



Windows Server 2008 Active Directory Certificate Services Step-By-Step Guide

Microsoft Corporation

Published: April 2007

Author: Roland Winkler

Editor: Debbie Swanson

Abstract

This step-by-step guide describes the steps needed to set up a basic configuration of Active Directory® Certificate Services (AD CS) in a lab environment.

AD CS in Windows Server® 2008 provides customizable services for creating and managing public key certificates used in software security systems employing public key technologies.



Copyright Information

This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release, and is the confidential and proprietary information of Microsoft Corporation. It is disclosed pursuant to a non-disclosure agreement between the recipient and Microsoft. This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2007 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, MS-DOS, Visual Basic, Visual Studio, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Contents

[Windows Server Active Directory Certificate Services Step-by-Step Guide 5](#_Toc178585789)

[AD CS Technology Review 5](#_Toc178585790)

[Requirements for Using AD CS 6](#_Toc178585791)

[AD CS Basic Lab Scenario 7](#_Toc178585792)

[Steps for Setting up a Basic Lab 7](#_Toc178585793)

[Step 1: Setting Up an Enterprise Root CA 8](#_Toc178585794)

[Step 2: Installing the Online Responder 9](#_Toc178585795)

[Step 3: Configuring the CA to Issue OCSP Response Signing Certificates 9](#_Toc178585796)

[Step 4: Creating a Revocation Configuration 11](#_Toc178585797)

[Step 5: Verifying that the AD CS Lab Setup Functions Properly 12](#_Toc178585798)

[AD CS Advanced Lab Scenario 13](#_Toc178585799)

[Steps for Setting Up an Advanced Lab 14](#_Toc178585800)

[Step 1: Setting Up the Stand-Alone Root CA 15](#_Toc178585801)

[Step 2: Setting Up the Enterprise Subordinate Issuing CA 15](#_Toc178585802)

[Step 3: Installing and Configuring the Online Responder 16](#_Toc178585803)

[Step 4: Configuring the Issuing CA to Issue OCSP Response Signing Certificates 17](#_Toc178585804)

[Step 5: Configuring the Authority Information Access Extension to Support the Online Responder 17](#_Toc178585805)

[Step 6: Assigning the OCSP Response Signing Template to a CA 18](#_Toc178585806)

[Step 7: Enrolling for an OCSP Response Signing Certificate 18](#_Toc178585807)

[Step 8: Creating a Revocation Configuration 19](#_Toc178585808)

[Step 9: Setting Up and Configuring the Network Device Enrollment Service 20](#_Toc178585809)

[Step 10: Verifying that the Advanced AD CS Test Setup Functions Properly 21](#_Toc178585810)

# Windows Server Active Directory Certificate Services Step-by-Step Guide

This step-by-step guide describes the steps needed to set up a basic configuration of Active Directory® Certificate Services (AD CS) in a lab environment.

AD CS in Windows Server® 2008 provides customizable services for creating and managing public key certificates used in software security systems that employ public key technologies.

This document includes:

 A review of AD CS features

 Requirements for using AD CS

 Procedures for a basic lab setup to test AD CS on a minimum number of computers

 Procedures for an advanced lab setup to test AD CS on a larger number of computers to more realistically simulate real-world configurations

## AD CS Technology Review

Using the Active Directory Certificate Services option of the Add Roles Wizard, you can set up the following components of AD CS:

 Certification authorities (CAs). Root and subordinate CAs are used to issue certificates to users, computers, and services, and to manage their validity.

 CA Web enrollment. Web enrollment allows users to connect to a CA by means of a Web browser in order to:

 Request certificates and review certificate requests.

 Retrieve certificate revocation lists (CRLs).

 Perform smart card certificate enrollment.

 Online Responder service. The Online Responder service implements the Online Certificate Status Protocol (OCSP) by decoding revocation status requests for specific certificates, evaluating the status of these certificates, and sending back a signed response containing the requested certificate status information.

Important

Online Responders can be used as an alternative to or an extension of CRLs to provide certificate revocation data to clients. Microsoft Online Responders are based on and comply with RFC 2560 for OCSP. For more information about RFC 2560, see the Internet Engineering Task Force Web site (<http://go.microsoft.com/fwlink/?LinkID=67082>).

 Network Device Enrollment Service. The Network Device Enrollment Service allows routers and other network devices to obtain certificates based on the Simple Certificate Enrollment Protocol (SCEP) from Cisco Systems Inc.

Note

SCEP was developed to support the secure, scalable issuance of certificates to network devices by using existing CAs. The protocol supports CA and registration authority public key distribution, certificate enrollment, certificate revocation, certificate queries, and certificate revocation queries.

## Requirements for Using AD CS

CAs can be set up on servers running a variety of operating systems, including Windows® 2000 Server, Windows Server® 2003, and Windows Server 2008. However, not all operating systems support all features or design requirements, and creating an optimal design requires careful planning and lab testing before you deploy AD CS in a production environment. Although you can deploy AD CS with as little hardware as a single server for a single CA, many deployments involve multiple servers configured as root, policy, and issuing CAs, and other servers configured as Online Responders.

Note

A limited set of server roles is available for a Server Core installation of Windows Server 2008 and for Windows Server 2008 for Itanium-based Systems.

The following table lists the AD CS components that can be configured on different editions of Windows Server 2008.

| **Components** | **Web** | **Standard** | **Enterprise** | **Datacenter** |
| --- | --- | --- | --- | --- |
| CA | No | Yes | Yes | Yes |
| Network Device Enrollment Service | No | No | Yes | Yes |
| Online Responder service | No | No | Yes | Yes |

The following features are available on servers running Windows Server 2008 that have been configured as CAs.

| **AD CS features** | **Web** | **Standard** | **Enterprise** | **Datacenter** |
| --- | --- | --- | --- | --- |
| Version 2 and version 3 certificate templates | No | No | Yes | Yes |
| Key archival | No | No | Yes | Yes |
| Role separation | No | No | Yes | Yes |
| Certificate Manager restrictions | No | No | Yes | Yes |
| Delegated enrollment agent restrictions | No | No | Yes | Yes |

## AD CS Basic Lab Scenario

The following sections describe how you can set up a lab to begin evaluating AD CS.

We recommend that you first use the steps provided in this guide in a test lab environment. Step-by-step guides are not necessarily meant to be used to deploy Windows Server features without accompanying documentation and should be used with discretion as a stand-alone document.

## Steps for Setting up a Basic Lab

You can begin testing many features of AD CS in a lab environment by using as few as two servers running Windows Server 2008 and one client computer running Windows Vista®. The computers for this guide are named as follows:

 LH\_DC1: This computer will be the domain controller for your test environment.

 LH\_PKI1: This computer will host an enterprise root CA for the test environment. This CA will issue client certificates for the Online Responder and client computers.

Note

Enterprise CAs and Online Responders can only be installed on servers running Windows Server 2008 Enterprise or Windows Server 2008 Datacenter.

 LH\_CLI1: This client computer running Windows Vista will autoenroll for certificates from LH\_PKI1 and verify certificate status from LH\_ PKI1.

To configure the basic lab setup for AD CS, you need to complete the following prerequisite steps:

 Set up a domain controller on LH\_DC1 for contoso.com, including some organizational units (OUs) to contain one or more users for the client computer, client computers in the domain, and for the servers hosting CAs and Online Responders.

 Install Windows Server 2008 on LH\_PKI1, and join LH\_PKI1 to the domain.

 Install Windows Vista on LH\_CLI1, and join LH\_CLI1 to contoso.com.

After you have completed these preliminary setup procedures, you can begin to complete the following steps:

[Step 1: Setting Up an Enterprise Root CA](#DSDOC_BKMK_AS1f7dfccc0_4f65_4d6f_a801_ae)

[Step 2: Installing the Online Responder](#DSDOC_BKMK_AS2f7dfccc0_4f65_4d6f_a801_ae)

[Step 3: Configuring the CA to Issue OCSP Response Signing Certificates](#DSDOC_BKMK_AS3f7dfccc0_4f65_4d6f_a801_ae)

[Step 4: Creating a Revocation Configuration](#DSDOC_BKMK_AS4f7dfccc0_4f65_4d6f_a801_ae)

[Step 5: Verifying that the AD CS Lab Setup Functions Properly](#DSDOC_BKMK_AS5f7dfccc0_4f65_4d6f_a801_ae)

### Step 1: Setting Up an Enterprise Root CA

An enterprise root CA is the anchor of trust for the basic lab setup. It will be used to issue certificates to the Online Responder and client computer, and to publish certificate information to Active Directory Domain Services (AD DS).

Note

Enterprise CAs and Online Responders can only be installed on servers running Windows Server 2008 Enterprise or Windows Server 2008 Datacenter.

To set up an enterprise root CA

|  |
| --- |
| 1. Log on to LH\_PKI1 as a domain administrator.  2. Click Start, point to Administrative Tools,and then click Server Manager.  3. In the Roles Summary section, click Add roles.  4. On the Select Server Roles page, select the Active Directory Certificate Services check box. Click Nexttwo times.  5. On the Select Role Services page, select the Certification Authority check box,andthen click Next.  6. On the Specify Setup Type page, click Enterprise,and then click Next.  7. On the Specify CA Type page, click Root CA, and then click Next.  8. On the Set Up Private Key and Configure Cryptography for CA pages, you can configure optional configuration settings, including cryptographic service providers. However, for basic testing purposes, accept the default values by clicking Next twice.  9. In the Common name for this CA box, type the common name of the CA, RootCA1, and then click Next.  10. On the Set the Certificate Validity Period page, accept the default validity duration for the root CA, and then click Next.  11. On the Configure Certificate Database page, accept the default values or specify other storage locations for the certificate database and the certificate database log, and then click Next.  12. After verifying the information on the Confirm Installation Options page, click Install.  13. Review the information on the confirmation screen to verify that the installation was successful. |

### Step 2: Installing the Online Responder

An Online Responder can be installed on any computer running Windows Server 2008 Enterprise or Windows Server 2008 Datacenter. The certificate revocation data can come from a CA on a computer running Windows Server 2008, a CA on a computer running Windows Server 2003, or from a non-Microsoft CA.

Note

IIS must also be installed on this computer before the Online Responder can be installed.

To install the Online Responder

|  |
| --- |
| 1. Log on to LH\_PKI1 as a domain administrator.  2. Click Start, point to Administrative Tools,and then click Server Manager.  3. Click Manage Roles. In the Active Directory Certificate Services section, click Add role services.  4. On the Select Role Services page, select the Online Responder check box.  You are prompted to install IIS and Windows Activation Service.  5. Click Add Required Role Services, and then click Next three times.  6. On the Confirm Installation Options page, click Install.  7. When the installation is complete, review the status page to verify that the installation was successful. |

### Step 3: Configuring the CA to Issue OCSP Response Signing Certificates

Configuring a CA to support Online Responder services involves configuring certificate templates and issuance properties for OCSP Response Signing certificates and then completing additional steps on the CA to support the Online Responder and certificate issuance.

Note

These certificate template and autoenrollment steps can also be used to configure certificates that you want to issue to a client computer or client computer users.

To configure certificate templates for your test environment

|  |
| --- |
| 1. Log on to LH\_PKI1 as a CA administrator.  2. Open the Certificate Templates snap-in.  3. Right-click the OCSP Response Signing template, and then click Duplicate Template.  4. Type a new name for the duplicated template, such as OCSP Response Signing\_2.  5. Right-click the OCSP Response Signing\_2 certificate template, and then click Properties.  6. Click the Security tab. Under Group or user name, click Add, and then type the name or browse to select the computer hosting the Online Responder service.  7. Click the computer name, LH\_PKI1, and in the Permissions dialog box, select the Read and Autoenroll check boxes.  8. While you have the Certificate Templates snap-in open, you can configure certificate templates for users and computers by substituting the desired templates in step 3, and repeating steps 4 through 7 to configure permissions for LH\_CLI1 and your test user accounts. |

To configure the CA to support Online Responders, you need to use the Certification Authority snap-in to complete two key steps:

 Add the location of the Online Responder to the authority information access extension of issued certificates.

 Enable the certificate templates that you configured in the previous procedure for the CA.

To configure a CA to support the Online Responder service

|  |
| --- |
| 1. Open the Certification Authority snap-in.  2. In the console tree, click the name of the CA.  3. On the Action menu, click Properties.  4. Click the Extensions tab. In the Select extension list, click Authority Information Access (AIA).  5. Select the Include in the AIA extension of issue certificates and Include in the online certificate status protocol (OCSP) extension check boxes.  6. Specify the locations from which users can obtain certificate revocation data; for this setup, the location is http://LH\_PKI1/ocsp.  7. In the console tree of the Certification Authority snap-in, right-click Certificate Templates, and then click New Certificate Templates to Issue.  8. In Enable Certificate Templates, select the OCSP Response Signing template and any other certificate templates that you configured previously, and then click OK.  9. Open Certificate Templates, and verify that the modified certificate templates appear in the list. |

### Step 4: Creating a Revocation Configuration

A revocation configuration includes all of the settings that are needed to respond to status requests regarding certificates that have been issued by using a specific CA key.

These configuration settings include the CA certificate, the signing certificate for the Online Responder, and the locations to which clients are directed to send their status requests.

Important

Before you create a revocation configuration, ensure that certificate enrollment has taken place so that a signing certificate exists on the computer and adjust the permissions on the signing certificate to allow the Online Responder to use it.

To verify that the signing certificate is properly configured

|  |
| --- |
| 1. Start or restart LH\_PKI1 to enroll for certificates.  2. Log on as a CA administrator.  3. Open the Certificates snap-in for the computer account. Open the Personal certificate store for the computer, and verify that it contains a certificate titled OCSP Response Signing.  4. Right-click this certificate, and then click Manage Private Keys.  5. Click the Security tab. In the User Group or user name dialog box, click Add, enter Network Service to the Group or user name list, and then click OK.  6. Click Network Service, and in the Permissions dialog box, select the Full Control check box.  7. Click OK twice. |

Creating a revocation configuration involves the following tasks:

 Identify the CA certificate for the CA that supports the Online Responder.

 Identify the CRL distribution point for the CA.

 Select a signing certificate that will be used to sign revocation status responses.

 Select a revocation provider, the component responsible for retrieving and caching the revocation information used by the Online Responder.

To create a revocation configuration

|  |
| --- |
| 1. Open the Online Responder snap-in.  2. In the Actions pane, click Add Revocation Configuration to start the Add Revocation Configurationwizard, and then click Next.  3. On the Name the Revocation Configuration page, type a name for the revocation configuration, such as LH\_RC1, and then click Next.  4. On the Select CA certificate Location page, click Select a certificate from an existing enterprise CA, and then click Next.  5. On the following page, the name of the CA, LH\_PKI1, should appear in the Browse CA certificates published in Active Directory box.   If it appears, click the name of the CA that you want to associate with your revocation configuration, and then click Next.   If it does not appear, click Browse for CA Computer and type the name of the computer hosting LH\_PKI1 or click Browse to locate this computer. When you have located the computer, click Next.  Note  You might also be able to link to the CA certificate from the local certificate store, or by importing it from removable media in step 4.  6. View the certificate and copy the CRL distribution point for the parent root CA, RootCA1. To do this:  a. Open the Certificate Services snap-in. Select an issued certificate.  b. Double-click the certificate, and then click the Details tab.  c. Scroll down and select the CRL Distribution Points field.  d. Select and copy the URL for the CRL distribution point that you want to use.  e. Click OK.  7. On the Select Signing Certificate page, accept the default option, Automatically select signing certificate, and then click Next.  8. On the Revocation Provider page, click Provider.  9. On the Revocation Provider Properties page, click Add, enter the URL of the CRL distribution point, and then click OK.  10. Click Finish.  11. Using the Online Responder snap-in, select the revocation configuration, and then examine the status information to verify that it is functioning properly. You should also be able to examine the properties of the signing certificate to verify that the Online Responder is configured properly. |

### Step 5: Verifying that the AD CS Lab Setup Functions Properly

You can verify the setup steps described previously as you perform them.

After the installation is complete, you should verify that your basic test setup is functioning properly by confirming that you can autoenroll certificates, revoke certificates, and make accurate revocation data available from the Onlline responder.

To verify that the AD CS test setup functions properly

|  |
| --- |
| 1. On the CA, configure several certificate templates to autoenroll certificates for LH\_CLI1 and users on this computer.  2. When information about the new certificates has been published to AD DS, open a command prompt on the client computer and enter the following command to start certificate autoenrollment:  certutil -pulse  3. On LH\_CLI1, use the Certificates snap-in to verify that the certificates have been issued to the user and to the computer, as appropriate.  4. On the CA, use the Certification Authority snap-in to view and revoke one or more of the issued certificates by clicking Certification Authority (Computer)/CA name/Issued Certificates and selecting the certificate you want to revoke. On the Action menu, point to All Tasks, and then click Revoke Certificate. Select the reason for revoking the certificate, and click Yes.  5. In the Certification Authority snap-in, publish a new CRL by clicking Certification Authority (Computer)/CA name/Revoked Certificates in the console tree. Then, on the Action menu, point to All Tasks, and click Publish.  6. Remove all CRL distribution point extensions from the issuing CA by opening the Certification Authority snap-in and then selecting the CA. On the Action menu, click Properties.  7. On the Extensions tab, confirm that Select extension is set to CRL Distribution Point (CDP).  8. Click any CRL distribution points that are listed, click Remove, and then click OK.  9. Stop and restart AD CS.  10. Repeat steps 1 and 2 above, and then verify that clients can still obtain revocation data. To do this, use the Certificates snap-in to export the certificate to a file (\*.cer). At a command prompt, type:  certutil -url <exportedcert.cer>  11. In the Verify and Retrieve dialog box that appears, click From CDP and From OCSP and compare the results. |

## AD CS Advanced Lab Scenario

The following sections describe how you can set up a lab to evaluate more features of AD CS than in the basic lab setup.

## Steps for Setting Up an Advanced Lab

To test additional features of AD CS in a lab environment, you will need five computers running Windows Server 2008 and one client computer running Windows Vista. The computers for this guide are named as follows:

 LH\_DC1: This computer will be the domain controller for your test environment.

 LH\_CA\_ROOT1: This computer will host a stand-alone root CA for the test environment.

 LH\_CA\_ISSUE1: This enterprise CA will be subordinate to LH\_CA\_ROOT1 and issue client certificates for the Online Responder and client computers.

Note

Enterprise CAs and Online Responders can only be installed on servers running Windows Server 2008 Enterprise or Windows Server 2008 Datacenter.

 LH\_ORS1. This server will host the Online Responder.

 LH\_NDES. This server will host the Network Device Enrollment Servicethat makes it possible to issue and manage certificates for routers and other network devices.

 LH\_CLI1: This client computer running Windows Vista will autoenroll for certificates from LH\_CA\_ISSUE1 and verify certificate status from LH\_ORS1.

To configure the advanced lab setup for AD CS, you need to complete the following prerequisite steps:

1. Set up a domain controller on LH\_DC1 for contoso.com, including some OUs to contain one or more users for LH\_CLI1, client computers in the domain, and for the servers hosting CAs and Online Responders.

2. Install Windows Server 2008 on the other servers in the test configuration and join them to the domain.

3. Install Windows Vista on LH\_CLI1, and join LH\_CLI1 to contoso.com.

After you have completed these preliminary setup procedures, you can begin to complete the following steps:

[Step 1: Setting Up the Stand-Alone Root CA](#DSDOC_BKMK_BS1f7dfccc0_4f65_4d6f_a801_ae)

[Step 2: Setting Up the Enterprise Subordinate Issuing CA](#DSDOC_BKMK_BS2f7dfccc0_4f65_4d6f_a801_ae)

[Step 3: Installing and Configuring the Online Responder](#DSDOC_BKMK_BS3f7dfccc0_4f65_4d6f_a801_ae)

[Step 4: Configuring the Issuing CA to Issue OCSP Response Signing Certificates](#DSDOC_BKMK_BS4f7dfccc0_4f65_4d6f_a801_ae)

[Step 5: Configuring the Authority Information Access Extension to Support the Online Responder](#DSDOC_BKMK_BS5f7dfccc0_4f65_4d6f_a801_ae)

[Step 6: Assigning the OCSP Response Signing Template to a CA](#DSDOC_BKMK_BS6f7dfccc0_4f65_4d6f_a801_ae)

[Step 7: Enrolling for an OCSP Response Signing Certificate](#DSDOC_BKMK_BS7f7dfccc0_4f65_4d6f_a801_ae)

[Step 8: Creating a Revocation Configuration](#DSDOC_BKMK_BS8f7dfccc0_4f65_4d6f_a801_ae)

[Step 9: Setting Up and Configuring the Network Device Enrollment Service](#DSDOC_BKMK_BS9f7dfccc0_4f65_4d6f_a801_ae)

[Step 10: Verifying that the Advanced AD CS Test Setup Functions Properly](#DSDOC_BKMK_BS10f7dfccc0_4f65_4d6f_a801_a)

### Step 1: Setting Up the Stand-Alone Root CA

A stand-alone root CA is the anchor of trust for the basic lab setup. It will be used to issue certificates to the subordinate issuing CA. Because it is critical to the security of the public key infrastructure (PKI), this CA is online in many PKIs only when needed to issue certificates to subordinate CAs.

To set up a stand-alone root CA

|  |
| --- |
| 1. Log on to LH\_CA\_ROOT1 as an administrator.  2. Start the Add RolesWizard. On the Select Server Roles page, select the Active Directory Certificate Services check box, and then click Next two times.  3. On the Select Role Services page, select the Certification Authority check box, and then click Next.  4. On the Specify Setup Type page, click Standalone, and then click Next.  5. On the Specify CA Type page, click Root CA, and then click Next.  6. On the Set Up Private Key and Configure Cryptography for CA pages, you can configure optional settings, including cryptographic service providers. However, for basic testing purposes, accept the default values by clicking Next twice.  7. In the Common name for this CA box, type the common name of the CA, RootCA1, and then click Next.  8. On the Set the Certificate Validity Period page, accept the default validity duration for the root CA, and then click Next.  9. On the Configure Certificate Database page, accept the default values or specify other storage locations for the certificate database and the certificate database log, and then click Next.  10. After verifying the information on the Confirm Installation Options page, click Install. |

### Step 2: Setting Up the Enterprise Subordinate Issuing CA

Most organizations use at least one subordinate CA to protect the root CA from unnecessary exposure. An enterprise CA also allows you to use certificate templates and to use AD DS for enrollment and publishing certificates.

To set up an enterprise subordinate issuing CA

|  |
| --- |
| 1. Log on to LH\_CA\_ISSUE1 as a domain administrator.  2. Start the Add RolesWizard. On the Select Server Roles page, select the Active Directory Certificate Services check box, and then click Nexttwo times.  3. On the Select Role Services page, select the Certification Authority check box, and then click Next.  4. On the Specify Setup Type page, click Enterprise, and then click Next.  5. On the Specify CA Type page, click Subordinate CA, and then click Next.  6. On the Set Up Private Key and Configure Cryptography for CA pages, you can configure optional settings, including cryptographic service providers. However, for basic testing purposes, accept the default values by clicking Next twice.  7. On the Request Certificate page, browse to locate LH\_CA\_ROOT1, or if, the root CA is not connected to the network, save the certificate request to a file so that it can be processed later. Click Next.  The subordinate CA setup will not be usable until it has been issued a root CA certificate and this certificate has been used to complete the installation of the subordinate CA.  8. In the Common name for this CA box, type the common name of the CA, LH\_CA\_ISSUE1.  9. On the Set the Certificate Validity Period page, accept the default validity duration for the CA, and then click Next.  10. On the Configure Certificate Database page, accept the default values or specify other storage locations for the certificate database and the certificate database log, and then click Next.  11. After verifying the information on the Confirm Installation Options page, click Install. |

### Step 3: Installing and Configuring the Online Responder

An Online Responder can be installed on any computer running Windows Server 2008 Enterprise or Windows Server 2008 Datacenter. The certificate revocation data can come from a CA on a computer running Windows Server 2008, a CA on a computer running Windows Server 2003, or from a non-Microsoft CA. An Online Responder will typically not be installed on the same computer as a CA.

Note

IIS must also be installed on this computer before the Online Responder can be installed. As part of the setup process a virtual directory named OCSP is created in IIS and the Web proxy is registered as an Internet Server Application Programming Interface (ISAPI) extension.

To install the Online Responder service

|  |
| --- |
| 1. Log on to LH\_ORS1 as an administrator.  2. Start the Add Roles Wizard. On the Select Server Rolespage, select the Active DirectoryCertificate Services check box, and then click Next two times.  3. On the Select Role Services page, clear the Certification Authority check box, select the Online Responder check box, and then click Next.  You are prompted to install IIS and Windows Activation Service.  4. Click Add Required Role Services, and then click Next three times.  5. On the Confirm Installation Options page, click Install.  6. When the installation is complete, review the status page to verify that the installation was successful. |

### Step 4: Configuring the Issuing CA to Issue OCSP Response Signing Certificates

As with any certificate template, the OCSP Response Signing template must be configured with the enrollment permissions for Read, Enroll, Autoenroll, and Write before any certificates can be issued based on the template.

To configure certificate templates for your test environment

|  |
| --- |
| 1. Log on to LH\_CA\_ISSUE1 as a CA administrator.  2. Open the Certificate Templates snap-in.  3. Right-click the OCSP Response Signing template, and then click Duplicate Template.  4. Type a new name for the duplicated template, such as OCSP Response Signing\_2.  5. Right-click the OCSP Response Signing\_2 certificate template, and then click Properties.  6. Click the Security tab. Under Group or user name, click Add and type the name or browse to select the computer hosting the Online Responder service.  7. Click the computer name, LH\_ORS1, and in the Permissions dialog box, select the Read and Autoenroll check boxes.  8. While you have the Certificate Templates snap-in open, you can configure certificate templates for users and computers by substituting the desired templates in step 3, and repeating steps 4 through 7 to configure permissions for LH\_CLI1 and your test user accounts. |

### Step 5: Configuring the Authority Information Access Extension to Support the Online Responder

You need to configure the CAs to include the URL for the Online Responder as part of the authority information access extension of the issued certificate. This URL is used by the Online Responder client to validate the certificate status.

To configure the authority information access extension to support the Online Responder

|  |
| --- |
| 1. Log on to LH\_CA\_ISSUE1 as a CA administrator.  2. Open the Certification Authority snap-in.  3. In the console tree, click the name of the CA.  4. On the Action menu, click Properties.  5. On the Extensions tab, click Select extension, and then click Authority Information Access (AIA).  6. Select the Include in the AIA extension of issue certificates and Include in the online certificate status protocol (OCSP) extension check boxes.  7. Specify the locations from which users can obtain certificate revocation data; for this setup, the location is http://LH\_ORS1/ocsp.  8. In the console tree of the Certification Authority snap-in, right-click Certificate Templates, and then click New Certificate Templates to Issue.  9. In Enable Certificate Templates, select the OCSP Response Signing template and any other certificate templates that you configured previously, and then click OK.  10. Open Certificate Templates, and verify that the modified certificate templates appear in the list. |

### Step 6: Assigning the OCSP Response Signing Template to a CA

Once the templates are properly configured, the CA needs to be configured to issue that template.

To configure the CA to issue certificates based on the newly created OCSP Response Signing template

|  |
| --- |
| 1. Open the Certification Authority snap-in.  2. Right-click Certificate Templates, and then click Certificate Template to Issue.  3. Select the OCSP Response Signing\_2 template from the list of available templates, and then click OK. |

### Step 7: Enrolling for an OCSP Response Signing Certificate

Enrollment might not take place right away. Therefore, before you proceed to the next step, confirm that certificate enrollment has taken place so that a signing certificate exists on the computer, and verify that the permissions on the signing certificate allow the Online Responder to use it.

To verify that the signing certificate is properly configured

|  |
| --- |
| 1. Start or restart LH\_ORS1 to enroll for the certificates.  2. Log on as a CA administrator.  3. Open the Certificates snap-in for the computer. Open the Personal certificate store for the computer, and then verify that it contains a certificate titled OCSP Response Signing\_2.  4. Right-click this certificate, and then click Manage Private Keys.  5. Click the Security tab. In the User Group or user name dialog box, click Add to type in and add Network Service to the Group or user name list, and then click OK.  6. Click Network Service, and in the Permissions dialog box, select the Full Control check box. Click OK twice. |

### Step 8: Creating a Revocation Configuration

Creating a revocation configuration involves the following tasks:

 Identify the CA certificate for the CA that supports the Online Responder.

 Identify the CRL distribution point for the CA.

 Select a signing certificate that will be used to sign revocation status responses.

 Select a revocation provider, the component responsible for retrieving and caching the revocation information used by the Online Responder.

To create a revocation configuration

|  |
| --- |
| 1. Log on to LH\_ORS1 as a domain administrator.  2. Open the Online Responder snap-in.  3. In the Actions pane, click Add Revocation Configuration to start the Add Revocation Configuration wizard, and then click Next.  4. On the Name the Revocation Configuration page, type a name for the revocation configuration, such as LH\_RC1, and then click Next.  5. On the Select CA Certificate Location page, click Select a certificate for an existing enterprise CA, and then click Next.  6. On the following page, the name of the CA, LH\_CA\_ISSUE1, should appear in the Browse CA certificates published in Active Directory box.   If it appears, click the name of the CA that you want to associate with your revocation configuration, and then click Next.   If it does not appear, click Browse for CA Computer and type the name of the computer hosting LH\_CA\_ISSUE1 or click Browse to locate this computer. When you have located the computer, click Next.  Note  You might also be able to link to the CA certificate from the local certificate store, or by importing it from removable media in step 5.  7. View the certificate and copy the CRL distribution point for the parent root CA, RootCA1. To do this:  a. Open the Certificate Services snap-in, and then select an issued certificate.  b. Double-click the certificate, and then click the Details tab.  c. Scroll down and select the CRL Distribution Points field.  d. Select and copy the URL for the CRL distribution point that you want to use.  e. Click OK.  8. On the Select Signing Certificate page, accept the default, Automatically select signing certificate, and then click Next.  9. On the Revocation Provider page, click Provider.  10. On the Revocation Provider Properties page, click Add, enter the URL of the CRL distribution point, and then click OK.  11. Click Finish.  12. Using the Online Responder snap-in, select the revocation configuration, and then examine the status information to verify that it is functioning properly. You should also be able to examine the properties of the signing certificate to verify that the Online Responder is configured properly. |

### Step 9: Setting Up and Configuring the Network Device Enrollment Service

The Network Device Enrollment Service allows software on routers and other network devices running without domain credentials to obtain certificates.

The Network Device Enrollment Service operates as an ISAPI filter on IIS that performs the following functions:

 Generates and provides one-time enrollment passwords to administrators

 Processes SCEP enrollment requests

 Retrieves pending requests from the CA

SCEP was developed as an extension to existing HTTP, PKCS #10, PKCS #7, RFC 2459, and other standards to enable network device and application certificate enrollment with CAs. SCEP is identified and documented on the Internet Engineering Task Force Web site (<http://go.microsoft.com/fwlink/?LinkId=71055>).

Before you begin this procedure, create a user ndes\_user1 and add this user to the IIS user group. Then, use the Certificate Templates snap-in to configure Read and Enroll permissions for this user on the IPSEC (Offline Request) certificate template.

To set up and configure the Network Device Enrollment Service

|  |
| --- |
| 1. Log on to LH\_NDES as an enterprise administrator.  2. Start the Add RolesWizard. On the Select Server Roles page, select the Active Directory Certificate Services check box, and then click Next two times.  3. On the Select Role Services page, clear the Certification Authority check box, and then select Network Device Enrollment Service.  You are prompted to install IIS and Windows Activation Service.  4. Click Add Required Role Services, and then click Next three times.  5. On the Confirm Installation Options page, click Install.  6. When the installation is complete, review the status page to verify that the installation was successful.  7. Because this is a new installation and there are no pending SCEP certificate requests, click Replace existing Registration Authority (RA) certificates, and then click Next.  When the Network Device Enrollment Service is installed on a computer where a registration authority already exists, the existing registration authority and any pending certificate requests are deleted.  8. On the Specify User Account page, click Select User, and type the user name ndes\_user1 and password for this account, which the Network Device Enrollment Service will use to authorize certificate requests. Click OK, and then click Next.  9. On the Specify CA page, select either the CA name or Computer name check box, click Browse to locate the CA that will issue the Network Device Enrollment Service certificates, LH\_CA\_ISSUE1, and then click Next.  10. On the Specify Registry Authority Information page, type ndes\_1 in the RA name box. Under Country/region,select the check box for the country/region you are in, and then click Next.  11. On the Configure Cryptography page, accept the default values for the signature and encryption keys, and then click Next.  12. Review the summary of configuration options, and then click Install. |

### Step 10: Verifying that the Advanced AD CS Test Setup Functions Properly

You can verify the setup steps described previously as you perform them.

After the installation is complete, you should verify that your advanced test setup is functioning properly.

To verify that the advanced AD CS test setup functions properly

|  |
| --- |
| 1. On the CA, configure several certificate templates to autoenroll certificates for LH\_CLI1 and users on this computer.  2. When information about the new certificates has been published to AD DS, open a command prompt on the client computer and enter the following command to start certificate autoenrollment:  certutil -pulse  3. On the client computer, use the Certificates snap-in to verify that the certificates have been issued to the user and to the computer, as appropriate.  4. On the CA, use the Certification Authority snap-in to view and revoke one or more of the issued certificates by clicking Certification Authority (Computer)/CA name/Issued Certificates and selecting the certificate you want to revoke. On the Action menu, point to All Tasks, and then click Revoke Certificate. Select the reason for revoking the certificate, and click Yes.  5. In the Certification Authority snap-in, publish a new CRL by clicking Certification Authority (Computer)/CA name/Revoked Certificates in the console tree. Then, on the Action menu, point to All Tasks, and click Publish.  6. Remove all CRL distribution point extensions from the issuing CA by opening the Certification Authority snap-in and then selecting the CA. On the Action menu, click Properties.  7. On the Extensions tab, confirm that Select extension is set to CRL Distribution Point (CDP).  8. Click any CRL distribution points that are listed, click Remove, and click OK.  9. Stop and restart AD CS.  10. Repeat steps 1 and 2 above, and then verify that clients can still obtain revocation data. To do this, use the Certificates snap-in to export the certificate to a file (\*.cer). At a command prompt, type:  certutil -url <exportedcert.cer>  11. In the Verify and Retrieve dialog box that appears, click From CDP and From OCSP and compare the results. |