Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

# 6426B

## Configuring and Troubleshooting Identity and Access Solutions with Windows Server® 2008 Active Directory®

*Companion Content*

Information in this document, including URL and other Internet Web site references, is subject to change without notice. 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.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

Product Number: 6426B

Released: 10/2009

# MICROSOFT LICENSE TERMS

# OFFICIAL MICROSOFT LEARNING PRODUCTS COURSEWARE – STUDENT EDITION – Pre-Release and Final Versions

These license terms are an agreement between Microsoft Corporation and you. Please read them. They apply to the licensed content named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this licensed content, unless other terms accompany those items. If so, those terms apply.

**By using the licensed content, you accept these terms. If you do not accept them, do not use the licensed content.**

**If you comply with these license terms, you have the rights below.**

1. **OVERVIEW.**

   **Licensed Content.** The licensed content includes software, printed materials, academic materials (online and electronic), and associated media.

   **License Model.** The licensed content is licensed on a per copy per device basis.

2. **INSTALLATION AND USE RIGHTS.**

   a. **Licensed Device.** The licensed device is the device on which you use the licensed content. You may install and use one copy of the licensed content on the licensed device.

   b. **Portable Device.** You may install another copy on a portable device for use by the single primary user of the licensed device.

   c. **Separation of Components.** The components of the licensed content are licensed as a single unit. You may not separate the components and install them on different devices.

   d. **Third Party Programs.** The licensed content may contain third party programs. These license terms will apply to your use of those third party programs, unless other terms accompany those programs.

3. **PRE-RELEASE VERSIONS.** If the licensed content is a pre-release ("beta") version, in addition to the other provisions in this agreement, then these terms also apply:

   a. **Pre-Release Licensed Content.** This licensed content is a pre-release version. It may not contain the same information and/or work the way a final version of the licensed content will. We may change it for the final, commercial version. We also may not release a commercial version. You will clearly and conspicuously inform any Students who participate in an Authorized Training Session and any Trainers who provide training in such Authorized Training Sessions of the foregoing; and, that you or Microsoft are under no obligation to provide them with any further content, including but not limited to the final released version of the Licensed Content for the Course.

   b. **Feedback.** If you agree to give feedback about the licensed content to Microsoft, you give to Microsoft, without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software, licensed content, or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your feedback in them. These rights survive this agreement.

   c. **Confidential Information.** The licensed content, including any viewer, user interface, features and documentation that may be included with the licensed content, is confidential and proprietary to Microsoft and its suppliers.

      i. **Use.** For five years after installation of the licensed content or its commercial release, whichever is first, you may not disclose confidential information to third parties. You may disclose confidential information only to your employees and consultants who need to know the information. You must have written agreements with them that protect the confidential information at least as much as this agreement.

      ii. **Survival.** Your duty to protect confidential information survives this agreement.

iii. **Exclusions**. You may disclose confidential information in response to a judicial or governmental order. You must first give written notice to Microsoft to allow it to seek a protective order or otherwise protect the information. Confidential information does not include information that

- becomes publicly known through no wrongful act;
- you received from a third party who did not breach confidentiality obligations to Microsoft or its suppliers; or
- you developed independently.

d. **Term**. The term of this agreement for pre-release versions is (i) the date which Microsoft informs you is the end date for using the beta version, or (ii) the commercial release of the final release version of the licensed content, whichever is first ("beta term").

e. **Use**. You will cease using all copies of the beta version upon expiration or termination of the beta term, and will destroy all copies of same in the possession or under your control.

f. **Copies**. Microsoft will inform Authorized Learning Centers if they may make copies of the beta version (in either print and/or CD version) and distribute such copies to Students and/or Trainers. If Microsoft allows to such distribution, you will follow any additional terms that Microsoft provides to you for such copies and distribution.

4. **ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.**

**a. Media Elements and Templates.** You may use images, clip art, animations, sounds, music, shapes, video clips and templates provided with the licensed content solely for your personal training use. If you wish to use these media elements or templates for any other purpose, go to www.microsoft.com/permission to learn whether that use is allowed.

**b. Academic Materials.** If the licensed content contains academic materials (such as white papers, labs, tests, datasheets and FAQs), you may copy and use the academic materials. You may not make any modifications to the academic materials and you may not print any book (either electronic or print version) in its entirety. If you reproduce any academic materials, you agree that:

- The use of the academic materials will be only for your personal reference or training use
- You will not republish or post the academic materials on any network computer or broadcast in any media;
- You will include the academic material's original copyright notice, or a copyright notice to Microsoft's benefit in the format provided below:

**Form of Notice**:

© 2008 Reprinted for personal reference use only with permission by Microsoft Corporation. All rights reserved.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the US and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

**c. Distributable Code.** The licensed content may contain code that you are permitted to distribute in programs you develop if you comply with the terms below.

**i. Right to Use and Distribute.** The code and text files listed below are "Distributable Code."

- REDIST.TXT Files. You may copy and distribute the object code form of code listed in REDIST.TXT files.
- Sample Code. You may modify, copy, and distribute the source and object code form of code marked as "sample."
- Third Party Distribution. You may permit distributors of your programs to copy and distribute the Distributable Code as part of those programs.

**ii. Distribution Requirements**. For any Distributable Code you distribute, you must

- add significant primary functionality to it in your programs;
- require distributors and external end users to agree to terms that protect it at least as much as this agreement;
- display your valid copyright notice on your programs; and
- indemnify, defend, and hold harmless Microsoft from any claims, including attorneys' fees, related to the distribution or use of your programs.

iii. **Distribution Restrictions.** You may not

- alter any copyright, trademark or patent notice in the Distributable Code;
- use Microsoft's trademarks in your programs' names or in a way that suggests your programs come from or are endorsed by Microsoft;
- distribute Distributable Code to run on a platform other than the Windows platform;
- include Distributable Code in malicious, deceptive or unlawful programs; or
- modify or distribute the source code of any Distributable Code so that any part of it becomes subject to an Excluded License. An Excluded License is one that requires, as a condition of use, modification or distribution, that
  - the code be disclosed or distributed in source code form; or
  - others have the right to modify it.

5. **INTERNET-BASED SERVICES.** Microsoft may provide Internet-based services with the licensed content. It may change or cancel them at any time. You may not use these services in any way that could harm them or impair anyone else's use of them. You may not use the services to try to gain unauthorized access to any service, data, account or network by any means.
6. **SCOPE OF LICENSE.** The licensed content is licensed, not sold. This agreement only gives you some rights to use the licensed content. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the licensed content only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the licensed content that only allow you to use it in certain ways. You may not
   - disclose the results of any benchmark tests of the licensed content to any third party without Microsoft's prior written approval;
   - work around any technical limitations in the licensed content;
   - reverse engineer, decompile or disassemble the licensed content, except and only to the extent that applicable law expressly permits, despite this limitation;
   - make more copies of the licensed content than specified in this agreement or allowed by applicable law, despite this limitation;
   - publish the licensed content for others to copy;
   - transfer the licensed content marked as 'beta' or 'pre-release' to any third party;
   - allow others to access or use the licensed content;
   - rent, lease or lend the licensed content; or
   - use the licensed content for commercial licensed content hosting services.
   - Rights to access the server software that may be included with the Licensed Content, including the Virtual Hard Disks does not give you any right to implement Microsoft patents or other Microsoft intellectual property in software or devices that may access the server.
7. **BACKUP COPY.** You may make one backup copy of the licensed content. You may use it only to reinstall the licensed content.
8. **TRANSFER TO ANOTHER DEVICE.** You may uninstall the licensed content and install it on another device for your personal training use. You may not do so to share this license between devices.
9. **TRANSFER TO A THIRD PARTY.** You may not transfer those versions marked as 'beta' or 'pre-release' to a third party. For final versions, these terms apply: The first user of the licensed content may transfer it and this agreement directly to a third party. Before the transfer, that party must agree that this agreement applies to the transfer and use of the licensed content. The first user must uninstall the licensed content before transferring it separately from the device. The first user may not retain any copies.
10. **EXPORT RESTRICTIONS.** The licensed content is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the licensed content. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.
11. **NOT FOR RESALE SOFTWARE/LICENSED CONTENT.** You may not sell software or licensed content marked as "NFR" or "Not for Resale."

12. **ACADEMIC EDITION.** You must be a "Qualified Educational User" to use licensed content marked as "Academic Edition" or "AE." If you do not know whether you are a Qualified Educational User, visit www.microsoft.com/education or contact the Microsoft affiliate serving your country.

13. **ENTIRE AGREEMENT.** This agreement, and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the licensed content and support services.

14. **APPLICABLE LAW.**

    a. **United States.** If you acquired the licensed content in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

    b. **Outside the United States.** If you acquired the licensed content in any other country, the laws of that country apply.

15. **LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the licensed content. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.

16. **DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED "AS-IS." YOU BEAR THE RISK OF USING IT. MICROSOFT GIVES NO EXPRESS WARRANTIES, GUARANTEES OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT EXCLUDES THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.**

17. **LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. $5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.**

    This limitation applies to

    - anything related to the licensed content, software, services, content (including code) on third party Internet sites, or third party programs; and
    - claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

    It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

**Please note: As this licensed content is distributed in Quebec, Canada, some of the clauses in this agreement are provided below in French.**

**Remarque : Ce le contenu sous licence étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.**

**EXONÉRATION DE GARANTIE.** Le contenu sous licence visé par une licence est offert « tel quel ». Toute utilisation de ce contenu sous licence est à votre seule risque et péril. Microsoft n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection dues consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit locale, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contrefaçon sont exclues.

**LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES.** Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 $ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.

Cette limitation concerne:

- tout ce qui est relié au le contenu sous licence , aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers ; et
- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s'applique également, même si Microsoft connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

**EFFET JURIDIQUE.** Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

# Module 1

## Exploring IDA Solutions

### Contents:

Lesson 2

# Active Directory Server Roles in IDA Management

## Contents:

# Question and Answers

## Configuring a Server Role in Windows Server 2008

**Question**: What is the purpose of AD RMS?

**Answer**: Protects information stored in documents, e-mail messages, or on Web sites from unauthorized viewing, modification, or use.

**Question**: Which server role can be installed to provide a company's employees access to the partner organization's Web applications without establishing domain or forest trusts?

**Answer**: AD FS

**Question**: Which server role provides the Certification Authority (CA) infrastructure?

**Answer**: AD CS

**Question**: What are some of the advantages of the AD LDS server role compared to AD DS?

**Answer**: It is simpler to work with, when installation does not change server configuration as AD DS does.

**Question**: Which server role is a prerequisite for the installation of other server roles?

**Answer**: Other roles that may be required are AD DS, DNS, DHCP, and Web Server. These would provide services that other IDA roles would require to be available before deployment.

# Detailed Demo Steps

## Demonstration: Configuring a Server Role in Windows Server 2008

## Demonstration steps:

1. Launch Virtual Machine **6426B-HQDC01**.
2. Log on with user name **Administrator** and password **Pa$$w0rd**.
3. Click Start, click Administrative Tools, and then click Server Manager.
4. In the **Server Manager** console, in the **Roles Summary** section, in the **Details** Pane, click **Add Roles**.
5. Click **Next** on the opening screen of the **Add Roles Wizard**, and then follow the steps in the Add Roles Wizard.
6. On the **Select Server Roles** screen, point out the roles related to IDA technologies.

# Module Reviews and Takeaways

## Review Question

**Question** 1: What are some benefits of using IDA solutions?

**Answer**: Answers can include enhanced security, better collaboration with organizations outside of your own, and control and streamlined access to network resources for users.

**Question** 2: What tool allows you to consolidate different repositories, and how is the repository information made available?

**Answer**: ILM 2007 allows you to combine various identity repositories into a single directory store, and they are made available within a single AD LDS instance via LDAP.

**Question** 3: What two products are combined together to make up ILM 2007, and what functionality do they provide?

**Answer**: MIIS 2003 and CLM 2007, and they provide metadirectory and user provisioning services and Certificate and Smart Card management services respectively.

## Real-world scenario

Identity and access is key to how businesses communicate in today's connected world. IDA solutions streamline the availability and control access to and management of information, and may help meet legal obligations around how information is retained and accessed.

## Best practices

### It is essential to

- Clearly define your business requirements.
- Identify which roles and solutions will best meet their needs.
- Thoroughly test the proposed solution before implementing any IDA solutions.

For more information, see: Microsoft Identity and Access Solutions – Home Page

# Lab Review Question and Answers

## In this lab, you have:

- Created a functionality framework
- Taken decisions on creating server roles to achieve required IDA management solutions
- Identified identity synchronization and user provisioning
- Identified certificate management
- Identified secure access across organizational boundaries
- Identified secure access beyond user names and passwords

# Module 2

## Deploying and Managing Active Directory® Certificate Services

### Contents:

Lesson 3

# Installing AD CS

## Contents:

# Question and Answers

## Demonstration: How to Install AD CS as a Root CA

**Question**: Where does the root CA get its own certificate from?

**Answer**: It has a self-signed certificate.

**Question**: If you desire an offline root CA, would you choose to install a stand-alone root or an enterprise root CA?

**Answer**: You would choose a stand-alone CA.

## Demonstration: Overview of the CA Administration Console

**Question**: Using the CA management tool, how would you manage a CA located on a different server?

**Answer**: In the Certification Authority Admin Console, right-click Certification Local and go to Retarget Certification Authority. This will then allow you to select another server.

**Question** :How would you manage a remote AD CS server from a Windows Vista® client?

**Answer**: One method would be to use remote desktop to connect to the server machine, providing your credentials and administering.

# Detailed Demo Steps

## Demonstration: How to Install AD CS as a Root CA

## Demonstration steps

1. Launch the **6426B-HQDC01** virtual machine and log in as **Contoso\Administrator** with the password **Pa$$w0rd**.
2. Go to **Start > Administrative Tools > Server Manager**.
3. Right-click the **Roles** node in the left navigation pane and select **Add Roles**. (Make sure you wait long enough for Server Manager to refresh all role data.)
4. Click **Next** on the **Add Roles** page.
5. Select the **Active Directory Certificate Services** role, and click **Next**.
6. On the **Introduction to Active Directory Certificate Services** page, click **Next**.
7. On the **Select Role Services** page, click **Next**.
8. On the **Specify Setup Type** page, select **Enterprise**, and click **Next**.
9. On the **Specify CA Type** page, select **Root CA**, and click **Next**.
10. On the **Set Up Private Key** page, keep the default selection, and click **Next**.
11. On the **Configure Cryptography** page, keep the default selection, and click **Next**.
12. Enter **Module 2 Demo CA** in the **Common Name** field, and click **Next**.
13. On the **Set Validity Period** page, keep the default selection, and click **Next** twice.
14. On the **Confirm Installation Selections** page, select **Install**.

## Demonstration: Overview of the CA Administration Console

## Demonstration steps

1. Ensure that the installation from the previous demonstration has completed (that AD CS has completed the installation on the 6426B-HQDC01 virtual machine) and that you are logged in as **Contoso\Administrator** with the password **Pa$$w0rd**.
2. Go to **Start > Administrative Tools > Certification Authority**.
3. The Certification Authority Admin Console should now be open.
4. Right-click **Module 2 Demo CA** (if you left in the defaults in the last demonstration, it will be called contoso-HQDC01-CA), and select **Properties**.
5. Walk through each of the tabs; click **Help** in any of the tabs to show the online explanation for all options on that tab.

Lesson 4

# Managing CAs

## Contents:

# Question and Answers

## How to Configure AIA and CRL Availability

**Question**: How do you manually publish the CRL?

**Answer**: You publish it in the Certification Authority Admin Console.

**Question**: How would you schedule the publication of the CRL?

**Answer**: You can schedule the publication via the Revoke Certificates Properties dialog box.

# Detailed Demo Steps

## Demonstration: How to Install AD CS as a Root CA

## Discussion steps

1. Return to the demo virtual machine that you used earlier (6426B-HQDC01) and ensure that you are logged in as **Contoso\Administrator** with the password **Pa$$w0rd**.
2. If it is not already open, open the Certificate Authority Admin Console by going to **Start > Administrative Tools > Certification Authority**.
3. In the Certification Authority Microsoft Management Console (MMC) snap-in, go to **Certificate Authority (Local)**, expand **Module 2 Demo CA** and right-click **Certificate Templates**, and select **Manage**.
4. Browse to the **OCSP Response Signing** template display name in the details pane, right-click, and then select **Properties**.
5. Open the **Issuance Requirements** tab.
6. Click **Help** to open Online Help for this topic. Explain to students that there are a number of options that will be explained further in the lab exercises.

### To view the CRL publication list, follow these steps:

1. Return to the Certificate Authority Admin Console. (If it is not already open, open the Certificate Authority Admin Console by going to **Start > Administrative Tools > Certification Authority**.)
2. In the Certification Authority Microsoft Management Console (MMC) snap-in, go to **Certificate Authority (Local)**, then expand **Module 2 Demo CA**.
3. Click the **Revoked Certificates** node.
4. From the **Action** menu, select **Properties**.
5. The Revoked Certificates Properties dialogue box appears.
6. Step through the two tabs and note the settings that they contain.

# Module Reviews and Takeaways

## Review Question

**Question 1**: What is the difference between a public key and a private key?

**Answer:** A public key is available to anyone and is typically used to decrypt a session key or digital signature. It can also be used to encrypt a message, guaranteeing that only the person with the corresponding private key can view the data. A private key is only in your possession and is typically used to encrypt a symmetric session key, digitally sign a message, or decrypt a message that has been encrypted with the corresponding public key.

**Question 2**: What are some reasons that an organization would utilize PKI?

**Answer:** To enhance security and control access to information.

**Question 3**: What are some reasons that an organization would use an enterprise root CA?

**Answer:** If the server was a member of a domain or if the organization wanted to use autoenrollment for certificate issuing

**Question 4**: What are some reasons that an organization would publish a CRL?

**Answer:** To make sure certificates which are out of date or have been cancelled can be identified

## Real-world issues and scenarios

The following is an example of a real-world scenario:

The Sales and Products databases in a pharmaceutical company are on different servers, each of which also hosts other databases. How can you logically consolidate the Sales and Products databases?

**Answer:** Externally published services or signed software code should always use “well-known” root CAs. The enterprise root CA should always be protected by using multiple form factors (online versus offline backup).

# Lab Review Question and Answers

## In this lab, you have:

- Installed the AD CS Server role with just the CA role service and configured it as a stand-alone root CA
- Installed an enterprise subordinate CA with the Web enrollment role service
- Issued the subordinate certificate
- Installed and verified the subordinate certificate
- Backed up the subordinate CA
- Restored the subordinate CA
- Examined the default CDPs and configured the CRL publication interval
- Manually published the CRL
- Viewed the published CRL

# Module 3

## Deploying and Managing Certificates

### Contents:

Lesson 1

# Configuring Certificate Templates

## Contents:

# Question and Answers

## Demonstration: How to Modify and Enable a Certificate Template

**Question**: Why would you need to modify a certificate template?

**Answer**: If you want to use a certificate for a specific purpose that isn't covered by one of the default templates.

**Question**:What is the difference between modifying an original certificate template and superseding an existing certificate template?

**Answer**: Modifying a template adds additional functionality. Superseding a template is used to collapse a certificate hierarchy.

# Detailed Demo Steps

## Demonstration: How to Modify and Enable a Certificate Template

## Demonstration steps:

1. Launch virtual machine **6426B-HQDC01-B**, and log on as **Contoso\Administrator** with password **Pa$$w0rd**.
2. Click **Start**, point to **Administrative Tools**, then select **Certification Authority**. (It is in this template that you can view and manage how certificates are handled.)
3. In the **Certification Authority**, expand **ContosoCA**, right-click **Certificate Templates**, and then click **Manage**. (It is in this console that you can define your template settings.)
4. Review the list of default templates and examine them and their properties.
5. In the **Details** Pane, click **IPSec**.
6. Scroll through the tabs and note what you are able to modify on each tab. On the **Security** tab, you define permissions for enrollment. Close the template by clicking **Cancel**.
7. Still in the **Certificate Templates** console, in the **Details** pane, right-click the **Exchange User certificate** template, and then click **Duplicate Template**.
8. In the **Duplicate Template** dialog box, click **Windows Server 2008, Enterprise Edition**, and then click **OK**.
9. In the **Properties of New Template** dialog box, type **Exchange User Test1** in the **Template display** name box.
10. Click the **Superseded Templates** tab, and then click **Add**.
11. Click the **Exchange User** template, and then click **OK**.
12. On the **Security** tab, for **Authenticated Users** click **Allow for Read, Enroll and Autoenroll permissions**, and then click **OK**.
13. Close the **Certificate Templates** console.

### Configure the new template to be issued by the CA.

1. In the Certification Authority console, issue the **Exchange User Test 1** certificate template.
2. Select any of the templates, right-click and go to **Help**, then walk through the online help explanations in the help file.

### Configure the new template to be issued by the CA.

1. In the Certification Authority console, right-click **Certificate Templates**.
2. Point to **New**, and then click **Certificate Template to Issue**.
3. In the **Enable Certificates Templates** dialog box, click the **Exchange User Test 1** template, and then click **OK**.
4. Go to the **Certificate Template** folder and look at the certificate templates listed. Note that the certificate template that you just created, **Exchange User Test1** through the template manager, shows up as ready to issue.
5. Select any of the templates, right-click and go to **Help**

Lesson 2

# Certificates by Using AD CS

## Contents:

# Question and Answers

## How to Manually Obtain a Certificate for a Web Service

**Question**: When you enable Web enrollment on the certificate server, how do you use the Web interface to obtain certificate services?

**Answer**: Use Internet Explorer to navigate to the Web enrollment Web site (normally http://ServerName/certsrv).

**Question**:When should you use the Web enrollment method to issue certificates?

**Answer**: When a certificate is needed for a service, such as a Web server or an e-mail server.

# Detailed Demo Steps

## Demonstration: How to Manually Obtain a Certificate for a Web Service

## Demonstration steps:

### We will modify the existing Web server template permissions first.

1. Launch virtual machine **6426B-HQDC01-B**, and log on as **Contoso\Administrator** if it is not already available.
2. Click **Start**, point to **Administrative Tools**, and then click **Certification Authority**.
3. In the **Certification Authority** console, expand the **ContosoCA** node, right-click **Certificate Templates**, and then click **Manage**.
4. In the **Details** pane, right-click the **Web Server** certificate template, and then click **Duplicate Template**.
5. In the **Duplicate Template** dialog box, select **Windows Server 2008, Enterprise Edition**, and then click **OK**.
6. In the **Properties of New Template** dialog box, type **Web Server Test** in the **Template display name** box.
7. In the **Web Server Properties** dialog box, click the **Security** tab, and then click **Authenticated Users**.
8. Under the **Permissions for Authenticated Users** node, select the **Allow check box for Enroll**, and then click **OK**.
9. Close the certificate template console.
10. In the **Certsrv - [Certification Authority (Local)]** console, right-click **Certificate Templates**, and go to **New > Certificate to Issue**.
11. Scroll down and select the **Web Server Test** certificate, and then click **OK**.
12. 12 Close the Certificate Templates console.
13. Close the **Certsrv - [Certification Authority (Local)]** console.

### We will now manually enroll the Web Server certificate.

1. Click **Start**. In the **Search** box, type **MMC**, and then press ENTER. The Console1-[Console Root] console appears.
2. In the Console1-[Console Root] console, click **File**, and then click **Add/Remove Snap-in**.
3. In the **Add or Remove Snap-ins** dialog box, click **Certificates**, and then click **Add**.
4. In the **Certificates snap-in** dialog box, click **Computer account**, and then click **Next**.
5. On the Select Computer page, click **Finish**, and then click **OK**.
6. Expand the **Certificates (Local Computer)** and **Personal** nodes.
7. Under the **Personal** node, right-click **Certificates**, point to **All Tasks**, and then click **Request New Certificate**. This launches the Certificate Enrollment wizard.
8. On the Before You Begin page, click **Next**.

9. On the Request Certificates page, select the **Web Server** check box, and then click **More information is required to enroll for this certificate**.
10. In the Certificate Properties dialog box, in the **Subject name** area, in the **Type** list, click **Common name**.
11. In the **Value** box, type **HQDC01**, and then click **Add**.
12. On the **General** tab, in the **Friendly name** box, type **Test Web Server**, and then click **OK**.
13. On the Request Certificates page, click **Enroll**. On the Certificates Installation Results page, click **Finish**.
14. Click the **Certificates** folder, and then examine the new Web server certificate.

Lesson 3

# Deploying Certificates by Using Autoenrollment

## Contents:

# Question and Answers

## Benefits and Uses of Autoenrollment

**Question:** How does autoenrollment simplify certificate management in your organization?

**Answer:** Autoenrollment will automatically request and provide a certificate for a specified purpose without manual user intervention.

**Question:**What are examples of applications that can benefit from autoenrollment?

**Answer:** Two-factor authentication, S/MIME e-mail security, smart-card logon.

Lesson 4

# Revoking Certificates

## Contents:

# Question and Answers

## How to Revoke A Certificate

**Question:** What are some reasons you would need to revoke an issued certificate?

**Answer:** A mobile device is lost, a user leaves the company.

**Question:**Is it possible to reverse a revocation on a certificate?

**Answer:** Yes, but certificates can only be unrevoked if they are revoked with reason "Certificate Hold."

## How to Configure an Online Responder

**Question:** Which tool can you use to configure the Online Responder?

**Answer:** Online Responder Management Console

**Question:**Which server operating systems support installation of the Online Responder?

**Answer:** Windows Server 2008

**Question:**Can you use non-Microsoft CAs with the Online Responder role service?

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

# Detailed Demo Steps

## Demonstration: How to Configure an Online Responder

### Firstly, we will examine and then configure the CRL publication interval.

1. Launch virtual machine **6426B-HQDC01-B**, and log on as **Contoso\Administrator** with password **Pa$$w0rd** if it is not already available.
2. Click **Start**, click **Administrative Tools**, and then click **Certification Authority**.
3. In the **Certification Authority (Local)** pane, right-click **ContosoCA**, and then click **Properties**.
4. In the **ContosoCA Properties** dialog box, on the **Extensions** tab, examine the default **CDPs**, and then click **Cancel** to close the dialog box.
5. Expand the **ContosoCA** node, right-click the **Revoked Certificates** folder, and then click **Properties**.
6. In the **Revoked Certificates Properties** dialog box, in the **CRL publication interval** list, select **Months**. Then in the **Publication interval** box, type **1**.
7. Again in the **Revoked Certificates Properties** dialog box, in the **Publish Delta CRLs** section, enter a **Publication interval** of **5 Days**, and then click **OK**.
8. Minimize the **Certification Authority** console.

### Now we will install the Online Responder Role.

1. Launch virtual machine **6426B-HQDC01-B**, and log on as **Contoso\Administrator** with password **Pa$$w0rd** if it is not already available.
2. Start **Server Manager** by clicking the **Server Manager** icon next to the **Start** button.
3. Expand the **Roles** node.
4. Right-click **Active Directory Certificate Services**, and then select **Add Role Services**.
5. Select **Online Responder** then click **Next**.
6. Select **Install**.

### Now we will configure the CA to include the Online Responder location in the authority information access (AIA).

1. Restore the **Certification Authority console**.
2. Right-click **ContosoCA**, and then click **Properties**.
3. In the **ContosoCA Properties** dialog box, on the **Extensions** tab, in the **Select extension** list, click **Authority Information Access (AIA)**, and then click **Add**.
4. In the **Add Location** dialog box, type **http://HQDC01/ocsp**, and then click **OK**.
5. Select the **Include in the AIA extension of issued certificates** check box.
6. Select the **Include in the online certificate status protocol (OCSP) extension** check box, and then click **OK**.
7. In the **Certificate Authority** box, restart **Active Directory Certificate Services** by clicking **Yes**.

### We will now issue the OCSP Response Signing template.

1. In the Certificate Authority console, right-click the **Certificate Templates** folder, and then click **Manage**.
2. In the **Certificate Templates** console, double-click the **OCSP Response Signing** template.
3. In the **OCSP Response Signing Properties** dialog box, click the **Security** tab. Then under **Permissions for Authenticated Users**, select the **Allow for Enroll** check box, and click **OK**.
4. Close the **Certificate Templates** console.
5. In the **Certification Authority** console, right-click the **Certificate Templates** folder, point to **New**, and then click **Certificate Template to Issue**.
6. In the **Enable Certificate Templates** dialog box, select the **OCSP Response Signing** template, and then click **OK**.

### Finally, we will configure the Online Responder.

1. Click **Start**, point to **Administrative Tools**, and then click **Online Responder Management**.
2. In the **Online Responder Management** console, right-click **Revocation Configuration**, and then click **Add Revocation Configuration**.
3. In the **Add Revocation Configuration** wizard, click **Next**.
4. On the **Name The Revocation Configuration** page, in the **Name** box, type **Test Online Responder**, and then click **Next**.
5. On the **Select CA Certificate Location** page of the wizard, click **Next**.
6. On the **Choose CA Certificate** page, click **Browse**, click the **ContosoCA** certificate, click **OK**, and then click **Next**.
7. On the **Select Signing Certificate** page, click **Next**.
8. On the **Revocation Provider** page, click **Finish**. The revocation configuration status will appear as Working.
9. Close the Online Responder console.

Lesson 5

# Configuring Certificate Recovery

## Contents:

# Question and Answers

## How to Configure Key Archival

**Question**: What groups by default are authorized to request a KRA certificate?

**Answer**: Only Enterprise Admins and Domain Admins are authorized to request a KRA certificate.

**Question**: Where by default in Active Directory are KRA certificates normally published?

**Answer**: Key Recovery Agent certificates are published to the key recovery agent container in Active Directory when enrollment occurs. The common name for the key recovery agent container is CN=KRA, CN=Public Key Services, CN= Services, CN=Configuration, DC=….

## How To Recover a Lost Key

**Question**: What piece of information will be most important to you while recovering lost keys?

**Answer**: The serial number of the certificate

**Question**: What command-line tool will you use to extract the key and to create the password-protected .pfx file, to be given back to the user?

**Answer**: The certutil.exe utility

# Detailed Demo Steps

## Demonstration: How to Configure Key Archival

## Demonstration steps:

### Remove the requirement for CA Manager approval and configure enrollment settings for the Key Recovery Agent (KRA) certificate

1. Launch virtual machine **6426B-HQDC01-B**, and log on as **Contoso\Administrator** with password **Pa$$w0rd** if it is not already available.
2. Click **Start**, point to **Administrative Tools**, and then click **Certification Authority**.
3. In the Certification Authority console, expand the **ContosoCA** node, right-click the **Certificates Templates** folder, and then click **Manage**.
4. In the **Details** pane, right-click the **Key Recovery Agent** certificate, and then click **Properties**.
5. In the **Key Recovery Agent Properties** dialog box, click the **Issuance Requirements** tab.
6. Clear the **CA certificate manager approval** check box.
7. Click the **Security** tab. Notice that Domain Admins and Enterprise Admins are the only groups that have the Enroll permission, and then click **OK**.
8. Close the Certificates Templates console.

### Configure the CA to issue KRA certificates

1. In the Certification Authority console, right-click the **Certificates Templates** folder, point to **New**, and then click **Certificate Template to Issue**.
2. In the **Enable Certificate Templates** dialog box, click the **Key Recovery Agent** certificate, and then click **OK**.

### Acquire the KRA certificate

1. Click **Start** in the **search** box type **MMC**, and then click **OK**.
2. In the **Console1-[Console Root]** console, click **File**, and then click **Add/Remove Snap-in**.
3. In the **Add or Remove Snap-ins** dialog box, add the **Certificates** snap-in for **My user** account. Click **Finish**, and then click **OK**. Expand the **Certificates - Current User** node, and right-click **Personal**.
4. Click **All Tasks**, and then click **Request New Certificate**. This launches the **Certificate Enrollment Wizard**.
5. On the **Before You Begin** page, click **Next**.
6. On the **Request Certificates** page, select the **Key Recovery Agent** check box. Click **Enroll**, and then click **Finish**.
7. Refresh the console, and view the KRA in the personal store, that is, scroll across the certificate properties and verify that the Certificate Template Key Recovery Agent is present.

### Configure the CA to allow key recovery

1. In the Certification Authority console, right-click **ContosoCA**, and then click **Properties**.

2. Click the **Recovery Agents** tab, and then click **Archive the key**.
3. Under **Key recovery agent certificates**, click **Add**.
4. In the **Key Recovery Agent Selection** dialog box, click the certificate that is displayed, and then click **OK** twice. When prompted to restart the CA, click Yes.

### Configure a custom template for key archival

1. In the Certification Authority console, right-click the **Certificates Templates** folder, and then click **Manage**.
2. In the Certificates Templates console, right-click the **User** certificate, and then click **Duplicate Template**.
3. In the **Duplicate Template** dialog box, click **Windows Server 2008, Enterprise Edition**, and then click **OK**.
4. In the **Properties of New Template** dialog box, on the **General** tab, in the **Template display name** box, type **Archive User**. On the **Request Handling** tab, select the **Archive subject's encryption private key** check box, and then click **OK**.
5. By using the archive key option, the KRA can obtain the private key from the certificate store.
6. Close the Certificates Templates console.
7. In the Certification Authority console, right-click the **Certificates Templates** folder, click **New**, and then click **Certificate Template to Issue**.
8. Click **Archive User**, and then click **OK**.
9. Close the Certification Authority console.

### Add a user to the Server Operators group

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** console box, click the **Executives OU**, right-click the user **Tony Wang**, and then click **Add to a group**.
3. In the **Select Groups** dialog box, type **Server Operators**, and then click **OK** twice.
4. Right-click **Tony Wang**, and then click **Properties**.
5. In the **Tony Wang Properties** dialog box, on the **General** tab, in the **E-mail** box, type **tony@Contoso.com**, and then click **OK**.
6. Close the **Active Directory Users and Computers** console box.
7. Log off from the **6426B-HQDC01-B** virtual computer but do not shut it down.

## Demonstration: How To Recover a Lost Key

## Demonstration steps:

1. Log on to the **6426B-HQDC01-B** virtual computer as **Contoso\Tony**, and use **Pa$$w0rd** as the password.
2. Click **Start** and in the **search** box, type **MMC**, and then click **OK**.
3. If the **UAC** dialog box appears, type **Pa$$w0rd**, and then click **OK**.

4. In the **Console1-[Console Root]** console, click **File**, and then click **Add/Remove Snap-in**.
5. Add the **Certificates** snap-in if required, click **My user account**, click **Finish**, and then click **OK**, otherwise just click **OK**.
6. Expand the **Certificates - Current User** node, and then right-click **Personal**.
7. Click **All Tasks**, and then click **Request New Certificate**. The Certificate Enrollment Wizard appears.
8. On the **Before You Begin** page, click **Next**.
9. On the **Request Certificate** page, select the **Archive User** check box, click **Enroll**, and then click **Finish**.
10. It may take a minute for the information to become available. If you receive an error, log off and then log back on again as **Contoso\Tony**.
11. Refresh the console, and view the **Archive User** certificate in the personal store; that is, scroll down to the end of the templates listed and see the **Archive User Template** listed.
12. Double-click the certificate based off the **Archive User** template, click the **Details** tab, and write down the serial number. You will use this serial number for recovery purposes.
13. Log off from the **6426B-HQDC01-B** virtual computer.
14. Log on as **Contoso\administrator**, and use **Pa$$w0rd** as the password.
15. Click **Start**. Click **Run**, type **CMD**, and then click **OK**.
16. In the Command window that appears, type **certutil –getkey "serial number" outputblob, that is, certutil –getkey "AA BB CC DD EE FF GG HH II JJ" outputblob**.
17. To convert the outputblob file into a .pfx file, in the Command window, type **Certutil –recoverkey outputblob tony.pfx**.
18. When prompted, type in **Pa$$w0rd** as the new password, and then confirm the password.
19. After the command is executed, close the command window.
20. Browse to **C:\Users\Administrator**, and then verify that tony.pfx—the recovered key—is created.
21. Close all windows and turn off the virtual computers. Discard undo disks.

# Module Reviews and Takeaways

## Review Question

**Question** 1: List the requirements to use autoenrollment for certificates.

**Answer:** This method is used for AD DS domain computers. The certificate must be configured for autoenrollment through Group Policy. You must have an Enterprise CA available.

**Question** 2: For what is the DACL in a certificate template used?

**Answer:** Associated with each certificate template is a discretionary access control list (DACL). It defines which security principals have permissions to read and configure the template, and to enroll or autoenroll for certificates based on the template.

**Question** 3: What are some of the advantages of using a version 3 certificate template?

**Answer:** They support several features of a Windows Server 2008 CA, such as Cryptography API: Next Generation (CNG). This feature provides support for Suite-B cryptographic algorithms such as Elliptic Curve Cryptography (ECC).

### When you use version 3 certificate templates, you can use CNG encryption and hash algorithms for:

- Certificate requests
- Issued certificates
- Protection of private keys for key exchange and key archival scenarios

**Question** 4: Why would you use manual certificate enrollment?

**Answer:** Use this method when the requestor cannot communicate directly with the CA or if the device does not support autoenrollment.

**Question** 5: What are the steps to configure an Online Responder?

**Answer:**

a. Configure the CA to support the Online Responder:
   - Enable the OCSP response signing certificate.
   - Configure autoenrollment.
   - Configure the AIA to support the OCSP extension.

b. Install the Online Responder role service.

c. Create a revocation configuration:
   - Link the CA with the Online Responder.
   - Select a signing certificate.

**Question** 6: What three methods can be used to export a certificate?

Answer:

a. Public-Key Cryptography Standards (PKCS) #12 (.pfx file) export from the Certificates MMC snap-in on Windows 2000, Windows XP, Windows Server 2003, Windows Vista, or Windows Server Longhorn.
b. PKCS #12 (.pfx file) export from the Outlook 2003 or Outlook 2007 client.
c. epf file format from the Outlook 2000 or Outlook 2002 client.

# Lab Review Question and Answers

## In this lab, you have:

- Duplicated, installed, and manually enrolled a certificate.
- Configured the template to be issued by the CA.
- Verified that the certificate is updated.
- Created, duplicated, and superseded the Local User template by using a new template that includes smart card logon.
- Configured the new template to be issued by the CA.
- Verified that the certificate is updated.
- Installed the Certification Authority Web enrollment role service.
- Configured permissions on the Web Server certificate template.
- Enrolled a Web Server certificate.
- Configured the Web enrollment site to use SSL.
- Requested and installed a basic EFS certificate by using Web enrollment.
- Duplicated and configured the User certificate template permissions to enable autoenrollment.
- Configured the template to be issued by the CA.
- Configured group policies to enable autoenrollment for users.
- Verified that autoenrollment works for a user account.
- Examined the default CDPs and configured the CRL publication interval.
- Installed the Online Responder component on a Web server.
- Configured CA to include the Online Responder location in the AIA.
- Issued the OCSP Response Signing template.
- Configured the Online Responder.
- Revoked a certificate.
- Published the CRL.
- Ensured that the CRL is downloaded to a client computer.
- Removed the requirement for CA Manager approval and verified who can enroll the KRA certificate.
- Configured the Contoso CA to issue KRA certificates.
- Acquired the KRA certificate.
- Configured the CA to allow key recovery.
- Configured a custom template for key archival.
- Added a user to the Server Operators group.
- Verified key archival functionality.

- Acquired Archive User's certificate serial number.
- Recovered the private key for the Archive User certificate.

# Module 4

## Configuring Active Directory® Lightweight Directory Services

### Contents:

Lesson 1

# Installing and Configuring AD LDS

## Contents:

# Question and Answers

## How To Install AD LDS Server Role

**Question**: Can AD LDS be installed on a member server?

**Answer**: You can run AD LDS on member servers or stand-alone servers.

**Question**: Can a single machine hold multiple AD LDS instances?

**Answer:** You can run multiple instances of AD LDS concurrently on a single computer, each with its own independently managed schema on server.

**Question**: Is an instance created automatically when the server role is installed?

**Answer:** After you add the AD LDS server role to your server, you can create an AD LDS instance.

**Question**: What may be some of the reasons for implementing AD LDS replication?

**Answer**: Providing an extranet authentication store, consolidating identity systems, providing a development environment, providing a configuration store for distributed applications in Windows Server, migrating legacy directory-enabled applications, and others.

# Detailed Demo Steps

## Demonstration: How To Install AD LDS Server Role

## Demonstration steps

### To install the AD LDS server role:

1. If it is not already started, start the **6426B-HQDC01** virtual machine, and log on as **Contoso\Administrator** with password **Pa$$w0rd**.
2. Start **Server Manager** by clicking the icon next to the **Start** menu.
3. Click the **Roles** node.
4. In the **Details** pane, click **Add Roles**.
5. On the **Before You Begin** page, click **Next**.
6. Select the **Active Directory Lightweight Directory Services** check box, and then click **Next**.
7. On the **Introduction** page, click **Next**.
8. On the **Confirm Installation Selections** page, click **Install**.
9. On the **Installation Results** page, click **Close**.

Lesson 2

# Configuring AD LDS Instances

## Contents:

# Question and Answers

## How to Modify an AD LDS Schema

**Question**: What is LDIF?

**Answer**: LDAP Data Interchange Format (LDIF) is a standard for a file format that can be used for performing batch operations against directories that conform to the LDAP standards. It can be used to export/import data by adding, creating, or modifying against Active Directory.

**Question**: Which Windows Server 2008 utility can be used to modify the schema?

**Answer**: The LDAP Data Interchange Format Data Exchange (LDIFDE) tool is a utility program that can be used to import and export Active Directory objects using LDIF-formatted files. LDIFDE is especially useful for doing batch operations that allow you to add, create, or modify multiple Active Directory objects at one time. The ldifde utility creates, modifies, and deletes directory objects and allows you to populate Active Directory Lightweight Directory Services (AD LDS) with data from other directory services. You can also use ldifde to extend the schema and export user and group information to other applications or services.

**Question**: What is defined in the AD LDS schema?

**Answer**: The AD LDS schema defines, using object classes and attributes, the type so objects and data that can be created and stored in an AD LDS directory.

## How To Configure an AD LDS Instance and an Application Partition

**Question**: Does each AD LDS instance have its own directory store?

**Answer**: Each AD LDS instance has a separate directory store.

**Question**: Do the instances that are part of the same configuration set run on the same or separate computers?

**Answer**: Instances that are part of the same configuration set can run on the same or separate computers

**Question**: You have created a new AD LDS instance but you forgot to create an application partition. How can you create an application partition without recreating the instance?

**Answer**: You can create an application partition during AD LDS setup or anytime after installation. Application directory partitions are typically managed through directory-enabled applications.

## How To Configure Access Control in AD LDS

**Question** Which security principals are available in AD LDS?

**Answer**: The term "security principal" refers to any object that has a security identifier (SID) and that can be assigned permissions to directory objects. AD LDS does not include any default security principals. However, AD LDS does provide importable schema extensions that you can use to create users in AD LDS. Users that are created from these user classes can be used as security principals. In addition, you can make any object class in the AD LDS schema a security principal by adding the msDS-bindableobject auxiliary class and the unicodePwd attribute to the schema definition of an object class. Each AD LDS security principal must be assigned an account and password, which AD LDS uses for authentication

**Question** Which tool can be used to customize access control in AD LDS?

**Answer**: You can administer users and groups in Active Directory Lightweight Directory Services (AD LDS) through the ADSI Edit snap-in or through your directory-enabled applications

**Question** What are the default role-based groups in AD LDS?

**Answer**: AD LDS provides four default role-based groups: Administrators, Instances, Readers, and Users. These groups reside in the configuration partition and in each application partition, but not in the schema partition.

# Detailed Demo Steps

## Demonstration: How to Modify an AD LDS Schema

## Demonstration steps

1. If it is not already started, launch virtual machine **6426B-HQDC01**, log on as **Contoso\Administrator** with password **Pa$$w0rd**, and install **AD LDS**.
2. Open **Server Manager** and expand the **Roles** node, and then click **Active Directory Lightweight Directory Services**.
3. In the **Details** pane, under the **Advanced Tools** section, click **AD LDS Setup Wizard**.
4. On the **Welcome to the Active Directory Lightweight Directory Services Setup Wizard** page, click **Next**.
5. On the **Setup Options** page, click **A unique instance**, and then click **Next**.
6. On the **Instance Name** page, in the **Instance name** box, type **ContosoApp1**, and then click **Next**.
7. On the **Ports** page, set the **LDAP port number** to **6389** and the **SSL port number** to **6636**, and then click **Next**.
8. On the **Application Directory Partition** page, click **Yes**, create an application directory partition, in **Partition name** box, type **OU=App1,dc=contoso,dc=local**, and then click **Next**.
9. On the **File Locations** page, accept the default data file locations, and then click **Next**.
10. On the **Service Account Selection** page, ensure that **Network service account** is selected, and then click **Next**.
11. On the **AD LDS Administrators** page, ensure that **Currently logged on user** is selected, and then click **Next**.
12. On the **Importing LDIF Files** page, select the **MS-User.LDF** check box, and then click **Next**.
13. On the **Ready To Install** page, review the selections and click **Next**.
14. Click **Finish**.

### You can also import after the installation via the command line. On the same virtual machine, import the AdamSyncSchema extensions into the LDS instance.

1. Go to the command prompt window and type **ldifde /?**.
2. Look through the resultant help text and get somewhat familiar with the syntax and switches.
3. Type **C:\Windows\ADAM\ldifde –i –f MS-AdamSyncMetaData.ldf –s HQDC01:6389 –j . –c "cn=configuration,dc=X" #configurationNamingcontext**.

   This imports the ADAMsync schema extensions. They could also have been installed during the creation of the instance but can be done here now in the cmd line as per the previous steps.
4. If you receive an error, open the file **C:\Windows\ADAM\ldf.log** and review the log entries to try to identify the problem.

## Demonstration: How To Configure an AD LDS Instance and an Application Partition

## Demonstration steps

1. If it is not already started, launch virtual machine **6426B-HQDC01**, log on as **Contoso\Administrator** with password **Pa$$w0rd**, and install **AD LDS**.
2. Open **Server Manager** and expand **Roles**. Then click **Active Directory Lightweight Directory Services**.
3. In the content pane, in the **Advanced Tools** section, click **ADSI Edit**. The ADSI Edit console appears.
4. In the ADSI Edit console, right-click **ADSI Edit**, and then click **Connect to**. The Connection Settings dialog box appears.
5. In the **Connection Settings** dialog box, in the **Name** box, type **ContosoApplication**.
6. Under **Connection Point**, in the **Select or type a Distinguished Name or Naming Context** box, type **OU=App1,dc=contoso,dc=local**.
7. Under **Computer**, select the **Select or type a domain or server box:(Server | Domain [:port])**, type **HQDC01:6389**, and then click **OK**.

Notice that you are now connected to the App1 Instance and that you can administer containers and objects by right-clicking them. You can have additional connections in the same ASDSI window by connecting as we did here. Notice also that the default communication port for the LDAP service is 389.

### You can also manage and configure an AD LDS instance by using Ldp.exe.

1. Click **Start**, and then click **Server Manager**.
2. In the console tree, double-click **Roles**, and then click **Active Directory Lightweight Directory Services**.
3. In the **Details** pane, under the **Advanced Tools**, click **Ldp.exe**.
4. On the **Connection** menu, click **Connect**.
5. In **Server**, type **HQDC01** and in **Port**, type the LDAP port number **6389**, and then click **OK**.
6. On the **Connection** menu, click **Bind**, select **Bind as currently logged on user**, and then click **OK**.
7. When you are finished specifying the bind options, click **OK**.
8. On the **View** menu, click **Tree**, and then type **OU=App1,dc=contoso,dc=local**.
9. Scroll through the objects listed under the application partition and look through the right-click menu. Note the options you have in relation to configuring the application partition.

### If you want to create an application partition by using LDP.exe, complete the following steps:

1. In the LDP window, while connected, on the **Browse** menu, click **Add child**.
2. In the **Dn** field, type **CN=Partition2,dc=Contoso,dc=local**.
3. Under **Edit entry**, type **ObjectClass** in the **Attribute** field and **container** in the **Values** field, and then click ENTER.

4. Under **Edit entry**, type **instanceType** in the **Attribute** box and **5** in the **Values** box, and then click ENTER.
5. Click **Run**.
6. If the new application directory partition is added successfully, the following information appears in the Details pane:
7. **Added {CN=Partition2,DC=Contoso}**
8. Click **Close**.
9. To refresh **Ldp.exe** and view your new directory partition, you must disconnect and then bind again to the AD LDS instance as follows:
    a. On the **Connection** menu, click **Disconnect**.
    b. Bind to your **AD LDS** instance as you did previously.
    c. To view the directory tree in **Ldp.exe**, on the **View** menu, click **Tree**.
    d. To view all directory partitions on the AD LDS instance, leave BaseDN blank, and then click **OK**.

## Demonstration: How To Configure Access Control in AD LDS

## Demonstration steps

1. If it is not already started, launch virtual machine **6426B-HQDC01**, log on as **Contoso\Administrator** with password **Pa$$w0rd**, and then install **AD LDS**.
2. In the **Server Manager** console, expand **Roles**, and then click **Active Directory Lightweight Directory Services**.
3. In the content pane, in the **Advanced Tools** section, click **ADSI Edit**. The ADSI Edit console If it is not already started, launch virtual machine **6426B-HQDC01**, log on as **Contoso\Administrator** appears.
4. In the **ADSI Edit console**, right-click **ADSI Edit**, and then click **Connect to**. The Connection Settings dialog box appears.
5. In the **Connection Settings** dialog box, in the **Name** box, type **ContosoApplication**.
6. Under **Connection Point**, in the **Select or type a Distinguished Name or Naming Context** box, type **OU=App1,dc=contoso,dc=local**.
7. Under **Computer**, select the **Select or type a domain or server box:(Server | Domain [:port])**, type **HQDC01:6389**, and then click **OK**.
8. On the ADSI Edit console, right click **OU=App1,dc=CONTOSO,dc=local**.
9. Point to **New**, and then click **Object**. The Create Object dialog box appears.
10. In the **Create Object** dialog box, under **Select a class**, click **user**, and then click **Next**.
11. In the **Value** box, type **User1**, click **Next**, and then click **Finish**.
12. In the ADSI Edit console, expand **OU=App1,dc=CONTOSO,dc=local**, right-click **CN=Roles**, point to **New**, and then click **Object**. The Create Object dialog box appears.
13. In the **Create Object** dialog box, under **Select a class**, click **group**, and then click **Next**.
14. In the **Value** box, type **Group1**, click **Next**, and then click **Finish**. The ADSI Edit console appears.

15. Under **OU=App1,dc=CONTOSO,dc=local, click CN=Roles**, and then under **Name**, double click **CN=Group1**. The CN=Group1 Properties dialog box appears.
16. In the **CN=Group1 Properties** dialog box, click **member**, and then click **Edit**. The **Multi-valued Distinguished Name With Security Principal Editor** dialog box appears.
17. In the **Multi-valued Distinguished Name With Security Principal Editor** dialog box, click **Add DN**.
18. In the **Enter a distinguished name (DN) for an object** box, type **CN=User1,OU=App1,dc=CONTOSO,dc=local**, and click **OK**. Then click **OK** twice.

Lesson 3

# Configuring AD LDS Replication

## Contents:

# Question and Answers

## How to Configure ADLDS Replication

**Question**:What tool provides the ability to create an AD LDS replica?

**Answer**: The AD LDS setup wizard allows you to create a replica of an existing instance .

**Question:** What information do you require to create an AD LDS replica?

**Answer**: You have to know the Domain Name System (DNS) name of the server that is running an AD LDS instance that belongs to the configuration set, as well as the Lightweight Directory Access Protocol (LDAP) port that was specified when the instance was created. You can also supply the distinguished names (also known as DNs) of specific application directory partitions that you want to copy from the configuration set to the AD LDS instance that you are creating.

**Question**: What is the type of replication that AD LDS uses?

**Answer**: AD LDS uses a type of replication known as multimaster replication. This means you can make changes to directory data on any AD LDS instance and AD LDS then replicates those changes to other members of the configuration set automatically.

# Detailed Demo Steps

## Demonstration: How to Configure AD LDS Replication

## Demonstration steps

1. If it is not already started, launch virtual machine **6426B-HQDC01**, log on as Launch virtual machine **6426B-HQSRV01**, and log on as **Contoso\Administrator**.

   **Note:** the virtual machine 6426B-HQDC01 should still be running in the background because the two virtual machines are required in this demo.

2. Open **Server Manager**, expand the **Roles** node, and then click **Active Directory Lightweight Directory Services**.
3. In the **content** pane, under the **Advanced Tools** section, click **AD LDS Setup Wizard**.
4. On the **Welcome To The Active Directory Lightweight Directory Services Setup Wizard** page, click **Next**.
5. On the **Setup Options** page, click **A replica of an existing instance**, and then click **Next**.
6. On the **Instance Name** page, in the **Instance Name** box, type **ContosoAppReplica**, and then click **Next**.
7. On the **Ports** page, in the **LDAP port number** box, type **6389**, and in the **SSL port number** box, type **6636**, and then click **Next**.
8. On the **Joining A Configuration Set** page, in the **Server** box, type **HQDC01**, and in the **LDAP port** box, type **6389**, and then click **Next**.
9. Ensure that the **Currently logged on user** check box is selected, and click **Next**.
10. In the **Copying Application Directory Partitions** window, select the **OU=App1,dc=contoso,dc=local** check box, and click **Next**.
11. In the **File Locations** window, click **Next**.
12. In the **Service Account Selection** window, click **Network service account**, and then click **Next**.
13. In the **AD LDS Administrators** window, ensure that the **Currently logged on user** check box is selected, and then click **Next**.
14. In the **Ready to Install** window, review the selections, and then click **Next**.
15. Click **Finish**.
16. Using the ADDI Edit console, connect to the newly created replica by using the following data in the **ADSI Edit Connection settings** dialog box:
    - **Name = ContosoAppReplica**
    - **Connection Point – Select or Type a distinguished Name or Naming Context = OU=App1,dc=Contoso,dc=local**
    - **Select or Type a domain or server: (Server | Domain:[port]) = HQSRV01:6389**
17. Click **OK**.
18. Verify that the replica instance contains previously created data.

**Note:** Replication within a site (Intrasite) occurs automatically and does not require any configuration beyond the construction of configuration sets. You may, however, configure the frequency.

Lesson 4

# Configuring AD LDS Integration with AD DS

## Contents:

# Question and Answers

## How to Add AD DS Users to AD LDS Groups

**Question**: What are the user types that you can add to AD LDS groups?

**Answer:** AD LDS does not include any default security principals. However, AD LDS does provide importable schema extensions that you can use to create users in AD LDS. Users created from these user classes can be used as security principals. AD LDS allows the use of Windows security principals for authentication and access control. Local Windows users and groups, as well as domain users and groups, can be used with AD LDS. In addition, you can add Windows security principals membership to AD LDS groups as members. By default, the security principal that you specify as the AD LDS administrator during AD LDS setup becomes a member of the Administrators group in the configuration partition. For Windows security principals, AD LDS relies on the Local Security Authority (LSA) on the local computer (for local accounts) or the LSA on a domain controller (for domain accounts) for authentication.

**Question**: What are the default AD LDS groups that are present in the application partition?

**Answer:** LDS provides four default, role-based groups: Administrators, Instances, Readers, and Users. These groups reside in the configuration partition and in each application partition, but not in the schema partition.

**Question** :What tool can you use to manage AD LDS users and groups?

**Answer:** Users and Groups can be managed using the ADSI Edit snap-in or through your directory-enable d application.

## How To Implement AD DS Synchronization

**Question**: What tools are required to prepare an AD LDS instance for synchronization?

**Answer:** LDIFDE and the ADSchemaAnalyzer tool are required. To ensure that your LDS schema matches the AD DS schema, use ADSchemaAnalyzer to create an LDIF file that will contain the target schema elements and then import this LDIF file into your base ADAM schema by using the ldifde tool.

**Question**: What tool is required to perform synchronization of AD DS objects to an AD LDS instance?

**Answer:** The Adamsync tool is required.

**Question**: What is the purpose of MS-AdamSyncConf.xml?

**Answer:** The MS-AdamSyncConf.xml file is a configuration that contains definitions of objects required during synchronization.

# Detailed Demo Steps

## Demonstration: How to Add AD DS Users to AD LDS Groups

## Demonstration steps

1. Launch virtual machine **6426B-HQDC01**, and log on as **Contoso\Administrator**.
2. Start **ADSI Edit (Administrative Tools/ADSI Edit)** and navigate to **OU=App1,dc=contoso,dc=local** section. Then click **CN=Roles**.
3. Right-click **CN=Group1** and click **Properties**.
4. In the **Properties** dialog box, click **member**, and then click **Edit**.
5. Click **Add Windows Account**.
6. In the **Enter the object names to select** box, type **Administrator**, and then click **OK** three times.

### To verify access permissions:

1. In ADSI Edit, in the console tree, right-click **ADSI Edit**, and select the **Connect to** check box.
2. In the **Connection Settings** dialog box, in the **Name** box, type **Windows User Test**.
3. Under **Connection Point**, in **Select or type a Distinguished Name or Naming Context** box, type **OU=App1,dc=contoso,dc=local**.
4. Under **Computer**, in the **Select or type a domain or server** box, type **HQDC01:6389**, and then click **Advanced**.
5. In the **Advanced** dialog box, select the **Specify Credentials** check box.
6. In the **Username** box, type **Contoso\Administrator**. In the **Password** box, type **Pa$$w0rd**, and then click **OK** twice.
7. Verify that the **Administrator** account has read access to objects in the **Security OU**.

## Demonstration: How To Implement AD DS Synchronization

## Demonstration steps

1. Launch virtual machine **6426B-HQDC01**, and log on as **Contoso\Administrator**.
2. Go to the file C:\Windows\ADAM\MS-ADAMSyncConf.xml.
3. Open it up in Notepad and walk through the structure, noticing some elements that would need to be changed, such as <source-ad-partition>, <target-dn>, and <base-dn>.
4. Go to the command prompt window and type **ADAMsync /?**.
5. Scroll through the switches and note the syntax and switches.
6. Type **ADAMsync /install HQDC01:6389 C:\Windows\ADAM\MS-ADAMSyncConf.xml**.

# Module Reviews and Takeaways

## Review Question

**Question** 1: How many instances of AD LDS can you install on a single server?

**Answer:** You can run multiple instances of LDS concurrently on a single server with an independently managed schema for each instance.

**Question** 2: What tool is used to modify the AD LDS schema?

**Answer:** The LDAP Data Interchange Format Data Exchange (LDIFDE) tool is a utility program that can be used to import and export Active Directory objects using LDIF-formatted files. LDIFDE is especially useful for doing batch operations that allow you to add, create, or modify multiple Active Directory objects at one time. The ldifde utility creates, modifies, and deletes directory objects and allows you to populate Active Directory Lightweight Directory Services (AD LDS) with data from other directory services. You can also use ldifde to extend the schema and export user and group information to other applications or services.

**Question** 3: What is a "configuration" used for in AD LDS?

**Answer:** A configuration set is a logical grouping of partitions or instances that hold copies of the same directory and schema partition/partitions. By grouping them as a configuration set, replication is automatic and this assists in fault tolerance and load balancing.

# Lab Review Question and Answers

**In this lab, you have:**

- Configured an AD LDS instance and an application partition
- Configured AD LDS Access Control
- Configured AD LDS Replication
- Configured AD DS and AD LcDS synchronization

# Module 5

## Configuring Active Directory® Federation Services

### Contents:

Lesson 1

# Overview of AD FS

## Contents:

# Question and Answers

## Identity Federation Business Requirements

**Question:** What are the business requirements that can lead to the deployment of an identity federation solution?

**Answer**: There are many possible answers to this question, but the root requirement will always be the secure exchange of information.

Lesson 3

# Deploying AD FS

## Contents:

# Question and Answers

## How to Install the AD FS Server Role

**Question:** What are the available AD FS role services?

**Answer:** The server role and the federation server role

**Question:**Which are the two role services that cannot be installed on the same computer?

**Answer:** The Federation Service and the Federation Service proxy

**Question:**What services are required to install the AD FS server role?

**Answer:** AD DS and AD CS

# Detailed Demo Steps

## Demonstration: How to Install the AD FS Server Role

## Demonstration steps

1. On the **6426B-HQDC01** virtual computer, logged on as **Contoso\Administrator**, click **Start**, click **Administrative Tools**, and then click **Server Manager**. The Server Manager console appears.
2. In the **console** pane, click **Roles**.
3. In the **Details** pane, click **Add Roles**. The Add Roles Wizard appears.
4. On the **Before You Begin** page, click **Next**.
5. On the **Select Server Roles** page, select the **Active Directory Federation Services** check box, and then click **Next**.
6. On the **Active Directory Federation Services (AD FS) introduction** page, click **Next**.
7. On the **Select Role Services** page, select the **Federation Service** check box.
8. In the **Add Roles Wizard** box, click **Add Required Role Services**. This installs the Web Server (IIS) prerequisite. Click **Next**.
9. On the **Choose A Server Authentication Certificate for SSL Encryption** page, click **Create a self-signed certificate for SSL encryption**, and then click **Next**.
10. On the **Choose A Token-Signing Certificate** page, click **Create a self-signed token-signing certificate**, and then click **Next**.
11. On the **Select Trust Policy** page, click **Next**.
12. On the **Web Server (IIS) introduction** page, click **Next** to accept the default path name for the trust policy.
13. On the **Select Role Services** page, click **Next** to accept the default settings for the Web server. Click **Install**. All specified roles, role services, and features will be installed.
14. On the **Installation Results** page, ensure that all tasks are successful, and then click **Close**.
15. On the **Server Manager console**, click the **Close** button.

Lesson 4

# Implementing AD FS Claims

## Contents:

# Question and Answers

## How to Configure AD FS Claim Mapping

**Question:** What are claims?

**Answer:** Claims are used to identify users. A claim specifies information about users, including identity and group memberships.

**Question:**What is claim mapping?

**Answer:** Claim mapping is the act of mapping, removing or filtering, or passing inbound claims into outbound claims. Claim mapping may be different for each federation partner.

**Question:**Why do you need to define identical claims for both AD FS partners?

**Answer:** The claim effectively states who the user is and what they can do. It is important that the information be consistent among partners to ensure appropriate access to resources and to ensure claims are properly mapped.

# Detailed Demo Steps

## Demonstration: How to Configure AD FS Claim Mapping

## Demonstration steps

> **Note:** To prepare for this demo, you must start both the 6426B-HQDC01-B and 6426B-NWTDC01 virtual machines and perform Exercises 1–5 in Lab A.

After Exercises 1–5 in Lab A are complete, perform the following steps (which are taken from Exercise 6 in Lab A) as a demonstration:

1. On the **6426B-HQDC01-B** virtual computer, logged on as **Contoso\Administrator**, click **Start**, point to **Administrative Tools**, and then click **Active Directory Federation Services**. The Active Directory Federation Services console appears.
2. In the **Active Directory Federation Services** console, expand the **Federation Service** node, the **Trust Policy** node, and the **My Organization** node.
3. Right-click **Organization Claims**, point to **New**, and then click **Organization Claim**.
4. In the **Create a New Organization Claim** box, under **Claim name**, type **TokenApp**.
5. Ensure that **Group claim** is selected, and then click **OK**.
6. In the console pane of the Active Directory Federation Services console, expand **Federation Service**, expand the **Trust Policy** node, expand the **My Organization** node, right-click **Account Stores**, point to **New**, and then click **Account Store**.
7. On the **Welcome To The Add Account Store Wizard** page, click **Next**.
8. On the **Account Store Type** page, ensure that **Active Directory Domain Services (AD DS)** is selected, and then click **Next**.
9. On the **Enable This Account Store** page, ensure that the **Enable this account store** check box is selected, and then click **Next**.
10. Click **Finish**. Under **Account Stores**, right-click **Active Directory**, then point to **New**, and then click **Group Claim Extraction**.
11. On the **Create A New Group Claim Extraction** page, click **Add**. In the **Select Users or Groups** box, type **TokenAppGroup**, and then click **OK**.
12. Ensure that **TokenApp** is displayed under **Map to this Organization claim**, and then click **OK**.
13. In the console pane of the Active Directory Federation Services console, expand **Partner Organizations**, right-click **Resource Partners**, point to **New**, and then click **Resource Partner**.
14. On the **Welcome to the Add Resource Partners Wizard** page, click **Next**.
15. On the **Import Policy File** page, click **Yes**.
16. Under **Partner interoperatability policy file**, type **C:\NWTPolicy.xml**, and then click **Next**.
17. On the **Resource Partner Details** page, click **Next**.
18. On the **Federation Scenario** page, click **Federated Web SSO with Forest Trust**, and then click **Next**.
19. On the **Resource Partner Identity Claims** page, click **Next**.

20. On the **Select UPN Suffix** page, select the **Pass all UPN suffixes through unchanged** option, and then click **Next**.
21. On the **Enable This Resource Partner** page, select the **Enable this resource partner** check box, and then click **Next**.
22. On the **Completing the Add Resource Partner Wizard** page, click **Finish**.
23. In the **AD FS console**, right-click **6426B-NWTDC01.NorthwindTraders.com**, click **New**, and click **Outgoing Group Claim Mapping**. The **Create a New Outgoing Group Claim Mapping** dialog box appears.
24. In the **Create a New Outgoing Group Claim Mapping** dialog box, select **TokenApp** from the **Organization group claims** list. In the **Outgoing group claim name** box, type **TokenAppMapping**, and then click **OK**.
25. Close the AD FS console

# Module Reviews and Takeaways

## Review questions

**Question** 1: What are some of the reasons why organizations deploy AD FS?

**Answer:** AD FS is deployed when organizations want to share information without creating new user accounts or trust relationships.

**Question** 2: How would you describe an AD FS claim?

**Answer:** An AD FS claim is the mechanism used to request authentication. The requestor “claims” to be an authorized entity, and the claim is then verified.

**Question** 3: What is the purpose of an AD FS resource partner?

**Answer:** The resource partner is the entity that contains the resources that are being used by the account partner.

**Question** 4: What two AD FS roles cannot be installed on the same server?

**Answer:** The Federation Service and Federation Service Proxy cannot exist on the same physical machine.

# Lab Review Questions and Answers

## Lab A: Configuring AD FS by Using the Federated Web SSO with Forest Trust Scenario

**In this lab, you have:**

- Installed the AD FS server role
- Configured the SSL certificate
- Installed the AD FS Web agent to support Windows token-based applications
- Ensured that the SSL certificate is bound to the default Web site
- Configured the token-based application
- Configured the AD FS Web agent
- Configured a forest trust between the intranet and the extranet forest
- Configured and exported the trust policy
- Created the TokenApp organization claim
- Added the Contoso.com Active Directory account store
- Added NorthwindTraders.com as a resource partner to Contoso's Federation Service
- Created an outgoing group claim mapping from the TokenApp organization claim to the TokenAppMapping outgoing claim
- Started the AD FS console and added the NorthwindTraders.com Active Directory account store
- Created the WGApp organization claim and mapped it to the WGAppUser security group
- Added Contoso.com as an account partner
- Created an incoming group claim mapping from the TokenAppMapping claim to the WGApp organizational group claim
- Added the token-based application to the Federation Service deployed in the extranet
- Configured browser settings to trust the Contoso federation server
- Accessed the application

## Lab B: Configuring AD FS by Using the Federated Web SSO Scenario

**In this lab, you have:**

- Installed the AD FS server role
- Exported the server authentication certificate to a file
- Imported the server authentication certificate into the Trusted Root Certification Authorities folder
- Installed the AD FS Web agent to support claims-aware applications
- Ensured that the SSL certificate is bound to the default Web site
- Configured the claims-aware application

- Configured Authorization Manager to support the ordering application
- Configured and exported the trust policy
- Created the account group organization claims by using the AD FS console
- Created the account custom organization claims
- Added the Contoso.com Active Directory account store
- Created group and custom claim extractions from Active Directory
- Added NorthwindTraders.com as a resource partner to Contoso's Federation Service
- Created outgoing group claim mappings
- Created outgoing custom claim mappings
- Created the resource group organization claims by using the AD FS console
- Created the resource custom organization claims
- Added Contoso as an account partner
- Created the incoming group claim mappings
- Created the incoming custom claim mappings
- Added the claims-aware application to AD FS
- Enabled each of the group and custom claims for the ordering application
- Configured browser settings to trust the Contoso federation server
- Installed client certificates
- Accessed the ordering application

# Module 6

## Configuring Active Directory® Rights Management Services

### Contents:

Lesson 2

# Installing and Configuring AD RMS Server Components

## Contents:

# Question and Answers

## How to Install the First Server of an AD RMS Cluster

**Question:** What tool would you use to install the AD RMS server role?

**Answer**: The Server Manager tool

**Question:**What are the various server roles that are required for the installation of the AD RMS server role?

**Answer**: AD DS, AD CS

**Question:**What servers can be included in an AD RMS cluster if Windows Internal Database is used?

**Answer**: The internal database does not accept remote connections, so you are limited to a single server.

# Detailed Demo Steps

## Demonstration: How to Install the First Server of an AD RMS Cluster

## Demonstration steps

1. To firstly install DNS and then configure a CNAME for the AD RMS cluster:
2. Launch virtual machine **6426B-HQDC01**, and log on with the credentials **Contoso\Administrator**.
3. Go to **Start > Administrative Tools > DNS**. (The DNS role is already installed.)
4. In **DNS Manager**, expand **HQDC01 > Forward Lookup Zones > Contoso.com**.
5. Right click **Contoso.com**, and go to **New Alias (CNAME)**.
6. In the **Alias Name** box, type **RMS**, and in the **fully qualified domain name (FQDN) for target host**, type **HQDC01.contoso.com**, and then click **OK**.
7. Close the **DNS Manager**.

### Install the AD RMS Server Role

1. On the **6426B-HQDC01** virtual computer, in the **Server Manager**, click the **Roles** node.
2. In the **Details** pane, click **Add Roles**.
3. On the **Before You Begin** page, click **Next**.
4. On the **Select Server Roles** page, select the **Active Directory Rights Management Services** check box.
5. When prompted, click **Add Required Role Services**, and then click **Next**.
6. Click **Next** twice.
7. On the **Create or Join an AD RMS Cluster** page, select **Create a new AD RMS cluster**, and then click **Next**.
8. On the **Select Configuration Database** page, select **Use Windows Internal Database** on this server, and then click **Next**.
9. On the **Specify Service Account** page, click **Specify**, type **Contoso\ADRMSService**, type **Pa$$w0rd** for the password, and click **OK** to provide a domain user account for the AD RMS service account. Then click **Next**.
10. On the **Configure AD RMS Cluster Key Storage** page, select **Use AD RMS** centrally managed key storage, and then click **Next**.
11. On the **Specify AD RMS Cluster Key Password** page, type **Pa$$w0rd** to confirm the AD RMS cluster key password, and then click **Next**.
12. On the **Select AD RMS Cluster Web Site** page, ensure that **Default Web Site** is selected, and then click **Next**.
13. On the **Specify Cluster Address** page, in the **Internal Address** box, type **rms.Contoso.com**, select **Use an unencrypted connection (http://)**, click **Validate**, and then click **Next**.
14. On the **Server Licensor Certificate** page, accept the default value of **HQDC01**, and click **Next**.

15. On the **Register AD RMS Service Connection Point** page, select **Register the AD RMS service Connection point now**, and click **Next**.
16. On the **Web Server (IIS)** page, click **Next**.
17. On the **Select Role Services** page, click **Next**.
18. On the **Confirm Installation Selections** page, view the informational messages, and then click Install to complete the installation.
19. After the installation is complete, click **Close**, and then log off of the **HQDC01** virtual computer.

Lesson 3

# Administering AD RMS

## Contents:

# Question and Answers

## How to Create a Rights Policy Template

**Question:** What are rights policy templates?

**Answer**: Rights policy templates are used to control the rights that a user or group has on a particular piece of rights-protected content.

**Question**: What is the purpose of archiving rights policy templates?

**Answer**: Archiving a template allows use licenses to continue to be granted but will not allow publishing new content.

**Question**: What is the difference between deployment of templates to Windows Vista released to manufacturing (RTM) and deployment of templates to the Windows Vista SP1 clients?

**Answer**: In Windows Vista SP1 and later, Policy Templates are automatically updated through the use of a scheduled job. Previous versions did not perform the update, so you needed to replace the template when changes occurred.

# Detailed Demo Steps

## Demonstration: How to Create a Rights Policy Template

## Demonstration steps

### Configure a distributed rights policy template.

1. Log on to the **6426B-HQDC01** virtual computer as **Contoso\Administrator**, with the password of **Pa$$w0rd**.

   **Note:** This should already have been started and AD RMS installed successfully as per previous demo.

2. In **Server Manager**, expand the **Roles** node, and then expand the **Active Directory Rights Management Services** node.
3. Expand **6426B-HQDC01**.
4. Browse to and click **Rights Policy Templates**.
5. In the **Actions** pane, under **Rights Policy Templates**, click **Properties**.
6. In the **Rights Policy Templates Properties** box, select **Enable export**. In the **Specify templates file location (UNC)** box, type **\\HQDC01\Templates**, and then click **OK**.
7. In the **Details** pane, click **Create Distributed Rights Policy Template**. Then, after the wizard is launched, click **Add**.
8. In the **Add New Template Identification Information** box, set **Language** to **English (United States)**, set **Name** to **Confidential Projects**, set **Description** to **Contoso Pharmaceuticals IT Department**, and click **Add**. Then click **Next**.
9. On the **Add User Rights** page, click **Add**, and in the **Add User or Group** box, type **ITAdmins@Contoso.com**, and then click **OK**.
10. Under **Rights for ITAdmins@Contoso.com**, select the **Edit** check box.
11. Click **Add**, select the **Anyone** option, and then click **OK**.
12. Under **Rights for ANYONE**, select the **View** check box, and then click **Next**.
13. On the **Specify Expiration Policy** page, select the **Expires after the following duration (days)** option to specify content expiration, and type **14** as the value.
14. Click **Finish**.
15. Go to **\\HQDC01\Templates** to view the template you just created.

### Manage Archived rights policy templates.

1. In the distributed **Rights Policy Template Information** window, highlight the template you just created, **Confidential Projects**.
2. In the **Actions** pane, click **Archive this rights policy template**.
3. In the **Archive Rights Policy Template** dialog box, read the information, and then click **Yes**.
4. In the **Details** pane, click the **Manage archived rights policy templates** link.
5. Highlight the **Confidential Projects** template, and in the **Actions** pane, click **properties**.

6. Step through the tabs to see what options are available.

Lesson 4

# Implementing AD RMS Trust Policies

## Contents:

# Question and Answers

## How to Configure Trust Policies

**Question:** What is the purpose of setting up TPDs?

**Answer**: TPDs are used when you want to process licensing requests from additional RMS clusters.

**Question:** What is the format in which TPD certificates are created?

**Answer**: The certificates use the XML format.

**Question:** What is the purpose of setting up trusted user domains?

**Answer**: To allow users who are licensed by a different RMS cluster access to protected content.

# Detailed Demo Steps

## Demonstration: How to Configure Trust Policies

## Demonstration steps

### Export a trusted user domain certificate.

1. On the HQDC01 virtual machine logged on as Contoso\Administrator, click Start, point to Administrative Tools, and then click Active Directory Rights Management Services.
2. Expand HQDC01 (local), expand Trust Policies, and then click Trusted User Domains.
3. In the Details pane, click the Enterprise object.
4. In the Actions pane, click Export Trusted User Domain.
5. In the File name box, type C:\Contoso.bin, and then click Save.

### Import a trusted user domain certificate.

1. In the AD RMS console expand HQDC01 (local), expand Trust Policies, and then click Trusted User Domains.
2. Right-click Trusted User Domains and go to Import Trusted User Domain.
3. On the Import Trusted User Domain page, in the trusted user domain file box, click Browse, locate the file D:\Labfiles\Mod06\NWTraders.bin, and then click Open.
4. In the display name box, type North wind Traders, and then click Finish.
5. In the Details pane of the trusted User Domains, notice the imported file.

### Configure Trusted Publishing Domains.

1. Under Trust Policies, click Trusted Publishing Domains.
2. In the Details pane, click Contoso Pharmaceuticals RMS.
3. In the Actions pane, click Export Trusted Publishing Domain.
4. In the Publishing domain file box, type C:\Contoso.xml.
5. Type and confirm the password, Pa$$w0rd.
6. Click Finish.

# Module Reviews and Takeaways

## Review questions

**Question** 1: What are some reasons to deploy AD RMS?

**Answer:** AD RMS allows organizations to protect content through the use of XrML certificates and helps to secure information in a more flexible manner than using encrypted content.

**Question** 2: What is the minimum operating system and service pack level required to install AD RMS?

**Answer:** Windows Server 2008 and SQL Server 2005. AD DCs must all be at least Windows 2000 SP3.

**Question** 3: Can S/MIME be used to secure documents outside of e-mail?

**Answer:** No

**Question** 4: What is a lockbox?

**Answer:** A lockbox is a dynamic-link library (DLL) that can be used to increase the security of the environment in which an Active Directory Rights Management Services (AD RMS) application runs. The lockbox verifies all licenses and certificates used by the application and, for AD RMS clients, protects the process space by limiting access to required and optional modules identified in the application manifest.

**Question** 5: What is a use license?

**Answer:** The use license specifies what a user can do with protected content.

**Question** 6: What special requirement must be met to install AD RMS on a domain controller?

**Answer:** This is not a recommended solution. When AD RMS is installed on a DC, the service account must be a member of the Domain Administrators role.

**Question** 7: What are some of the fields contained within a rights policy?

**Answer:** Full Control, View, Save, Edit, Extract, Export, Print, Forward

# Lab Review Questions and Answers

**In this lab, you have:**

- Installed and configured AD RMS
- Managed the AD RMS templates
- Configured AD RMS Rights Policy Template Distribution for Windows Vista SP1 clients
- Used Group Policy Management Console to distribute the AD RMS Rights Policy Template to clients prior to Windows Vista SP1
- Exported the Trusted User Dobmains policy
- Exported the Trusted Publishing Domains policy
- Imported the Trusted User Domain policy from the Contoso domain
- Imported the Trusted Publishing Domains policy from the Contoso domain
- Created a rights-protected document
- Started the 6426B-HQCL01 virtual computer and logged on as a Standard user
- Started the 6426B-HQCL01 virtual computer and logged on as an authorized recipient

# Module 7

## Maintaining Access Management Solutions

### Contents:

Lesson 1

# Supporting AD CS

## Contents:

# Question and Answers

## How to Configure CA Event Auditing

**Question:** How do you activate object access auditing?

**Answer**: Use the Group Policy Management snap-in to edit the computer policy for each CA server.

**Question:** Where are the audit events logged?

**Answer**: They are logged to the Windows® Event Log.

**Question:** How do you activate CA event auditing?

**Answer**: Also use the Group Policy Management snap-in, but edit the Audit Policy for CA machines.

# Detailed Demo Steps

## Demonstration: How to Configure CA Event Auditing

## Demonstration steps

1. On the **6426B-HQDC01-B** virtual machine logged in as **Contoso\Administrator**, click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**.
2. Expand **Forest: Contoso.com**, expand **Domains**, expand **Contoso.com**, and then click **Group Policy Objects**.
3. Right-click the **Default Domain Controllers Policy**, and then click **Edit**.
4. In the Group Policy Management Editor, expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, and then expand **Local Policies**.
5. Click **Audit Policy**.
6. Right-click **Audit object access**, and then click **Properties**.
7. Select the check box next to **Define these policy settings**.
8. Under **Audit these attempts**, select the check box next to **Success and Failure**, and then click **OK**.
9. Close the **Group Policy Management Editor** and the **Group Policy Management console**.
10. Click **Start**, and then click **Command prompt**.
11. In the Command Prompt window, type **gpupdate /force**, and then press ENTER.
12. Close the Command Prompt window.

### Configure CA event auditing

1. On the **6426B-HQDC01-B** virtual computer logged in as **Contoso\Administrator**, click **Start**, point to **Administrative Tools**, and then click **Certification Authority**.
2. In the **certsrv – [Certification Authority (Local)]** window, right click **ContosoCA**, and then go to **Properties**.
3. Go to the **Auditing** tab.
4. Note the list of events available to audit.
5. On the **Auditing** tab, in the **Events to Audit** section, select all seven check boxes, and then click **OK** in the resultant **Microsoft Active Directory Certificate Services** message box.
6. Click **OK** to close the **ContosoCA Properties** box.
7. On the **Action** menu, point to **All Tasks**, and then click **Stop Service** to stop the service.
8. On the **Action** menu, point to **All Tasks**, and then click **Start Service** to start the service.

### To verify your configuration, access the Application Log in Event Viewer on the CA server to view the audit results.

1. Click **Start**, point to **Administrative Tools**, and then click **Event Viewer**.
2. Click to **Event Viewer**, and then expand **Windows Logs**.

3. Click **Application**.
4. Scroll through the events listed in the details pane.

Lesson 2

# Maintaining AD LDS

## Contents:

# Question and Answers

## How to Back Up and Restore AD LDS Instances

**Question:** What is the built-in tool can you use to back up and restore AD LDS instances?

**Answer**: Windows Server Backup

**Question:** Where is the default location of AD LDS instance files?

**Answer**: %Program Files%\Microsoft AD LDS*instance name* where *instance name* indicates the AD LDS instance name

**Question:** Will you choose to stop or run the AD LDS instance during the backup and restore processes?

**Answer**: For Backup no, but for Restore, yes.

# Detailed Demo Steps

## Demonstration: How to Back Up and Restore AD LDS Instances

## Demonstration steps

1. On the **6426B-HQDC01-B** virtual machine, log in as **Contoso\Administrator**, with password **Pa$$w0rd** and perform the following steps:
2. Click **Start**, point to **Administrative Tools**, and then click **Windows Server Backup**.
3. Go to the **Action** menu and click **Backup Once**.
4. In the **Backup Once Wizard**, on the **Backup Options** page, click **Different options**, and then click **Next**.
5. On the **Select Backup Configuration** page, click **Custom**, and then click **Next**.
6. Select the volume or volumes that contain the AD LDS database and log files, and then click **Next**.
7. On the **Specify Destination Type** page, select **Local drives or Remote** shared folder, depending on whether you want your backup to be stored locally or remotely.
8. On the **Select Backup Destination** page, specify the appropriate drive where you want the backup to be stored.
9. Complete the wizard to begin the backup operation.

> **Note:** You will not be able to complete a restore unless a backup has first been performed.

### To restore an existing instance:

1. Again on the **6426B-HQDC01-B** virtual machine, logged in as **Contoso\Administrator** with password **Pa$$w0rd**, click **Start**, point to **Administrative Tools > Server Manager**, and then click **Active Directory Lightweight Directory Services**.
2. In the details pane, in the **System Services** section, right-click the **AD LDS** instance you want to stop, and then click **Stop**.
3. Click **Start**, click **Administrative Tools**, and then click **Windows Server Backup**.
4. On the **Action** menu, click **Recover**.
5. Follow the steps in the **Recovery Wizard** to specify the location of the source backup data and identify the specific backup from which you want to recover instance data.
6. In **Select recovery type**, click **Files and folders**, and then click **Next**.
7. In **Select items to recover**, browse to and select the folder that contains the instance data files. By default, AD LDS database and log files are located in %Program Files%\Microsoft ADAM\instance_name\data, where instance_name is the AD LDS instance name.
8. In **Specify recovery options**, click **Original location** and **Overwrite existing files with recovered files**, and then click **Next**.
9. To complete the restore, click **Recover**.

10. After the restore is complete, close **Windows Server Backup**.

### Start the AD LDS instance as follows:

1. Click **Start**, point to **Administrative Tools > Server Manager > AD LDS > System Services**.
2. Right-click the AD LDS instance, and then click Start.

Lesson 3

# Maintaining AD FS

## Contents:

# Question and Answers

## How to Monitor AD FS Events

**Question:** What are the prerequisites for AD FS to log errors?

**Answer**: The local security policy must be configured to audit events.

**Question:** Where can you change the default levels of the AD FS event log?

**Answer**: Use the local security policy or Group Policy Management.

**Question:** How can you activate AD FS debugging?

**Answer**: Use the Active Directory Federation Service management snap-in and configure debug from the troubleshooting tab.

# Detailed Demo Steps

## Demonstration: How to Monitor AD FS Events

## Demonstration steps

1. On the 6426B-HQDC01-B virtual machine, log in as **Contoso\Administrator** with password **Pa$$w0rd**.
2. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.
3. Right-click the **Trust Policy** node and then click **Properties**.
4. Scroll to the **Event Log** tab.
5. Under **Event log level**, click to select **All events**, and then click **OK**.

### To view logged events:

1. Click **Start**, point to **Administrative Tools**, and then click **Event Viewer**.
2. Expand **Windows Logs**, and then click **Application**.

Lesson 4

# Maintaining AD RMS

## Contents:

# Question and Answers

## How to Verify AD RMS Logging

**Question:** What are the types of databases used by AD RMS?

**Answer**: Configuration, Logging, and Directory Services.

**Question:** What is the role of the logging database?

**Answer**: The logging database contains message and event logs generated by RMS activity.

**Question:** What is the name of the tool that you can use to administer logging for the AD RMS cluster?

**Answer**: The Active Directory Rights Management Service management snap-in.

# Detailed Demo Steps

## Demonstration: How to Verify AD RMS Logging

## Demonstration steps

1. On the **6426B-HQDC01-B** virtual computer log on as **Contoso\Administrator** with password **Pa$$w0rd**, open the **Active Directory Rights Management Services console**, and expand the **HQDC01 (Local) cluster**.
2. Right-click the **HQDC01 (Local) cluster**, and click **Properties**.
3. On the **Logging** tab, ensure the **Enable Logging** check box is selected, and then click **OK**. Close the **Active Directory Rights Management Services console**.

**Ensure that the AD RMS service is running by accessing the Event Viewer on the AD RMS server and ensuring that error codes 94 or 114 do not exist.**

1. Click **Start**, point to **Administrative Tools**, and then click **Event Viewer**.
2. In **Event Viewer**, expand **Windows Logs**.
3. Click **Application**.
4. Look for entries where source is equal to **Active Directory Rights Management Services** and note the **Event ID** associated with each entry.
5. Ensure that there are no entries with **ID 94** or **114**. (Explanations of these event IDs are included here.)
6. 94 = The Active Directory Rights Management Services (AD RMS) logging service does not exist or is not registered on this computer.
7. 114 = The Active Directory Rights Management Services (AD RMS) logging service does not exist or is not registered on this computer.
8. This will verify that the logging service is enabled and configured successfully.
9. Go to the URL **http://go.microsoft.com/fwlink/?LinkId=164393**. (AD RMS Logging service availability: this article lists event IDs related to AD RMS.) Ensure that none of the error codes listed in the following reference exist in regard to AD RMS.

# Module Reviews and Takeaways

## Review questions

**Question** 1: What events are available to audit in AD CS?

**Answer:** All object access and certificate enrollment events are available to audit.

**Question** 2: What tool is used to back up AD CS?

**Answer:** Windows Server Backup

**Question** 3: What are the types of databases used by AD CS?

**Answer:** There is a single database that contains a record of all AD CS Transactions.

# Lab Review Questions and Answers

**In this lab, you have:**

- Used Enterprise PKI to view the health of the CA
- Enabled auditing of object access
- Enabled CA auditing
- Delegated role specific permissions
- Scheduled a task to perform CA backup
- Reset the AD RMS cluster key password
- Reset the AD RMS service account
- Changed the AD RMS service account
- Installed Microsoft Report Viewer
- Viewed AD RMS System Health reports
- Viewed AD RMS Statistics reports
- Enabled logging for the cluster
- Limited the disk space usage for message queuing

# Module 8

## Troubleshooting IDA Solutions

### Contents:

Lesson 1

# Troubleshooting AD CS

## Contents:

# Question and Answers

## How To Use Enterprise PKI to Troubleshoot AD CS

**Question:** Can you use the Enterprise PKI snap-in to monitor multiple CAs?

**Answer**: Yes

**Question:** Can you use the Enterprise PKI snap-in to resolve the issues?

**Answer**: No

**Question:** What information is available in the Enterprise PKI snap-in?

**Answer**: The Enterprise PKI snap-in provides overall health information about the CA and provides Key Performance Indicators that assist in determining what action that needs to be taken to maintain the CA.

# Detailed Demo Steps

## Demonstration: How To Use Enterprise PKI to Troubleshoot AD CS

## Demonstration steps

1. Launch the **6426B-HQDC01-B** virtual machine and log in as **Contoso\Administrator** with password **Pa$$word**.
2. Click **Start** and in **search** box type **MMC** then press ENTER.
3. In the Microsoft Management Console window, click **File** and then click **Add/Remove Snap-in**.
4. In the **Add or Remove Snap-in** window, click **Enterprise PKI**.
5. Click **Add**, and then click **OK**.
6. View the results of the **Enterprise PKI** window. Note the various health indicators and what they represent.

# Module Reviews and Takeaways

## Review questions

**Question** 1: List some common AD FS configuration issues.

**Answer:** These issues include certificate problems and return Uniform Resource Locators (URLs) in the application Web.config file that are incorrectly configured.

**Question** 2: What is the most common cause of AD FS setup failures?

**Answer:** Certificate authentication issues.

**Question** 3: What is the most common cause of AD CS autoenrollment failure?

**Answer:** Group Policy replication or configuration issues.

# Lab Review Questions and Answers

**In this lab, you have:**

- Identified built-in IDA solutions tools
- Described the troubleshooting steps to identify the possible causes for various issues

# Resources

## Contents:

# Microsoft Learning

This section describes various Microsoft Learning programs and offerings.

- Microsoft Skills Assessments

  Describes the skills assessment options available through Microsoft

- Microsoft Learning

  Describes the training options available through Microsoft — face-to-face or self-paced

- Microsoft Certification Program

  Details how to become a Microsoft Certified Professional, Microsoft Certified Database Administrators, and more

- Microsoft Learning Support
  - To provide comments or feedback about the course, send e-mail to support@mscourseware.com.
  - To ask about the Microsoft Certification Program (MCP), send e-mail to mcphelp@microsoft.com

# Technet and MSDN Content

- Device Management and Installation
- Windows Server 2008
- Cryptography Next Generation
- CAPolicy.inf Syntax
- Revoking certificates and publishing CRLs
- Checklist: Creating a certification hierarchy with an offline root certification authority
- Active Directory Certificate Services Role
- Certificate Template Overview
- Certificate Templates
- AD CS Certification Authority Upgrade
- Installing and Upgrading Certificate Templates
- Advanced Features
- Certificates
- Certificate Life Cycle
- Selecting a Certificate Enrollment and Renewal Method
- How to Obtain a Digital Certificate Using the Web Enrollment Form
- AD CS: Network Device Enrollment Service
- Certificate Autoenrollment in Windows Server 2003
- AD CS: Policy Settings
- Certificate Revocation and Status Checking
- Revoke an issued certificate
- AD CS Online Responder
- Online Responder Installation, Configuration, and Troubleshooting Guide
- Key Archival and Management in Windows Server 2003
- Security Watch Deploying EFS: Part 1
- AD LDS Getting Started Step-by-Step Guide
- Understanding the AD LDS Schema
- Working with Instances
- Working with Directory Partitions
- Understanding AD LDS Instances
- Working with Authentication and Access Control
- Understanding AD LDS Users and Groups
- Administering AD LDS Replication, Sites, and Configuration Sets

- Introduction to Administering AD LDS Replication and Configuration Sets
- Administering AD LDS Replication, Sites, and Configuration Sets
- Synchronize with Active Directory Domain Services
- Adamsync
- Using the ADAM Administration Tools
- What's New in AD FS in Windows Server 2008
- Active Directory Federation Services
- Federation scenarios
- Active Directory Federation Services Role
- What's New in AD FS in Windows Server 2008
- Active Directory Rights Management Services Overview
- Understanding AD RMS Clusters
- AD RMS Step-by-Step Guide
- AD RMS Deployment in a Multi-forest Environment Step-by-Step Guide
- Pre-installation Information for Active Directory Rights Management Services
- AD RMS Rights Policy Templates Deployment Step-by-Step Guide
- Creating and Modifying Rights Policy Templates
- Trusted User Domains
- AD RMS with AD FS Identity Federation Step-by-Step Guide
- Active Directory Rights Management Services
- Active Directory Rights Management Services Overview
- Understanding AD RMS Clusters
- Creating and Modifying Rights Policy Templates
- AD RMS with AD FS Identity Federation Step-by-Step Guide
- Troubleshoot Active Directory Certificate Services
- Enterprise PKI Overview
- ADAM troubleshooting and frequently asked questions (FAQs)
- Troubleshooting AD FS
- Troubleshooting: AD RMS
- Reports - Reports Results Pane
- AD RMS Logging Service
- AD RMS Service Connection Point Registration
- Optimization—Build a More Dynamic IT
- Active Directory Lightweight Directory Services

- Active Directory Certificate Services
- Active Directory Federation Services
- Active Directory Rights Management Services
- Microsoft Identity Lifecycle Manager 2007 FP1

# MSDN

There is no MSDN content for this course.

# Communities

This section includes content from Communities for this course.

- The IDA Guys: FIM 2010 RC1 Resource Management Client Sample Announcement
- Infrastructure Optimization
- Microsoft Identity Lifecycle Manager 2007 Frequently Asked Questions
- Microsoft Identity and Access Solutions
- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework: 2527
- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework: 3647
- Implementing and Administering Certificate Templates in Windows Server 2008
- After you upgrade Windows 2000 Server to Windows Server 2003, you must upgrade the certification authority
- Microsoft SCEP Implementation Whitepaper
- Cisco Systems' Simple Certificate Enrollment Protocol draft-nourse-scep-19
- Active Directory Certificate Services Longhorn Beta3 Key Archival and Recovery Whitepaper
- Determine Applied Schema Extensions with AD DS/LDS Schema Analyzer
- Synchronize Active Directory to ADAM with ADAMSync (step-by-step)
- Microsoft Windows Rights Management Services Client with Service Pack 2 - x86
- Microsoft Windows Rights Management Services Client with Service Pack 2 - X64 Edition
- Microsoft Windows Rights Management Services Client with Service Pack 2 - IA64 Edition

# Send Us Your Feedback

You can search the Microsoft Knowledge Base for known issues at Microsoft Help and Support before submitting feedback. Search using either the course number and revision, or the course title.

---

**Note** Not all training products will have a Knowledge Base article – if that is the case, please ask your instructor whether or not there are existing error log entries.

---

## Courseware Feedback

Send all courseware feedback to support@mscourseware.com. We truly appreciate your time and effort. We review every e-mail received and forward the information on to the appropriate team. Unfortunately, because of volume, we are unable to provide a response but we may use your feedback to improve your future experience with Microsoft Learning products.

## Reporting Errors

When providing feedback, include the training product name and number in the subject line of your e-mail. When you provide comments or report bugs, please include the following:

- Document or CD part number
- Page number or location
- Complete description of the error or suggested change

Please provide any details that are necessary to help us verify the issue.

---

**Important** All errors and suggestions are evaluated, but only those that are validated are added to the product Knowledge Base article.

---