs associated with digital certificates and smart cards by enabling organizations to more efficiently deploy, manage, and maintain a certificate-based infrastructure. CLM streamlines the provisioning, deprovisioning, configuration, and auditing of digital certificates and smart cards, while increasing security through strong, multi-factor authentication technology.

Increasingly, organizations are realizing that traditional username and password solutions are no longer sufficient to secure access control for business assets and sensitive data. In response to this need, technology firms are offering sophisticated authentication solutions such as smart cards with digital certificates. IT administrators need a centralized point of management for these certificates that is easy to deploy and maintain.

CLM is designed based on the principle that every organization is unique, and therefore has unique security and management requirements. Using CLM, both digital certificates and smart cards can be managed as part of the same system—including requirements for smart card logon, signed e-mail, VPN and other requirements. This functionality includes inventory management, card enrollment, recovery, revocation, unblocking, and other features required for successful deployment. CLM simplifies the administrative processes required to convey trust, and ensures distribution in a more secure and structured manner. The result is a highly configurable and robust solution that provides easy deployment, improved manageability, and increased flexibility.

The CLM server acts as administrative proxy to the CAs and provides a Web-based user interface. CLM 2007 is integrated with Active Directory and Active Directory Certificate Services. CLM stores profile template configuration information in Active Directory. CLM stores workflow and audit information in a SQL Server database known as the CLM database that is accessed by the CLM server and the CA modules.

The features of CLM are:

- Delegated request and approval engine for distributed environments
- Face-to-face and self-service management capabilities
- Tight integration with Active Directory and the Windows Server 2003 Certificate Services
- Easy-to-use Web interface
- Policy support for workflow and registration data collection

- Smart card initialization features at a user's desktop
- Complete personal identification number (PIN) management features for resetting and unblocking PINs that can be managed in a self-serve manner or by an administrative user
- Reporting and the ability to audit all smart card lifecycle activities
- Card inventory system that updates on activation of the card

CLM Beta 2 supports the following smart card middleware:

- Axalto version 5.x
- AET SafeSign Standard 2.1.8
- Siemens HiPath Scurity Card API V3.1
- Gemplus GemSafe 4.2
- Aladdin RTE 3.65

This document explains the procedure of integrating WISEKey CertifyID Black Box Certificate Services with Microsoft Certificate Life Cycle Manager.

About WISEKey CertifyID TrustCentre (BlackBox)

The WISEKey CertifyID TrustCentre™ (CertifyID Blackbox™) is a unique product offering a complete and affordable out-of-the box solution for establishing a Trusted Identity Infrastructure dedicated to your organisation.

The CertifyID TrustCentre™ enables easy and effective digital certificate and identity management within your organisation by extending the organisation's PKI and enabling the issuance of S/MIME and SSL certificates chained to WISEKey's pre-distributed root certificate. WISEKey's certificate is present in the majority of web browsers worldwide, and is available in most popular operating systems, servers, and email clients.

Across many sectors and countries, an increasing amount of organisations are installing their own Certification Authorities (CA) or Certificate Service Providers (CSP). The majority of such CAs are not trusted (or recognised) by the the most popular Internet browsers such as Mozilla Firefox, Internet Explorer or email clients such as Thunderbird, or Microsoft Outlook.

Users thus receive warnings that the organisation's signed email, and websites are not trusted. This creates a huge problem for the organisation, as it results in damage to their reputation, loss of confidence and trust in that organisation by the user. It would be practically impossible for each such organisation to meet the needs and requirements that are necessary to embed their Roots in those applications. However there is no need for organisations to undertake this expensive exercise and burden, WISEKey developed the CertifyID Trust Service, delivered in the cost-effective CertifyID TrustCenter to address the need of such organisations.

The Root CA of such an organisation can be very simply chained under the OISTE WISEKey embedded Root Certificate. Organisations thus benefit from:

Global Trust Recognition & Acceptance

The OISTE WISEKey Root is a globally accepted Root Certification Authority, and thus permits all other Certification Authorities that subscribe to the CertifyID Trust Service, and are chained under it, to benefit from its presence and acceptance in the

majority of Internet browsers and operating systems. Thus all the certificates of the organisation's certification authority become recognised and trusted internationally, ensuring the global use and acceptance of their certificates across business sectors, and geographies.

Global Interoperability and Neutrality

The International Organisation for Secure Electronic Transactions (ISETO/OISTE) is a Swiss based not-for-profit organisation that owns the OISTE WISEKey Global Root certification authority.

OISTE appoints WISEKey as the private operator responsible for managing this Root Certification Authority on behalf of the OISTE organisation. WISEKey created the CertifyID Trust Service as a commercial offering linking organisations to the OISTE Root through a certificate signing service.

Customers of the CertifyID Trust Service can request representation at the OISTE organisation to have complete oversight of the Root certification practices and operations, and participate in the OISTE Geneva Security Forum and other events.

OISTE ensures Swiss neutrality, and multipartite responsibility – CertifyID TrustCentre customers can thus have transparency and participate in the Root process.

Privacy and Independence

The Organisation remains in complete sovereign control of their certification authority.

Independent Management

Management of the certificate lifecycle, such as issuance, revocation, and suspension of certificates, is done by the enterprise, and does not involve WISEKey nor OISTE.

CP/CPS Template / Customisable Policies

The organisation has the advantage of a template set of policies and practices that he is free to customise to produce his own policies. Guidelines are provided for key management, Security policies, personnel policies, and other organisation policies. The organisation can use these documents as is, with little or no modification, or can customise it to their needs and submit it for approval.

Brand Name

The organisation chooses its own brand name that can be completely independent of WISEKey. This brand name is used in the customer's certification authority, and all of the certificates that it issues.

Easy Integration

The CertifyID Trust Service has been specifically designed to interoperate with the most popular commercial operating systems, notably Microsoft Windows Server, and it takes advantage of Windows Certificate Services to provide an effective solution for global trust assurance.

Organisations can integrate closely with Active Directory and their Identity and Access Management solutions thus significantly reducing the typical cost of ownership of a PKI.

About WISEKey Smartcards and USB Tokens

WISEKey provides smartcards, readers, and secure USB tokens for individuals and enterprises. WISEKey smart cards are high quality multipurpose cards that can be used for a variety of purposes including:

- Secure files and documents

- Securely exchange information
- Secure electronic email
- Securely access facilities (wireless proximity access – special version)
- Securely access desktops and servers
- Digital sign documents and files for more efficient electronic workflow and approvals
- In addition to signature and PKI applications, and access control systems, the smart card can be used to secure many other sensitive applications, such as payment systems.

The Alinghi Smartcard 2007 is a WISeKey card that has been co-branded by Alinghi for their use the Defense of the 32nd Americas Cup, in which they were successful.

The WISeKey Smart Card (2007) is implemented using a Philips P8WE5032 integrated circuit, which has been certified as ITSEC E4 high.

Features:

- ISO/IEC compatibility
- Secure messaging
- Hierarchical ISO file system
- DES, 3DES
- State machine
- Logical channel support
- Deletion of files (EF) and applications (DF)
- Enhanced hardware security
- High performance
- Implementation of various access controls (authentication)
- Data encryption with asymmetric RSA keys up to a key length of 1,024 bits
- Generation and verification of digital signatures with RSA and DSA
- On-card RSA key generation up to a key length of 1,024 bits
- Digital signature application can be certified ITSEC E4 high

The provided middleware allows smart card or tokens to be used in all conventional PKI applications such as secure mail, SSL or network login. The smart card middleware consists of an easy-to-use installation routine and the middleware itself. This serves to connect the hardware to applications and operating systems. A utility for token management is also included.

To achieve optimum interoperability the smart card middleware supports more than 70 different smart card operating systems (Starcos, JCOP, CardOS, Multos, SmartCafe, etc.), thus ensuring future longevity and flexibility of the deployed infrastructure.

Supported operating systems:

- Windows 98/ME/NT 4.0/2000/XP/2003 server
- MAC OS X
- Linux
- Solaris
- Windows CE

A selection of the supported applications:

- MS Windows 2000/XP log-on
- MS Windows terminal server/Citrix
- Secure e-mail clients, e.g. MS Outlook (Express, 98, 2000, XP), Netscape Messenger, Novell Groupwise 6, Baltimore Mail-Secure, Utimaco Sign & Crypt, Entrust Entelligence
- Secure e-mail plug-ins for Lotus Notes from Utimaco, Secude, SSE, Baltimore
- WISeCrypt

- SSL authentication with browsers such as MS Internet Explorer, Netscape Navigator
- WISEKey PKI, Baltimore PKI, Entrust PKI, RSA Keon PKI, VeriSign PKI or GlobalSign PKI
- VPN clients from Microsoft, NCP, Cisco, Checkpoint, SafeNet
- SSH Secure Shell clients
- PGP, RSA SecurID, Celo eSigner, Lotus Notes Rnext, Citrix Metaframe, Novell NMAS
- SSO from eTrust, Protocom

The following interfaces are supported:

- PKCS#11 meeting the RSA specification
- PKCS#12 transport format
- PKCS#15 token information syntax format
- CSP for MS CryptoAPI
- PC/SC 1.0 several class 2/3 readers
- A004

Token management utility

- Token initialization (incl. loading of applets in the case of a Java™-based token)
- PIN definition
- Key generation
- Multi-language support
- Automatic registration of certificates in MS applications
- Customized adaptations (e.g. menu options on/off)

Copyright

No part of the contents of this document may be reproduced or distributed in any form or by any means without the prior written permission of WISeKey SA.



is a registered trademark of WISeKey SA.



is a registered trademark of WISeKey SA.

Microsoft, MS are registered trademarks, and Windows is a trademark of Microsoft Corporation. Parts of this document are extracted and reproduced from the Identity Life Cycle Manager Library available in Microsoft Technet website.

Written and published in Geneva, Switzerland, by WISeKey SA.
Copyright © 2007 WISeKey SA.
All Rights Reserved.

Target Audience

It is assumed that the user of this guide is well-versed with the installation and deployment of:

- WISEKey CertifyID TrustCentre (BlackBox)
- Microsoft Windows Certificate Services
- Active Directory
- Microsoft SQL Server™ 2005
- Microsoft Internet Information Services
- Smart Card (AET SafeSign Standard)

Document Conventions

This User Guide uses the following conventions:

- **NOTE** means *reader take note*. Notes contain helpful suggestions.
- **IMPORTANT** means the reader must follow the instructions strictly.
- Descriptions for significant fields are available.

Terminologies Used in the Document

The following table lists the meaning of key terms used in this User Guide.

Term	Description
Microsoft Certificate Life Cycle Manager (CLM)	Microsoft Certificate Lifecycle Manager 2007 is a policy and workflow driven solution that helps organizations manage the lifecycle of digital certificates and smart cards.
Smart Card	A smart card, chip card, or integrated circuit card (ICC), is defined as any pocket-sized card with embedded integrated circuits which can process information. Today's cryptographic smart cards are also able to generate key pairs on board, to avoid the risk of having more than one copy of the key.
Certification Authority (CA)	A CA is an entity that is trusted to issue and manage certificates. A CA is part of a Public Key Infrastructure, which is typically used to provide the underlying security services that are part of the security solution for conducting business on the Internet, ensuring that electronic transactions are conducted with confidentiality, data integrity, proper user authentication, and protection against repudiation.
Certificate	A Digital Certificate issued by a Certification Authority.

Requirements

HARDWARE REQUIREMENTS

Hardware	Description
RAM	1,024 megabytes (MB) of RAM. We recommend that you install 2 gigabytes (GB) or more of RAM.
Hard disk	A 40 GB or larger hard disk. Disk space requirements vary based on use and log file management.
DVD drive	A DVD drive is required to install Microsoft SQL Server™ database software from a DVD-ROM.
Display	A Super VGA (SVGA) display with a resolution of 800 x 600 or higher and 256 colors.
Mouse	A mouse or other input device.
Network	A LAN connection with at least a 56K modem. A network connection is required for distributed management.

SOFTWARE REQUIREMENTS

Software	Description
Certification authority (CA)	WISeKey CertifyID BlackBox™ Advanced or Standard CA should be installed.
Microsoft Certificate Lifecycle Manager 2007	At least one instance of the software installed on a server that is running Microsoft® Windows Server® 2003, Enterprise Edition or Microsoft® Windows Server® 2003, Datacenter Edition.
Microsoft SQL Server	CLM supports Microsoft SQL Server 2005, Standard Edition, Service Pack 1 and Microsoft SQL Server 2005, Enterprise Edition, Service Pack 1. CLM also supports Microsoft SQL Server 2000 Service Pack 4.
Internet Information Services (IIS) 6.x	CLM uses IIS as its Web server to run the CLM Web site.
The Microsoft .NET Framework 2.0	CLM is a Microsoft .NET-connected application. You must install the Microsoft .NET Framework 2.0 on the server.
Microsoft Internet Explorer® 6.x	Because CLM requires Secure Sockets Layer (SSL) and Transport Layer Security (TLS) for administrative traffic and certificates, Internet Explorer 6.x is required. In addition, CLM has advanced scripting features that are optimized for Internet Explorer.

Installation Process

Typical Deployment

CLM has the following components for certificate management:

A server running the CLM software, which includes the CLM Web site and the core CLM server components that integrate with the following infrastructure:

- Active Directory
- WISEKey CertifyID Black Box Advanced or Standard CA
- Microsoft SQL Server™ 2005
- Simple Mail Transfer Protocol (SMTP) mail services, which is required only if you choose to integrate e-mailing one-time passwords to users

One or more Microsoft Windows® XP Service Pack 2 (SP2) computers running the following software:

- Microsoft Certificate Lifecycle Manager Client, which allows users to request smart card certificates
- Bulk Smart Card Issuance Tool, which administrators can use to perform batch operations for smart card certificates

Pre-requisite Tasks for Installing CLM

INSTALLING WISEKEY CERTIFYID BLACKBOX™ & CERTIFICATE SERVICES

CertifyID BlackBox is a set of applications that allow the installation of a globally trusted Certification Authority (CA) on the customer's premises. The WISEKey CertifyID service enables customers to incorporate their certification authority (CA) into the CertifyID Trust Network.

IMPORTANT NOTE

A WISEKey CertifyID Advanced CA or WISEKey CertifyID Standard CA is required to be installed before beginning the CLM installation.

Prior to beginning the installation of Microsoft CLM and the WISEKey smart card products that is explained in this guide, you should have completed the installation of a CertifyID Standard or Advanced Certification Authority. Your certification authority should be fully functional and capable of issuing certificates, suspending and revoking certificates.

The CertifyID CA installation procedure is described in the CertifyID BlackBox User Manual and Solution Guide.

INSTALLING INTERNET INFORMATION SERVICES ON CLM SERVER

Microsoft Internet Information Services shall be installed in the CLM server through **Add and Remove Windows Components** in **Control Panel**. The following components shall be enabled:

- ASP.NET
- Network COM+ access
- WWW
- Active Server Pages

INSTALLING .NET FRAMEWORK 2.0

Microsoft .NET framework shall be installed and enabled as web service extension in IIS.

INSTALLING MS-SQL SERVER 2005

Insert the SQL Server 2005 DVD into your DVD drive, and then follow the instructions provided in the Help or visit <http://msdn2.microsoft.com/en-us/library/ms143516.aspx> for online help.

MODIFYING THE ACTIVE DIRECTORY SCHEMA

To modify the Active Directory schema, you must be a member of the Schema Admins group for the Active Directory forest.

Before you install CLM 2007, you must apply the schema modifications that are defined in Clm.ldif, which is a Lightweight Directory Access Protocol (LDAP) Data Interchange Format (LDIF) file. You can use either of the following methods to apply the modifications:

- Run the LDAP Data Interchange Format Data Exchange tool, ldifde.exe. ldifde.exe is part of Windows Support Tools, which assist support personnel and network administrators in managing their networks and troubleshooting problems. They are not installed with the Windows operating system; you must install them separately from the Windows XP or Windows Server 2003 installation CD. To install the tools, you run Suptools.msi, which you can find on the Windows installation CD at the following location: Support\Tools.
- Run the ModifySchema.vbs sample script. ModifySchema.vbs modifies the schema on the default forest using the current credentials for the user. If your settings differ from the default settings, you must edit the script before you run it. Clm.ldif and ModifySchema.vbs are on the CLM installation CD at the following location: CLM\Schema.

ENABLING THE DEFAULT KEYRECOVERYAGENT CERTIFICATE TEMPLATE

An enrollment agent is an IT administrator who requests certificates on behalf of a user. **EnrollmentAgent** is the default certificate template for the key recovery agent

in CLM. The certificate template is only available if it is enabled on an active BlackBox CA in the CA hierarchy.

To enable the default KeyRecoveryAgent certificate template in BlackBox CA

Note: A user who is assigned the Manage CA permission to the enterprise CA must perform the following procedure.

<i>Steps</i>	<i>Instructions</i>
1	Click Start , point to Administrative Tools , and then click Certification Authority .
2	In Certification Authority , expand the set of folders for the default CA.
3	In the console tree, right-click Certificate Templates , point to New , and then click Certificate Template to Issue .
4	In New Certificate Template to Issue , select Key Recovery Agent , and then click OK .

ENABLING THE DEFAULT ENROLLMENTAGENT CERTIFICATE TEMPLATE

An enrollment agent is an IT administrator who requests certificates on behalf of a user. **EnrollmentAgent** is the default certificate template for the enrollment agent in CLM. The certificate template is only available if it is enabled on an active BlackBox CA in the CA hierarchy.

To enable the default EnrollmentAgent certificate template in BlackBox CA

Note: A user who is assigned the Manage CA permission to the enterprise CA must perform the following procedure.

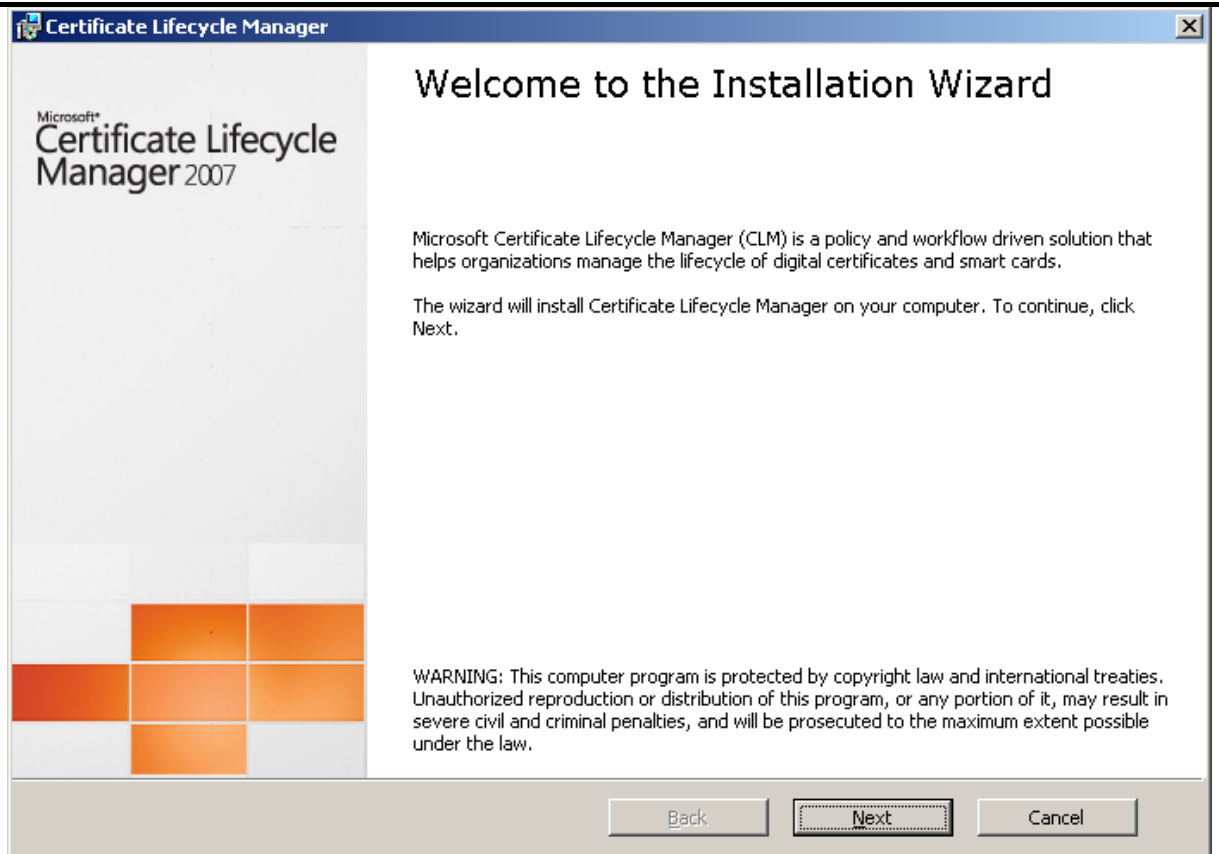
<i>Steps</i>	<i>Instructions</i>
1	Click Start , point to Administrative Tools , and then click Certification Authority .
2	In Certification Authority , expand the set of folders for the default CA.
3	In the console tree, right-click Certificate Templates , point to New , and then click Certificate Template to Issue .
4	In New Certificate Template to Issue , select Enrollment Agent , and then click OK .

Installing CLM on Server

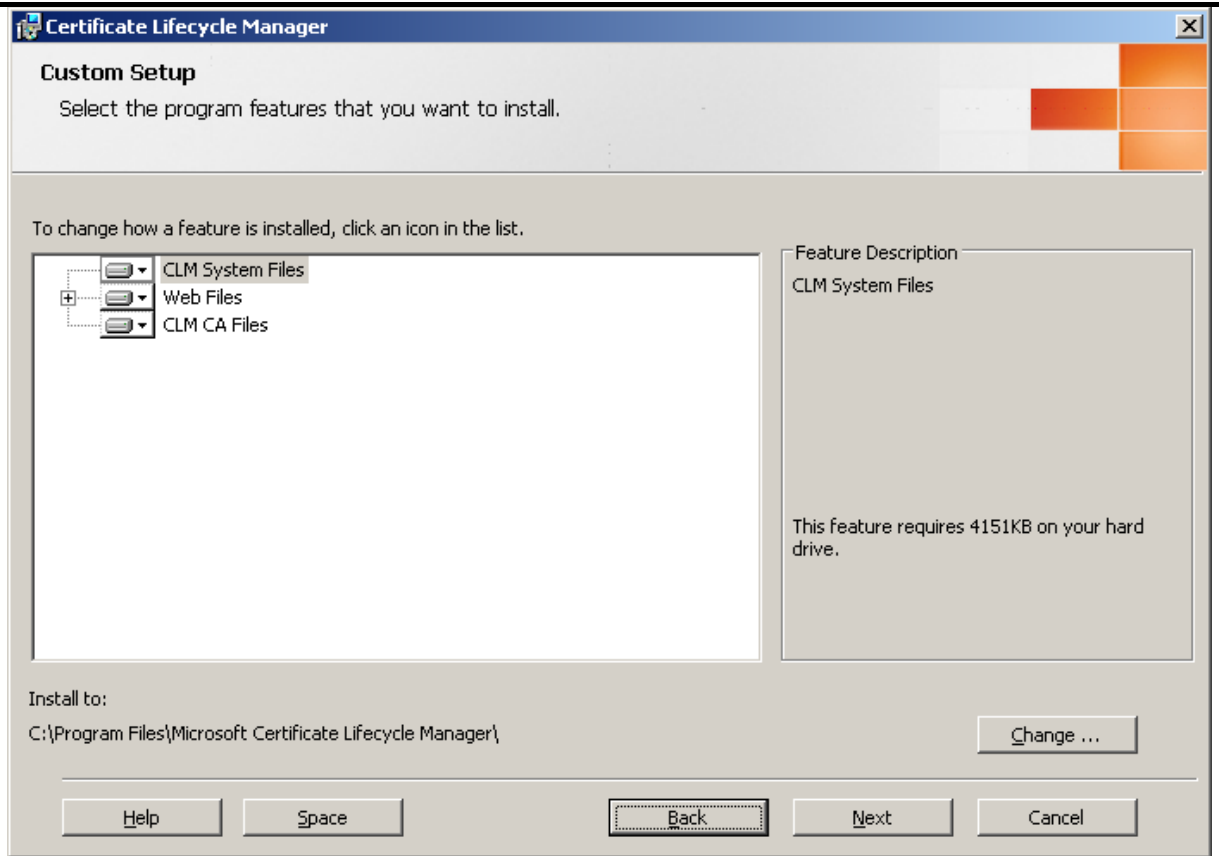
INSTALLING CLM AND CA ON SAME SERVER

Prior to install CLM and the CA on the same server, evaluate the hardware specifications for the server to ensure that it has a capable CPU and enough available hard drive space to accommodate both CLM and the CA.

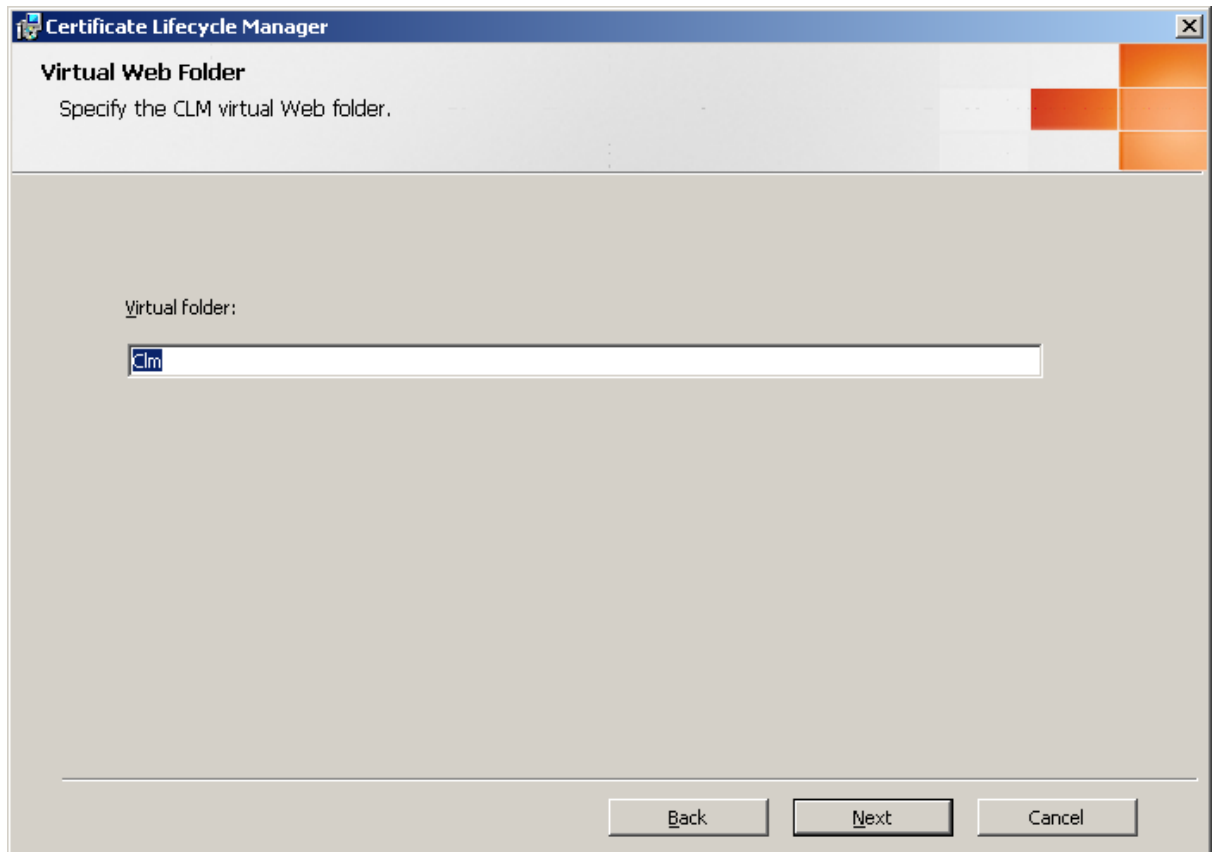
<i>Steps</i>	<i>Instructions</i>
1	From the CLM installation CD, run CLM.msi. CLM.msi is located at <i>Drive\CLM\</i> . <i>Drive</i> is the name of your CD or DVD drive. On the Welcome to the Installation Wizard page, click Next .



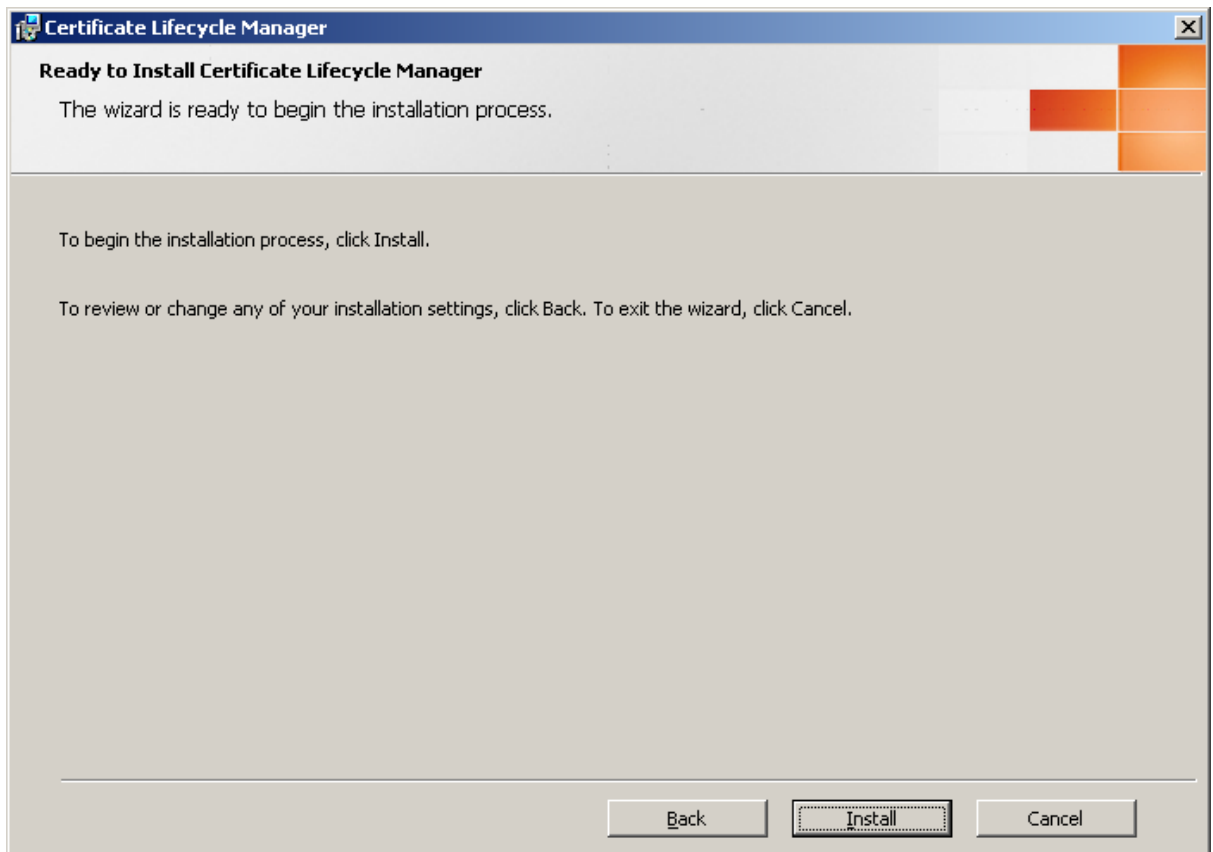
- 2 On the **Certificate Lifecycle Manager License Agreement** page, read the license terms, select **I accept the terms in the license agreement**, and then click **Next**. Enter the product key in the **Product Key** page and click **Next**.
- 3 On the **Custom Setup** page, verify that all of the available components are selected. To change where you install the files, click **Change**, choose a different location, and then click **OK**. The default location is %ProgramFiles%\Microsoft Certificate Lifecycle Manager. On the **Custom Setup** page, click **Next**.



- 4 On the **Virtual Web Folder** page, specify a name for a virtual Web folder. This folder will be the address for the CLM Web site. The default virtual Web folder name is **Clm**.



- 5 On the **Ready to Install Certificate Lifecycle Manager** page, click **Install**.



- 6 On the **Certificate Lifecycle Manager Installation Complete** page, clear the **Launch the CLM Configuration Wizard** check box, and then click **Finish**.

INSTALLING CLM WEBSITE ON SERVER SEPARATE FROM THE CA

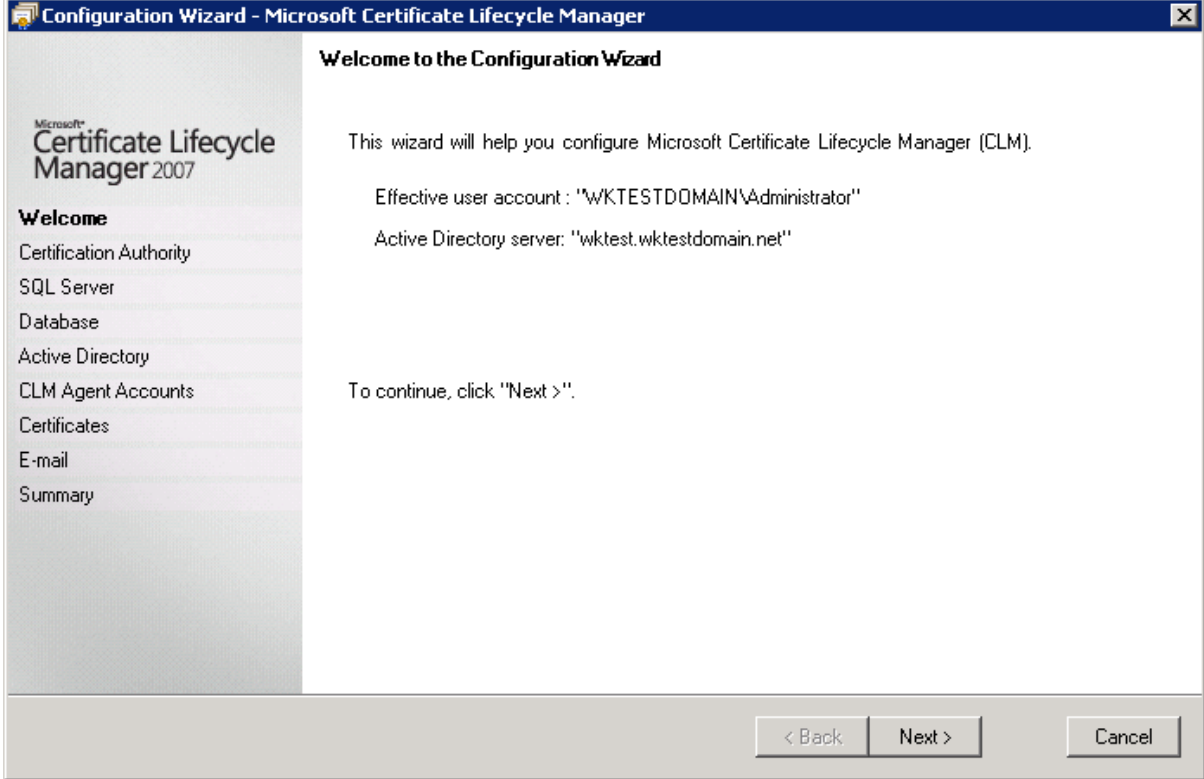
You can install the CLM Web site on a different server than where the CA is installed. You might do this to physically separate the CLM and CA roles.

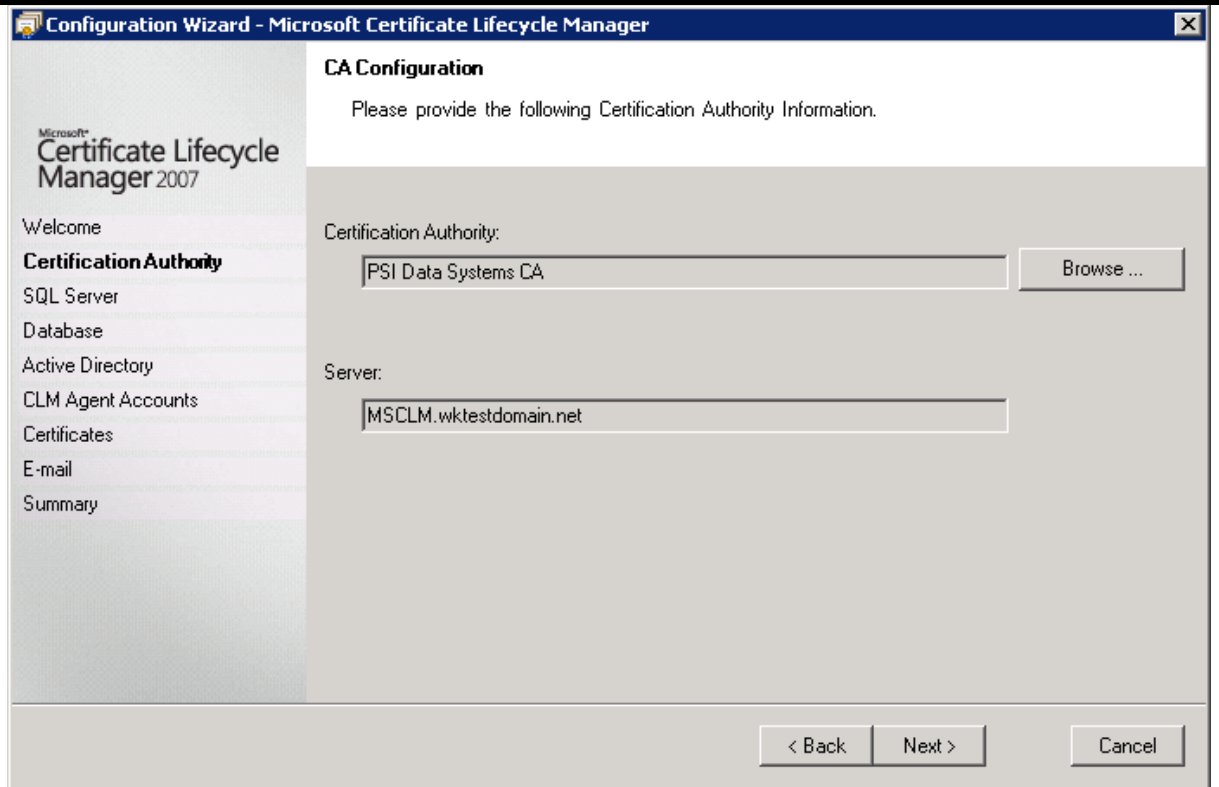
By default, the CLM Installation Wizard installs the server component, the Web site, and the CA policy and exit modules on the same server. To install the CLM Web site on a server separate from the CA, you must choose a custom setup in the CLM Installation Wizard to install the policy and exit modules on the CA server with the CLM server component. The detailed instructions can be found in the [Microsoft Technet Website](#).

Configuring CLM Using Configuration Wizard

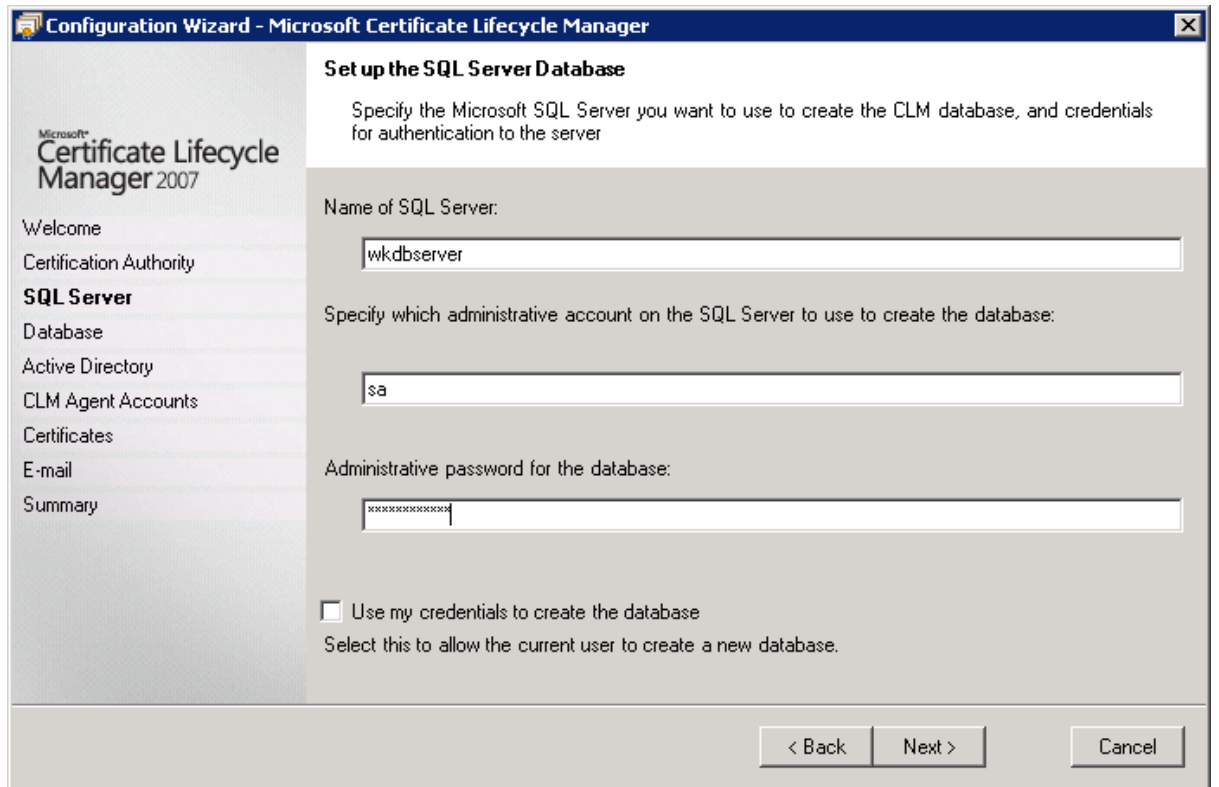
To configure the CLM on the CLM server, you shall run the CLM Configuration Wizard. We recommend that you run CLM Configuration Wizard from a user account that is a member of the Enterprise Admins group. That group has the necessary permissions for the relevant profile templates and certificate templates. However, if you plan to run the CLM Configuration Wizard from a user account that is a child domain administrator, you must first assign specific user rights and permissions to the Domain Admins group as explained in the [Microsoft Technet Website](#).

RUNNING CONFIGURATION WIZARD

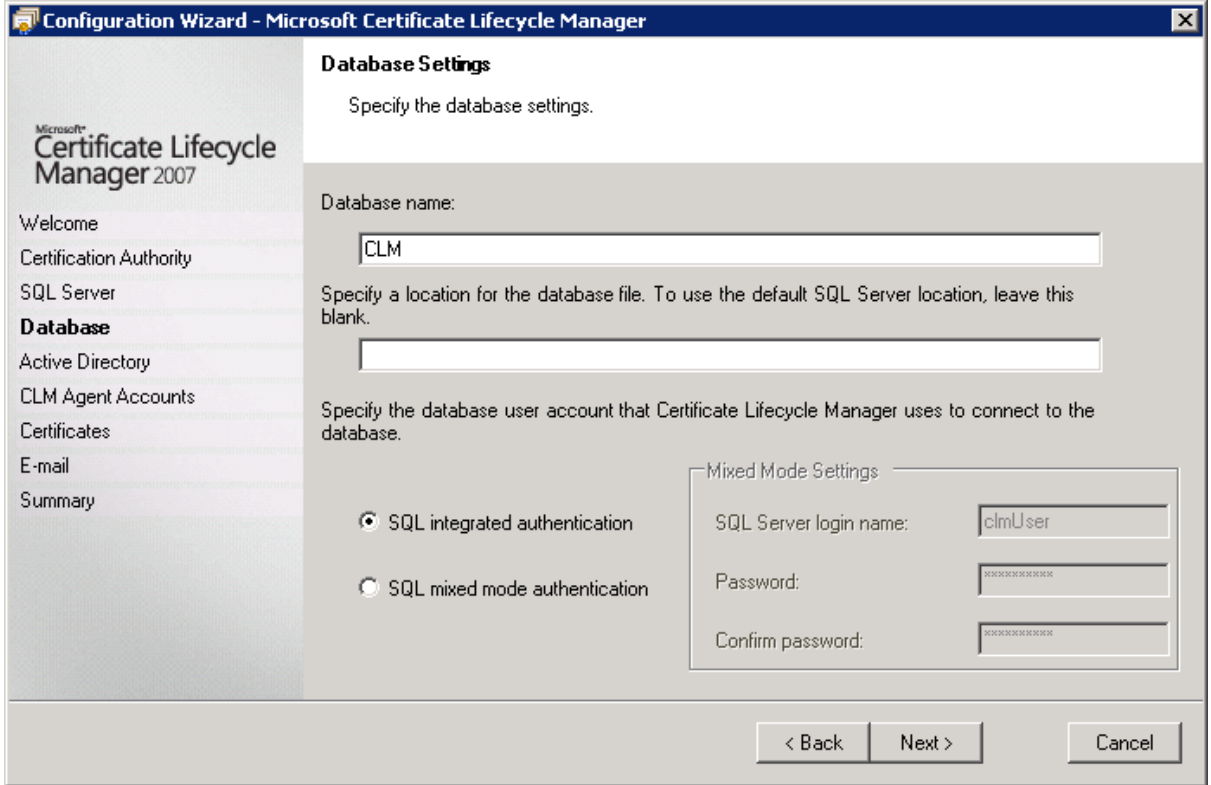
Steps	Instructions
1	<p>Click Start, point to Programs, point to Microsoft Certificate Lifecycle Manager, and then click Configuration Wizard. On the Welcome to the Configuration Wizard page, click Next.</p> 
2	<p>On the CA Configuration page, verify the name of the CA and the Domain Name System (DNS) name for the CA server, and then click Next.</p> <p><i>Note: If you want to specify a remote CA, do the following steps:</i></p> <ol style="list-style-type: none"> 1. Click <i>Browse</i>, and then select any enterprise CA in the forest shown in the <i>Select Certification Authority</i> dialog box. 2. Verify the CA and DNS names, and then click <i>OK</i>.



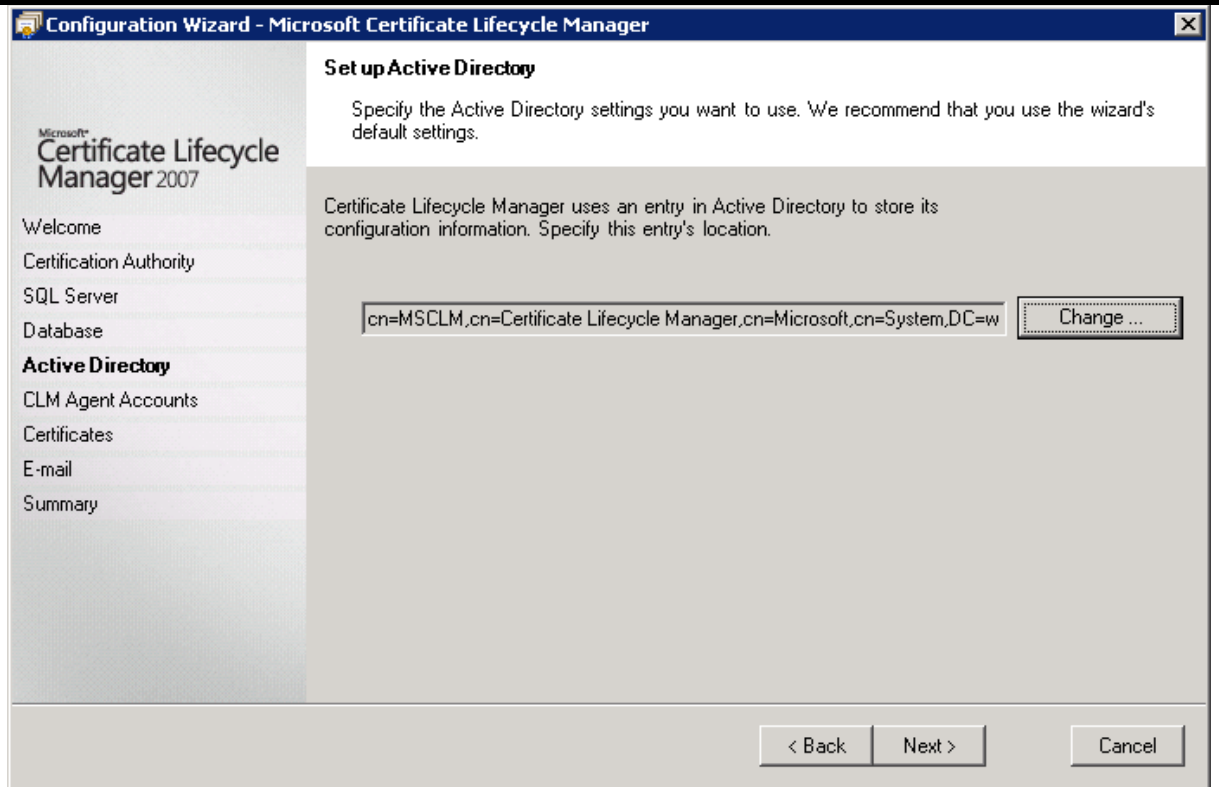
- 3 On the **Set up the SQL Server Database** page, configure SQL Server for use with CLM. In **Name of SQL Server**, type the IP address of the SQL Server database. If the SQL Server database is on the same computer, use the default value, which is **(local)**. Configure SQL Server service account and password. To use the account information, select the **Use my credentials to create the database** check box. click **Next** to proceed.



- 4 On the **Database Settings** page, under **Database name**, specify the name for the CLM database. Under **Specify a location for the database file**, you can enter a location or use the null value. If you use the null value, CLM uses the default location for the SQL Server database file. Under **Specify the database user account that Certificate Lifecycle Manager uses to connect to the database**, choose either **SQL integrated authentication** or **SQL mixed mode authentication**. Configure with necessary credentials if you are selecting SQL mixed mode authentication. Click **Next** to proceed.

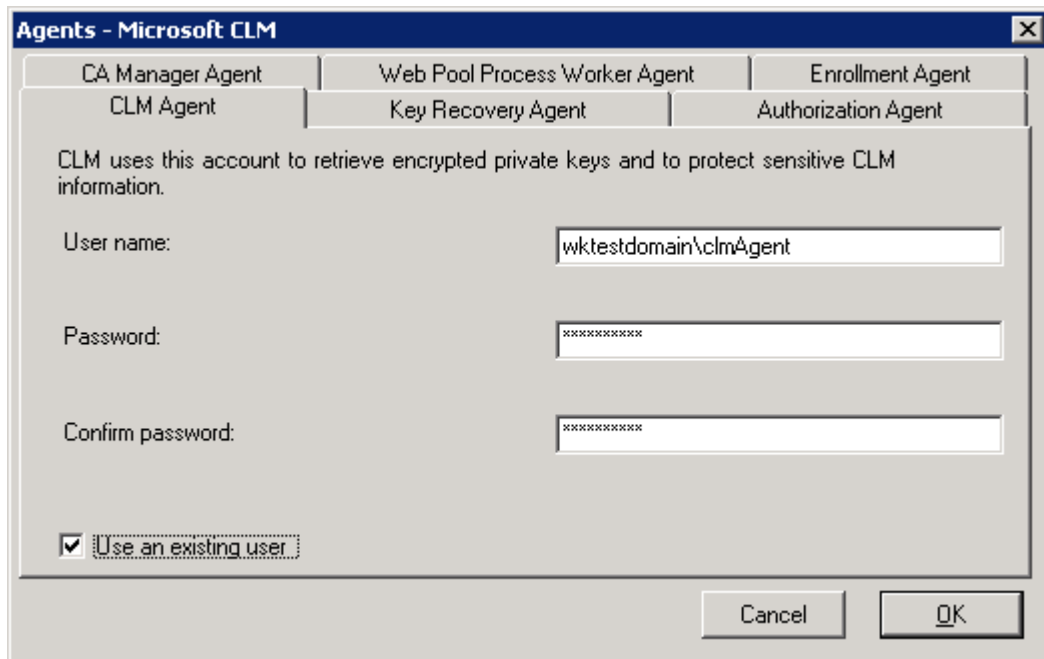


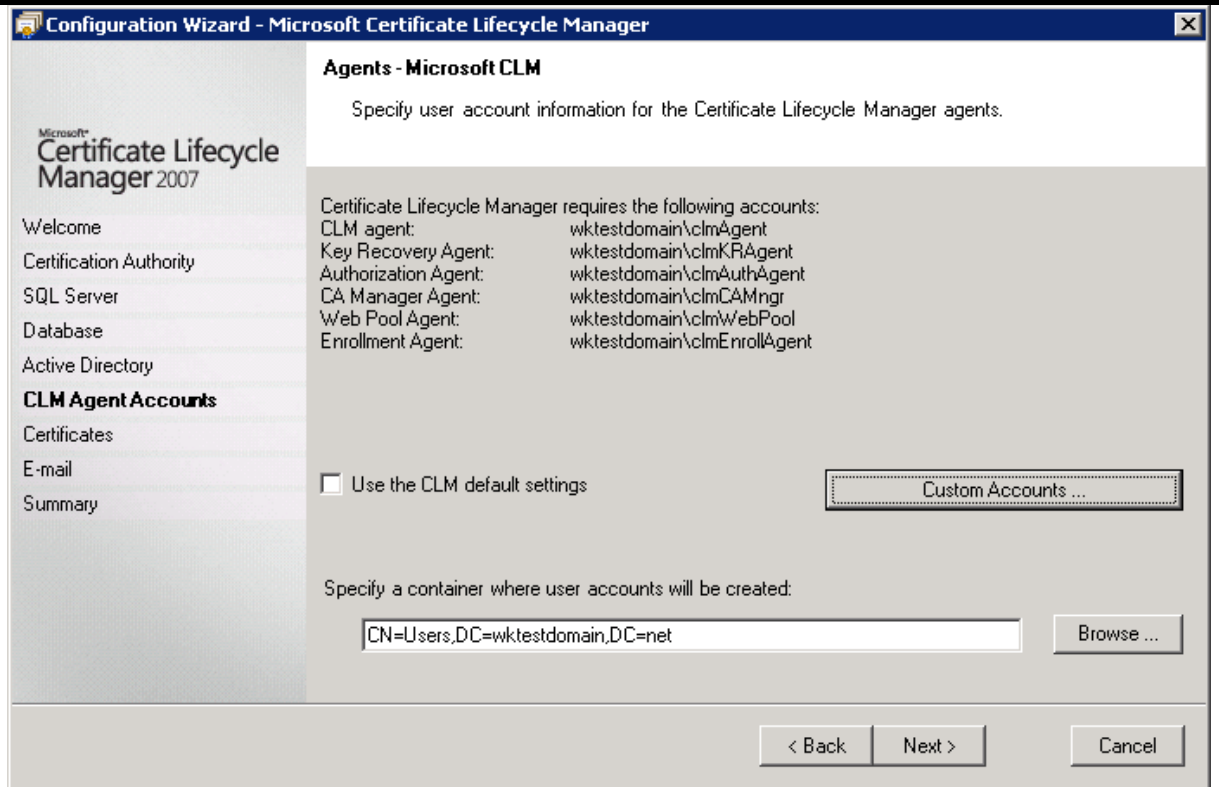
- 5 On the **Set up Active Directory** page, type the name of the directory entry that Active Directory uses to store CLM configuration information. Use the default values on the **Directory Settings** page, and then click **Next**.



- 6 On the **Agents - Microsoft CLM** page, perform one of the following actions:
- To use the default user accounts, leave the check boxes unchanged.
 - To create a custom user account, clear the **Use the CLM default settings check box**, and then click **Custom Accounts**.

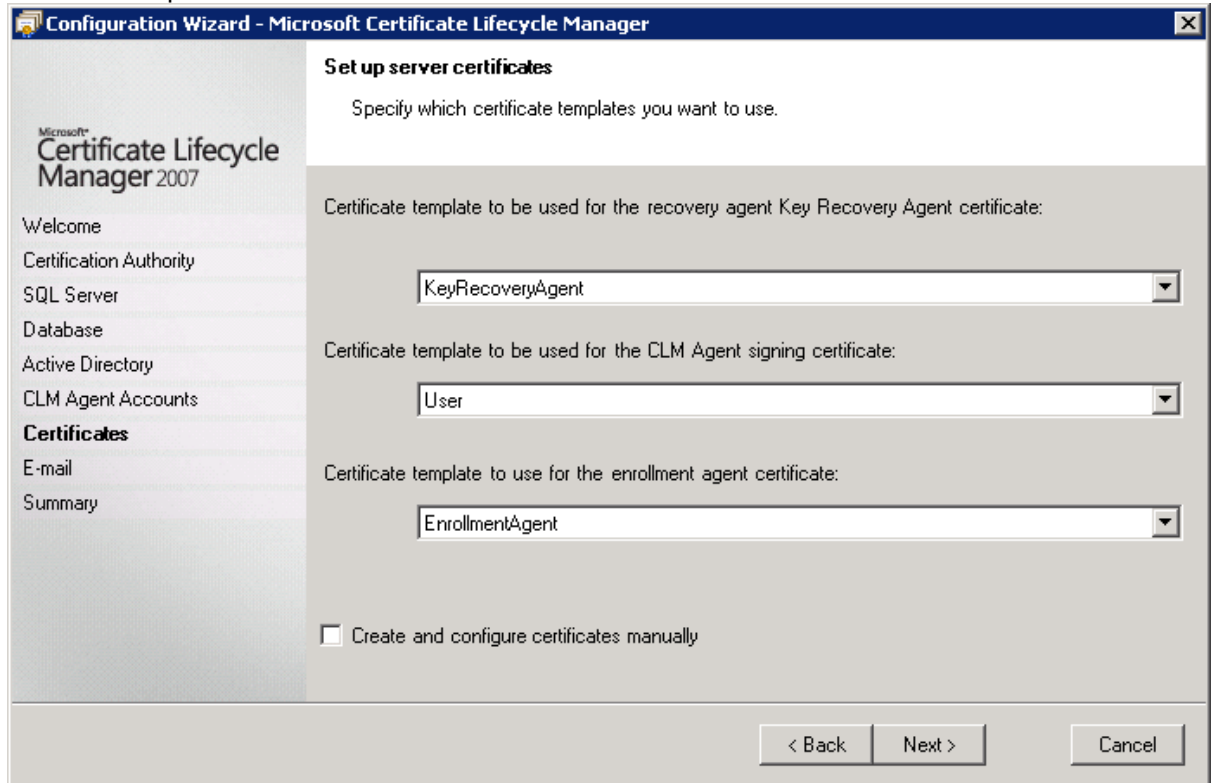
Click **Next** to proceed.

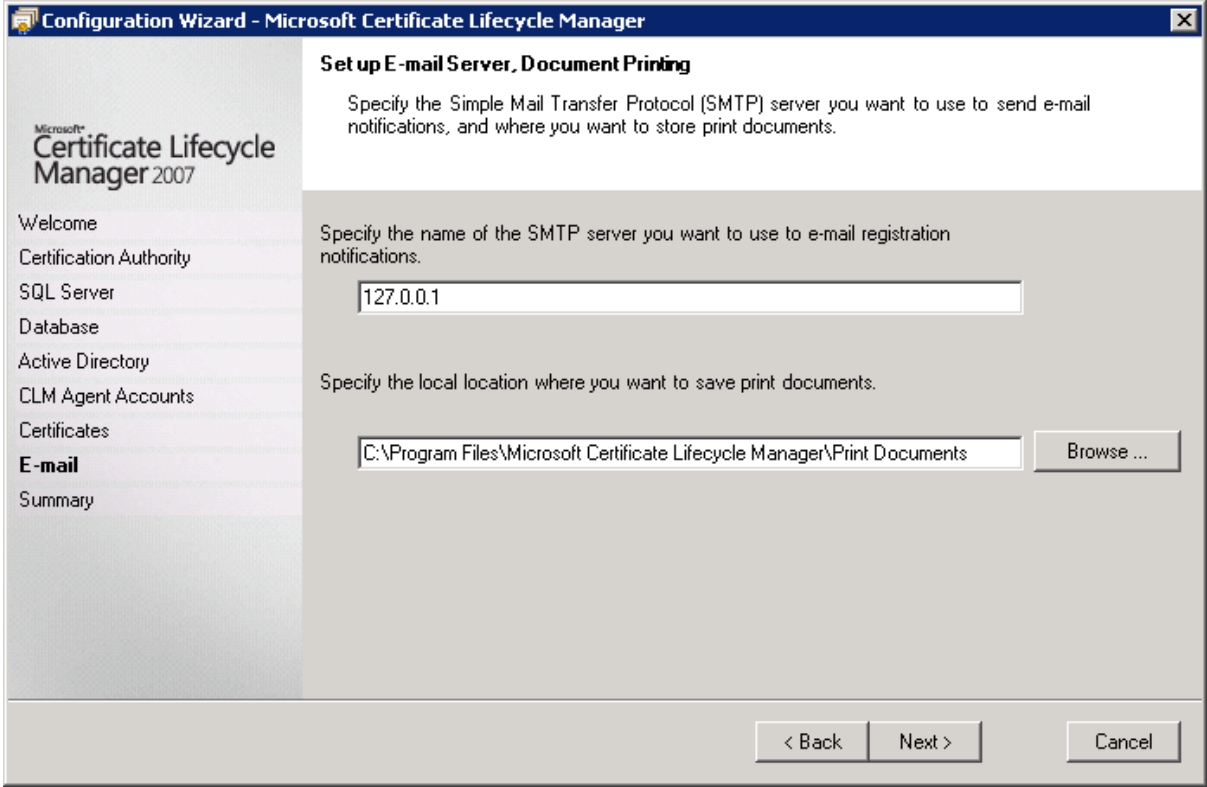


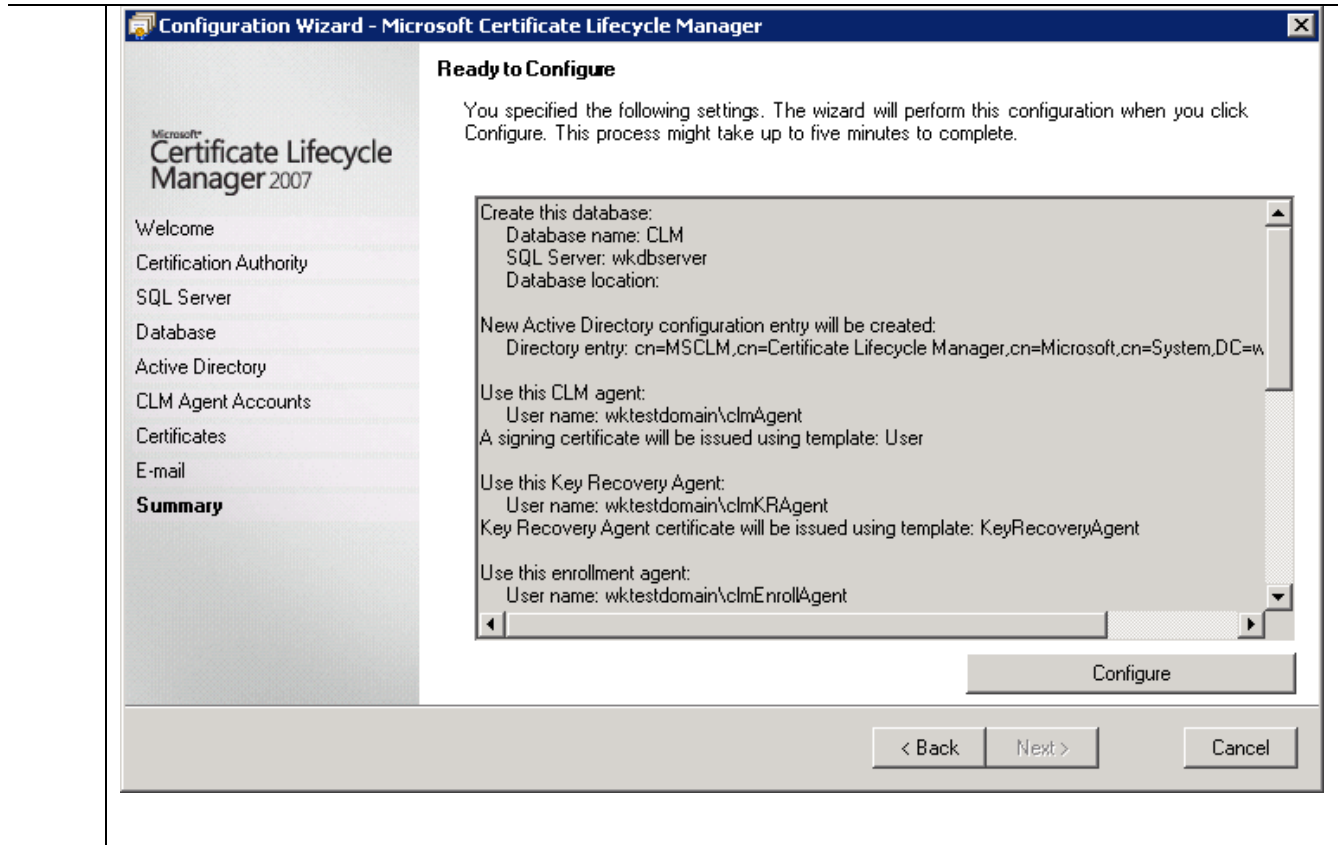


- 7 On the **Set up server certificates** page, perform one of the following actions:
- To use the default certificate templates for the key recovery agent, the CLM agent, and the enrollment agent, leave the check boxes unchanged.
 - To manually create and configure the certificate templates, select the **Create and configure certificates manually** check box.

Click **Next** to proceed.



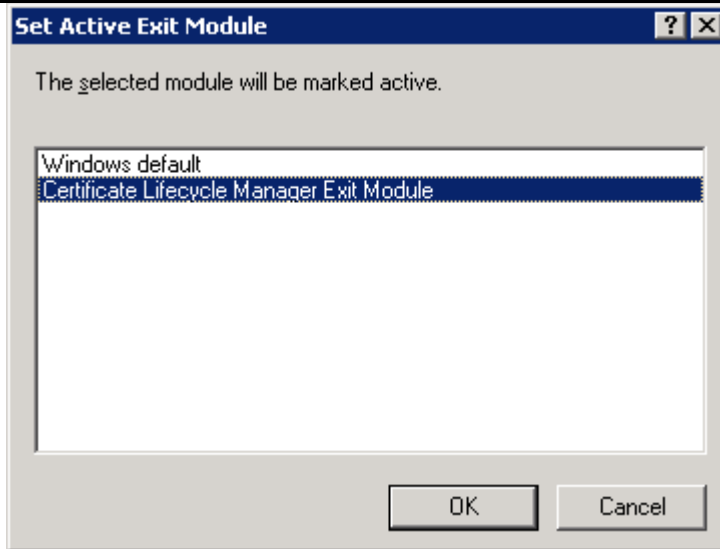
<p>8</p>	<p>On the Set up E-mail Server, Document Printing page, type the IP address or DNS name of the Simple Mail Transfer Protocol (SMTP) host that CLM uses to send e-mail notifications. The default SMTP IP address is 127.0.0.1, which indicates that CLM uses the local SMTP service.</p> <p>Type the name of the folder where CLM stores files to send to a printer. The default folder for these files, Print Documents, is at the following location: %ProgramFiles%\Microsoft Certificate Lifecycle Manager\Print Documents.</p> <p>Click Next to proceed.</p> 
<p>9</p>	<p>On the Ready to Configure page, verify the selected settings, and then click Configure. This might take a few minutes. When the configuration completes, click Finish to exit the CLM Configuration Wizard.</p>



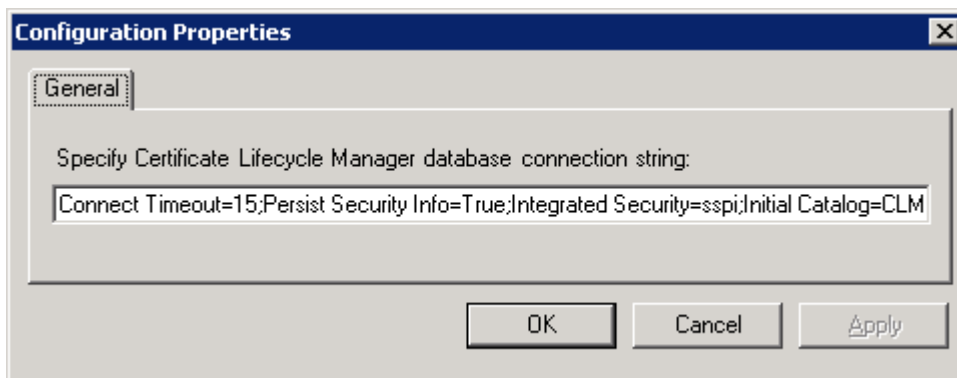
Configuring the CA for CLM

CONFIGURING EXIT MODULE

Steps	Instructions
1	Click Start , point to Administrative Tools , and then click Certification Authority . In the Certification Authority snap-in, right-click <i>CAName</i> , and then click Properties . <i>CAName</i> is the name of the CA. At the <i>CAName Properties</i> dialog box, click the Exit Module tab, and then click Add .
2	In the Set Active Exit Module dialog box, select CLM Enterprise Exit Module , and then click OK .

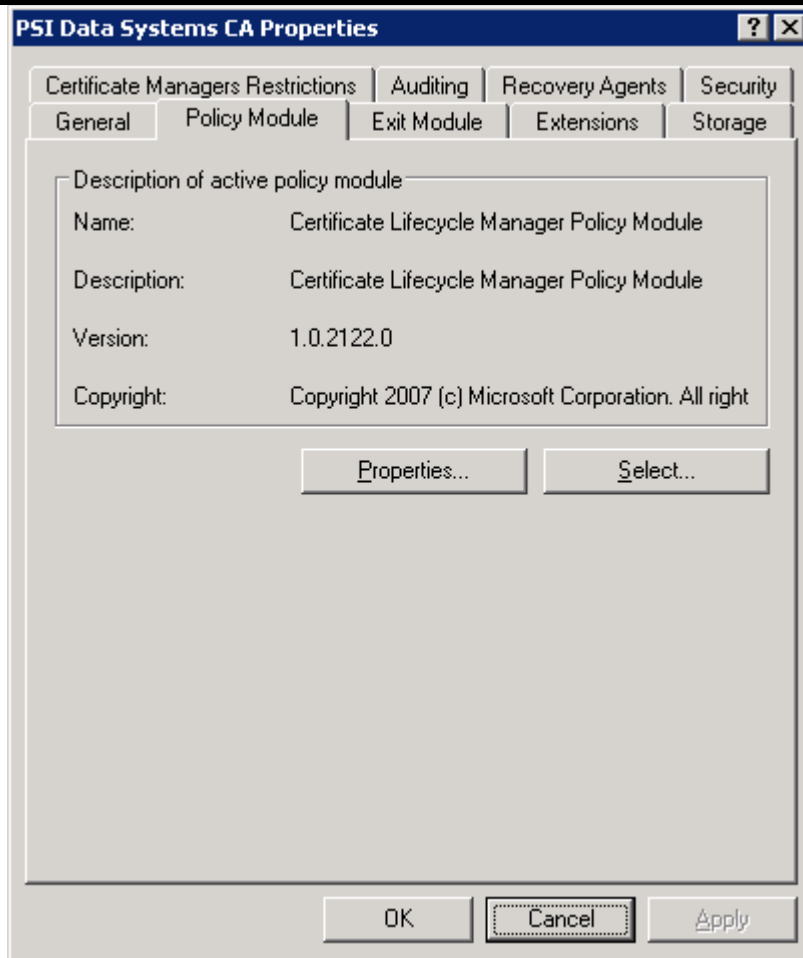


- 3 In the **CANAME Properties** dialog box, on the **Exit Module** tab, in **Exit Modules**, select **CLM Enterprise Exit Module**, and then click **Properties**. In the **Configuration Properties** dialog box, type the connection string for the SQL Server that hosts the CLM database, and then click **OK**. If the configuration wizard is completed successfully then the details will come as default. Click **OK** to return.

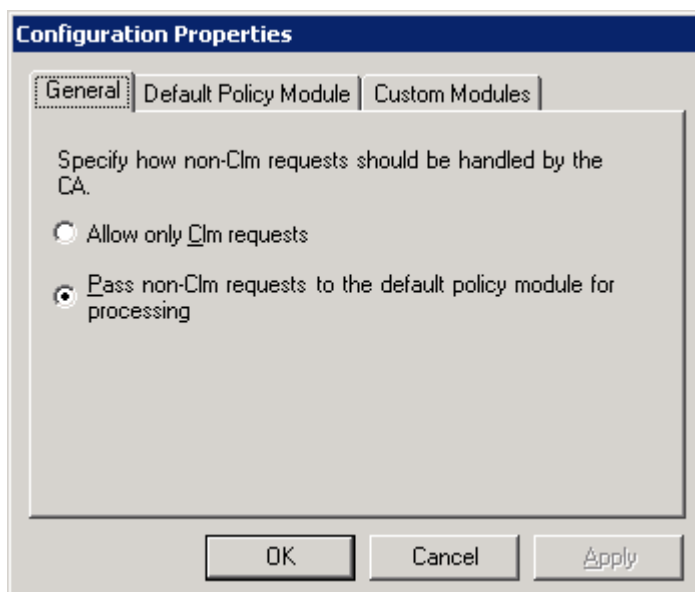


CONFIGURING POLICY MODULE

Steps	Instructions
1	Click Start , point to Administrative Tools , and then click Certification Authority . In the Certification Authority snap-in, right-click CANAME , and then click Properties . CANAME is the name of the CA. In CANAME Properties , click the Policy Module tab, and then click Select to designate the Active Policy Module . In the Set Active Policy Module dialog box, select CLM Enterprise Policy Module and then click OK .



- 2 On the **Policy Module** tab of the *CAName Properties* dialog box, click **Properties**. In the **Configuration Properties** dialog box, on the **General** tab, select **Pass non-CLM requests to the default policy module for processing**. In the **Configuration Properties** dialog box, on the **Default Policy Module** tab, click **Properties**. In the **Default Policy Module** dialog box, select **Follow the settings in the certificate template**, if applicable. Otherwise, automatically issue the certificate, and then click **OK**. In the **Configuration Properties** dialog box, click **OK**.



Note 1: For configuration changes to take effect, you might have to restart Certificate Services.

Note 2: Check the CertificateAuthority Table in configured CLM database whether the CAName, CAServerName are updated correctly.

Creating Users in Active Directory and giving Access Permissions

Users and Groups have to be created in Active Directory and given necessary permissions to access the CLM website, creating and managing profile templates enroll for certificates, apply for smart cards and related smart card operations. More information regarding these procedures can be obtained in [Microsoft Technet Website](#).

Creating and Configuring CLM Profile Template

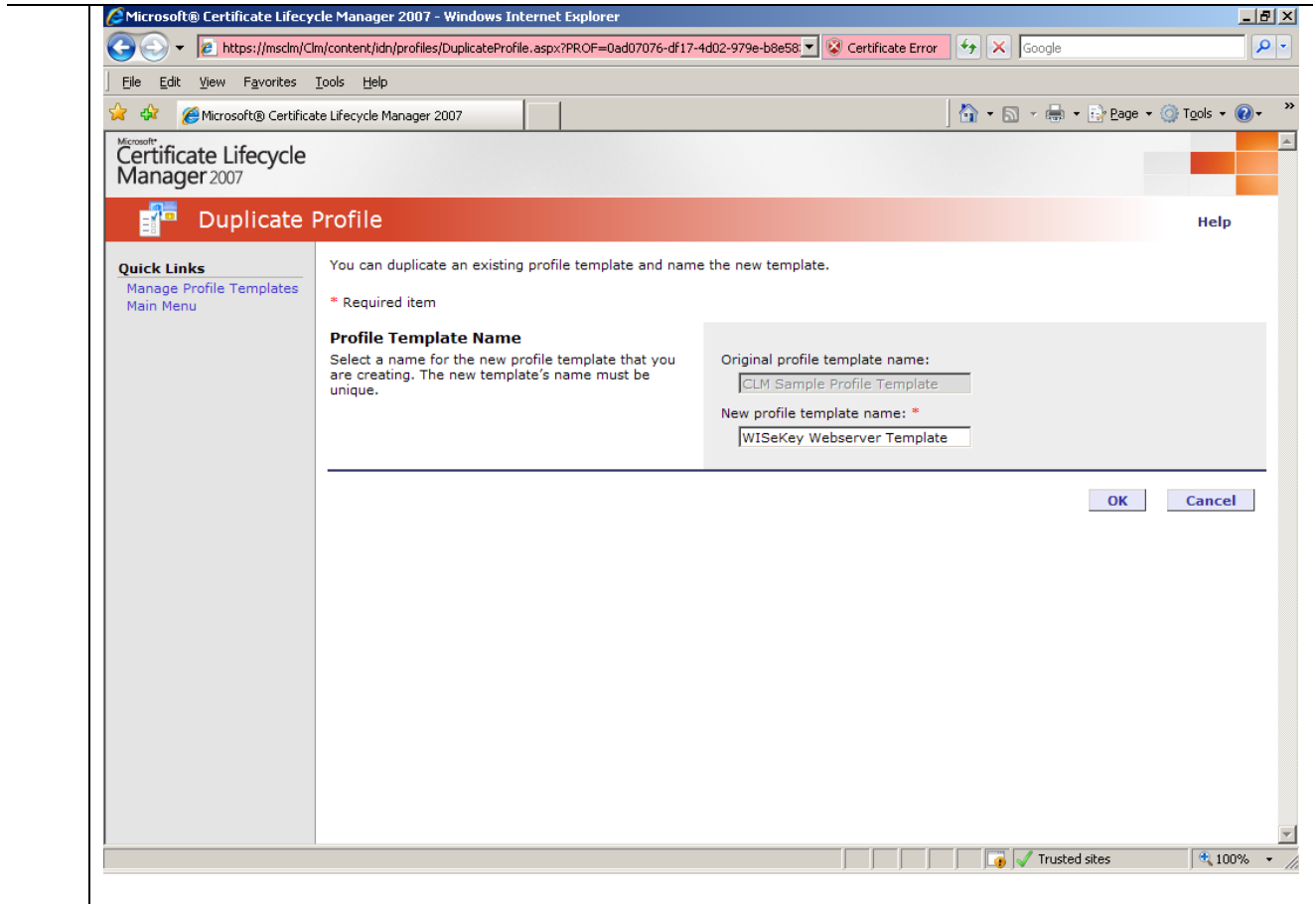
There are two types of profile templates in CLM namely software profile templates and smart card profile templates. You shall create a user and security group that are delegated the minimum permissions necessary to perform the procedures. More information regarding these procedures can be obtained in [Microsoft Technet Website](#). To create a new Profile Template you will need to copy an existing template. Two sample templates are provided with CLM for this purpose.

Note:

On each computer where you want to use to access the CLM Web site, you must add the CLM Web site to the Trusted Sites Web content security zone in Internet Explorer. Because the CLM Web site enforces the use of trusted sites, it does not function correctly if you do not add the CLM Web site to Trusted Sites.

CREATING PROFILE TEMPLATE

Step	Instruction
1	Log in as user who has permission to create Profile Template.
2	Open Internet Explorer . In Internet Explorer, open https://CLMServer/clm. Click the Microsoft Certificate Lifecycle Manager logo.
3	On the Home page of the CLM Web Portal, in the Administration section, click Manage profile templates . On the Profile Template Management page, in the Profile Template List section, enable the check box next to CLM Sample Profile Template , and then click Copy a selected profile template .
4	On the Duplicate Profile page, in the Profile Template Name section, in the New Profile Template Name box, type a new Template Name (for e.g. WISeKey Webserver Template), and then click OK . Likewise copy CLM Smart Card Logon Profile Template and create WISeKey Smart Card Template .

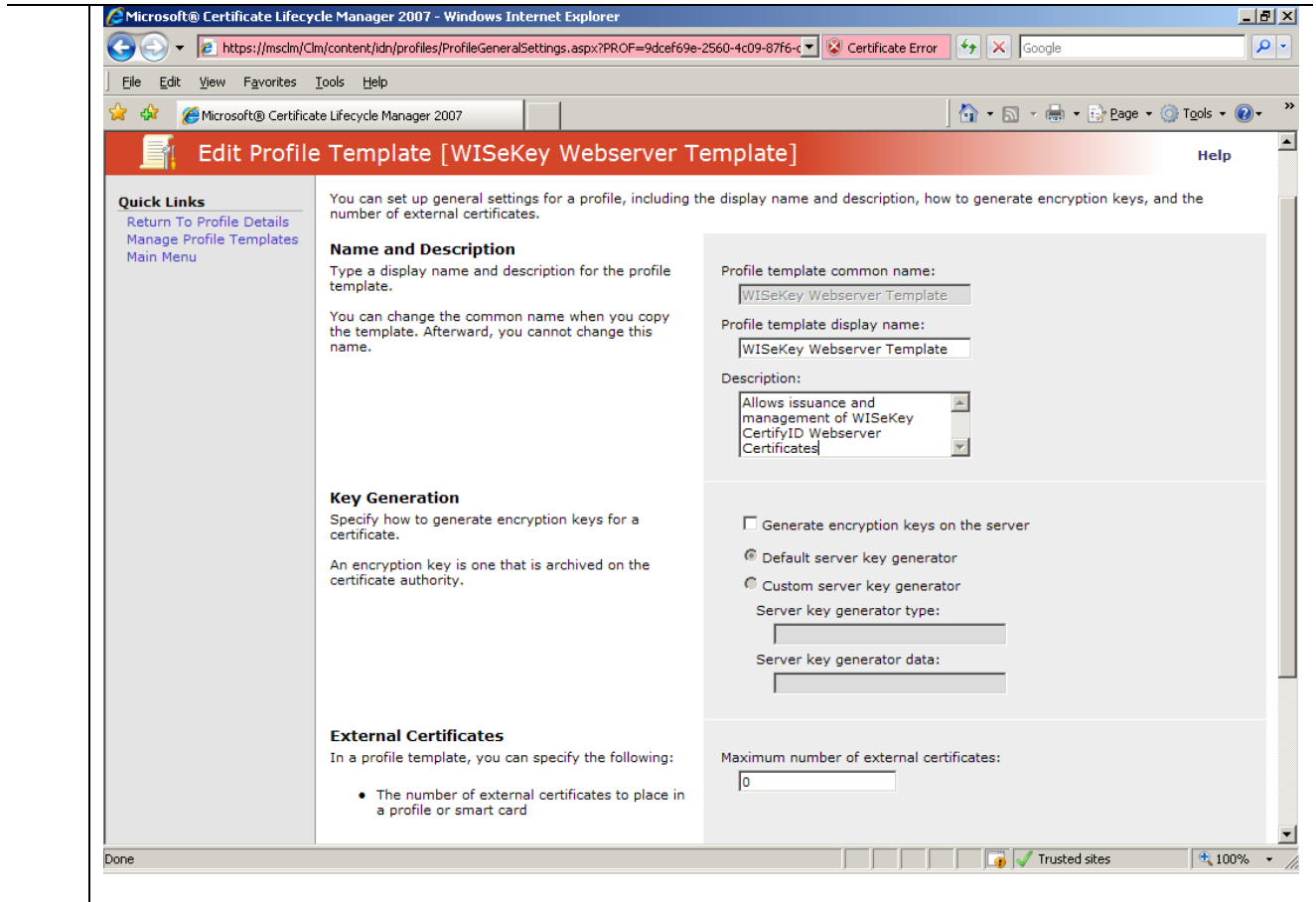


CONFIGURING PROFILE TEMPLATES

For each Profile Template, you must configure a set of **General Settings**, as well as settings for the Certificate Template that is used by the Profile Template.

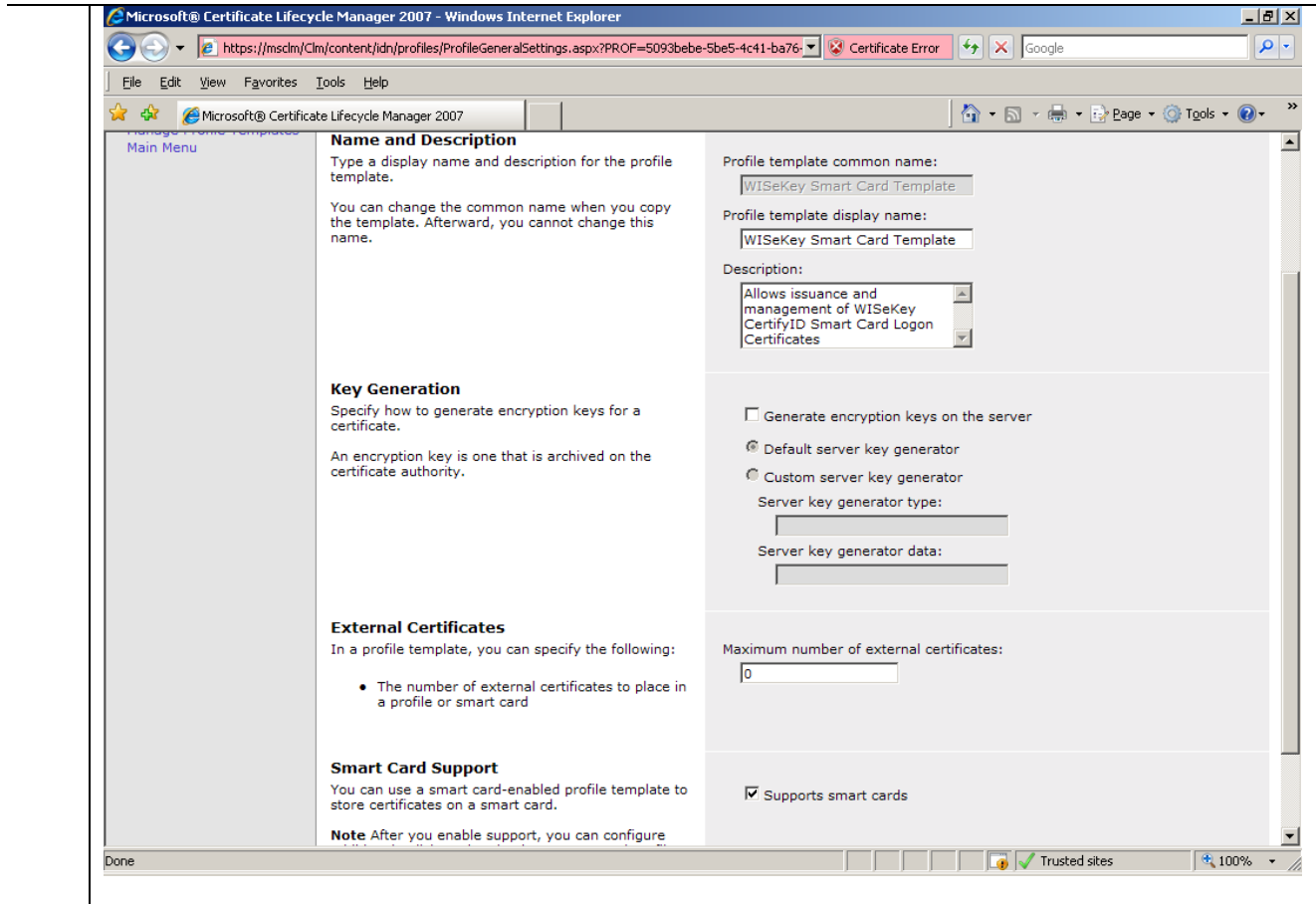
Modifying General Settings for Software Profile Template

Step	Instruction
1	In the CLM Web Portal, in the left-hand pane, in the Select a view section, ensure that Profile Details is selected. On the Edit Profile Template [WISeKey Webserver Template] page, in the General section, click Change general settings .
2	On the Edit Profile Template [WISeKey Webserver Template] page, in the Name and Description section, in the Description box, type Allows issuance and management of WISeKey CertifyID Webserver Certificates . Leave all other settings at their default value, and then at the bottom of the page, click OK .



Modifying General Settings for Smart Card Profile Template

Step	Instruction
1	In the CLM Web Portal, in the left-hand pane, in the Select a view section, ensure that Profile Details is selected. On the Edit Profile Template [for WISeKey Smart Card Template] page, in the General section, click Change general settings .
2	On the Edit Profile Template [WISeKey Smart Card Template] page, in the Name and Description section, in the Description box, type Allows issuance and management of WISeKey CertifyID Smart Card Logon Certificates . Leave all other settings at their default value, and then at the bottom of the page, click OK . Make sure to enable the checkbox Support Smart Cards if it is not enabled.



Modifying the Smart Card Configuration settings

Step	Instruction
1	On the Edit Profile Template [WISeKey Smart Card Logon Template] page, in the Certificate Templates section, click Add new certificate template(s) to profile template .
2	<p>Click Change Settings under Smart Card Configuration of [WISeKey Smart Card Template] page and make changes as under:</p> <ul style="list-style-type: none"> • Select the cryptographic provider from the Provider Name list (for e.g. SafeSign Identity Client) • Enable check boxes : Initialize new card prior to use, Reuse retired card, Use secure key injection, Install certificate authority certificates • Enter value in Administrative PIN length field. Maximum allowed value is 8. • Select User PIN policy as Server distributed. • Enter value in User PIN length field. Maximum allowed value is 8. <p>Leave all other fields with default value and at bottom of the page, click OK.</p>

Microsoft® Certificate Lifecycle Manager 2007 - Windows Internet Explorer

https://msclm/Clm/content/idn/profiles/ProfileSmartCardSettings.aspx?PROF=95dedebe-b44c-4047-a5 Certificate Error Google

File Edit View Favorites Tools Help

Microsoft® Certificate Lifecycle Manager 2007

Quick Links
[Return To Profile Details](#)
[Manage Profile Templates](#)
[Main Menu](#)

You can review and change detailed smart card configuration settings for this profile template

Provider Information
 Select the smart card provider name. This is the friendly name for the provider. The Web.config file defines these settings.

Provider name:
 Provider ID:

Processing
 Configure smart card processing.

Initialize new card prior to use deletes all existing key and certificate information from the card

Reuse retired card allows a previously retired card to be used when a new card is required, potentially for a different user and/or profile template.

Certificate label text can use dynamic data at the time the certificate is processed. You can use the following tags:

- {User}
- {User!attribute}
- {Template!attribute}

where *attribute* is an attribute name in Active Directory and *User* and *Template* are the User and certificate template objects in the directory.

Microsoft Smart Card Base CSP
 Specify the settings you want to use with the Microsoft Smart Card Base Cryptographic Service Provider (CSP).

Initialize new card prior to use
 Reuse retired card
 Use secure key injection
 Install certificate authority certificates

Certificate label text: *

Maximum number of certificates:
 Unlimited
 Set value:

Diversify Admin Key
 Admin key initial value (hex):

Smart Card Initialization Provider

Done

Microsoft® Certificate Lifecycle Manager 2007 - Windows Internet Explorer

https://msclm/Clm/content/idn/profiles/ProfileSmartCardSettings.aspx?PROF=95dedebe-b44c-4047-a5 Certificate Error Google

File Edit View Favorites Tools Help

Microsoft® Certificate Lifecycle Manager 2007

Administrative PINs
 Specify settings you want to use for the administrative Personal Identification Number (PIN).

Note These settings are not applicable when using the Microsoft Smart Card Base CSP.

User PINs
 Select specific details of the user PIN.

Note If you use custom, server-distributed user PIN generation, you must have a fully-qualified .NET assembly type configured in Certificate Lifecycle Manager. When selecting the CustomUserPinGeneration option, the .NET type configured in Web.Config must implement the ICustomUserPinGenerator interface.

Printing
 Specify any card printing options you want to use. The tags you enter are replaced with dynamic information.

Field Mapping Format
 You can use the following tags:

- {User}
- {Manager}
- {Originator}
- {User!attribute}
- {Manager!attribute}
- {Originator!attribute}
- {SCSerialNumber}
- {SCPIN}
- {SCSequence}
- {LongDate}
- {ShortDate}
- {LongTime}

Administrative PIN rollover

Administrative PIN length: Administrative PIN character set:
 Administrative PIN initial value:

User PIN policy:

User PIN length: User PIN character set:

Print smart card

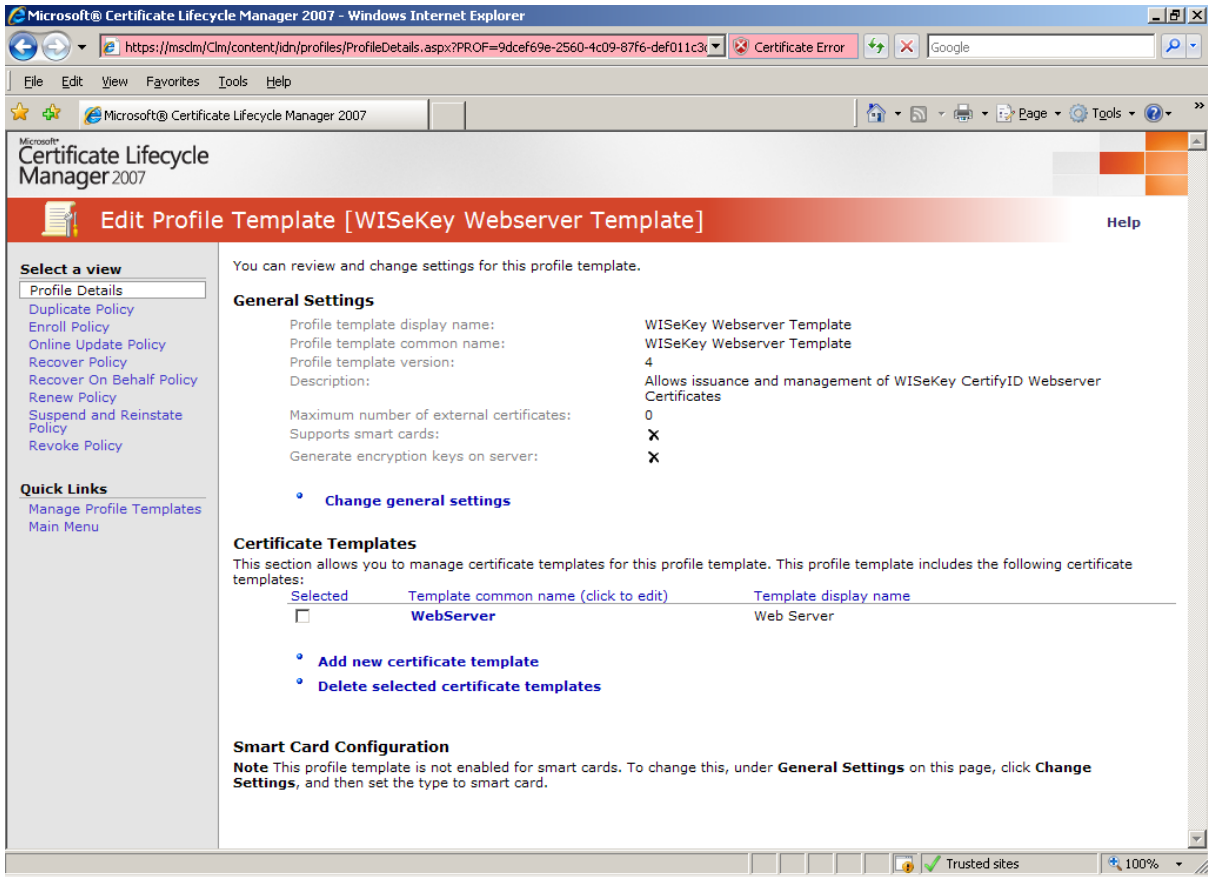
Print project name:

Card name:

Print project field mapping:

Done

Modifying the Certificate Template settings for Software Profile Template

Step	Instruction
1	<p>On the Edit Profile Template [WISeKey Webserver Template] page, in the Certificate Templates section, click Add new certificate template(s) to profile template.</p>
2	<p>Make the following changes on the Edit Profile Template [WISeKey Webserver Template] page:</p> <ul style="list-style-type: none"> • In General Options, enable Allow Raw Request. • In Certificate Authorities, select corresponding Certificate Authority. • In Certificate Templates, enable Web Server. <p>At the bottom of the page, click Add.</p>
3	<p>In the Certificate Templates section, enable the User check box, and then click Delete selected certificate templates. In the Microsoft Internet Explorer dialog box, click OK to delete the selected items.</p>  <p>The screenshot shows the 'Edit Profile Template [WISeKey Webserver Template]' page in Microsoft Internet Explorer. The page title is 'Microsoft Certificate Lifecycle Manager 2007'. The main content area is titled 'Edit Profile Template [WISeKey Webserver Template]'. It contains several sections:</p> <ul style="list-style-type: none"> Select a view: Profile Details, Duplicate Policy, Enroll Policy, Online Update Policy, Recover Policy, Recover On Behalf Policy, Renew Policy, Suspend and Reinststate Policy, Revoke Policy. Quick Links: Manage Profile Templates, Main Menu. General Settings: Profile template display name: WISeKey Webserver Template; Profile template common name: WISeKey Webserver Template; Profile template version: 4; Description: Allows issuance and management of WISeKey CertifyID Webserver Certificates; Maximum number of external certificates: 0; Supports smart cards: X; Generate encryption keys on server: X. Certificate Templates: This section allows you to manage certificate templates for this profile template. It includes a table with the following columns: Selected, Template common name (click to edit), and Template display name. The table contains one entry: 'WebServer' with the 'Selected' checkbox unchecked. Smart Card Configuration: Note: This profile template is not enabled for smart cards. To change this, under General Settings on this page, click Change Settings, and then set the type to smart card.

CONFIGURING THE ENROLL POLICY

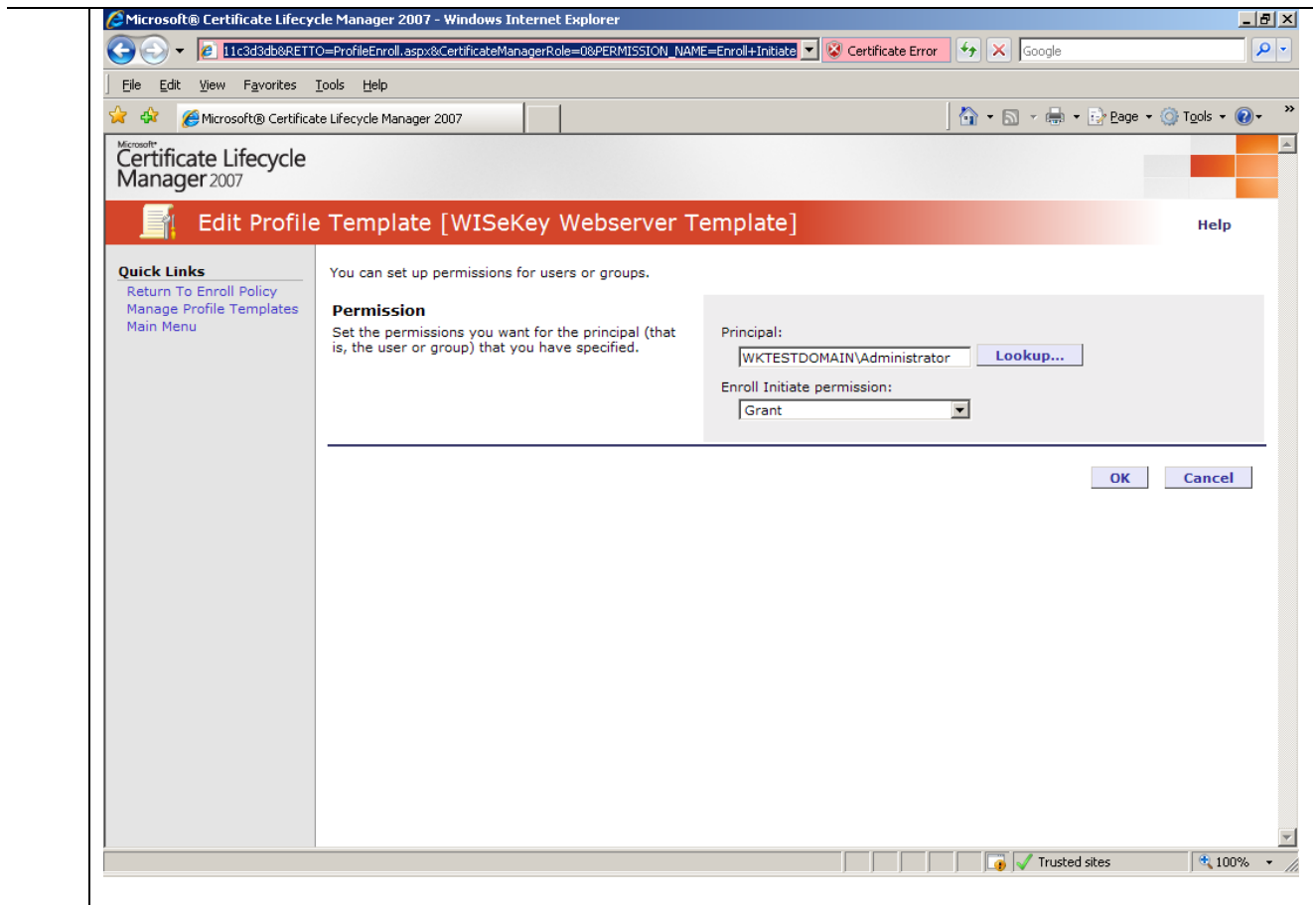
Each Profile Template has a set of management policies that can be configured for it.

Defining the General Workflow Settings

<i>Step</i>	<i>Instruction</i>
1	In the left-hand pane, in the Select a view section, click Enroll Policy .
2	On the Edit Profile Template [WISeKey User Template] page, in the Workflow: General section, click Change general settings .
3	Ensure that the following options are set on the Edit Profile Template [WISeKey User Template] page: <ul style="list-style-type: none"> • Enable policy: Enabled • Use self-server: Enabled • Require enrollment agent: Disabled • All comments to be collected: Disabled • Allow request priority to be collected: Disabled • Default request priority: 0 • Number of approvals: 0 • Number of active or suspended profiles/smart cards allowed: Unlimited

Defining who can initiate Enrollment Request

<i>Step</i>	<i>Instruction</i>
1	In the Workflow: Initiate Enroll Requests section, enable the check box next to NT AUTHORITY/SYSTEM , and the click Delete principal(s) for enroll request initiation .
2	In the Microsoft Internet Explorer dialog box, click OK to confirm the deletion.
3	If you need to add a principal to initiate the request click Add new principal for enroll request initiation . Type the <i>domainname\username</i> in the Principal field. You can search the domain and select the user using Lookup . Select Grant in the Enroll Initiate permission to grant permission to the selected user.



Important: After creating and configuring the profile template, check the Active Directory whether the certificate users have Read and CLM Enroll permissions on the said profile template.

Requesting Web Server Certificates through CLM Website

Before requesting for a certificate through CLM, create the certificate request in PKCS#10 format using the utility available with the web server.

Step	Instruction
1	Login as the user who can enroll for certificate. Open CLM website in Internet Explorer. Click the Microsoft Certificate Lifecycle Manager logo. On the Home page, in the Select a view section, click Manage my info .
2	On the Home page, in the Common Tasks section, click Request a new set of certificates . In the Select a Profile Template section, select WISeKey Webserver Template , and click Next .
3	In the Data Collection section, in Web Server hostname , type ServerName , and then click Next .
4	On the Installing Certificates page, in the Key Generation: Web Server section, in Name , type ServerName , right-click the Raw certificate request text area, and then click Paste . Ensure that the request file contents appear, and the click Next .
5	On the Installing Certificates page, in the Template Common Name (click to download) column, click WebServer . In File Download , click Save . In Save As , in File name , type FileName (for e.g. c:\clmcert), and then click Save . If the Download Complete dialog appears, click Close .
6	On the Installing Certificates page, ensure that the Success column shows as a check mark, and then click Next .

Requesting Smart Card Certificates through CLM Website

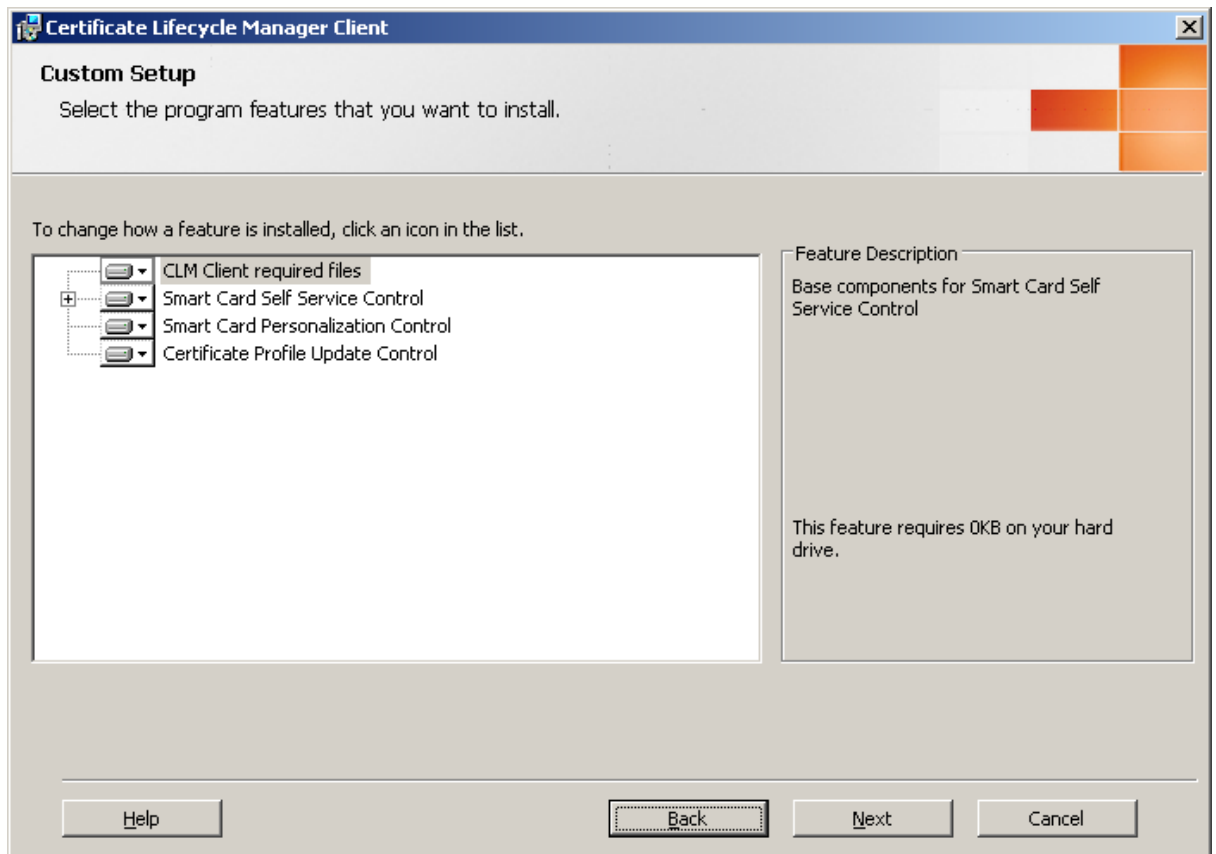
Before requesting for a smart card through CLM, Certificate Life Cycle Manager Client must be installed in the client machine from where the request is generated. The drivers and utilities of smart card also need to be installed prior to requesting the certificate.

Note:

*On each computer where you want to use to access the CLM Web site, you must add the CLM Web site to the Trusted Sites Web content security zone in Internet Explorer. You must enable **Initialize and script ActiveX controls not as marked safe for scripting** in the Custom Level of Trusted Sites so as to avoid prompting at the time requesting certificate.*

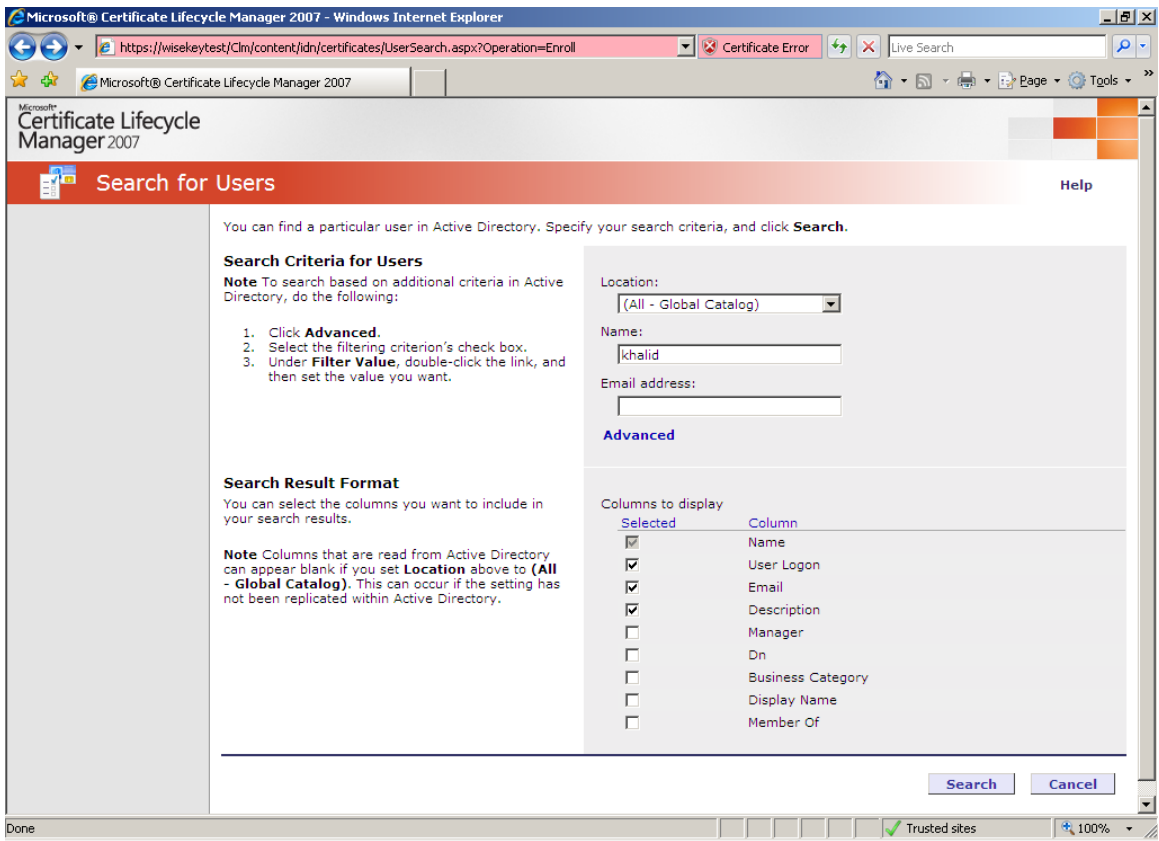
INSTALLING CLM CLIENT

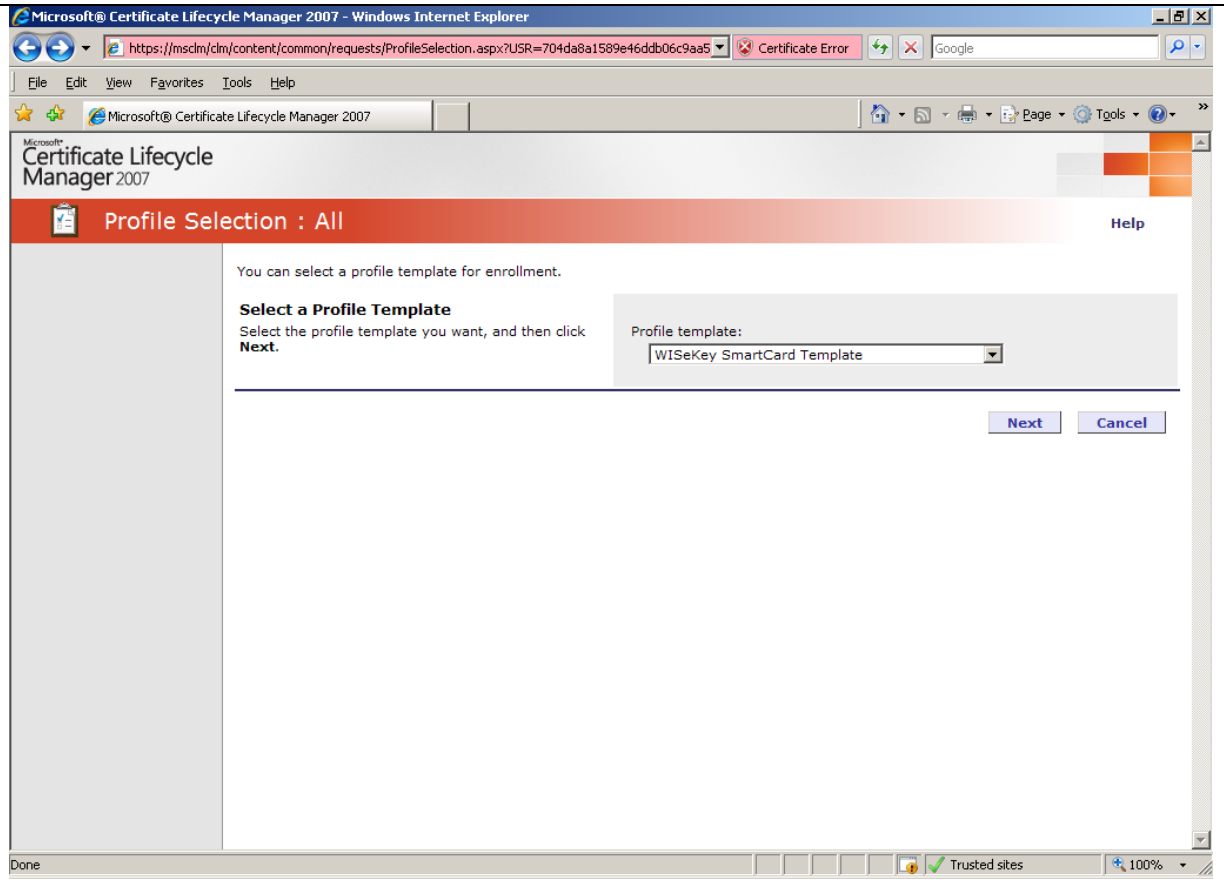
Steps	Instructions
1	From the CLM installation CD, run CLMClient.msi. CLMClient.msi is located at <i>Drive\CLMClient\</i> . <i>Drive</i> is the name of your CD or DVD drive. On the Welcome to the Installation Wizard page, click Next .
2	On the Certificate Lifecycle Manager License Agreement page, read the license terms, select I accept the terms in the license agreement , and then click Next . Enter the product key in the Product Key page and click Next .
3	On the Custom Setup page, verify that all of the available components are selected. To change where you install the files, click Change , choose a different location, and then click OK . The default location is %ProgramFiles%\Microsoft Certificate Lifecycle Manager. On the Custom Setup page, click Next .



5	On the Ready to Install Certificate Lifecycle Manager page, click Install .
6	On the Certificate Lifecycle Manager Installation Complete page, click Finish .

ENROLLING FOR A SMART CARD CERTIFICATE

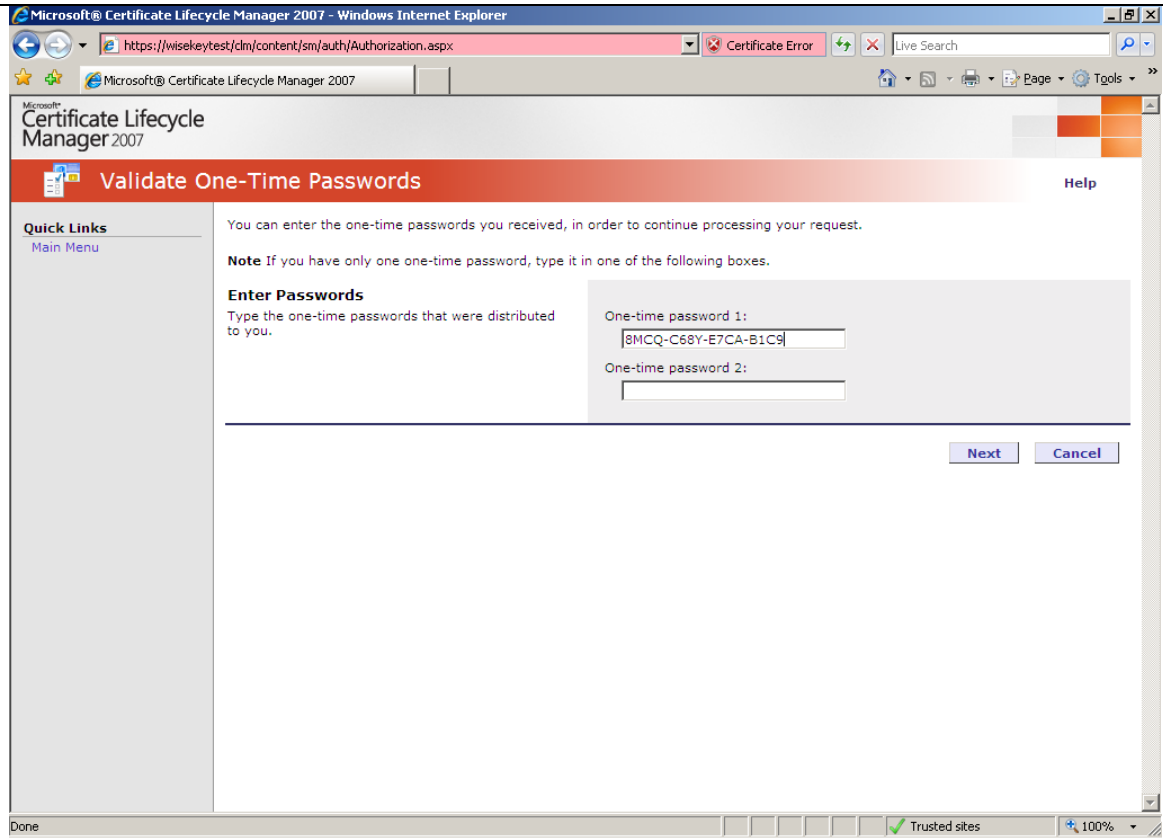
Step	Instruction
1	Login as the user who can enroll for certificate. Open CLM website in Internet Explorer. Click the Microsoft Certificate Lifecycle Manager logo. On the Home page, in the Select a view section, click Manager Operations .
2	On the Home page, in the Common Tasks section, click Enroll a user for new set of certificate or smart card . Search for the user from the domain using either Name or Email address for whom the smart card is issued.
	
3	In the Select a Profile Template section, select WISeKey Smart Card Template , and click Next .



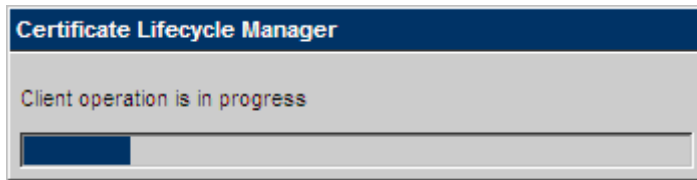
- 4 CLM will generate a one time password for the user. Based on the configuration the one time password will be displayed on the screen or will be sent to the user via email.

EXECUTING THE SMART CARD CERTIFICATE REQUEST

<i>Step</i>	<i>Instruction</i>
1	Login as the user for whom the smart card certificate is requested. Open CLM website in Internet Explorer. Click the Microsoft Certificate Lifecycle Manager logo. On the Home page, click Complete request with one-time passwords .
2	On the Validate One-Time Passwords page, enter the one-time password(s) received by the user in the Enter Passwords field(s) and click Next .



- 3 Keypair will be generated in the card. Make sure you don't remove the card for the reader. Certificate will be generated and stored in the card. Click **OK** to return to home page.



- 4 You can view the certificate and smart card details by clicking the **Show details of my certificate** or **Show details of my smart card** in the home page under section **View My Information**.

The screenshot shows the Microsoft Certificate Lifecycle Manager 2007 web interface in Internet Explorer. The browser address bar shows the URL: https://msclm/Clm/content/sm/certificates/MyUserDetail.aspx. The page title is "Certificate Lifecycle Manager 2007". The main heading is "User Details" with a "Help" link. On the left, there are sections for "Profile Status" (All, New, Assigned, Active, Disabled, Suspended, Retired) and "Quick Links" (Main Menu). The main content area includes:

- Profile Status:** You can review information about your enrolled profiles.
- User Details:** This section contains your information from Active Directory.
 - User name: CN=Khalid Ebadulla
 - E-mail: khalid@wktestdomain.net
 - Account name: WKTESTDOMAIN\khalid
- Smart Card Profiles:** This section contains the smart card profiles that are issued to you. Each smart card profile corresponds to a smart card issued to a user. A card has at least one certificate installed on it.
 - To view details or manage a profile, click the smart card serial number.
 - To view details of a certificate, click the certificate common name.

Legend for Smart Card Profiles:

- = Permanent [primary] card
- = Duplicate card
- = Temporary card

Serial number	Provider	Profile template	Status	Issued
0191126300101F31	A.E.T. Europe B.V.	WISeKey SmartCard Template	Active	8/29/2007 12:48 AM

Common name	Certificate template	Status	Expires
Users Khalid Ebadulla	User	Valid	8/28/2008 12:38 AM

The browser status bar at the bottom shows "Trusted sites" and "100%" zoom level.

Troubleshooting

CertifyID TrustCentre (CertifyID BlackBox)

Please refer to WISEKey's CertifyID BlackBox manual for troubleshooting the CertifyID Certification Authority that you have installed. Further support is available in the support section of WISEKey's web site.

Troubleshooting Microsoft CLM 2007

Please refer to the Microsoft CLM manual for troubleshooting your CLM installation. Further support is available through Microsoft's web site.

Troubleshooting WISEKey Smart Cards, Readers, USB Tokens

Please refer to the respective WISEKey product manual for troubleshooting the smart card, reader, or USB token that you have installed. Further support is available in the support section of WISEKey's web site.